OS CIBERCRIMES E A INVESTIGAÇÃO DIGITAL: NOVOS PARADIGMAS PARA A PERSECUÇÃO PENAL

MORAES, Alexandre Rocha Almeida de[1]; SILVA, Isabella Tucci[2]; SANTIAGO, Bruno[3].

RESUMO

O presente artigo trata de um dos temas mais atuais na esfera penal, já que o uso da internet está presente na maioria das relações humanas. O principal objetivo é explicar como são praticados os crimes por meio da internet e sua relação com os crimes já existentes e descritos no Código Penal e a necessidade de desenvolvimento de novos paradigmas de investigação.

Palavras-chave: Internet. Preservação da prova. Aplicação da lei penal. Investigação digital.

ABSTRACT

This article deals with one of the most current topics in the criminal sphere, since the use of the Internet is present in most human relations. The main objective is to explain how crimes are practiced through the internet and their relation with the crimes already existing and described in the Penal Code and the need to develop new research paradigms.

Keywords: Internet. Preservation of evidence. Application of criminal law. Digital research.

[1] Mestre e Doutor em Direito Penal (PUC/SP), Promotor de Justiça (MPSP), Professor de Direito Penal.
[2] Advogada graduada na UNIFAAT.
[3] Advogado, Especialista em Direito Penal Digital (*in memorian*).

1 A internet e a revoluçao tecnológica

Assim como o tempo, que "é o árbitro supremo das épocas e das quadras históricas da sociedade humana" (DIP e MORAES, 2002, p. 252), este artigo tem prazo de validade.

Durante toda a história, a evolução humana, em busca de satisfação de suas necessidades, foi pautada por invenções, descobertas e avanços que mudaram, por vezes, o rumo da história.

Assim como a transição da manufatura para as máquinas, a invenção do computador, a revolução tecnológica e dos meios de comunicação representam verdadeiros marcos na história da humanidade.

O avanço das tecnologias ganhou maior vulto após a Revolução Industrial, em meados do século XVIII, porém os efeitos chegaram ao Brasil somente após a Segunda Guerra Mundial.

A chegada dos computadores ao Brasil ocorreu entre as décadas de 80 e 90 do século XX, facilitando cada vez mais as operações, desde as mais simples, como fazer compras, até grandes transações financeiras, tornando cada vez mais inócuo ir aos bancos.

Nessa singela busca de satisfação de suas necessidades, desde a máquina a vapor em 1712 (Thomas Newcomen), a humanidade descobriu a bateria elétrica (1800 – Alessandro Volta), o telefone (1876 – Alexander Graham Bell), a lâmpada elétrica (1879 – Thomas Alva Edison), o rádio (1901 – Guglielmo Marconi), as válvulas eletrônicas (1904 – John Ambrose Fleming), o walkie-talkie (1943 – Motorola), o computador a válvulas de rádio (1946 – Vannevar Bush), a televisão (1947), os chips de silício e as válvulas eletrônicas (1948), o pager (1956), até o lançamento, em 1965, dos primeiros satélites de comunicação, que inauguraram a era da transmissão de dados eletrônicos.

Daí aos discos laser (1972), à telefonia celular (1977), ao primeiro navegador para a internet (1990), a revolução não teve e não tem previsão de fim.

A revolução que os computadores causaram na vida dos seres humanos foi um tanto quanto silenciosa, apesar de impactante. A quebra do silêncio só se deu com a interligação dos computadores, o que mudou inclusive as referências de tempo e de espaço.

Nessa esteira, com a mudança da sociedade, o Direito não poderia ficar estático, principalmente o Direito Penal, o qual é o fiel retrato da ética social, mesmo porque a

criminalidade da pós-modernidade também se amoldou à evolução tecnológica.

A interligação das redes de computadores se deu através da internet, possibilitando a comunicação instantânea sem fronteiras.

A globalização, antes imaginada para fins econômicos, tornou-se cultural e, como todas as grandes revoluções da humanidade, trouxe benefícos e ônus como a criminalidade cibernética.

Atualmente, não há quase nada que se possa fazer sem a tecnologia e sem acesso à internet, mas, como mencionado, se de um lado possibilitou a democratização do acesso à informação, dimunição das distâncias nos relacionamentos sociais e facilitação das atividades cotidianas, de outro trouxe inúmeros gravames, como por exemplo servir de plataforma e instrumento para a prática de novas formas criminosas. Nesse sentido:

> A Internet não pode ser entendida como uma terra sem lei, uma vez considerado que as operações aliefetivas sempre têm como fundamento relações entre seres humanos, devendo, pois, tais relacionamentos, obrigatoriamente, ser regidos pelos princípios gerais de direito, ou seja, se houver lesão ou ameaça a liberdades individuais ou a interesse público, deverá o Estado atuar para coibir tais práticas nefastas desse regime de proteção; a conduta humana sempre será objeto do direito, ainda que realizada por intermédio de computadores (LIMA, 2011, p. XVI)

Diante da rápida difusão da criminalidade pelo meio eletrônico, a política criminal não podia ficar anacrônica. Resta, contudo, avaliar se ela tem atendido às expectativas, ou seja, se a dogmática penal e processual penal contemporânea, assim como as formas de investigação, se prestam a proteger de forma suficiente os bens da vida mais relevantes e se conduzem a mecanismos eficientes de prevenção e repressão dessas novas formas de criminalidade.

É evidente, portanto, que perante os riscos e contradições da era pós-industrial a delinquência informática passou a ser um fenômeno social que precisa ser controlado:

> Também a doutrina já é clara em apontar a criminalidade informática como forma de ilícito complexo, decorrente da sociedade de risco. Parte dela, entretanto, a entende como mero fenômeno associado ao tempo de nascimento de novos riscos, ou ainda, como um problema derivado da própria sociedade de riscos, mas sem que se figure um novo risco (CRESPO, 2011, p. 235)

Os riscos de morte prematura deram lugar a uma população que passou a gerar novos conflitos, inclusive de criminalidade. A mesma máquina criada para o progresso serviu, por exemplo, para matar em acidentes automobilísticos. A industrialização e os meios de transporte alçaram novos bens para o Direito Penal. Os riscos advindos das máquinas e dos meios de transporte, por certo, geraram novas demandas à vida e à integridade física das pessoas que, até então, não existiam (CRESPO, 2011, p. 50).

Da mesma maneira, a revolução tecnológica vem desencadeando alterações políticas, econômicas e sociais profundas: novos atores sociais, novos costumes e uma nova sociedade. Nesse sentido, destaca Beck,

> Seguir as pistas de novos conceitos, que já se mostram em meio aos cacos dos antigos, é empreendimento difícil. Para uns, soa a "mudança sistêmica" e cai na área turva de competência dos serviços de inteligência. Outros se encapsularam em convicções irrevogáveis e, diante de uma fidelidade aos princípios sectários sustentada mesmo contra o impulso mais íntimo – e ela pode ter muitos nomes: marxismo, feminismo, pensamento quantitativo, especialização –, começam agora a se bater contra tudo aquilo que lembra o cheiro da dissidência extraviada (2010, pp. 14-15).

A revolução tecnológica, com os contornos da globalização, representa um dos fatores da enorme mudança de valores em todo o planeta. Isso porque globalizou-se a informação, a economia, o crime, as instituições sociais, enfim, universalizou-se muita coisa, sem a prévia preocupação de se construir uma carta de princípios minimamente consensual (MORAES, 2016, p. 77). Bauman (2008) salienta que a ausência de um sistema jurídico igualmente planetário, assim como de uma jurisdição global, seu braço executivo, torna ainda mais nebulosa a esperança de solução dos paradoxos trazidos à modernidade com a revolução tecnológica (2008, p. 130).

Utiliza-se a expressão "pós-modernismo" para as mudanças ocorridas nas ciências, nas artes, nas sociedades desde 1950. Um novo contexto pautado por novos paradigmas: cibernética, robótica industrial, biologia molecular, medicina nuclear, tecnologia dos alimentos, terapias psicológicas e religiões alternativas, climatização, técnicas de embelezamento, a mídia (da televisão à internet), a revolução tecnológica dos meios de comunicação, o aumento do consumo, o hedonismo e a busca constante da autossatisfação, o niilismo, enfim, inúmeras circunstâncias e características que alteraram profundamente todas as formas de controle social (MORAES, 2016, p. 68).

Compreender essa transição implica a conjugação de diversos fatores que vão desde a crise da industrialização, da massificação dos meios de comunicação e transporte, da informática, da eletrônica, da telemática à diversificação e crise das instituições sociais, à urbanização crescente e ao surgimento das megalópoles, dos protestos e das lutas sociais, enfim, à alteração dos papéis sociais.

Os avanços tecnológicos do século XXI se processam em uma velocidade cada vez maior, deixando evidente a frágil mobilidade dos sistemas jurídicos. A gravidade, ilustrada, por exemplo, pelos crimes cibernéticos, se reflete na atitude adotada pela maior empresa

fornecedora de segurança na internet do mundo: com a missão de combater os crescentes ataques e roubos de informações na rede, a empresa instalou-se em um antigo abrigo nuclear construído durante a guerra fria (FRAGA, 2005).

A própria ideia de velocidade (e mais ainda a de aceleração), quando se refere à relação entre tempo e espaço, supõe sua variabilidade e, simultaneamente, a incerteza.

Quando a distância percorrida numa unidade de tempo passou a depender da tecnologia, de meios artificiais de transporte, todos os limites à velocidade do movimento existentes ou herdados poderiam, em princípio, ser transgredidos: "a velocidade do movimento e o acesso a meios mais rápidos de mobilidade chegaram nos tempos modernos à posição de principal ferramenta do poder e da dominação" (FRAGA, op. Cit.).

Enquanto na sociedade industrial a lógica da produção de riqueza dominava a lógica da produção de riscos, na sociedade tecnológica essa relação se inverte. Como ressalta Beck,

> No modelo da sociedade industrial, de formas diversas – como no esquema de "classes", "família nuclear", "trabalho assalariado", na compreensão de "ciência", "progresso", "democracia" –, elementos constitutivos de uma tradicionalidade industrial imanente são incorporados, seus fundamentos fragilizados e suspensos pela reflexibilidade das modernizações. Por mais estranho que possa parecer: as irritações de época assim desencadeadas são em todos os sentidos resultado do êxito das modernizações, que atualmente já não ocorrem nos, e sim contra os trilhos e categorias da sociedade industrial. Vivenciamos uma transformação dos fundamentos da transformação (BECK, 2010, p. 17).

