São Paulo, Brazil
November 4-5, 2019

The Eleventh International Conference on
FORENSIC COMPUTER SCIENCE and CYBER LAW

www.ICoFCS.org

DOI: 10.5769/C2019004 or http://dx.doi.org/10.5769/C2019004

Cibercrime como Crime Permanente

Felipe Otávio Moraes Alves[1]

(1) Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP), E-mail: felipeotavioma@gmail.com.

Resumo: Hodiernamente, a internet intermedia incontáveis condutas criminosas, carecendo de manutenção do Código Penal e Processual Penal para readequarem-se a esta tecnologia. Uma interpretação extensiva das normas pode ser suficiente à devida incidência cível e criminal sobre os cibercrimes, destoante ao notório positivismo jurídico vigente. O desprovimento de remediações diretas e suficientemente rápidas ao usuário é o principal problema, replicando a ineficácia dos aparatos investigativos em alcançar o devido combate dos cibercrimes por obra, em grande parte, da morosidade de mandados judiciais. Pela conduta do sujeito ativo dos delitos virtuais ser, via de regra, indireta, anônima e permanente, os efeitos são majoritariamente mais expressivos que um delito perpetrado no mundo real. Assim, o presente estudo contextualizou o atual panorama da internet, perscrutou a tutela jurídica atual do cibercrimes – com as singularidades jurídicas deste meio digital – e problematizou a inclusão, na previsão de flagrante em infrações permanentes, dos crimes cibernéticos cuja consumação se estendam no tempo. Ademais, questionou a necessidade de mandado judicial na Busca e Apreensão dos aparatos de cibercriminosos em flagrante delito. As considerações finais perquiriram concluir esta incidência como legítima e potencialmente eficaz a fim de proteger o usuário. Foi adotado, como método de procedimento, a pesquisa bibliográfica, legislativa e jurisprudencial e, como método de abordagem, o teórico-dedutivo.

Palavras-Chave: Cibercrime, Crime Permanente, Internet, Mandado Judicial, Direitos Fundamentais.

1. Introdução

O termo "cibercrime" surgiu no final da década de 90 por um subgrupo das nações do G8 formado após encontro em Lyon, na França, ao analisar a criminalidade via internet. Por exemplo, o cibercrime acontece entre pessoas físicas, quando um usuário pratica hackeamento ou ofende a integridade moral doutro; entre pessoas jurídicas, quando vítimas de difamação; entre pessoa jurídica e pessoa física, quando a primeira extrapola o contrato digital ou, em geral, os direitos de privacidade do usuário; e Estado e pessoas jurídicas ou físicas, quando os segundos invadem ilegalmente sistemas estatais. Em âmbito nacional, raramente se considera um ato primariamente do Estado como cibercrime.

Isto posto, como objetivo, o trabalho questionará o tratamento jurídico tradicional, dado aos crimes cibernéticos, com morosos e escassos combates. Para isto, partirá da comprovação de que o Estado tem legitimidade e imprescindibilidade na tutela da Internet e da constatação, da premissa menor, de que os cibercrimes são carentes de melhores aparos normativos e políticas públicas, concluindo pela possibilidade da correlação entre cibercrime e crime permanente. Neste contexto, há duas

hipóteses cabíveis, manter a condição atual com as tipificações já existentes numa perspectiva jurídico-econômica liberal ou implementar medidas públicas que auxiliem no processo investigativo, representado pelo Inquérito Policial. O presente trabalho se dedicará a esta última, problematizando a adaptação do flagrante à realidade da internet – garantindo soluções práticas à perpetuidade do conteúdo e perecividade das provas – ao incluir, dentro da previsão da prisão em flagrante em infrações permanentes, os crimes cibernéticos.[1]

Para a construção do estudo, é adotado o método teórico-dedutivo. As perguntas abordadas durante o trabalho são elucidadas com apoio de doutrinadores e especialistas na área penal e digital, com comparações por doutrina, jurisprudência e legislação, inclusive internacional. O referencial teórico, tocante ao crime permanente, é o de Guilherme de Souza Nucci.

2. Panorama da Realidade Cibernética

No artigo 5º do Marco Civil da Internet, há a definição terminológica e conceitual da internet como "o sistema constituído de conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes". Objetivamente, a internet é o conjunto de recursos tecnológicos, *hardwares* (como os servidores, *modems*, roteadores etc.) e *softwares* (*browser*/navegadores, aplicativos, *plug-ins* etc.) interconectados por meios de comunicação (linha telefônica, fibra ótica, satélite, redes locais etc.) que associam vários serviços mediante, principalmente, de página de *websites*.

