XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I

SÉRGIO AUGUSTIN

SÉRGIO HENRIQUES ZANDONA FREITAS

D597
Direito penal, processo penal e constituição I [Recurso eletrônico on-line] organização CONPEDI/ UNISINOS
Coordenadores: Sérgio Augustin; Sérgio Henriques Zandona Freitas. – Florianópolis: CONPEDI, 2018.

Inclui bibliografia
ISBN: 978-85-5505-715-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Tecnologia, Comunicação e Inovação no Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. XXVII Encontro Nacional do CONPEDI (27 : 2018 : Porto Alegre, Brasil).

CDU: 34

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

Universidade do Vale do Rio dos Sinos
Porto Alegre – Rio Grande do Sul - Brasil
http://unisinos.br/novocampuspoa/

XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I

Apresentação

É com muita satisfação que apresentamos o Grupo de Trabalho (GT) denominado "DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I" do XXVII Congresso Nacional do CONPEDI Porto Alegre/RS promovido pelo CONPEDI em parceria com a Universidade do Vale do Rio dos Sinos (UNISINOS), com enfoque na temática "Tecnologia, Comunicação e Inovação no Direito", o evento foi realizado entre os dias 14 e 16 de novembro de 2018 no Campus de Porto Alegre, Av. Dr. Nilo Peçanha, 1600 / Bairro Boa Vista - Porto Alegre/RS.

Trata-se de publicação que reúne artigos de temas diversos atinentes ao Direito Penal, Criminologia e o Processo Penal apresentados e discutidos pelos autores e coordenadores no âmbito do Grupo de Trabalho e Linha de pesquisa. Compõe-se de artigos doutrinários, advindos de projetos de pesquisa e estudos distintos de vários programas de pós-graduação do país, que colocam em evidência para debate da comunidade científica assuntos jurídicos relevantes.

Assim, a coletânea reúne gama de artigos que apontam questões relativas aos (des)caminhos do processo penal: o silêncio dos intelectuais; estado de exceção: legitimidade estatal em crise no cenário da criminalidade; o espetáculo midiático do processo penal: análise acerca da colisão entre o direito à informação e o direito a um justo julgamento; paradigmas e legados da operação lava jato para enfrentamento da cultura da corrupção, criminalização da política e crise de representatividade democrática; a importância do ofendido na relação processual penal; a proteção do patrimônio genético humano: por uma política criminal prospectiva; as relações entre compliance e a possível responsabilização da pessoa jurídica; cooperação jurídica internacional em matéria penal: noções fundamentais e paradigmas atuais frente a novas perspectivas globais; crime de terrorismo e crime político: definições, aproximações e distinções; expectativas e jurisdição: dinâmica de poder e a atuação do julgador no processo penal; o crime continuado e a possibilidade de uma interpretação fraterna; a aplicabilidade da justiça restaurativa nos casos de perturbação ao sossego e tranquilidade; a audiência de custódia e sua (in)capacidade de alteração do cenário prisional brasileiro; comissão técnica de classificação; o exercício de greve pelos militares: proibição, sanções penais e anistia; a execução provisória da pena e a presunção de inocência: notas sobre uma contenção democrática do poder punitivo; o sigilo das comunicações e o uso das interceptações telefônicas como meio de prova no processo penal: em busca da proteção da privacidade; e a

cadeia de custódia e a prova pericial: conectando aspectos inovadores ao direito processual penal.

Em linhas gerais, os textos reunidos traduzem discursos interdisciplinares maduros e profícuos. Percebe-se uma preocupação salutar dos autores em combinar o exame dos principais contornos teóricos dos institutos, aliando a visão atual da jurisprudência com a prática jurídica dos estudiosos do Direito. A publicação apresentada ao público possibilita acurada reflexão sobre tópicos avançados e desafiadores do Direito Contemporâneo. Os textos são ainda enriquecidos com investigações legais e doutrinárias da experiência jurídica estrangeira a possibilitar um intercâmbio essencial à busca de soluções para as imperfeições do sistema jurídico penal e processual penal brasileiro.

O fomento das discussões a partir da apresentação de cada um dos trabalhos ora editados, permite o contínuo debruçar dos pesquisadores do Direito visando ainda o incentivo aos demais membros da comunidade academica a submissao de trabalhos aos vindouros encontros e congressos do CONPEDI.

Sem dúvida, esta publicação fornece instrumentos para que pesquisadores e aplicadores do Direito compreendam as múltiplas dimensões que o mundo contemporâneo assume na busca da conjugação da promoção dos interesses individuais e coletivos para a consolidação de uma sociedade dinâmica e multifacetada.

Na oportunidade, os Organizadores prestam sua homenagem e agradecimento a todos que contribuíram para esta louvável iniciativa do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI), em especial, a todos os autores que participaram da presente coletânea de publicação, em especial, pelo comprometimento e seriedade demonstrados nas pesquisas realizadas e na elaboração dos textos de excelência.

Convida-se a uma leitura prazerosa dos artigos apresentados de forma dinâmica e comprometida com a formação de pensamento crítico, a possibilitar a construção de um Direito voltado à concretização de preceitos insculpidos pela Constituição da República.

Porto Alegre, novembro de 2018.

Professor Dr. Sérgio Augustin

Universidade de Caxias do Sul

Professor Dr. Sérgio Henriques Zandona Freitas

Universidade FUMEC e Instituto Mineiro de Direito Processual

PERSPECTIVIAS EXPANSIONISTAS DO DIREITO PENAL EM FACE DOS CRIMES VIRTUAIS NA SOCIEDADE DE RISCO

EXPANSIONIST PERSPECTIVITIES OF THE CRIMINAL LAW IN THE FACE OF VIRTUAL CRIMES IN THE RISK SOCIETY

Rogério Gesta Leal
Mauro Evely Vieira De Borba

Resumo

O objetivo desse trabalho é verificar se o sistema jurídico brasileiro está apto para enfrentar o fenômeno da criminalidade virtual, em face de suas especificidades hipercomplexas, gerando condutas de difícil responsabilização. Justifica-se a abordagem pelo fato de que tais crimes estão em franca expansão global, causando danos a interesses individuais e sociais. O problema é: se há legislação criminal adequada a persecução desses crimes, e quais os déficits a serem atendidos neste particular? Como hipótese: é possível, com os instrumentos normativos que já temos, promover ações curativas e preventivas de combate à criminalidade virtual. Utiliza-se o método hipotético dedutivo.