A tradição, a durabilidade e o apego dão lugar ao instantâneo, ao envelhecimento e à reciclagem. O entulho e a substituição que traz lucro hoje não mais convivem com durabilidade e confiabilidade do produto e muito menos dos valores (MORAES, 2016, p. 64).

A desintegração da rede social, a derrocada das agências de controle social é muitas vezes recebida como lamentável efeito colateral imprevisto da nova leveza e fluidez do poder cada vez mais móvel, escorregadio, evasivo e fugitivo.

Mas a desintegração social, ressalta Bauman,

> É tanto uma condição quanto um resultado da nova técnica do poder, que tem como ferramentas principais o desengajamento e a arte da fuga. Para que o poder tenha liberdade de fluir, o mundo deve estar livre de cercas, barreiras, fronteiras fortificadas e barricadas (BAUMAN, 2001, p. 18).

O poder ou os poderes globais são antagônicos a qualquer tradição, à densidade dos laços sociais, ao enraizamento territorial. A revolução tecnológica e o advento da instantaneidade conduzem "a cultura e a ética humana a um território não mapeado e inexplorado, onde a maioria dos hábitos aprendidos para lidar com os afazeres da vida perdeu

sua utilidade e sentido" (BAUMAN, 2001, p. 147).

Como a "memória do passado e a confiança no futuro foram até aqui os dois pilares em que se apoiavam as pontes culturais e morais entre a transitoriedade e a durabilidade, a mortalidade humana e a imortalidade das realizações humanas" (BAUMAN, id), essa revolução pela qual passa a humanidade, pautada pelo imediatismo, rompeu profundamente com a própria percepção de tempo e de espaço.

O presente da sociedade tecnológica é tal qual o presente artigo: efêmero e fugaz.

Há uma ressonância natural entre a carreira espetacular do agora, ocasionada pela tecnologia compressora do tempo, e a lógica da economia orientada para o consumidor (BAUMAN, 1999, p. 90).

Ao tornar precárias as tradicionais restrições territoriais e, pois, a percepção dos sentimentos comunitários, desnudam-se os territórios que, concomitantemente, confinam pessoas sem identidade coletiva, tal qual se constata em redes sociais de computadores (MORAES, 2016, p. 66).

Nesse contexto, há evidentemente novas fontes de conflito e de consenso:

> Em lugar da superação da carência, entra a superação do risco. Ainda que a consciência e as formas de organização política para tanto (ainda) não existam, pode-se, no entanto, dizer que a sociedade de risco, na dinâmica de ameaça que ela desencadeia, impugna tanto as fronteiras nacionais quanto as fronteiras dos sistemas federais e dos blocos econômicos (BECK, 2010, p. 57).

O risco mudou de natureza e de escala, como se, demasiadamente generalizado (risco social), se tornasse tão inseguro e incerto, ou que, demasiadamente elevado (risco tecnológico maior), se tornasse incalculável.

Ost, nesse sentido, aponta um dilema: "como precaver-se do risco, na medida em que, infigurável, logra as nossas capacidades de avaliação, ou que, demasiado grande, desencoraja as nossas capacidades ético-políticas de responsabilização?" (OST, 1999, p. 343).

O medo pela própria sobrevivência que leva os povos a lançarem-se nos braços do Leviatã de Hobbes (2006) dá lugar na sociedade pós-moderna à "heurística do medo".

O princípio de precaução, que recebe hoje as suas primeiras traduções jurídicas, surge assim como a forma contemporânea da prudência face a um risco transformado – "a maneira contemporânea de assumir as promessas do futuro, de aceitar a posta do futuro numa sociedade confrontada com riscos maiores e irreversíveis" (OST, 1999, p. 343).

Essa é a equação da formatação da sociedade de riscos: uma sociedade tecnológica, cada

vez mais competitiva, passou a deslocar para a marginalidade um grande número de indivíduos, que imediatamente são percebidos pelos demais como fonte de riscos pessoais e patrimoniais (PRITTWITZ, 2004, p. 44).

Esse tema e suas consequências ao Direito Penal recordam Alflen da Silva, "foram amplamente analisados e criticados pela Escola de Frankfurt, originariamente por Prittwitz, o qual já observava o surgimento de um 'Direito Penal do risco' (*riskostrafrecht*) que, longe de aspirar conservar o seu caráter fragmentário, como *ultima ratio*, tem se convertido em *sola ratio*, mais precisamente um Direito Penal expansivo..." (2004, pp. 93-94).

Independentemente do papel exagerado da mídia e da sensação de insegurança da sociedade pós-moderna, todos os elementos até aqui apresentados vêm contribuindo para formatar um modelo de Política Criminal bastante diverso do modelo de inspiração clássica. Uma das facetas desse novo modelo de política criminal pós-moderna é justamente o objeto do presente artigo: é decorrência lógica da crise das demais formas de controle social e de uma sociedade de risco: os crimes digitais e as respectivas dificuldades de regulação jurídica.

2 As relações entre direito e informática

O Direito existe para regularizar as relações humanas e a informática está presente na maioria dessas relações, mesmo que seja de maneira indireta.

O Código Penal de 1940 possui inúmeros bens jurídicos forjados em uma época em que inexistia a ideia de informática, redes sociais digitais e internet.

A tecnologia decorrente da globalização facilitou, em primeiro lugar, a própria maneira de ocultação e lavagem de capitais.

A especialização profissional, cuja manifestação mais relevante é o domínio funcional operativo dos meios tecnológicos, prejudica, ainda mais, a detecção pelos Estados desse tipo de crime. Nesse esteio, confirma Cervini que "*a efectos de dimensionar este riesgo, debe tenerse presente, por ejemplo, que el 90% de los flujos financeiros normales son meramente especulativos*" – para mostrar a dificuldade de investigação e punição e limitação diante de falta de tecnologia e velocidade de processamento das informações (2000, p. 72).

O combate a esse tipo de criminalidade exige a especialização dos próprios agentes de segurança do Estado, que precisam incorporar ao instrumento de investigação noções sobre provedores de acesso, provedores de conteúdo, instituições bancárias *online*, representantes de

e-commerce, sem se olvidar das especificidades da prática de pedofilia pela rede mundial de computadores.

Nas redes sociais, além de apologias ao crime, que já é considerada uma prática rotineira, pode-se encontrar explicitações de racismo, várias espécies de invasões de privacidade, além do popular *bullying*, especialmente entre adolescentes. Há também a prática de uma série de crimes comuns de computador como o uso de programas espiões para apropriação indevida de dados bancários ou estelionato (LIMA, 2011, p. 56).

É certo que a informática e a internet, quando utilizadas como instrumentos para a prática de crimes, atingem bem jurídicos que já se encontram no Código Penal:

> com a difusão da tecnologia informática, tornando-se uma presença constante na maioria das relações sociais, o direito deve cuidar de reconhecer valores penalmente relevantes, criando normas protetoras a fim de estabelecer a segurança dessas relações. também é dever do direito penal a proteção de bens jurídicos tradicionalmente reconhecidos e lesionados com o uso da tecnologia informática, bem como a proteção de outros valores jurídicos recentes havidos com o advento e a proliferação dos computadores.
> há de ser considerado, de um lado, que parte da nova criminalidade informática somente tem utilizado meios computadorizados para a prática de infrações penais comuns, com ataques a bens jurídicos já tradicionalmente protegidos pelo ordenamento penal. trata-se de atentados perpetrados contra a intimidade, o patrimônio, a propriedade intelectual ou industrial, a fé pública, a segurança nacional, entre outros, podendo-se afirmar que, em qualquer desses casos, o bem da vida a ser preservado será o correspondente a cada uma das condutas ilícitas cometidas (lima, 2011, pp. 02-03).

É possível, nesse esteio, a utilização de algumas normas penais já existentes para as infrações perpetradas por meios tecnológicos. Contudo, é preciso reconhecer que os crimes cibernéticos propriamente ditos são a porta de entrada para outras condutas criminosas, facilitando a utilização do computador como instrumento para cometer outros delitos, e o legislador não contemplou, por exemplo, a invasão de sistemas, como os de *computação na nuvem*, optando por restringir o objeto material àquilo que denominou dispositivo informático, sem, contudo, defini-lo.

Atividades de comercialização de dispositivos para *quebra de criptografia* e de engenharia reversa de programas também não foram objeto da norma.

Reale, aliás, justifica o surgimento da juscibernética e suas peculiaridades da seguinte forma:

> Finalmente, cabe lembrar que, no quadro da renovação dos conhecimentos jurídicos, está se consituindo a Cibernética Jurídica ou Juscibernética, que se propõe a compreender a conduta jurídica segundo modelos cibernéticos (o comportamento humano em termos de “comportamento” das máquinas) e a colocar à disposição

> imediata dos juristas os recursos dos computadores eletrônicos, por exemplo, na tarefa legislativa, na ordenação polivalente dos dados jurídicos e a realização rigorosa de cálculos resultantes da aplicação das regras jurídicas onde seja possível a quantificação.
> Parte relevante da Juscibernética é a Informática Jurídica, que delineia novas e fecundas perspectivas no sentido de fornecer ao jurista um "banco de dados". É preciso, porém, evitar deformações incabíveis quanto à redução final do "qualitativo" ao "quantitativo", ou à substituição da apreciação do juiz pela memória decisória dos autômatos...
> No Estado de Justiça Social, que é, por definição, um Estado de múltiplas atribuições, essa interferência deve obedecer às modernas técnicas do planejamento, aplicáveis inclusive ao Direito, sendo essencial, sob esse prisma, a utilização de computadores. Isto exigirá por parte dos juristas, especializados em "Direito do planejamento", o aprendizado da linguagem cibernética, para a elaboração eletrônica dos dados jurídicos (2002, p. 335-336).

Para a construção de uma doutrina de crimes digitais é preciso, preliminarmente, recorrer ao texto constitucional:

> No que se refere ao Direito Constitucional, a relação com a informática é manifesta, já que a Constituição Federal é a base do sistema jurídico. Um exemplo claro é a liberdade de comunicação, especialmente via internet, onde se verifica uma das expressões fundamentais da liberdade de pensamento. Há, ainda, a impossibilidade de se interferir na comunicação alheia, de forma que se tutela expressamente a intimidade e a vida privada de cada indivíduo (CRESPO, 2011, p. 40).