E nesse contexto, a Blue Coat Systems e a Elastica [1] avaliaram, no Brasil, o comportamento de grandes e médias empresas, apurando que, em média, as empresas têm 110 categorias de aplicativos *shadow*, aplicações que estão sendo utilizadas dentro das companhias sem o conhecimento das áreas de TI. Através desses aplicativos, informações sigilosas dos negócios são compartilhadas com outros funcionários ou publicamente, evidenciando uma carência generalizada de capacitação dos empregados. De acordo com Norton Cyber Security [2], em 4 anos o número só aumentou: a cada 13 segundos, um brasileiro foi vítima da tentativa de fraude com informações furtadas da internet, sendo 28 milhões de brasileiros já atingidos. Ameaças e cibercrimes custam cerca de R$ 16 bilhões de reais anualmente ao país.

De acordo com Zaharia [3], há, em média, um lapso temporal de 170 dias da infecção para se detectá-lo. No ano de 2015, por exemplo, aduziu que a cada 100 tentativas infecção, mais de 82% ocorreram *offline*.[2] Com efeito, por querer economizar, o usuário se expõe, poluindo seu próprio *hardware*. Ainda, 68% dos arquivos perdidos resultantes de ciberataques são declarados irrecuperáveis, um dado interessante para a associação do crime digital como crime permanente. Porém, o dado com o maior número de conteúdo prejudicial é o dos *spams*. Estima-se um total de 28 bilhões de *spams* enviados por e-mails por dia. Ainda, de acordo com a Symantec [4], meio bilhão de informações pessoais foram roubadas ou perdidas em 2015.

Empresas em escala global não acompanham os avanços e demandas do mercado. Assim como em 2014 [5], as 10 principais vulnerabilidades exploradas em 2015 eram conhecidas há mais de um ano, com 68% tendo sido reportadas há três anos ou mais. Ou seja, não é pela falta de conhecimento do problema e sim pela incapacitação e desinteresse dos provedores. Além disso, há meios para utilizar vias ilícitas já

[1] Isto é, cibercrimes cuja consumação se estendam no tempo pela permanência da publicação original em determinado sítio eletrônico ou pela disseminação e replicação do conteúdo delituoso na rede mundial de computadores, ainda que haja exclusão, posterior ao flagrante, do conteúdo. Ou seja, tratar-se-ia de praticamente todos cibercrimes já que permanentemente offline, são raros os casos.

[2] A infecção é *offline*; já a transmissão dos dados ao cibercriminoso, é *online*.

corrigidas. Os *hackers* e *malwares* se movem rapidamente; já as defesas, não. Na lógica de mercado, notadamente, a omissão dessas informações de segurança procede da demanda ao máximo lucro, atropelando direitos dos consumidores. Por exemplo, costumeiramente, provedores omitem a notificação aos clientes quando são hackeados, violando o dever de informar e a boa-fé objetiva. A insuficiência empresarial não é um fenômeno momentaneamente epidêmico, persistindo pelas características intrínsecas de mercado e das particularidades da internet.

Nesta circunstância, os cibercriminosos progridem, com pretensões bem definidas como o de ganhos financeiros. De acordo com dados da Symantec [6], TrendMicro [7] e SecureWorks [8], existe uma tabela de preços de informações no mercado negro na *deep web*, dependendo do vendedor e de sua credibilidade: US$ 0,5 a US$ 20,00 por detalhes do cartão de crédito; US$ 70 a 150 dólares, por 1 milhão de *spams*; US$ 300 dólares ou menos, conta de banco com US$ 70.000,00 a US$ 150.000,00 etc. A operação Sheik é um exemplo de combate. Três pessoas foram detidas em Goiás, pelo acesso a mais de quatro mil contas bancárias, movimentando indevidamente cerca de R$ 2 milhões. A PF participou, em parceria com o FBI e a Europol, de outra operação, a Darkode, que resultou na prisão de outros dois *hackers*, acusados de terem movimentado mais de R$ 1 milhão pela venda de dados bancários roubados. E em diversos países, a operação prendeu cerca de setenta cibercriminosos. Logo, há, teoricamente, a possibilidade de coordenação conjunta de Estados diferentes, porém são tão esparsas, morosas e pontuais que são objetivamente eficazes, mas irrelevantes no cenário global.

3. Tutela Jurídica da Internet

Mundialmente, o principal e único instrumento jurídico significativo o qual possui regras gerais e específicas para tutelar cibercrimes é a Convenção de Budapeste (2001) [9], com normas majoritariamente de Direito Penal Material. Os principais destaques da Convenção sobre os Cibercrimes são as definições de: cibercrimes (Capítulo I), tipificando-os como infrações contra sistemas e dados informáticos (Capítulo II, Título 1); infrações relacionadas com computadores (Capítulo II, Título 2); infrações relacionadas com o conteúdo, como a pornografia infantil (Capítulo II, Título 3); e, também, infrações relacionadas com a violação de direitos autorais (Capítulo II, Título 4). Jurisdição e integração internacional são vistas no artigo 22, o qual aponta quando e como uma infração é cometida, além de recomendar aos seus aderidos a "jurisdição mais apropriada para o procedimento legal". Consoante ao relativismo e flexibilidade da Convenção, o Brasil não adere às suas diretrizes pois não fora um dos signatários originais do tratado, podendo somente ser convidado pelo Comitê de Ministros do Conselho Europeu.