Palavras-chave: Crimes virtuais, Expansão do direito penal, Inovações normativas, Sistema jurídico brasileiro, Sociedade de risco

Abstract/Resumen/Résumé

The objective of work is to verify if the Brazilian legal system is able to face the phenomenon of virtual criminality, due to its hypercomplex specificities, generating behaviors of difficult accountability. The justification is that such crimes are in global expansion, causing damage to individual and social interests. The problem is: if there is adequate criminal legislation to prosecute these crimes, and what deficits to be served in this particular? As hypothesis: it's possible, with the normative instruments that we already have, to promote curative and preventive actions to combat virtual crime. The deductive hypothetical method is used.

Keywords/Palabras-claves/Mots-clés: Virtual crimes, Expansion of criminal law, Normative innovations, Brazilian legal system, Risk society

Introdução

As relações humanas e institucionais contemporâneas estão marcadas, de forma inexorável e ao menos ao que interessa aos sistemas jurídicos, pela realidade virtual e seus inéditos paradigmas de tempo e espaço. Isto tem implicações multifacetadas, eis que, por vezes, reduz os níveis de cognição, valoração e tomada de decisão com consciência plena dos sujeitos de direito protagonistas de atos, fatos e negócios jurídicos.

É que o universo em que opera a realidade virtual é constituído pela automatização complexa dos processos de elaboração e circulação de dados e informações, numa velocidade e modo em média superior a capacidade humana de assimilação racional, e este fato, por si só, já representa desafios às tentativas dos sistemas jurídicos em regulá-lo completamente. Por certo que estes elementos não dizem respeito somente aos aspectos e dificuldades cognitivos das ações humanas, mas também aos âmbitos decisionais, relacionados às escolhas e manifestações de vontade decorrentes disto, e que podem ter valor e relevância jurídica de múltiplas naturezas (civis, administrativas, penais).

O problema é que no mundo virtual o contingente de informações e dados é tão vasto e de procedências tão difusas que a certeza sobre as suas origens (lícita ou ilícita, confiável ou não, científica ou não) está constantemente ameaçada. E é com base em tais elementos que juízos de cognição e valor são forjados, escolhas são feitas e manifestações de vontade geram atos e consequências as mais diversas.

Demarcamos como problema deste artigo verificar se há legislação criminal adequada a persecução de comportamentos desta natureza, e quais os déficits a serem atendidos neste particular, e como hipótese a premissa de que é possível, com os instrumentos normativos que já temos, promover ações curativas e preventivas de combate à criminalidade virtual. A metodologia utilizada neste trabalho foi a hipotética dedutiva. Neste texto pretendemos, pois, verificar em que medida o Brasil está preparado em termos normativos para o enfrentamento desta nova realidade virtual e seus impactos no âmbito da criminalidade.

1. Da criminalidade física à virtual na Sociedade de Riscos: ações e reações do Direito Penal e Processual Penal

O conceito de risco desde há muito constitui nuclearmente as relações sociais hodiernas, sendo que da segunda metade do século XX em diante temos assistido sua intensificação, seja objetiva (no sentido de maior presença de riscos e perigos conectados ao modo de produção e de vida); seja subjetiva (no sentido de uma mais aguda percepção dos

riscos e perigos tomados em si) (BECK, 1998).

Nestes cenários, as demandas por tutelas penais encontram cada vez mais abstratas legitimações pelo fato de que o caráter difuso dos problemas sobre os quais estamos falando imprime níveis de insegurança pública muito significativos não somente à incolumidade individual, mas igualmente a bens coletivos, como saúde pública, proteção dos consumidores, do meio ambiente, das relações econômicas, dentre outros.

Em apertada síntese, podemos afirmar que a legitimação do Direito Penal em contextos de insegurança iminentes está muito vinculada a ideia da precaução, sempre mais frequentemente lembrado quando se trata de demarcar responsabilidades dos sujeitos que possuam relação direta ou indireta com a provocação de danos. Ou seja, em situações nas quais há incertezas científicas e tecnológicas sobre atitudes potencialmente lesivas em face do uso de determinadas substâncias, procedimentos, sistemas de manejo de bens protegidos pelo sistema jurídico vigente, impõe-se a disposição de adequadas tutelas protetivas (individuais e coletivas).

Em termos de culpa, a previsibilidade de evento danoso pode conectar-se mesmo que somente à possibilidade que este venha a se verificar, isto porque esta revela, de forma muito concreta, as potencialidades lesivas das condutas do agente. Neste sentido, quando se trata de matéria atinente à tutela da vida humana (na sua forma singular ou coletiva/difusa), o risco que o agente representa pode fazer-se efetivo em face, inclusive, da possibilidade de que a ausência de medidas cautelares preventivas possa induzir dúvidas não meramente conjecturais, mas iminentes, sobre a possível produção de consequências materialmente danosas.

Por outro lado, como na realidade física, também no mundo virtual tem surgido inéditas formas de lesões a interesses privados e públicos, desde o terrorismo, a pedofilia, o bulyng, piratarias, racismos, xenofobias, furtos, dentre outros. Isto tem se alastrado tanto que os órgãos de segurança pública e privada em todo o mundo tem desenvolvido estratégias e treinamento para o seu enfrentamento, a despeito de que a legislação no ponto ainda seja deficitária (USA, FBI, <htttps://www.fbi.gov>).

Sem sombra de dúvidas que os criminosos *on line* são de todos os tipos, e podem minar a segurança de nações inteiras, como é o caso do terrorismo, o tráfico de armas, pessoas e órgãos, além do que o comercio eletrônico tem igualmente provocado danos individuais e coletivos, drenando recursos financeiros de consumidores menos avisados e atentos; a própria representação política e as eleições são atingidas – direta ou indiretamente – por comportamentos virtuais de duvidosa licitude.

2

A partir da WEB pessoas aliciam crianças, arregimentam fundamentalistas religiosos, racistas, fomentam o preconceito étnico e de gênero, divulgam propagandas de ódio e violência, alimentam os extremismos políticos e ideológicos, compram e vendem o que pudermos imaginar, roubam dados de pessoas físicas e jurídicas, e os utilizam no mercado virtual. Ainda se opera, a partir da rede virtual de relações, o que os especialistas chamam de desinformação, ora entendida como difusão de informações falsas e distorcidas que, transitando de um lado a outro, é capaz de condicionar a opinião pública.

As oportunidades criadas pela internet têm transformado muitas atividades econômicas, relações de trabalho, de família, afetivas e sexuais, projetos de pesquisa e produção científica, ações políticas, com níveis de qualidade e sofisticação sem precedentes, contribuindo em muito para o avanço de vários setores e pessoas em toda parte. Ocorre que também a criminalidade lança mão destes recursos para evoluir e complexificar seu ofício, criando dificuldades materiais e formais para seu controle e responsabilização.