Diante do exposto, torna-se claro que direito e informática criaram um vínculo cada vez mais indissociável: a influência que o mundo tecnológico criou sobre os seres humanos é irreversível, e o direito, como produto cultural da humanidade, para uma adequada regulação jurídica, precisa aperfeiçoar-se com caracteres próprios e peculiares.

Os delitos praticados por meios eletrônicos representam qualquer conduta humana, seja omissiva ou comissiva, típica, antijurídica e culpável, em que a máquina tenha sido utilizada para facilitar a execução ou a consumação da figura delituosa, ainda que cause danos a pessoas sem que o autor se beneficie (LIMA, 2011, p. 13).

Apesar de ser possível a prática de crimes de várias naturezas por meio do ciberespaço, a tendência evidente é de que o que mais atrai os criminosos que se encaixam neste *"modus operandi"* são os crimes com intenção de lucro ou obtenção de vantagens ilícitas de caráter pecuniário:

> Evidencia-se que o artigo que se apresenta mais atraente para os delinquentes são os valores econômicos, portanto, os sistemas que podem estar mais expostos à fraude são os que tratam de pagamentos, bem como aqueles que possuem lista de nomes, de vendas, ou de compras.
> Nesse espaço virtual é mais fácil converter transações fraudulentas em dinheiro, que é logo desviado para alguma conta-corrente segura para o infrator. Por essas razões, as empresas de cartões de crédito, lojas e leilões virtuais, além de bancos e companhias de seguros, estão hoje mais expostas a

> fraudes que as demais companhias. Contudo, é possível ainda afirmar que hoje são as empresas financeiras e seus sistemas as vítimas com maior risco (LIMA, 2011, p. 16).

Percebe-se, pelos fatos recentes, que crimes são praticados atingindo vítimas distintas, pois o furto ou fraudes cibernéticas possuem vítimas, por vezes, difusas, sem prejuízo de atingirem sistemas, instituições ou empresas.

Atingir sistemas é fato próprio e peculiar dessa nova forma de criminalidade e, nesse caso, "mais importante do que o trajeto é a velocidade com que a informação deve chegar ao destino", para uma devida apuração ou prevenção (ROSSINI, 2004, p. 164).

Delimitar as alterações que o espaço virtual causa é de suma importância, pois muito do que nele ocorre produz efeitos diversos no mundo real, ou seja, nem sempre as mesmas regras são seguidas no mundo virtual.

Outro grande ponto que influi muito nos crimes cometidos em meio digital é a problemática quanto à custódia da prova.

Os crimes cibernéticos apresentam grandes dificuldades para sua comprovação, pois a ação criminosa é facilitada pela fragilidade na verificação de vestígios e exige qualificação técnica específica que nem sempre é disponível em todos os locais em que os crimes se consumam.

Ademais, os resultados dos delitos são transitórios e as provas só existem por um curto período de tempo, razão pela qual podem ser perdidos detalhes de tudo o que ocorreu, fomentando um cenário de impunidade e aumento relevante da subnotificação.

Não obstante, os sujeitos ativos nesse tipo de infração têm maior capacidade de encontrar os atalhos para a prática das infrações, eis que se trata de um perfil de criminoso com capacidade intelectual acima do perfil médio do criminoso patrimonial do mundo real (ROSSINI, 2004, p. 134).

Não se trata de compreender que esses crimes, pelos atributos especiais de conhecimento da tecnologia, seriam próprios, trata-se, isso sim, de compreender esse novo perfil de agente criminoso:

> Em princípio, é criminoso de informática alguém que conhece a vulnerabilidade dos sistemas, dos programas de computadores e de tudo que circunda em tal ambiente. Deve possuir habilidade de planejar o crime sob esse terreno, percebendo as oportunidades que facilitam sua prática delitiva e seu anonimato após a descoberta de sua conduta.
> Os indivíduos que cometem os chamados "crimes de computador" possuem certas características peculiares, isto é, os sujeitos ativos têm habilidades para

> o manejo dos sistemas informáticos e, no mais das vezes, encontram-se em seu ambiente de trabalho em posições estratégicas, que lhes permitem acesso à informação de caráter sensível. Com o tempo se pôde comprovar que os autores dos delitos informáticos são muito diversos e que o que os diferencia entre si é a natureza dos delitos cometidos" (LIMA, 2011, p. 40).

Diferentemente do que ocorre com a maioria das espécies de delitos, tem-se como primeira premissa aos crimes praticados por meio da internet que os agentes são das camadas média e alta da sociedade, devido à bagagem cultural que se deve ter para tanto (ROSSINI, 2004, p. 134).

Outro ponto peculiar e de certa forma problemático é em relação à faixa etária de quem pratica os respectivos delitos. O acesso fácil à informação e às novas tecnologias permite que a prática criminosa no ambiente em questão não seja exclusiva das pessoas com capacidade penal: cada vez mais, apesar de necessária bagagem técnica para a prática, o maior número de infratores ostenta pouca idade, o que causa uma enorme dificuldade de se traçar uma política criminal que deveria, necessariamente, ser construída tanto no âmbito penal quanto da infância e juventude (ROSSINI, 2004, p. 139).

Vale ainda ressaltar interessante peculiariedade: a proximidade eletrônica dos envolvidos – autor e vítima – e a distância real.

A proximidade eletrônica e o distanciamento real compõem o perfil criminológico do sujeito ativo. A telemática aproxima os protagonistas e funciona, sem sombra de dúvida, como um dos facilitadores dos delitos neste ambiente. "Afinal, muitos dos autores não infrigiriam normas penais se não estivessem a uma distância segura de suas vítimas, diferentemente do que ocorre na criminalidade tradicional" (ROSSINI, 2004, p. 140).

Como curiosidade, insta mostrar a classificação que está sendo desenvolvida dos agentes de delitos de computador: "hackers", "crackers", "carders", "lammers", "wannabes" e os "phreakers", dentre outros.

Outra questão relevante diz respeito à circunstância que afeta a apuração de crimes dessa natureza quando atingem vítimas difusas: muitas vezes, apesar de apurado o delito rapidamente, grandes empresas que foram lesadas, para que não sejam alvo de publicidade negativa quanto aos seus sistemas de segurança, optam por não acionar o sistema de justiça e investigação do Estado, contribuindo para as elevadas cifras ocultas (ROSSINI, 2004, p. 134).

Enfim, peculiariedades da forma pela qual os delitos são perpetrados e novos perfis criminológicos de autores e vítimas por certo demandam cautelas na análise da proteção ou

regulação jurídica pertinentes, sem prejuízo de já conhecidos problemas para a construção de uma teoria jurídica dos crimes digitais: a aplicação da lei no tempo e no espaço.

3 A dogmática penal e os *cibercrimes*: processo penal e investigação na era digital

Greco Filho (2000), ao questionar a busca imediata de uma legislação para atender às novas demandas penais decorrentes dos avanços tecnológicos da internet, ironicamente destacava:

> A conclusão, portanto, salvo demonstração em contrário, é a de que devemos deixar o direito penal em paz, porque está ele perfeitamente apto a atender à proteção dos direitos básicos das pessoas e se houver alguma modificação a fazer deve ser feita dentro de uma perspectiva de proteção genérica de um bem jurídico e não porque eu tenho um Pentium II de 300 Mh, disco rígido de 4 Gb, 64 Mb de memória RAM, 4 Mb de memória de vídeo e monitor de 20 (GRECO FILHO, 2000, p. 35).

Ao que parece, essa previsão não estava acertada.

O Direito tem como precípua função a regulamentação das condutas dos membros da sociedade e, logicamente, previnir e reprimir os comportamentos contrários aos bens jurídicos mais caros para a organização humana, dentre os quais estão o patrimônio, a privacidade, a honra, entre outros tantos (LIMA, 2011, p. 108).

Assim, diante das transformações que os computadores e suas características trouxeram, as relações socioculturais merecem urgentemente tratamento legislativo que contemple suas problemáticas.

No entanto, é extremamente possível que se puna pelos meios já existentes. Cabe, nesse momento, uma explanação entre os padrões do Direito Penal em relação aos crimes cometidos pela internet.

O tema em questão também é relevante nas relações informáticas, justamente porque no âmbito dos crimes digitais muitos dos delitos só ocorrem se a própria vítima contribuir decisivamente:

> A situação de um usuário de computador que se utiliza de serviços Bancários on-line, contando com banda larga para conexão à internet, e que ignora ou aparenta ignorar as orientações constantes dos fornecedores desses serviços, aparentemente é algo que pode configurar a autolocação em risco quanto a crimes digitais. Da mesma forma alguém que navegue pela internet sem estar devidamente protegido por programa antivírus, firewall, anti-phishing, ou, ainda, aquela pessoa que visita quaisquer sites, inclusive os de hackers. Isso sem esquecer aqueles que sempre clicam em tudo e qualquer conteúdo que recebem por e-mail, como cartões virtuais, vídeos, apresentações (LIMA, 2011, pp. 107-108).

Há de se distinguir a situação de quem sofre as consequências do crime daquela que contribui para o crime, o que não é objeto do presente estudo. Porém, a aplicação da teoria não pode ocorrer se há golpes anteriores à conduta sob análise, o que ocorre na maioria das vezes.

No mesmo esteio, a fixação do tempo do crime é de extrema importância por vários aspectos, sobretudo para determinar a lei vigente ao tempo que o crime se consumou. Isso importa para o caso de sucessão de leis no tempo e para saber a idade do agente quando do cometimento, além de vários outros aspectos.

O Código Penal em seu formato atual adota a teoria da atividade, onde considera tempo do crime o momento da ação ou omissão do agente e, com o uso da internet, fica difícil saber a que tempo este foi cometido, principalmente pela insuficiência de evidências, o que gera dificuldades no tocante à imputabilidade e prescrição, além da dificuldade sobre a circunstância de não se saber qual lei deve-se aplicar ao caso.

Assim, percebe-se que o problema na resolução e punição dos crimes está mais em reunir as provas do que verdadeiramente aplicar a norma, pois a norma da maneira que está, ainda que não seja completa, é possível de ser utilizada pelo aplicador do direito até que se consolidem fatos e valores aptos a indicar novos caminhos seguros para a disciplina jurídica e que não se tornem, rapidamente, obsoletos.

Tal qual a definição da lei penal no tempo, tem-se como importante paradigma a ser enfrentado a questão da fixação de competência.