Nesta lógica, o Estado cumpre o papel de consolidador dos direitos básicos da sociedade, desagregando a noção de "Estado-árbitro", como monopólio da sanção e imposição do cumprimento do ordenamento, do "Estado produtivo", fornecedor dos bens públicos. Um "Estado Mínimo" teria uma única função de proteger os direitos individuais contra qualquer forma de violação dos mesmos. Surgindo, assim, novos limites constitucionais consoante à atual crise do "Estado Assistencial" ou do bem-estar social [10]. As motivações para a obediência às normas estatais não são autossuficientes, sendo somente explicativas. Afinal, a justificação não supera o paradoxo da legitimidade do Estado estar em normas e diretrizes jurídicas fundamentais propostas pelo mesmo. A justificativa incorre, portanto, pela prática, com resultados e consequências. E são estas consequências observadas, principalmente, pelos liberais. Como escreve Offe [11], quanto mais a política se fizer concreta, mais multiplicarão os conflitos e os efeitos da polarização. Estará, assim, declarado o caminho à crise política, devido à incapacidade de coordenar satisfatoriamente todos os interesses do complexo social ao mesmo tempo.

Os sistemas políticos democrático-liberais demonstrariam sua superioridade assegurando um máximo de eficiência econômica, justiça social e liberdade individual. A tendência do liberalismo contemporâneo é demonstrar a incapacidade do

Estado burocráticos em dirimir as mazelas sociais, pelo fatal desvio das organizações de funções prefixadas e pelo paradoxo intrínseco entre a lógica das máquinas burocráticas e a lógica da participação. Logo, esse liberalismo anti-utilitarista acredita que a resposta aos paradigmas da justiça e da segurança social está ao nível da sociedade civil e não do instituto estatal, mediante subsistemas autônomos do sistema político, com iniciativas independentes e convergentes, realizadas por forças sociais espontâneas. Mesmo diante do pensamento mais liberal, compete ao Estado apenas a tarefa de garantir para todos a lei ordinária, sendo um órgão equilibrador e incentivador de iniciativas autônomas da sociedade civil. Esta é a lógica pela qual o liberalismo é regido e doutrinado [12].

A chamada desregulação, eventualmente proposta em um determinado setor de atividades, não significa a extinção da regulação, mas a subtração de uma dimensão da regulação estatal. Assim, o argumento por detrás da desregulação não poderá ser que o setor funcionaria melhor sem intervenção estatal [13]. Em suma, como deduzido, notórios são os problemas jurídicos na internet, um ambiente minimamente liberal. Válido é lembrar que estruturas jurídico-normativas influenciam as lógicas de mercado, mesmo que indiretamente. Destarte, a regulação é necessidade imperiosa da constatação de que o próprio Direito e a sociedade criaram entes que desequilibram as relações humanas de acumulação de capital, técnicas e vantagens competitivas [14].

O afastamento do Estado de tal regulação só se justifica caso comprovada sua inatividade no direcionamento deste setor regulado, rumo à compensação social, resultando "em maior eficácia dos direitos fundamentais envolvidos". O exemplo da internet é evidência da insuficiência do mercado como um ente vivo inteligente e eficiente, em vez de entendê-lo como um produto da atuação regulatória, ou seja, de atuação político-jurídica capaz de formatá-lo em benefício geral de todos direitos fundamentais. Se não fosse uma atuação governamental ativa, mesmo que ínfima, o mercado teria "enterrado" a internet [15].