O interessante é que, no mundo virtual, a criação das condições de possibilidade das ações criminosas geralmente é concebida/arquitetada por poucos indivíduos, que podem se valer (pessoalmente ou através de outros), em escalas imensas, de *modus operandi* matricialmente formatados para incontáveis situações lesivas e ilícitas. Em razão disto, a replicação de eventos delituosos virtuais – e suas vítimas - toma proporção quase descontrolável. Daí a importância de contarmos com mecanismos eficientes de prevenção e responsabilização no ponto, e mesmo com tipos penais adequados para tanto.

Há dados que nos informam que as ações criminais virtuais estão progressivamente sendo operadas por organizações criminosas – nacionais e internacionais -, a partir de estruturas de comando, hierarquia e controle profissionais, cooptando técnicos altamente especializados em informática, contadores e administradores de empresas que passam a gestar os interesses escusos que se formam. Aliás, o crime organizado nem sempre precisa gastar muito para ter acesso a quadros profissionais de apoio aos seus alvos, eis que podem manter com eles relações não de colaboração remunerada, mas conseguir o que querem através de ameaças, violência e coações.

Sob o ponto de vista da estratégia criminosa, o espaço virtual é privilegiado para o cometimento de crimes, pois o controle, visibilidade e transparência das ações que ali ocorrem são baixíssimas, podendo os delinquentes terem tempo maior para o planejamento e execução das suas artimanhas. Neste ponto, a investigação destes crimes, por operar com a lógica e práxis dos crimes físicos e tradicionais, por vezes não tem instrumentos adequados, por vezes é engessada por procedimentos restringidos por Direitos Fundamentais Individuais

(privacidade, intimidade, propriedade privada).

Desde o acesso não autorizado a sistemas de dados através do chamado *hackeamento* (que diz respeito ao acesso a sistemas privados, contornando medidas de segurança fornecidas no sistema que é violado); o chamado *superzaping* (que configura o uso não autorizado de utilitários que permitem o acesso a qualquer lugar virtual, por mais protegido que seja, viabilizando que se apague, copie, insira ou use os dados armazenados nele); o *scavengning* (que consiste na coleta de informações residuais, físicas, manuais, diagramas, notas de programação, ou lógicas, residuais, arquivos temporários, para conhecer as formas de acessar o sistema); o *salemislacing* (que é a retirada diária de pequenas quantias em milhares de contas), dentre outros[1], vivemos em tempos de profunda insegurança em nossas relações sociais e institucionais.

No mundo virtual inexistem fronteiras, e isto constitui característica muito atraente para quase todas as atividades criminais. Quando as autoridades tentam controla-lo encontram muitas dificuldades, a começar pelo fato de que a internet costuma ofertar facilidades e estímulos para a consecução de muitos comportamentos potencial ou efetivamente criminosos, como o anonimato, que fornece instrumentos ideais para atividades próprias da criminalidade organizada. Ou seja, o segredo da autoria virtual – quando ocorre – revela-se como chave estratégica e oportunidade excelente à realização de atos delinquentes, ou dissimulados, utilizando-se de formas jurídicas aparentemente lícitas (principalmente empresas de fachada que só existem para a prática de crimes).

Por outro lado, para complicar mais estes cenários, temos alguns outros níveis de circulação de dados virtuais ainda mais complexos e de difícil investigação, como os chamados *deep web* e *dark web*; o primeiro, identificado como

> a parte da rede cujo conteúdo não está disponível ou indexado nos principais mecanismos de pesquisa (google, bing, yahoo). Ela é formada por milhões de páginas, com dimensão inimaginável e com crescimento similar ao da Internet Visível. Já a dark web refere-se as páginas não indexadas, que não seguem as regras do ICANN e não possuem nomes registrados no serviço de DNS. Essas páginas só podem ser acessadas com softwares específicos para navegação em ambientes criptografados e anônimos, como TOR, Invisible Internet Project (i2p) e FreeNeT (SHIMABUKURO, SILVA, 2018, p. 255).

Para além disto, vale lembrar, por exemplo, que as máfias, em passado não muito longínquo, tinham interesses em vários setores da economia dos países em que operava

1 Como a transferência eletrônica de fundos, destruição ou inutilização de arquivos, modificação de programas, dados ou documentos eletrônicos, apreensão de arquivos ou programas ou descoberta de segredos industriais ou comerciais.

(imobiliário, restaurantes, casa de jogos), e nestes aportava recursos e investimentos, inclusive para lavagem de dinheiro, chamando para si a atenção das autoridades (PUCCIO-DEN, 2008). Hoje, todavia, há determinados espaços de ocupação por parte destas mesmas máfias que são fundamentalmente virtuais, como: (a) mercado de ações; (b) participações societárias difusas, a partir de pessoas jurídicas fictícias; (c) os novos *e-commerces* totalmente virtuais.

Em boa medida, a sinergia entre crime organizado e internet só aumenta e se sofistica em termos de presente e futuro, fornecendo esta nova fronteira alternativas para negócios e lucros consideráveis com níveis de riscos muito baixos. Nesta onda nova, profissionais especializados de sistemas de segurança bancária vendem serviços ilegais para organizações criminosas, como clonagem de banco de dados privados para os fins de incluir neles operações financeiras de lavagem de dinheiro em fundos regulares de importantes instituições públicas e privadas. Neste sentido é elucidativa a lembrança de Musacchio (2002, [s.n.])

> Durante la fine gli anni 90 ci sono stati numerosi casi di organizzazioni criminali che hanno sfruttato Internet soprattutto nel settore del cd. e-commerce. Tutto questo è stato fatto con coercizione e attraverso il controllo totale degli istituti di mediazione economico-bancaria. Internet, inoltre, è stato usato per distribuire informazioni che hanno determinato artificialmente il prezzo dei mercati borsistici. Negli Stati Uniti, i clan mafiosi coinvolti in questo genere di affari erano membri delle famiglie Bonnano, Genovese e Colombo come pure membri immigrati appartenenti alla mafia russa

Veja-se que a relativa complacência em usar a força e a intimidação se adapta muito bem ao desenvolvimento da cyber-extorsão, pois, na experiência da indústria da internet estes comportamentos se concretizam frequentemente em ameaças de interromper as informações e os sistemas de comunicação, bem como destruir dados importantíssimos de instituições. O crescimento destes tipos de extorsões telemáticas apresenta-se como novas tendências da criminalidade moderna, alcançando universo tão amplo de interesses e patrimônios que colocam suas vítimas em estado de inexigibilidade de outra conduta a não ser a cooperação para o cometimento ou aprofundamento dos ilícitos perpetrados (HUNTER, LASTOWKA, 2003).