Nos crimes no mundo físico, de certa forma, encontrar o local do crime é relativamente fácil, posto que para o agente se livrar de evidências é mais difícil, o que já é muito diferente em relação aos delitos telemáticos.

Em relação a esses crimes peculiares, o operador do direito deve formular um raciocínio igual ao que tem em relação ao crimes ditos tradicionais. O que não é uma tarefa simples quando relacionamos a rede mundial de computadores.

Assim, quando analisadas as evidências e colhidas as possíveis provas, o racicínio do operador deve ser igual entre os crimes tradicionais e telemáticos, vinculando o local da consumação do crime à competência, quando se trata de regra geral.

Apesar de toda evolução da tecnologia, quem pratica os delitos continua, apesar da tecnologia de inteligência artificial, sendo o ser humano, ou seja, a pessoa humana se insere no ciberespaço para praticar crimes, age em um espaço virtual, mas de certa forma ocupa um espaço físico, concreto e palpável (ROSSINI, 2004, p. 172), por isso, o local do crime tem a

mesma importância para qualquer que seja o espaço em que se pratica a conduta.

Nesse mesmo sentido, seria possível que se utilizassem as mesmas regras para delimitar os crimes cometidos por meio da internet, pois apesar de cometidos pelas ondas da rede, o agente, como ser humano, encontra-se em local físico.

Portanto, em relação aos crimes praticados por meio da internet, é necessário analisar se a lei aplicada ao caso será a nacional ou estrangeira, de acordo com o princípio da defesa universal e baseando-se nos tratados e convenções assinados pelo Brasil.

É preciso, ainda, ressaltar que a competência em relação a esses crimes se apoia na ideia de crimes plurilocais, a rede trouxe reflexões sobre os temas das normas já existentes, mas não teve força necessária para mudar os institutos nelas descritos (ROSSINI, 2004, p. 178).

Ademais, as regras de competência estabelecidas pelo Código de Processo Penal têm aplicabilidade sobre a criminalidade informática, de modo que o *modus operandi* utilizado na prática destes crimes se coaduna com as exigências da matéria de competência, não havendo necessidade de mudanças na norma.

> Nenhum delito será excluído da apreciação jurisdicional, muito menos aqueles conceituados neste trabalho como sendo "infrações penais telemáticas". Assim, se porventura as investigações não apontarem exatamente o local da infração telemática, o domicílio e a residência do réu fixarão o juízo competente; caso a autoridade incumbida das investigações também não localize o domicílio ou residência do réu, as hipóteses seguintes serão consideradas, até se chegar à última e definitiva delas, que é a prevenção (ROSSINI, 2004, p. 174).

Assim, em relação à competência, novas normas devem ser criadas apenas se para o *modus operandi* aplicado existir regra equivalente e suficiente para tanto.

Cuidado especial deve ser tomado no tocante à preservação das provas.

A Convenção de Budapeste para crimes cibernéticos, da qual o país ainda não é signatário, em seu título 2, prevê expressamente a "conservação expedita de dados informáticos armazenados" como medida legislativa a ser adotada pelos países signatários.

Isso porque a comunicação para que o servidor interpele a ação se faz necessária pelo fato de o Brasil não possuir uma legislação que obrigue a manter o tráfego de informações de seus clientes, concomitantemente a polícia civil ou a federal, quando for o caso, devem ser acionadas, além de um perito, de modo que possam tomar providências em relação ao fato, cada qual dentro da sua atribuição (FURLANETO NETO; SANTOS; GIMENES, 2012, p. 163).

Para que se chegue ao número que identifica um dispositivo de informática de um criminoso (IP ou "*Internet Protocol*"), nem sempre há necessidade de autorização judicial, visto

que é um documento de acesso público.

Após a identificação do respectivo endereço, deverá o provedor oferecer os dados cadastrais do usuário, sem que seja necessária autorização judicial, somente exigida quando da confirmação na investigação criminal, nos termos do inciso XII do artigo 5º da Constituição Federal, posteriormente regulamentado pela Lei nº 9.296/1996.

A investigação dos dados cadastrais do suspeito, por sua vez, pode se dar de forma linear, onde as informações obtidas junto ao provedor se dão pelo cadastro do usuário que utilizou determinado IP; e, para os processos mais complexos, deve ser usada a investigação não linear, por ser mais eficiente, que exige uma engenharia regressiva, buscando a localização do IP originário, sem que haja invasão da privacidade de seu usuário (FURLANETO NETO; SANTOS; GIMENES, 2012, p. 163).

A Lei do estado de São Paulo nº 12.228/06 obriga, por exemplo, as "*lanhouses"*, "*cibercafés* e *ciberoffices"* a manter em arquivo os dados cadastrais dos usuários de seus serviços, pelo prazo mínimo de sessenta meses, sendo certo que tal cadastro deverá conter o nome e endereço completos, data de nascimento, telefones e número de identidade, o horário de início e término da utilização da máquina e identificar também o aparelho utilizado.

Com essa medida, foi possível cercar infratores que se utilizavam de máquinas alheias para o cometimento dos delitos, já com o intuito de dificultar a persecução criminal.

Outrossim, adotar parâmetros de como proceder em caso de se perceber que sua máquina foi invadida é essencial para que a melhor investigação criminal seja feita.

> Segundo o guia de melhores práticas para apreensão de evidências publicado pelo Departamento de Segurança Interna e o Serviço Secreto dos EUA, quando o policial civil chegar a um lugar de crime e verificar que o computador pessoal ou doméstico está ligado, deve inicialmente verificar se está conectado a uma rede. Caso não esteja, impõe-se que, preliminarmente, fotografe o local com ilustração da tela e dos cabos conectados à CPU. Caso a imagem da tela esteja em módulo de descanso, a única providência a ser tomada será o deslocamento do mouse ou o acionamento da tecla de espaço, visando recuperar a imagem ativa da tela para ilustração fotográfica. Em seguida, deve ser retirado o cabo de força da parte de trás da torre, operação que visa a impedir o perdimento da memória ram (FURLANETO NETO; SANTOS; GIMENES, 2012, pp. 165-166).

Como medida preventiva, o conhecimento desse tipo de padronização de conduta para a preservação da prova deve ser difundido entre os usuários, para que a rede não seja mais um local desprovido de segurança.

Todavia, na maioria dos casos, causando grande desvantagem para a investigação, a polícia somente começa a investigar quando a vítima já apagou as evidências da memória de

seu computador. O cuidado em preservar os dados é ainda mais essencial quando se trata de operações fraudulentas em instituições bancárias.

Nesse sentido, uma ampla campanha à população e usuários de cuidados preventivos facilitaria e muito o trabalho investigativo, criando verdadeiro protocolo de comportamento a favor da prevenção da criminalidade cibernética.

As leis brasileiras que tratam especificamente sobre investigação digital são ínfimas, valendo destacar que as primeiras iniciativas ocorreram somente com o advento do CONIN (Plano Nacional de Informática), por meio da Lei nº 7.232/84, que delimitou as diretrizes da informática no território nacional, e com a Lei nº 7.646/87, posteriormente revogada pela Lei nº 9609/98, primeiro instrumento normativo a descrever condutas delitivas cibernéticas. Ocorre que as referidas Leis tratavam somente da propriedade intelectual dos programas de computador e sua comercialização em território nacional (LIMA, 2011, p. 111).

Portanto, é evidente que no que se refere aos instrumentos de investigação, o ordenamento jurídico pátrio não oferece grandes soluções para as condutas lesivas praticadas por meio da internet e que não encontrem adequação típica aos delitos já existentes.

De qualquer sorte, é preciso reconhecer que o Marco Civil da Internet (Lei nº 12.965 de 23 de abril de 2014) representa uma grande conquista da sociedade em relação à legislação e o uso da internet, assim como tende a ser a nova Lei Geral de Proteção de Dados (Lei nº 13.709/2018[4]), não obstante não se aplicar, dentre outros, para fins de investigação criminal (art. 4º, III, "d").

Quanto ao Marco Civil, houve efetiva tentativa de regulamentar as relações dos indivíduos por meio da rede mundial de computadores, neste momento, apesar de a nova Lei ainda não ser objeto de grandes análises por se tratar de tema extremamente recente, é necessária a sua menção superficial. Estabelece, para tanto, princípios a serem respeitados, direitos e deveres dos usuários, denominações específicas, que passaram a preencher lacunas de normas em branco, os limites do uso, bem como o tratamento de dados e informações sigilosas dos usuários, além de outras especificações.

Apesar de não tratar especificamente dos crimes cometidos na rede, o estudo da

[4] Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

mencionada norma passa a estabelecer bases para que uma possível Lei penal ou microssistema jurídico possa ser desenvolvido com técnica legislativa própria de criminalização, instrumentos investigativos e adequados, instrumentos cautelares e de produção de prova no processo.

No tocante à metodologia da investigação criminal é um fenômeno, que além de processual, é social:

> O gerenciamento estratégico na condução da investigação criminal demonstra profissionalismo e direciona a administração pública exercida pelo Poder Executivo no sentido de melhores resultados na busca da verdade dos fatos para a solução de todos os casos concretos que se apresentem, sejam simples ou complexos, na atividade institucional de combate ao crime (MALAQUIAS, 2013, p. 132).

Em busca da realidade dos fatos, no sentido literal da palavra, provar significa mostrar a verdade sobre algo. Neste sentido, é certo que somente os fatos que ensejam dúvida merecem produção de provas. Para o Direito não deixa de ser diferente, posto que além de provar a ocorrência dos fatos, a prova tem o condão de persuadir o julgador, para o fim de convencê-lo do que se alega.

Enquanto a prova visa, além de mostrar a realidade, a convencer o julgador, os meios de prova são os recursos utilizados por quem almeja demonstrar a dita verdade real, sendo certo que os crimes cibernéticos, objeto do estudo, se submetem às mesmas condições e princípios. Assim, a investigação criminal e suas técnicas devem prezar tanto pelo respeito aos direitos fundamentais dos indivíduos quanto pela tutela efetiva dos bens da vida alçados à proteção jurídica (MALAQUIAS, 2013, p. 155).

Mesmo com a modernidade das novas tecnologias e de tudo o que estas proporcionam, as diretrizes do Processo Penal e os ditames do Direito Constitucional devem ser respeitados de um lado; mas é precisa uma modulação hermenêutica para se entender os contornos necessários para a licitude e legitimidade da prova de crimes praticados por meio digitais.