Estamos convictos de que o espaço virtual tem ocupado protagonismo diferenciado diante da criminalidade, empurrado pelas numerosas vulnerabilidades decorrentes dos sistemas de informação e dados virtuais, e exemplo disto pode ser dado em face do ocorrido no final do ano de 2001, quando uma variação do virus conhecido como *love bug* (o inseto do amor) foi usado para violar o sistema de segurança de várias instituições

bancárias dos Estados Unidos da América e da Suíça, causando prejuízos milionários a muitas pessoas físicas e jurídicas, não sendo claro até hoje quem foi o responsável por tal ataque. O ocorrido revela as estreitas relações colaborativas e mesmo de cumplicidade delinquente entre o crime organizado, *hackers* e *crakers*, que vendem seus serviços para tais fins, cobrando altíssimas recompensas, ou por vezes sendo alvos de ameaças e violência.[2]

Veja-se que os ciber crimes quando vinculados ao crime organizado apresentam múltiplos problemas que envolvem sejam os mecanismos de investigação, sejam os jurisdicionais. Um exemplo desta problemática pode ser o ocorrido com o chamado *inseto do amor* – já referido. Quando agentes do FBI conseguiram identificar o culpado deste ataque cibernético – por mais incauto que fosse -, um estudante filipino, Reonel Ramones, descobriu também que nas Filipinas inexistia legislação que pudesse lhe incriminar pelo feito (COMPUTERWORLD, 2000, <httP://www.computerworld.com>). Após o ocorrido as Filipinas adotaram legislação sobre crimes desta espécie, assim como muitos outros países no Ocidente.

A despeito destes cenários e o progressivo agravamento de recorrências em tais casos, há ainda vazios normativos muito impactantes para estes temas, seja pelo seu ineditismo e a consequente dificuldade de trata-lo adequadamente, seja pela ausência de interesse político de alguns setores que teriam condições de fazê-lo, o que somente amplia a impunidade de comportamentos ilícitos decorrentes. Por outro lado, é possível que algumas instituições, públicas e privadas, adotem condutas permissivas para atrair o comércio ilícito virtual, criando zonas francas de segurança e impunidade para os infratores, em troca de benefícios diretos e indiretos dos frutos rentáveis gerados.

Neste espaço incontrolável da internet seguramente a lavagem de dinheiro ocorre em escalas desconhecidas, alimentando em termos de financiamento e recursos parte do comércio internacional. Tenhamos em mente os cada vez mais prestigiados leilões virtuais, oferecendo oportunidades de movimentar dinheiro através de aquisições aparentemente legítimas, pagando por produtos muito mais, ou menos, do que eles valem no mercado. No Rio Grande do Sul, Brasil, tem-se a notícia de que a Delegacia de Repressão ao Roubo de Veículos de Porto Alegre, deflagrou operação conhecida como Macchina Nostra, para desarticular os responsáveis pela clonagem dos veículos roubados nesta cidade e na Região Metropolitana, e que depois eram vendidos por meio de leilões virtuais. A quadrilha investigada e presa possuía organização

2 A diferença entre hacker e craker, é que o primeiro tem como escopo, modo geral, vulnerar programas informáticos, enquanto que o segundo vai mais longe, pois busca não somente invadir programas ou ater acesso às informações, mas visa adulterá-los (FIORILLO, 2016).

empresarial com núcleos responsáveis pela liderança e financiamento, clonagem, venda e receptação, estelionato, falsificação de documentos, assaltos e lavagem de dinheiro (G1, 2017, <http://www.g1.globo.com>).

Outro setor de lavagem de dinheiro que ocupa em muito estes leilões virtuais – e físicos também – é o mercado das artes, isto porque ele possui algumas características que facilitam o anonimato dos seus protagonistas, tanto em face da seletividade daqueles que tem condições de dispor recursos significativos que o envolve, como também pelo fato de haver obras de arte que tem origens absolutamente ilícitas e cujos antecedentes e precedência são dolosamente sonegados, justamente para tornar mais interessante a lavagem de dinheiro que alimenta este segmento da economia. Neste ponto, Thomas Christ, membro do conselho do Instituto de Governança da Basileia, organização suíça sem fins lucrativos que investiga estas questões, referiu que este Mercado é ideal para o cometimento de ilícitos e é preciso que haja mais transparência em sua operação, tanto para saber de onde veio o dinheiro que o sustenta, como para saber para onde ele vai (GAZETA DO POVO, 2017, <http://www.gazetadopovo.com>).

Algumas casas importantes de artes no mundo, como a Christie's e a Sotheby's, tem aprimorado suas políticas de segurança nos últimos tempos, passando a exigir que agentes que queiram vender obras em seus estabelecimentos revelem o nome dos proprietários dos objetos que representam. Independentemente disto o volume de dinheiro que circula neste âmbito, principalmente em vendas virtuais, é astronômico (aproximadamente US$70 bilhões em 2017) (ROTH, 2016).

Estes são apenas alguns exemplos das possibilidades de ilicitudes que são cometidas pela internet, algumas operações com aparência de regular licitude, outras explicitamente ilícitas.

Vai na mesma direção as facilidades atuais que as operações bancárias eletrônicas proporcionam ao movimento de capitais estrondosos sem controles preventivos mais amplos de suas fontes e origens – a despeito dos rastros que deixam. E se diz isto porque, após consumadas as transferências eletrônicas de dinheiro, é muito difícil (pela velocidade com que isto se dá) evitar a circulação e disponibilidade destes recursos (ao menos parcial), até porque muitas das informações, dados e recursos que são veiculados nestes espaços o são de forma criptografada – fruto da associação entre hackers e criminalidade -, apresentando obstáculos ao monitoramento e controle. Veja-se o ocorrido na Itália:

> Nel mese di settembre del 2002, per esempio, due membri di un gruppo conosciuto in America con il nome di "Phonemasters" sono stati condannati per la violazione dei sistemi di elaborazione dati di numerose aziende di telecomunicazioni. I due cibercriminali avevano rubato vari sistemi cifrati di crittografia che hanno venduto ad alcuni gruppi appartenenti alla criminalità organizzata americana ed italiana. La

> cosa può apparire non molto grave: invece così non è. La nuova criminalità organizzata usa Internet per le comunicazioni (cifrate) e per tutti gli altri scopi, di conseguenza un sistema cifrato di crittografia può essere molto vantaggioso (es. ordinare un omicidio via Internet o reclutare donne per lo sfruttamento della prostituzione o vendere armi ed organi umani) (MUSACCHIO, 2002, [s.n.]).