Isso porque, como dito, a dificuldade com a produção e o armazenamento da prova nos crimes cibernéticos representa ponto crucial para essa nova hermenêutica dos crimes digitais (MALAQUIAS, 2013, p. 55).

É evidente que, de acordo com o princípio da proporcionalidade, havendo conflito entre os valores resguardados pelos referidos princípios, deverá haver equilíbrio entre estes, e só se analisará qual deles deve se sobressair aos outros, de acordo com o caso concreto. Nesse sentido:

> É que os homens, embora possuam direitos de índole constitucional à produção da prova (direito de ação, de ampla defesa e do contraditório), tais direitos têm

> de conviver harmonicamente com outros direitos, também de ordem constitucional, de modo que nenhum deles seja irregularmente exercido e venha a colocar em risco a ordem pública e direitos de outrem (MALAQUIAS, 2013, p. 21).

Ainda em conformidade a esse princípio dos princípios, há entendimento de que, mesmo que protegidas pela Constituição, a intimidade e a privacidade das pessoas não são absolutamente intangíveis, posto que se bens jurídicos mais nobres e relevantes para o Direito Penal estiverem em confronto em relação à intimidade e a privacidade, suas proteções deverão ser minimizadas, em verdadeiro balanceamento de interesses.

Muito também se discute sobre a vulnerabilidade das provas nos processos sobre crimes digitais, o que também remete ao tema em estudo sobre a validade das provas apresentadas nos autos destes processos.

Cumpre esclarecer, como já brevemente mencionado, que todo usuário dos computadores ou internautas possuem um número de endereçamento de sua máquina e um acesso denominado IP (*Internet Protocol*), o qual descreve todo o "caminho" percorrido pelo usuário na rede mundial de computadores.

De outra parte, muito se discute sobre a efemeridade dos criminosos cibernéticos, sob o argumento de que isso ocorre, principalmente, pela falta de preparo técnico por parte de quem gere a investigação criminal, com o pensamento arcaico de que todos os documentos que estão "na rede" são de fácil modificação (MALAQUIAS, 2013, p. 91).

Em que pese a necessidade de profissionais qualificados para a melhor e mais eficiente investigação, o argumento de que os documentos e vestígios deixados pelos criminosos cibernéticos são voláteis não é uma verdade absoluta, posto que existem diversos mecanismos para salvaguardar a segurança:

> A maneira mais eficiente de superar a vulnerabilidade das provas documentais originadas em publicações na Internet, mensagens de e-mail, invasão de bancos de dados etc., devem ser efetivadas com a imposição de mecanismos que impeçam (firewall) ou interceptem a tentativa de invasão do cracker ou hacker nos sistemas informatizados ou computadores pessoais, com o objetivo de impedir a violação de documentos eletrônicos, sejam públicos ou privados (MALAQUIAS, 2013, p. 83).

Nesse mesmo sentido, cada vez mais se observa a semelhança entre os documentos digitais e os clássicos, sendo evidente que todos podem, por inúmeros exemplos práticos, ser modificados e adulterados.

Note-se que os documentos, tanto os clássicos quanto os digitais, devem ser tratados da

mesma forma pelo processo penal, visto que sua única diferença é o local – físico ou virtual – em que foram realizados.

Como consequência da semelhança entre os documentos, a afirmativa de que os documentos digitais são um tanto quanto mais vulneráveis à adulteração que os documentos clássicos e que por isso não poderiam ser aceitos no processo penal é totalmente descabida e inócua. Assim como a prova documental, o magistrado deve tratar todas as provas oriundas da infração cibernética como todas as outras provenientes de fatos sujeitos à norma penal. No processo penal sobre crimes cibernéticos, a função da prova é idêntica aos processos costumeiros, tendo a incumbência de formar, por meio da persuasão, o livre convencimento motivado do juiz.

Neste passo, o magistrado, seja em relação aos crimes cibernéticos ou em relação aos crimes comuns, não pode aceitar provas ilícitas e ilegítimas para a formação do seu convencimento:

> Sem embargo, já se esboça na doutrina um movimento no sentido de não emprestar a esse princípio constitucional que inadmite as provas obtidas ilicitamente uma importância que supere o direito de liberdade. Na verdade, se a inadmissibilidade das provas ilícitas está no capítulo destinado aos direitos e garantias fundamentais do homem, não pode repugnar à comum consciência jurídica o fato de a defesa conseguir por meio ilícito prova que demonstre a inocência do imputado. Poder-se-á, então, dizer: "male captum, bene retentum". Essa mesma corrente, por esse "critério de proporcionalidade sobre o qual se baseia a exceção aos princípios de exclusão da prova ilícita", não empresta um valor inquebravelmente àquela proibição constitucional (TOURINHO FILHO, 2012, pp. 572-573).

A inadmissibilidade das provas ilegais, gênero de provas ilícitas e ilegítimas, se apoia no inciso LVI, do artigo 5º da Constituição Federal e no artigo 157, do Código de Processo Penal. Outrossim, a questão não afasta o fato de que a pessoa que obtiver a prova por meios ilícitos seja punida, se for o caso. A utilização da prova é diferente da apuração do possível ilícito penal cometido para a sua obtenção.

> Embora a norma não o diga expressamente, mesmo que tenha sido indeferida a juntada aos autos da prova considerada inadmissível, o Juiz deverá determinar sua destruição. Contudo, a determinação da inutilização da prova poderá acarretar sérios problemas processuais. Isso porque, dependendo do meio empregado para sua obtenção, ela será considerada objeto material de um delito. Nesse caso, somente poderá ser destruída após a elaboração do laudo pericial e quando não mais interessar ao processo que apura o crime decorrente de sua obtenção (MARIANO DA SILVA, 2016, p. 27).

Nota-se que o que verdadeiramente se modificou foi a maneira pela qual os crimes são cometidos, visto que os meios de obtenção das provas, suas exigências e limites continuam os

mesmos, claro que com mudanças pontuais que acompanham a evolução das referidas tecnologias e do meio de execução dos crimes cibernéticos, bem como as proteções e diretrizes trazidas pela Constituição Federal e pelas normas infraconstitucionais.

É evidente que o advento da tecnologia permite cada vez mais novos mecanismos para a investigação. As céleres mudanças nas formas de se praticar crimes por meio das novas tecnologias e em ambiente virtual demonstram uma tentativa, ainda lenta, de tentar mudar a política criminal e legislativa.

A já mencionada Lei nº 12.965/14 estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Em seu art. 3º, disciplina o uso da internet no país, calcada nos seguintes princípios: garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; proteção dos dados pessoais, na forma da lei; preservação e garantia da neutralidade de rede; preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; responsabilização dos agentes de acordo com suas atividades, nos termos da lei; preservação da natureza participativa da rede; liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos na Lei, sem prejuízo de outros princípios previstos no ordenamento jurídico, dentre os quais os inúmeros bens jurídicos, de caráter constitucional, ou previstos em tratados internacionais e que também configuram bens jurídicos penais.

A criminalidade cibernética é mais ampla, inovadora, criativa e se adapta, tal qual a mudança tecnológica, tornando sempre a disciplina jurídica anacrônica.

Tanto é verdade, que o art. 22 da Lei do Marco Civil da Internet já evidencia essa preocupação no tocante à dificuldade de produção da prova.

Essa capacidade de saltar entre países, uma das maiores forças da internet, cria enormes problemas jurisdicionais e administrativos para a polícia, e é uma das principais razões pelas quais a investigação de crimes virtuais é tão desafiadora e, muitas vezes, inútil. Um policial em Paris não tem autoridade para realizar uma prisão em São Paulo (GOODMAN, 2015, p. 17).

O recente histórico legislativo também demonstra como é difícil criar marcos jurídicos para mudanças tão aceleradas e avassaladoras.

Antes mesmo da mencionada lei, outro texto legal – a Lei nº 9.296 – já previa a possibilidade de interceptação telemática, utilizando a expressão "interceptação do fluxo de comunicações em sistemas de informática e telemática".

Já a Lei nº 12.737/12, criada para coibir a invasão de dispositivo informático, assim como interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e falsificação de cartão, demonstra que já nasceu defasada ou, ao menos, insuficiente para os fins a que se destinava.

É, pois, necessário desenvolver uma nova abordagem: exige-se uma nova forma de trabalhar e apoiar o desenvolvimento de novas ferramentas de investigação.

Recentemente, um ataque global explorou uma falha no serviço do Windows, que é utilizado pela maioria das pessoas, e, com isso, exigiu um pagamento em *bitcoins*, tendo prejudicado e tirado do ar uma grande gama de sites, inclusive governamentais, mostrando a fragilidade que temos em dias atuais e a necessidade de um sistema de contra-ataque cibernético.

Uma das razões para a dificuldade de combater a grande variedade de ameaças tecnológicas em nossa vida é que houve um grande aumento no número dos chamados ataques *zero day*. Um ataque *zero day* se aproveita de uma vulnerabilidade até então desconhecida em um aplicativo que desenvolvedores e equipes de segurança não tiveram tempo para resolver. (GOODMAN, 2015, p. 20).

Além do uso de moedas virtuais que temos nos dias de hoje, as *e-currency*[5] adotadas por cibercriminosos, há a já famosa *bitcoin*, embora anônima no funcionamento, ainda há registro de todas as transações realizadas em um *"ledger blockchain"*[6], que pode revelar muita informação. Por isso, muitos criminosos acabaram adotando algumas moedas virtuais que são difíceis de rastrear: *Litecoin, Peercoin, Dogecoin, Monero.*

A moeda virtual acaba sendo amplamente utilizada, dada sua facilidade de utilização, eis que o usuário pode armazenar seu dinheiro em uma carteira digital, através de um simples aplicativo ou até mesmo em um simples pen drive.

Atualmente, o "*bitcoin"* vale aproximadamente R$9.000,00 (nove mil reais), o que

[5] Dinheiro Eletrônico, ou Moeda Digital, o Dinheiro Eletrônico é a forma de pagamento utilizada para transações de e-commerce, facilitando o comércio entre diferentes países.

[6] *Blockchain* é a estrutura de dados que representa uma entrada de contabilidade financeira ou um registro de uma transação. Cada transação é assinada com o objetivo de garantir sua autenticidade e que ninguém a altere, de forma que o registro e as transações existentes dentro dela sejam considerados de alta integridade.

permite imaginar o valor de um resgate na hipótese de uma invasão cibernética a um hotel que possui sistema de fechaduras eletrônicas conectadas por um servidor, como se deu recentemente em Aspen[7].

Os criminosos usaram um "*Ransomware"*, ou seja, um tipo de "*malware"*[8] que sequestra o computador da vítima e cobra um valor em dinheiro pelo resgate, geralmente usando a moeda virtual "*bitcoin*", que torna quase impossível rastrear o criminoso que pode vir a receber o valor. Este tipo de "vírus sequestrador" age codificando os dados do sistema operacional de forma com que o usuário não tenha mais acesso.

Portanto, o desafio para o policiamento é ir além da forma tradicional de investigação, e isso requer uma mudança na estrutura de ataque e prevenção de crimes, podendo inclusive ser adotadas estratégias de inteligência artificial como a usada pela IBM, através do modelo denominado "Watson".[9]

Todo o fundamento de uma política preventiva e de mínima eficácia repressiva ainda não é visível quando se trata de crimes perpetrados digitalmente: todos os dias vários crimes são cometidos sem qualquer tipo de punição, mecanismos de prevenção e sem qualquer conhecimento público. Aliás, é até impossível imaginar, neste momento, a taxa de notificação desse tipo de criminalidade.

Movimentar dinheiro de um país para outro, mediante evasão, lavagem de dinheiro e transferência de "*bitcoins"*; roubo de propriedade intelectual ou uso indevido de informações, roubo de serviços, roubo de propriedade como, por exemplo, hardware de computador e chips; invasão de privacidade, negação de serviços (ataque ddos[10]); sabotagem mediante a alteração ou destruição maliciosa de dados; extorsão mediante o uso de "*malwares"* que acionam a câmera do computador da vítima, gravando vídeos íntimos, conversas pessoais, ambientes domiciliares; espionagem; terrorismo; criação de comunidades virtuais para fazer apologia ao uso e tráfico de drogas; novas formas de pornografia infantil, estelionato, dentre outros, representam alguns exemplos da falta de regulação jurídica suficiente para uma política

[7] Nesse sentido: Disponível em: http://veja.abril.com.br/blog/headlines/hackers-trancam-hospedes-de-hotel-para-fora-de-quartos. Acesso em: 07 ago. 2020.
[8] *Malware* refere-se a qualquer tipo de software malicioso que tenta infectar um computador ou dispositivo móvel.
[9] Ver neste sentido: **What can IBM Watson Analytics do for you?** Disponível em :www-01.ibm.com/software/analytics/infographics/watson-analytics/full-potential.html. Acesso em: 08 jul. 2020.
[10] Ver nesse sentido: **O que é DoS e DDoS?** Disponível em: https://canaltech.com.br/o-que-e/o-que-e/O-que-e-DoS-e-DDoS/. Acesso em: 08 jul. de 2017.

criminal minimamente eficiente.

Compreender essa ampla variedade e formas de crimes cibernéticos é crucial, eis que demanda atitudes diferentes para melhorar a segurança computacional, tendo em vista que a internet não possui fronteiras e acaba gerando sérias dificuldades para enfrentamento, criando um custo-benefício enorme que fomenta o aumento dessas práticas.

Essa modalidade de crime exige profissionais especializados, com amplo conhecimento em computação, segurança da informação, tecnologia, criação de softwares e outras áreas afins, com capacidade suficiente para investigar quem, como e quando um crime cibernético foi praticado, ou seja, um profissional capaz de identificar autoria, materialidade e dinâmica de um crime digital.

Os principais exames forenses realizados estão entre exames periciais em dispositivos de armazenamento computacional como HDs, CDs, DVDs, Blu-rays, pendrives, smartphones, nuvem e outros dispositivos de armazenamento como smart TVs, tablets, sites, e-mails, dentre outros.

Logo, além do horizonte, estão surgindo novas tecnologias, incluindo robótica, inteligência artificial, genética, biologia sintética, nanotecnologia, fabricação 3D, a ciência do cérebro e a realidade virtual, que causarão grande impacto em nosso mundo e representam um arsenal de ameaça de segurança que fará com que o cibercrime de hoje pareça uma brincadeira infantil. Essas inovações terão um papel essencial em nossa vida diária em apenas alguns anos, embora ainda não exista estudo amplo e profundo para nos ajudar a compreender os riscos não intencionais que representam (GOODMAN, 2015, p. 23).

Daí a necessidade de uma política técnico-científica apta a elaborar laudos apropriados a essa dinâmica, à materialidade e à autoria de ilícitos em meios digitais.

Deve-se ter em mente que é necessária uma cooperação com os provedores de serviço (Gmail, Google, Facebook, Hotmail, Yahoo etc.), pois é através do acesso de tal provedor que é possível localizar potenciais criminosos através do seu registro IP (*Internet Protocol*) que, como se sabe, no país, sequer é individualizado (BRITO, 2013).

Muitos cibercriminosos utilizam redes VPN (Virtual Private Network), ou seja, uma rede privada, podendo realizar um monitoramento passivo, em que um hacker pode simplesmente recolher informações sem criptografia do usuário ou sequestro de *DNS*[11], onde o

[11] O DNS, do inglês Domain Name System (Sistema de Nomes de Domínios), funciona como um sistema de tradução de endereços IP para nomes de domínios.

hacker consegue redirecionar o navegador do usuário para um servidor controlado fingindo ser um site, método de espelhamento e assim podendo obter as informações da pessoa, como login, senha etc.

Com o IP do suposto criminoso é possível descobrir o seu provedor de acesso, através de endereços simples e, com isso, seria possível pedir informações sobre aquele endereço do provedor de acesso.

Além disso, muitos dos usuários utilizam alguns navegadores achando que ajudariam no "anonimato'', como Tor, Freenet, Tails, I2p, Zeronet.

O I2P, o Freenet e o Zeronet são redes diferentes que alcançam o anonimato de maneiras diferentes do que o Tor: essas redes permitem o envio e-mails, mensagens; permitem configurar sites e baixar arquivos anonimamente. É justamente o "anonimato" presente na denominada Deep Web que permite uma navegação nas camadas mais baixas, mais independentemente e mais difícil de rastreamento[12].

Na verdade, o termo "web profunda" diz respeito muito mais aos motores de busca do que com qualquer uma dessas coisas. Uma página da web é considerada parte da "web profunda" se não for indexada pelos motores de busca padrão como Google e Bing.

A internet é feita de camadas, das quais algumas conhecidas, que são utilizadas pela maioria das pessoas, e as camadas restritas, que somente podem ser navegadas a partir de certo conhecimento ou mecanismos apropriados ou tendo o link direto para acesso. Algumas dessas redes são acessadas com extensões diretas, como a rede "*onions*".

A mais famosa de todas talvez seja a Deep Web, mas essa é somente uma das camadas, valendo destacar: *Charter Web, Marianas Web, Intermediary Web, The Fog, Vírus Soup, The Primarch System* etc.

As camadas que existem depois da *Bergie Web* (limite de indexação pelo Google) incluem, por exemplo, o famoso "4chan" (aqui, alguns resultados "bloqueados" do Google ficam escondidos, assim como vários servidores *FTP*).

Assim como no mundo real, você não pode simplesmente bater na porta de qualquer casa do bairro e conseguir um quilo de metanfetamina. O mesmo é valido para o submundo digital. Você não chegará lá apenas digitando um endereço em seu navegador Firefox na

[12] Exatamente a ausência de indexação e dificuldade de localização do endereço eletrônico de pedófilos que compartilham pornografia infantil que ensejou, por exemplo, a alteração da Lei n. 8.069/90 (ECA), criando nos arts. 190-A a 190-E a figura do agente infiltrado para esse tipo de investigação digital.

esperança de ser magicamente transportado para o santuário interno de CRIME S.A (GOODMAN, 2015, p. 211). Você precisa de um passaporte e um guia para orientá-lo. A jornada começa como TOR – o *Onion Router*, ferramenta de software que fornece a coisa mais próxima do verdadeiro anonimato na internet.

E é justamente nessas camadas mais profundas da internet, sem qualquer mecanismo de indexação e, portanto, sem acesso simples por qualquer usuário e investigador, que ocorrem graves crimes digitais.

Exemplo do que ocorreu em um site que operava com venda de drogas na *Deep Web* (*Silk Road*): entre fevereiro de 2011 e julho de 2013, o *Silk Road* movimentou cerca de US$ 1,2 bilhão em tráfico de drogas, antes de ser fechado pelo FBI.

Ao utilizar o TOR, todos os compradores e vendedores de mercadorias ilícitas permaneciam anônimos, identificando-se apenas por meio de um pseudônimo de sua escolha. Para proteger mais os usuários e suas atividades ilegais, a única forma de pagamento aceita no *Silk Road* era o *Bitcoin*, um novo tipo de moeda eletrônica que permite que as partes troquem fundos com uma forte proteção de privacidade (GOODMAN, 2015, p. 268).

Há várias maneiras e formas de se infectar uma máquina: sites maliciosos, links suspeitos por e-mail ou por *whatsapp*, instalação de aplicativos vulneráveis, por meio de redes sociais, ou seja, todo o conteúdo compartilhado na rede e inclusive fora dela pode ser alvo e ser invadido por diversos tipos de ataques.

Nesse sentido, na mesma medida e proporção é necessário que se criem formas de persecução penal, novos métodos de investigação e proteção dos inúmeros bens jurídicos ameaçados e violados.

Conforme mencionado, exemplo que poderia ser adotado que ajudaria na manutenção de servidores, aprendendo com falhas sistêmicas e até linguagens criminais específicas seria o projeto "Watson" da IBM.

O Watson seria uma plataforma de computação cognitiva, que aprende com o ensinamento, por conta de um sofisticado mecanismo de inteligência artificial: alerta 24 horas, pode avisar possíveis ataques e até monitorar, tanto online como off-line, inclusive em câmeras ligadas a sistemas para prevenção de ataques.

Exemplo do emprego de inteligência artificial é o "DoNotPay", que é um "chatbot", um robô em forma de aplicativo de chat que usa inteligência artificial funcional para interagir com humanos, sendo que seu princípio básico é o aprendizado constante com o próprio usuário. Esse

sistema conseguiu reverter mais de 160 mil multas, utilizando uma ferramenta de busca específica para atuar.[13]

Essas iniciativas estão colocando a inteligência artificial de supercomputadores nas mãos tanto de microempresas quanto de pessoas físicas, e no futuro, muito provavelmente também nas mãos da *Crime S.A.* Ao utilizar ferramentas de inteligência artificial que funcionam 24 horas por dia, 7 dias por semana, quanta lavagem de dinheiro, roubo de identidade ou fraude fiscal Watson poderia cometer? (GOODMAN, 2015, p. 349).