Ou seja, para o crime organizado tem se tornado os recursos telemáticos eficientes instrumentos de organização e execução de vários delitos e condutas sequer normatizadas como ilícitas, razão pela qual há importantes vozes – públicas e privadas – sustentando que é chegada a hora de organismos internacionais e nacionais darem respostas mais efetivas a estas situações, tanto no âmbito do direito material como no processual, sendo que, neste último, inúmeros desafios se apresentam à investigação e instrução probatória, o que passamos a abordar.

Por todas estas razões é que a Convenção de Budapeste – da qual, aliás, o Brasil não é signatário -, previu a necessidade de regulamentação da responsabilidade penal dos provedores por crimes praticados no meio ambiente digital, em especial em seu art.12. Providência absolutamente necessária em face dos riscos e perigos causados pela atuação livre de provedores de fachada para ocultar ações criminosas das mais diversas espécies[3] (MPF, CONVENÇÃO SOBRE CIBERCRIME, 2001, <http://www.mpf.mp.br>).

Pelo já visto podemos afirmar que a crescente utilização de instrumentos telemáticos para a transmissão, recepção e elaboração de informações e dados (pessoais e institucionais), tem criado verdadeiro universo de bens que chama a atenção também do Mercado (formal e informal, lícito e ilícito), transformando-se em produtos de alta valorização. Tais bens e produtos são objetos de disputa por segmentos variados: política, indústria, comércio, relações pessoais, o que se evidencia nos campos da manipulação de dados e informações para fins de pressão política, para roubo e furto de segredos industriais, para pirataria comercial, dentre outros.

---

3 Art.12. Responsabilidade de Pessoas Colectivas. 1. Cada Parte adoptara´as medidas legislativas e outras que se revelem necessaŕias para assegurar que as pessoas colectivas possam ser consideradas responsaveis por infracc̃oẽs estabelecidas de acordo com a presente Convenc̃ao̗, quando cometidas em seu benefićio por uma pessoa singular agindo quer individualmente, quer como membro de um oŕgaõ da pessoa colectiva que exerc̃a no seu seio uma posic̃aõ de direcc̃aõ, com base no seguinte: a) Poder de representac̃aõ da pessoa colectiva; b) Autoridade para tomar decisoẽs em nome da pessoa colectiva; c) Autoridade para exercer controlo no seio da pessoa colectiva. 2. Aleḿ dos casos ja´previstos no nr. 1 deste artigo, cada Parte adoptara´as medidas necessaŕias para assegurar que uma pessoa colectiva possa ser considerada responsavel quando a ausência de supervisaõ ou de controlo por parte de uma pessoa singular, mencionada no nr. 1 tornou possivel a pratica de infracc̃oẽs previstas na presente Convenc̃aõ, em benefićio da referida pessoa colectiva por uma pessoa singular agindo sob a sua autoridade. 3. De acordo com os princípios juriḋicos da Parte, a responsabilidade de uma pessoa colectiva pode ser criminal, civil ou administrativa. 4. Essa responsabilidade deve ser determinada sem prejuiźo da responsabilidade criminal das pessoas singulares que cometeram a infracc̃aõ (MPF, CONVENÇÃO SOBRE CIBERCRIME, 2001, <http://www.mpf.mp.br>).

Nestas situações exemplificativas descritas, restam explícitos os riscos e perigos de cometimento de ilícitos de diversas ordens (civis, administrativos, penais) envolvendo os interesses e bens jurídicos acima destacados, o que reclama dos sistemas jurídicos e de justiça adequações paradigmáticas e procedimentais para tentar dar respostas curativas e preventivas eficientes aos problemas daí decorrentes.

Pensemos nas inúmeras possibilidades de anonimato que oferece a rede virtual mundial, somado as dificuldades criadas pela outorga de um mesmo endereço de *Internet Protocol* – IP (funciona como o número da carteira de identidade do equipamento utilizado para navegar na rede virtual) a mais de uma pessoa, em face do exaurimento de endereços IP. Esta situação tem feito com que alguns provedores registrem um mesmo IP para vários usuários ao mesmo tempo, com a inexorável consequência de se tornar muito difícil – quiçá impossível – identificar a posição real a partir da qual eventual conduta criminal foi posta em prática.

De igual sorte podemos imaginar as situações criadas pela utilização dos chamados *server proxy*, instrumentos que se interpõe entre o cliente e o usuário da rede, desempenhando a função de conexão do computador (local) à rede externa (Internet). Como os endereços locais do computador não são válidos para acessos externos, cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando-a para o computador. É muito comum hoje termos proxy que mascaram os verdadeiros IPs dos usuários, ou mesmo que sequestram IPs e os utilizam sem o conhecimento do real proprietário, através inclusive de vírus específicos criados para tanto, fazendo com que o número de suspeitos e investigados em determinados crimes cibernéticos possam se aproximar do infinito.

Ainda que seja possível identificar de forma segura o equipamento de informática do qual provém determinada atividade ilícita, é possível que o proprietário destes não tenha nenhuma participação no ocorrido – como nas casas de locação de serviços de internet (LAN House). E se determinado usuário destes serviços consegue burlar os sistemas de segurança, por exemplo, contra sites de pornografia infantil, e pratica crimes de tal natureza, só será possível estabelecer a autoria do delito mediante outras formas de prova que o proprietário da LAN House manter em seu estabelecimento, como câmaras de monitoramento dos usuários – as quais, por sua vez, também implicam acesso à imagem daqueles (que deve, em tese, ser autorizada, ou comunicada). Com razão, pois, Luca Lupária (2009, p. 113), ao dizer que:

> L'aspetto problematico del rapporto tra mezzi di ricerca della prova e materiale informatico risiede nella natura ontologicamente volatile e alterabile del dato digitale, su cui possono spesso incidere condotte involontarie atte ad ingenerare fenomeni di “inquinamento”, ciò che richiede la puntuale previsione di tecniche volte ad assicurare la genuinità dell'accertamento.

Por isto a importância de contarmos com marcos normativos claros e pontuais sobre estes temas, dando maior segurança tanto aos órgãos investigativos como à Sociedade, os quais terão o desafio de encontrar pontos de equilíbrio dentre os diversos interesses em jogo, dentre os quais, a exigência (até em face da natureza volátil e de difícil apreensão dos dados e informações virtuais) de que o Estado possa investigar de maneira eficiente e, por vezes, de surpresa, evitando assim os riscos de desaparecimento de provas importantes (evidencias digitais) à elucidação de problemas jurídicos; de outro, a garantia do exercício do direito de defesa por parte das pessoas físicas e jurídicas imputadas ou investigadas.