Com esse sistema, é possível, por exemplo, construir robôs que ficassem conectados na rede 24 horas, para que pudessem assim estudar e juntar comportamentos estranhos na rede.

O uso de inteligência artificial e a criação de um sistema ao máximo interligado são fundamentais: é preciso utilizar a ideia de dados estruturados, ou seja, indexar dados e transformá-los em informação para agir preventiva e repressivamente.

Como se sabe, o algoritmo é uma sequência finita de instruções bem definidas e não ambíguas, cada uma das quais devendo ser executada mecânica ou eletronicamente em um intervalo de tempo finito e com uma quantidade de esforço finita.[14]

Um algoritmo não representa, necessariamente, um programa de computador, e sim os passos necessários para realizar uma tarefa: sua implementação pode ser feita por um computador, por outro tipo de autômato ou mesmo por um ser humano. Diferentes algoritmos podem realizar a mesma tarefa usando um conjunto diferenciado de instruções em mais ou menos tempo, espaço ou esforço do que outros. Tal diferença pode ser reflexo da complexidade computacional aplicada, que depende de estruturas de dados adequadas ao algoritmo.

O governo americano, sensível a tudo que está sendo descrito, já possui um departamento exclusivo de ciberataque construído também com a lógica de inteligência artificial, pois compreendeu que não se trata apenas de uma simples invasão e desvio de dinheiro, mas da potencial possibilidade de ataques às fontes de energia e abastecimento, acionamento de armas nucleares, enfim, de potenciais chances de se instalar um caos e novas

[13] Ver: **'Advogado-robô' reverte 160 mil multas de trânsito em NY e Londres,** disponível em: http://g1.globo.com/tecnologia/noticia/2016/06/advogado-robo-reverte-160-mil-multas-de-transito-em-ny-e-londres.html. Acesso em: 18 jul. 2020.

[14] O conceito de um algoritmo foi formalizado em 1936 pela Máquina de Turing de Alan Turing e pelo cálculo lambda de Alonzo Church, que formaram as primeiras fundações da Ciência da Computação.

formas de criminalidade que se equiparam a ataques verdadeiramente terroristas, com todo o contexto que envolve a acepção da palavra terrorismo.

Com um sistema monetário ilícito que não pode ser rastreado, o crime já não é algo que se pode cometer, mas que se pode comprar. O "Crime as a Service" (CaaS), ou crime como serviço, é o novo modelo de negócio e permite que um crime ou parte dele seja realizado por outros, enquanto o empreendedor, que organizou e investiu no golpe, tem seu lucro garantido. Assim como as grandes corporações, um número cada vez maior de criminosos está usando o software como serviço para realizar suas operações corporativas, além de suas competências essenciais (GOODMAN, 2015, p. 225).

Hoje redes sociais on-line (OSNs) têm crescido exponencialmente. O uso inicial de mídias sociais para fins benignos e particulares deu lugar a inúmeras atividades maliciosas: cibercrimes, ciberterrorismo e guerra cibernética.

Redes de distribuição de dados iniciais, como provedores, podem ter seu tráfego ou fluxo analisado, por sistemas, robôs, programas e pessoas especializadas que podem descobrir e decifrar se uma rede está trabalhando de forma anômala ou até mesmo se a distribuição de dados está sendo enviada para outro servidor diretamente.

Considerações finais

É preciso reconhecer que o uso nefasto dessas novidades tecnológicas representa uma ameaça significativa e difusa para a sociedade e, portanto, requer atenção à investigação e pessoas preparadas e capacitadas.

Assim, como a natureza da internet demanda o enfrentamento e rediscussão de tradicionais questões jurídicas processuais (jurisdição e competência, cooperação jurídica internacional etc.), ela também exige uma grande discussão sobre novos métodos para investigação, nova formação das carreiras jurídicas e dos cursos acadêmicos de direito, novos perfis de profissionais voltados à investigação desses crimes.

Em suma: é evidente que há insegurança jurídica por conta da insuficiência dos métodos de investigação, assim como é evidente a crucial necessidade de desenvolvimento de uma doutrina própria e de um modelo próprio de processo e de investigação de crimes digitais.

Diante desta situação, é inevitável a evocação – ainda que vaga – de uma "dialética do moderno", no sentido de que esses interesses e esses sinais distintivos se autonomizaram,

passaram a ter vida própria e conduziram o Direito Penal a uma fronteira na qual os objetivos originários de um sistema voltado para as consequências inevitavelmente desvirtuam-se: "o sistema penal atual se apresenta acima de tudo como um instrumento efetivo da política interna ou de segurança pública, rejeita sumariamente a indagação crítica sobre sua aptidão instrumental e desvencilha-se pouco a pouco dos grilhões representados pelos princípios" (HASSEMER, 1993, p. 47).

A ilação, segundo Hassemer, de que aqui se está diante de uma sede de punir já seria anacrônica: "pelo contrário, o que está atuando é nada mais que a herança do Direito Penal voltado para as consequências" (HASSEMER, 1993, p. 47).

Tais premissas são fundamentais, conforme já brevemente salientado, da imperiosa necessidade de que o país, não obstante a criação de uma cultura hermenêutica de novos mecanismos de prova e investigação, trace efetivos marcos jurídicos aderindo à Convenção de Budapeste.

Esta, em seu capítulo II, ao tratar da dogmática penal, contempla inúmeras normas de criminalização que não foram observadas a contento pelo legislador brasileiro, disciplinadas nos seguintes títulos: a) Infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos (Acesso ilegítimo, Intercepção ilegítima, Interferência em dados, Interferência em sistemas, Uso abusivo de dispositivos); b) Infracções relacionadas com computadores (Falsidade informática, Burla informática); c) Infracções relacionadas com o conteúdo (Infracções relacionadas com pornografia infantil, Infracções relacionadas com a violação do direito de autor e dos direitos conexos), dispondo de forma expressa sobre a responsabilidade de pessoas jurídicas.

Já no tocante ao processo penal, prevê dispositivos como a injunção ou obrigação de comunicar os dados informáticos específicos, na sua posse ou sob o seu controle e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; a busca e apreensão de dados informáticos armazenados; a recolha em tempo real de dados informáticos; e a intercepção de dados relativos ao conteúdo.

Como medida mais salutar, diante da forma pela qual esses delitos são perpetrados, prevê a essencial cooperação jurídica internacional ou o "auxílio mútuo relativamente a poderes de investigação".

Aliás, em seu título 3, prevê, dentro da ideia de prevenção constante e cooperação

internacional, a "Rede 24/7", prevendo que

> Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infracções penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma electrónica, de uma infracção penal. O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas: a) A prestação de aconselhamento técnico; b) A conservação de dados em conformidade com os artigos 29º e 30º; e c) A recolha de provas, informações de carácter jurídico e localização de suspeitos.[15]

É, portanto, evidente que a Lei do Marco Civil da Internet se revela insuficiente para a proteção jurídica suficiente dos bens e garantias fundamentais assegurados na Constituição e nos tratados internacionais de direitos humanos ou de garantismo social (Pacto de San José, Convenção de Mérida, Convenção de Combate à Pedofilia, Convenção de combate à Lavagem de Dinheiro, Convenção de Palermo, Convenção de Combate ao Terrorismo etc.), assim como dos novos bens difusos lesados por conta dessa nova forma de criminalidade.

Vale ressaltar, ademais, que a Lei nº 12.965/14, ao estabelecer os princípios, garantias, direitos e deveres para o uso da internet no país, estabelece como fundamento, dentre outros, o respeito aos direitos humanos, à pluralidade e à diversidade, à abertura e à colaboração, preservando a estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas, bem como responsabilizando os agentes de acordo com suas atividades, nos termos da lei.

No art. 23, parágrafo único, prevê, inclusive, de forma explícita, que os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte, embora até hoje não tenha agido politicamente para subscrever a Convenção de Budapeste.

Ademais, as diretrizes traçadas pelo legislador no art. 24 (dentre as quais, estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica, promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos, promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade, otimização da infraestrutura das redes) evidenciam-

[15] CONSELHO DA EUROPA. Convenção sobre o cibercrime. Budapeste: Conselho da Europa, 2001.

se em normas meramente programáticas que demandam, ao lado da adesão à mencionada convenção e complementação dos marcos jurídicos penais e processuais penais, uma política efetiva e eficiente voltada às consequências dessas novas formas de criminalidade, sob pena de se institucionalizar, tal qual se verifica pelas enormes taxas de vitimização, a proteção deficiente de inúmeros bens e garantias individuais e difusas.

Referências

ALFLEN DA SILVA, Pablo Rodrigo. **Leis Penais em Branco e o Direito Penal do Risco:** aspectos críticos e fundamentais. Rio de Janeiro: Lumen Juris, 2004.

ANDRADE, Fábio Martins de. **Mídia e Poder Judiciário:** A influência dos Órgãos da Mídia no Processo Penal Brasileiro. Rio de Janeiro: Lumen Juris, 2007.
ANTONIO MARINA, José Antonio. **Cronicas de la Ultramodernidad**. Barcelona: Anagrama, 2000.

BARRETO, Tobias. **Introdução Ao Estudo do Direito**: Política Brasileira, São Paulo: LANDY, 2001.

BATISTA, Nilo. **Mídia e Sistema Penal no Capitalismo Tardio**. Discursos Sediciosos: Crime, Direito e Sociedade, Rio de Janeiro: Revan, Instituto Carioca de Criminologia, ano 7, nº 12, p. 271-288, 2º semestre de 2002.

_____. **Novas Tendências do Direito Penal**, Rio de Janeiro: Editora Revan, 2004.

BAUMAN, Zygmunt. **Globalização: As Consequências Humanas**, Rio de Janeiro: Zahar, Trad. Tradução: Marcus Penchel, 1999.
_____. **Medo Líquido**. Rio de Janeiro: Zahar, Trad. Tradução: Carlos Alberto Medeiros, 2008.

_____. **Modernidade Líquida**, Rio de Janeiro: Zahar, 2001.

_____. **Sobre Educação e Juventude (Conversas com Ricardo Mazzeo)**, Rio de Janeiro: Zahar, Trad. Tradução: Carlos Alberto Medeiros, 2013.