Agora, se estamos defendendo a tese da importância de termos ou criarmos ferramentas, técnicas e procedimentos de precaução/responsabilização ao cometimento de crimes - sejam eles virtuais, sejam utilizando-se de mecanismos virtuais - com maior efetividade em ambientes como estes que estamos falando, fundada em regulamentos claros, devemos nos questionar o que pode ou deve fazer o Estado enquanto eles não existirem?

Em outras palavras, a expansão incontrolada da informação e dos mecanismos de comunicação tecnológica, como o emprego difuso das redes sociais para múltiplas atividades que vão desde as relações pessoais de amizade e afetivas até as relações de trabalho, comércio, atividades acadêmicas, etc., tem imposto a constituição de gestão e análise de dados virtuais a todo tempo e por muitos setores da vida cotidiana, inclusive para os campos do Direito, no particular pelo Direito Penal e Processual Penal, eis que elementos uteis à investigação por qualquer tipo de crime praticado hoje podem ser conservados – até com esquemas de segurança e segredo imensos – em formatos digitais (estamos falando de computadores pessoais, servidores de empresas, banco de dados em nuvens, pens drives).

Por outro lado, temos inúmeras imprecisões conceituais neste novo universo de bens e produtos virtuais, o que implica deficiências de suas categorizações e compreensões. Mas com certa tranquilidade conceitual, a literatura especializada tem referido que uma definição de evidência digital para o Direito Penal e Processual Penal diz respeito a qualquer informação probatória cuja relevância processual depende dos conteúdos dos dados, ou da particular alocação sobre determinado dispositivo, ou mesmo pelo fato de ter sido transmitido por alguma modalidade informática ou telemática que esteja relacionada, direta ou indiretamente, com atividade criminosa (MARAFIOTI, 2011).

10

Outro problema/característica da investigação informática diz respeito a natureza imaterial do dados e informações com os quais se trabalha, isto é, alguns elementos buscados pelos organismos investigativos consistem em impulsos elétricos, e a impalpabilidade de fato destes confere o caráter de volatilidade, imaterialidade e fragilidade da fonte digital, basta pensarmos em um arquivo digital como imagem em formato *jpg*, compreendendo aproximadamente um milhão de bits, e no qual a mudança de apenas um bit pode implicar alteração irreversível a ponto de fazer com que o arquivo reste ilegível ou corrompido. Temos de atentar para o fato de que basta o arquivo eletrônico ter sido aberto/acessado uma vez para que já exista o risco de ele ser corrompido, assim como os metadados relativos à data do último acesso, podendo ainda ser anulada qualquer relevância probatória decorrente disto.

Daí porque tem-se dito que uma das modalidades técnicas mais confiáveis em termos de segurança na obtenção de dados e na sua preservação é aquela conhecida como *bit stream image*, ou imagem legal, porque nela se realiza certo tipo de clone do disco rígido, obtendo-se cópia analítica idêntica ao disco original – ou a qualquer outro suporte de memória, alcançando, em tese, as informações e dados contidas no espaço do *cluster*, assim como fragmentos de informações presentes no que se denomina de *slack space*, ou *unallocated space* dos *cluster*. Tais medidas seriam mais eficientes do que a mera cópia de conteúdo do *hard disk*, isto porque não se limitaria a garantir a identidade conteudística dos dados presentes nos dois suportes, mas asseguraria que cada *file* do *hard disk* clonado tenha a mesma alocação do correspondente *file* do disco de origem (NATIONAL INSTITUTE OF JUSTICE, 2008, <https://www.nij.gov/>).

Ou seja, estas características peculiares das fontes de prova digitais, e especialmente sua imaterialidade e potencial depauperamento, impõe que sejam colhidas e tratadas unicamente por pessoas/técnicos com conhecimentos específicos; que os operadores do sistema de justiça encarregados para tanto, desde um primeiro contato com os dados na flagrância dos fatos investigados ou descobertos, tomem cuidados para suas preservações integras. Nesta direção o Código de Processo Penal Italiano, em seu art. 254, ampliou a possibilidade do sequestro de correspondência, dizendo que:

> 1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato.

Mas no Brasil, como estão estas questões normativas? É o que passamos a ver.

2. Aspectos introdutórios do tratamento da criminalidade virtual no Brasil:

No Brasil o processo de regulação desta matéria ainda é lenta, até porque foi somente no ano de 1997 que o pais, através do Ministério da Ciência e Tecnologia, estabeleceu o chamado Programa para a Sociedade da Informação, que resultou na edição do Livro Verde da Sociedade da Informação, através do qual foram indicadas diversas metas com o escopo de incluir o Brasil neste contexto (PAESANI, 2007).

A partir deste tempo é que vamos começar a contar com alguns instrumentos normativos sobre a matéria, tanto em nível de direito penal material como processual, e isto já tarde, considerando que, consoante informe recente do Superior Tribunal de Justiça

> o uso cada vez mais intenso e diversificado da internet vem abrindo caminhos para a prática de novas fraudes, ou para novas formas de cometimento de velhos crimes, em casos nem sempre fáceis de enquadrar no ordenamento jurídico. O STJ tem interpretado normas infraconstitucionais em relação aos ilícitos praticados pela rede (CONJUR, 2018, [s.n.], <www.conjur.com.br>).

Este Tribunal apresenta em seu relato algumas situações exemplificativas destas questões, a saber: (1) decidiu manter preso preventivamente homem que usou a internet para obter fotos e vídeos com conteúdo erótico e depois extorquiu mulheres para não divulgar as imagens; (2) tem adotado a tese de que é ilícita a prova obtida diretamente dos dados armazenados no celular do acusado, e que são inválidas mensagens de texto, SMS e conversas, por meio de aplicativos como o WhatsApp, obtidas diretamente pela polícia no momento da prisão em flagrante, sem prévia autorização judicial - AgRg no RHC 92.801; (3) a sua Terceira Seção firmou entendimento no sentido de que a subtração de valores de conta-corrente mediante transferência eletrônica fraudulenta configura crime de furto, previsto no artigo 155, parágrafo 4º, inciso II, do Código Penal – Conflito de Competência nr.145576; (4) entendeu também a Corte que a criação de sites na internet para vender mercadorias com a intenção de nunca entregá-las é conduta que se amolda ao crime contra a economia popular, previsto no artigo 2º, inciso IX, da Lei 1.521/51 – Conflito de Competência nr.133.534; (5) nas hipóteses de ameaças feitas por redes sociais como o Facebook e aplicativos como o WhatsApp, o STJ tem decidido que o juízo competente para julgamento de pedido de medidas protetivas será aquele de onde a vítima tomou conhecimento das intimidações, por ser este o local de consumação do crime previsto no artigo 147, do Código Penal – Conflito de

12

Competência nr.156.284 (BRASIL, SUPERIOR TRIBUNAL DE JUSTIÇA, 2018, <http://www.stj.jus.br>).

O problema é que, em termos de direito material penal, a legislação brasileira tem apresentado poucos avanços, a despeito de importantes, mas podemos afirmar que desde o ano de 2006, com a edição da Lei nr.11.419/2006, que instituiu a informatização do processo judicial, o tema dos recursos virtuais para o sistema de justiça nacional veio à agenda nacional definitivamente, a despeito de que mais para o processo civil naquela quadra histórica do que para o processo penal.

Poucos anos após vamos ter algumas normas específicas se ocupando do Direito Processual Penal, envolvendo o que se convencionou chamar de *reforma* do Código de Processo Penal - CPP, com alguns dispositivos que se ocuparam de fazer uso das tecnologias virtuais para o processo, dentre as quais podemos destacar: (1) a previsão de depoimentos e interrogatório por meios de gravação magnética ou eletrônica – dentre outros já existentes – para obter maior fidelidade e celeridade na colheita de provas, conforme as disposições do art.475, do CPP, alterado pela Lei nr.11.689/2008; (2) a determinação de que, sempre que possível, os registros das partes envolvidas no processo serão feitos por gravação magnética ou digital (mais as tradicionais), nos termos do parágrafo primeiro, art.405, do CPP, alterado pela Lei nr.11.719/2008; (3) a autorização para que o juiz, se necessário em face da segurança de todos e para ter maior eficiência em termos de busca da verdade, faça a inquirição do réu por videoconferência, nos termos do art.217, do CPP, alterado pela Lei nr.11.690/2008; (4) a autorização para que juiz, excepcionalmente, realize o interrogatório do réu preso por sistema de videoconferência ou outro recurso tecnológico de transmissão de sons e imagens em tempo real, desde que tal medida seja necessária para atender finalidades especificadas no parágrafo segundo, do art.185, do CPP, alterado pela Lei nr.11.900/2009. Este mesmo artigo do CPP, em seu parágrafo quarto – alterado pela Lei referida -, autoriza que o réu possa acompanhar pelo mesmo sistema tecnológico a realização de todos os atos da audiência única de instrução e julgamento; e no seu parágrafo oitavo expande o uso destas tecnologias para outros atos processuais importantes.

Ainda poderíamos falar aqui, como querem Fiorillo e Conte, que outros avanços já podem ser sentidos diante dos instrumentos normativos que dispomos neste campo de utilização da realidade virtual para o processo penal: (a) como, na fase da investigação criminal, a possibilidade de contarmos com o chamado *boletim de ocorrência eletrônico* e do encaminhamento de *notitia criminis on line*; (b) a progressiva informatização dos inquéritos policiais (digitalização de documentos, reproduções fotográficas, autos de apreensão e

vistorias, coleta de prova testemunhal); (c) interceptação telemática (Lei nr.9.296/96); (d) digitalização de impressões do IIRGD (sistema fênix de identificação em face de registro sobre marcas do corpo, identificação timbrática da voz ou antropométrica); (e) rede de integração nacional de informações de segurança pública, justiça e fiscalização – INFOSEG; (f) peticionamentos eletrônicos com certificação digital (FIORILLO, CONTE, 2016).

E tais medidas são importantíssimas haja vista a informação do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, que dá conta do aumento do número de ataques a servidores web, tentativas de fraude eletrônica e propagação de códigos maliciosos no país nos últimos anos, sendo que em 2017 chegaram a mais de 830.000 incidentes (CERT, <htttp://www.cert.br>).

Mas nada disto é novo mesmo no Brasil, já no ano de 2006, a Polícia Federal desencadeou operação chamada de *I-Commerce*, voltada para alcançar o comércio eletrônico ilegal praticado no pais (que alcança em termos de consumidores cerca de 42% da população nacional), tendo alcançado os Estados da Bahia, Distrito Federal, Goiás, Mato Grosso do Sul, Minas Gerais, Paraíba, Pernambuco, Paraná, Rio de Janeiro, Rio Grande do Norte, Rondônia, Rio Grande do Sul, Santa Catarina e São Paulo, identificando, pelo menos, 81 pessoas (a maioria jovem, de 18 a 30 anos, pertencentes a classe média). Os cálculos são de que o prejuízo causado pela quadrilha às indústrias pode ultrapassar R$ 10 milhões (CONJUR, 2006, <www.conjur.com.br>).

Por outro lado, não temos conseguido – e muito pouco tem se feito em outros países – criar políticas de prevenção e responsabilização diante de fenômenos como os das chamadas máquinas zumbis ou botnets, computadores caseiros controlados remotamente por invasores para o cometimento de crimes sem que o proprietário da máquina se dê conta do que está acontecendo. A partir destas máquinas acessadas ilicitamente são enviados *spams*, invadem-se outros computadores e sistemas privados e públicos de dados em bancos (acesso de informações sigilosas, desvio de dinheiro, uso de cartões de créditos), empresas (pirataria industrial e comercial), setores de segurança pública (polícia, judiciário, ministério público). O problema é que a legislação material e processual para o enfrentamento adequado destas questões, no Brasil e fora, ainda é incipiente.

Conclusão

Por todas estas razões é que as respostas ao crescimento do crime organizado e do cybercrime estão a reclamar estratégias amplas e profundas, nacionais e internacionais, de

maneira integrada e cooperativa envolvendo tanto o Estado e suas forças de segurança, como o Mercado e a Sociedade, e neste sentido, os princípios chaves que têm guiado as respostas da comunidade internacional no ponto podem servir de exemplo – como a Convenção do Conselho da Europa sobre Cybercrime.

O grupo de expertos financeiros internacionais que constituem o *Financial Action Task Force – FATF*, instituído pelo G-7 no ano de 1989, tem tentado construir normativas de nível internacional para os governos e as instituições financeiras determinando o desenvolvimento de leis, regulamentações e mecanismos de execução a nível nacional visando enfrentar muitos dos crimes praticados também pela via virtual. A despeito de críticas que se tem feito ao FATF, ele seguidamente tem lançado campanhas importantes de orientação e monitoramento de situações e cenários de riscos e perigos envolvendo ações financeiras criminosas – muitas delas virtuais – não alcançadas por normativas, regulamentos e instrumentos de controle (FATF, <http://www.farf-gafi.org>).

Vários tratados bilaterais de cooperação entre países nesta área têm surtido efeitos para fins de assistência legal e troca de informações e dados que contribuem em muito para o controle e responsabilização das ações criminosas, principalmente porque ampliam o poder instrutório e probatório das investigações e processos administrativos e jurisdicionais. Tais iniciativas inclusive possibilitam convergir compatibilidades de cooperação ou criar outras que são necessárias à eficácia das medidas de enfrentamento destas ameaças (como termos sistemas jurídicos com tipos penais idênticos ou análogos e ferramentas processuais adequadas, principalmente para cooperação internacional). Na expressão de Musachhio (2002, [s.n.])