BECHARA, Fábio Ramazzini. **Cooperação Jurídica Internacional em matéria penal (eficácia da prova no exterior)**, São Paulo: Saraiva, 2011.

BECK, Ulrich. **O que é globalização?** São Paulo: Paz e Terra, Tradução: André Carone, 1999.

_____. **Sociedade de Risco – Rumo a uma outra modernidade**, Ed. 34, Tradução de Sebastião Nascimento, 2010.

BIANCHINI, Alice. **Pressupostos Materiais Mínimos da Tutela Penal**. Revista dos Tribunais, Série As Ciências Criminais do Século XXI, v. 7, 2002.

BONJARDIM, Estela Cristina. **O Acusado, sua Imagem e a Mídia**. São Paulo: Max Limonad, 2002.

BRITO, Edivaldo. **O que é o IP? Descubra para que serve e qual é seu número**, disponível em http://www.techtudo.com.br/artigos/noticia/2013/05/o-que-e-o-ip-descubra-para-o-que-serve-e-qual-e-seu-numero.html. Acesso em: 10 jun. 2020.

CAMPILONGO, Celso Fernandes. **O Direito na Sociedade Complexa**. Apresentação e ensaio de Raffaele De Giorgi. Ed. Max Limonad, 2000.

CARDOSO, Pedro. **O que é Ransomware?** Disponível em: http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html. Acesso em: 17 maio de 2020.

CARVALHO FILHO, Carlos Henrique de. (diretor responsável). **Escritos em homenagem a Alberto Silva Franco.** São Paulo: Editora Revista dos Tribunais, 2003.

CARVALHO, Natália Oliveira de. **Trialby Media: o Sistema Penal é a Pauta!** Boletim IBCCRIM. São Paulo, ano 15, n. 185, abr. 2008.

CASSIRER, Ernest. **A Filosofia do Iluminismo**. Campinas: Unicamp, 1992.

CAVALCANTI, Eduardo Medeiros. **Crime e Sociedade Complexa**. Campinas: LZN, 2005.

CERVINI, Raúl. **Criminalidad Organizada y Lavado de Dinero**. Belo Horizonte: Del Rey, Direito Criminal - Coleção JUS AETERNUN, Coordenador: José Henrique Pierangeli, 2000, v. 1.

COLLI, Maciel. **Violência cibernética, investigação preliminar e prevenção da participação no suicídio na Internet.** Proceedingsofthethirdinternationalconferenceofforensiccomputerscience. v.3, n. 1, 2008.

CONSELHO DA EUROPA. **Convenção sobre o cibercrime**. Budapeste: Conselho da Europa, 2001.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva, 2011.

DELEUZE, Gilles. Apud LÉVY, Pierre. **O que é virtual?** Tradução: Paulo Neves. E-book. Disponível em: http://www.mom.arq.ufmg.br/mom/arq_interface/6a_aula/o_que_e_o_virtual_-_levy.pdf. Acesso em: 05 mar. 2020.

DIAS, Jorge de Figueiredo. **O Direito Penal entre a Sociedade Industrial e a Sociedade do**

Risco. Revista Brasileira de Ciências Criminais. São Paulo, v. 9, n. 33, jan./mar. 2001.

DIP, Ricardo; MORAES Jr., Volney Corrêa Leite de. **Crime e Castigo – Reflexões Politicamente Incorretas**. Campinas: Millennium, 2002.

FRAGA, Érica. **O bunker virtual**. 'Folha de São Paulo', edição de 29 mai. 2005, Caderno 'Mais!'. Disponível em: http://www1.folha.uol.com.br/fsp/mais/fs2905200506.htm. Acesso em: 28 fev. 2020.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico. -** 1. ed. São Paulo: Edipro, 2012.

GOODMAN, MARC. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso/** Marc Goodman; tradução de Gerson Yamagami-São Paulo: HSM editora, 2015.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. São Paulo: Revista Direito Mackenzie n. 1, 2000.

HASSEMER, Winfried. **Três Temas de Direito Penal**, *In* Publicações Fundação Escola Superior do Ministério Público, 1993.

HOBBES, Thomas. **Leviatã**. São Paulo: Martin Claret, 2006.

HUNGRIA Hoffbauer, Nélson. **Comentários ao Código Penal**. Rio de Janeiro: Forense, 3 ed. v. I, Tomo 1º, arts. 1 a 10.

JAKOBS, Günther. **La Ciencia Del Derecho Penal Ante Las Exigencias Del Presente**. Universidad Externado de Colombia – Centro de Investigaciones de Derecho Penal Y Filosofía del Derecho, 2000, Tradução de Teresa Manso Porto.

LÉVY, Pierre. **Cibercultura.** Tradução: Carlos Irineu da Costa. 1°. Ed. São Paulo: Editora 34, 1999.

_____. **O que é virtual?** Tradução: Paulo Neves. E-book. Disponível em: http://www.mom.arq.ufmg.br/mom/arq_interface/6a_aula/o_que_e_o_virtual_-_levy.pdf. Acesso em: 05 maio 2020.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** 2. ed. São Paulo: Atlas, 2011.

LIPOVETSKY, Gilles. **A Era do Vazio: Ensaios sobre o Individualismo Contemporâneo**. São Paulo: Manole, 2005.

LUHMANN, Niklas. **Sociologia del Rischio**. Milão: Burno Mondadori, 1996.

MACHADO, André Augusto Mendes. **A investigação criminal defensiva**. 2009. Dissertação (Mestrado), Faculdade de Direito de São Paulo, São Paulo.

MALAQUIAS, Roberto Antônio Darós. **Crimes cibernético e prova: a investigação criminal em busca da verdade.** Curitiba: Juruá, 2013.

MARIANO DA SILVA, Cesar Dario. **Provas ilícitas.** 7. Ed. Curitiba: Juruá, 2016.

MASCARENHAS, Oacir Silva. **A Influência da Mídia na Produção Legislativa Penal Brasileira**, *In* **Âmbito Jurídico,** Rio Grande, XIII, n. 83, dez 2010. Disponível em: http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=8727&revista_caderno=3. Acesso em: 18 ago. 2020.

MAZONI. Ana Carolina. **Crimes na Internet e a Convenção de Budapeste.** Dissertação (monografia), 2009, Faculdade de Ciências Jurídicas e Sociais, Brasília.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 8. ed. São Paulo: Saraiva, 2013.

MORAES, Alexandre Rocha Almeida de. **Direito Penal do Inimigo: A Terceira Velocidade do direito penal**, Curitiba: Juruá, 2008.

_____. **Direito Penal Racional: Propostas para a construção de uma teoria da legislação e para uma atuação criminal preventiva**. Curitiba: Juruá, 2016.

MORAES, Alexandre Rocha Almeida de; SMANIO, Gianpaolo Poggio, PEZZOTTI, Olavo Evangelista. **A discricionariedade da ação penal pública.** Argumenta Journal Law, Jacarezinho, n. 30, p. 353-390, 2019. http://dx.doi.org/10.35356/argumenta.v0i30.

NATÁRIO, Rui Manuel Piteira. Tenente-Coronel. **O combate ao cibercrime: Anarquia e ordem no ciberespaço.** Revista Militar, Ed. 2541; 2013. Disponível em: https://www.revistamilitar.pt/artigo/854, Acesso em: 07 set. 2020.

OLIVEIRA, Carlos Alberto Álvaro de. **Efetividade e Processo de Conhecimento**. Disponível em: http://www.abdpc.org.br/abdpc/artigos/Carlos%20A%20A%20de%20Oliveira(3)%20-formatado.pdf. Acesso em: 15 mar. 2020.

OST, François. **O Tempo do Direito**. Lisboa: Instituto Piaget, 1999, Trad. Maria Fernanda de Oliveira.

PACKER, Herbert. **The Limits of the Criminal Sanction**. Califórnia: Stanford, 1968.

PASCHOAL, Janaina Conceição. **Constituição, Criminalização e Direito Penal Mínimo**. São Paulo: Revista dos Tribunais, 2003.

PETRINI, João Carlos. **Pós-modernidade e Família – Um Itinerário de Compreensão**. Bauru: EDUSC, 2003.

PRITTWITZ, Cornelius. **O Direito Penal entre Direito Penal do Risco e Direito Penal do Inimigo: tendências atuais em direito penal e política criminal**. São Paulo: Revista dos Tribunais. Revista Brasileira de Ciências Criminais, v. 47, mar./abr. 2004, Trad.HelgaSabotta de Araújo e Carina Quito.

REALE, Miguel. **Lições preliminares de direito.** 17 ed. São Paulo: Saraiva, 2002.

RESTA, Elgio. **Relato sobre Aspectos Sociales-Económicos**. *In* XI Congreso Internacional de Defensa Social: La internacionalización de las sociedades contemporáneas en el campo de la criminalidad y las respuestas del Movimiento de la Defensa Social, México, 1991.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e Direito Penal.** São Paulo: Memória Jurídica, 2004.

SANTOS, Coriolano Aurélio Camargo. **Atual cenário dos Crimes Cibernéticos no Brasil**. Disponível em: http://pt.scribd.com/doc/41224053/Crimes-Ciberneticos. Acesso em: 10 jun. 2020.

SCALCON, Raquel Lima. **Mandados Constitucionais (implícitos) de Criminalização?** Monografia de Conclusão de Curso UFRS, Porto Alegre, 2009, p. 14, disponível em http://www.lume.ufrgs.br/bitstream/handle/10183/31323/000779559.pdf. Acesso em: 17 jan. 2020.

SCHWABE, Jürgen. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Trad. Beatriz Henninget al. Leonardo Martins, Leonardo Martins; Mariana Bigelli de Carvalho; Tereza Maria de Castro; Vivianne Geraldes Ferreira. Montevideo, Konrad-Adenauer-Stiftung, 2005.

SILVA SÁNCHEZ, Jesús-Maria. **A Expansão do Direito Penal: Aspectos da Política Criminal nas Sociedades Pós-industriais**, São Paulo: Revista dos Tribunais, Série as Ciências Criminais no Século XXI – v. 11, Tradução: Luiz Otavio de Oliveira Rocha, 2002.

STRECK, Lenio. **Hermenêutica Jurídica e(m) Crise: uma exploração hermenêutica da construção do direito**. 10 ed. Porto Alegre: Livraria do Advogado, 2011.

TOURINHO FILHO Fernando da Costa. **Manual de processo penal.** São Paulo: Saraiva, 2012, 15. ed. rev. e de acordo com a Lei n. 12.403/2011.