> La cooperazione internazionale è enormemente facilitata dalla convergenza delle fattispecie incriminatrici nelle giurisdizioni nazionali e transnazionali. Con l'imposizione di leggi simili in diversi paesi, i rischi che le organizzazioni criminali devono affrontare saranno maggiori. In effetti, maggior efficacia spaziale ha la legge e meno “zone franche ” sono offerte ai criminali garantendo loro, spesso, l’impunità.

Ou seja, todos os países devem investir na adequação legislativa e estrutural das instituições e parcerias que tenham como escopo o combate à criminalidade virtual, aprimorando seus métodos e ferramentas de investigação e produção da prova necessária a identificação da autoria, materialidade e culpabilidade das ações delituosas. Para além disto, outro componente estratégico importante neste campo é a associação entre Estado e setores da indústria informática, eis que atividades coordenadas entre eles poderiam dar saltos

importantes na efetivação de políticas de gestão destes problemas (mesmo sabendo-se dos riscos e, por vezes, das dificuldades que existem para tal cooperação).

Bibliografia

BECK, Urlich. *La sociedade del riesgo. Hacia una nueva modernidad*, trad. Jorge Navarro, Daniel Jimeńez y M.a Rosa Borraś, Barcelona, Paidoś, 1998.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. *Crimes pela internet, novos desafios para a jurisprudência.* Disponível em <http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/noticias/Not%C3%ADcias/Crimes-pela-internet,-novos-desafios-para-a-jurisprud%C3%AAncia>. Acesso em 18/06/2018.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Disponível em <HTTPS://WWW.CERT.BR/STATS/INCIDENTES/>. Acesso em 19/06/2018.

COMPUTERWORLD. *'Love Bug' investigation wrapping up in Philippines.* Disponível em <HTTPS://WWW.COMPUTERWORLD.COM/ARTICLE/2596151/IT-MANAGEMENT/-LOVE-BUG--INVESTIGATION-WRAPPING-UP-IN-PHILIPPINES.HTML>. Acesso em 12/12/2017.

CONJUR.. STJ divulga jurisprudência sobre conceitos de crimes pela internet. 2018. Disponível em <https://www.conjur.com.br/2018-jun-17/stj-divulga-jurisprudencia-conceitos-crimes-internet>. Acesso em 19/06/2018.

_____. *Polícia Federal faz operação contra produtos piratas na internet. 2006.* Disponível em < https://www.conjur.com.br/2006-out-16/policia_federal_faz_operacao_piratas_internet>. Acesso em 10/10/2010.

FATF, Financial Action Task Force. Disponível em <http://www.fatf-gaflorg/about/>. Acesso em
27/12/2017.

FIORILLO, Celso Antonio Pacheco. CONTE, Christiany Pegorari. *Crimes no Meio Ambiente Digital e a Sociedade da Informação.* São Paulo: Saraiva, 2016.

GAZETA DO POVO. *Lavagem de dinheiro desafia o tradicional sigilo no mercado de arte.* Disponível em <HTTP://WWW.GAZETADOPOVO.COM.BR/VIDA-E-CIDADANIA/LAVAGEM-DE-DINHEIRO-DESAFIA-O-TRADICIONAL-SIGILO-NO-MERCADO-DE-ARTE-72KA19PCNHVTI8T5OO5V9UB8B>. Acesso em 12/12/2017.

G1. *Polícia realiza terceira fase de operação contra grupo que fazia leilões virtuais de carros roubados no RS.* Disponível em <HTTPS://G1.GLOBO.COM/RS/RIO-GRANDE-DO-SUL/NOTICIA/POLICIA-REALIZA-TERCEIRA-FASE-DE-OPERACAO-CONTRA-GRUPO-QUE-FAZIA-LEILOES-VIRTUAIS-DE-CARROS-ROUBADOS-NO-RS.GHTML, acesso em 12/12/2017.

16

HUNTER, Dan and LASTOWKA, Gregory. *Virtual Crimes*. In http://www.nyls.edu/institute_for_information_law_and_policy/wp-content/uploads/sites/139/2013/08/lastowka.pdf, acesso em 18/04/2018.

LUPÁRIA, Luca. *Computer crimes e procedimento penale.* In GARUTI, Giulio. Modelli differenziati di accertamento. Roma: Utet, 2009.

MARAFIOTI, Luca. *Digital evidence e processo penale.* In Rivista Cassazione Penale, Volume: 51, fascicolo 12, 2011.

MINISTÉRIO PÚBLICO FEDERAL. *CONVENÇÃO SOBRE CIBERCRIME, 2001*. Disponível em <HTTP://WWW.MPF.MP.BR/ATUACAO-TEMATICA/SCI/NORMAS-E-LEGISLACAO/LEGISLACAO/LEGISLACOES-PERTINENTES-DO-BRASIL/DOCS_LEGISLACAO/CONVENCAO_CIBERCRIME.PDF>. Acesso em 20/03/2018.

MUSACCHIO, Vincenzo. *Criminalità organizzata e cybercrime*. In https://www.diritto.it/osservatori/scienze_criminali/dottrina/musacchio3.html, acesso em 28/11/2017.

NATIONAL INSTITUTE OF JUSTICE. *Digital evidence in the courtroom: A guide for law enforcement and prosecutors*.2008. Disponível em <https://www.nij.gov/>. Acesso em 28/11/2017.

PAESANI, Liliana Minardi. Sociedade da Informação e seu lineamento jurídico. O direito na Sociedade da Informação. São Paulo: Atlas, 2007.

PUCCIO-DEN, Deborah. *The Sicilian Mafia: transformation to a global evil*. In Etnográfica - Revista do Centro em Rede de Investigação em Antropologia, Vol.12, 2, 2008. Acesso pelo site https://etnografica.revues.org/1763, em 28/11/2017.

ROTH, Monika. *Money Laundering and the Art Market*. In http://www.roth-schwarz-roth.ch/images/Jusletter_money-laundering-and_bd85361006_de.pdf, acesso em 18/03/2018.

SHIMABUKURO, Adriana. SILVA, Melissa Garcia Blagitz de Abreu. *Internet, Deep Web e Dark Web.* In SILVA, Ângelo Roberto Ilha da. (org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado, 2018.

USA. FBI. Disponível em <HTTPS://WWW.FBI.GOV/INVESTIGATE/CYBER> Acesso em 21/11/2017.