Mesmo quando inexistem legislações específicas, cabe ao jurista enfrentar os novos problemas que, em parte, são "velhos temas com novas roupagens", mormente a responsabilidade civil e legislação complementar vigente [16]. Alguns cibercrimes utilizam técnicas distintas, pelas particularidades do meio digital, dos delitos tutelados pelo ordenamento jurídico-penal brasileiro, mas o fim que se pretende é o mesmo da conduta já tipificada, ou seja, são crimes relativos. É neste contexto que, em 2014, surge o Marco Civil da Internet (MCI), oficialmente chamada de Lei n.º 12.965, de 23 de abril de 2014. É a principal lei que trata o uso da internet no Brasil, através de princípios e garantias, direitos e deveres para quem usa a rede, bem como algumas diretrizes para a atuação do Estado, substancialmente semelhante à citada Convenção sobre o Cibercrime. Contudo, seu maior enfoque fora com os provedores de serviços da internet e suas responsabilidades *lato sensu*. O texto da lei trata de temas como neutralidade da rede, privacidade, retenção de dados, a função social da rede, a garantia da liberdade de expressão e da transmissão de conhecimento. Também trata, através do *caput* do art. 17, da obtenção de dados pessoais pelo Estado, referentes aos registros de conexões e de acesso de provedores de internet, que é condicionada a uma prévia decisão judicial devidamente fundamentada, já que esses dados podem servir para compor conjunto probatório em ações. Um dos assuntos mais importantes são as aparições de decisões judiciais condenando os provedores, por ação ou omissão, pelo conteúdo ilícito publicado pelos usuários. Os provedores de conteúdo alegam que não dispõem de meios técnicos e humanos para fiscalizarem previamente todo o ambiente virtual. Afinal, há uma responsabilidade dos provedores de conteúdo e também na proteção e guarda de dados, outro problema fático para a apuração do ordenamento.

Mesmo com o Marco Civil, não existe uma legislação que abarque a totalidade dos crimes cibernéticos[3] a fim de resolvê-los e contribuir na investigação policial dos litígios digitais.

[3] A título de exemplo, o cibercrime acontece entre pessoas físicas, quando um usuário pratica hackeamento ou ofende a integridade moral doutro; entre pessoas jurídicas, quando vítimas de difamação;

Notadamente, podemos extrair os seguintes ordenamentos jurídicos os quais tratam de alguns dos tipos de cibercrimes, são eles: Lei n.º 12.965/2014: o Marco Civil da Internet; Lei n.º 12.737/2012: Lei Carolina Dieckmann; Código Penal: crime de ameaça (art. 147), divulgação de segredo (art. 153), violação do segredo profissional (art. 154), extorsão (art. 158), extorsão Indireta (art. 160), dano (art. 163), apropriação indébita (art. 168), estelionato (art. 171), violação de direito autoral (art. 184), escárnio por motivo de religião (art. 208), favorecimento da prostituição (art. 228), ato obsceno (art. 233), escrito ou objeto obsceno (art. 234), incitação ao crime (art. 286), apologia de crime ou criminoso (art. 287), falsa identidade (art. 307), exercício arbitrário das próprias razões (art. 345), dentre outros; Lei n.º 8.069/1990: pedofilia (art. 241); Lei n.º 7.716/1989: crime de divulgação do nazismo (art. 20, §2º); Constituição Federal: Artigo 5º, incisos IV, V, X, XII, XIV; Código Civil: arts. 186, 187, 205, 206, 212, 225, 927, parágrafo único, 932, inciso III, 1016; Código de Processo Civil: arts. 332 e 333; Código de Processo Penal: arts. 156, 157 e 239; Lei n.º 9296/1996: Lei de Interceptação, arts. 1º, 3º, 9º e 10º; CLT: arts. 482, alíneas b, g, h; Lei n.º 6.404/1976: Lei das Sociedades Anônimas, arts. 153, 154, 155, 157, 158 e 159; Lei n.º 7.716/1989: Lei de Racismo etc.

Leonardi [17] trata do modelo geral de regulação de Lawrence Lessig, subdividindo-o em quatro modalidades de regulação: o direito – o ordenamento nem sempre é a maneira mais eficaz de compensação da vítima, as normas sociais – regulam tão somente o comportamento na rede e não possuem regras estabelecidas, o mercado – regula também o comportamento na rede através da cobrança dos serviços prestados, e a arquitetura – sua modificação para proteger determinado direito. Essas quatro modalidades de regulação interagem entre si, imutabilizando o direito diante da hiperdinâmica internet.

4. Singularidades Jurídicas da Internet

As singularidades da internet intervêm na regulamentação da internet e das políticas públicas, sendo cruciais ao justificar a diferenciação da internet ao ponto da carência de tutela específica. Observar-se-á, por consequência, certa inaplicabilidade de noções doutrinárias penais ou civis à luz da desconsideração, *a priori*, da matriz paradigmática da realidade virtual.

A característica basilar para uma regulamentação da internet é a dificuldade de identificação pelo anonimato dos usuários. Hodiernamente, há ínfimas possibilidades de identificação de cibercriminosos através da própria rede, pela dissociação de sua identidade, localização e comportamento pelo seu *Internet Protocol*, além de entraves legais e indisposição empresarial na investigação. Inobstante, é a Polícia Federal que pericia majoritariamente os casos, para milhares no ordenamento jurídico. Empresas privadas raramente identificam o usuário, tampouco cooperam em investigações e, muito menos, os denunciam ou sancionam. Como pontifica Leonardi [18], “se não há uma maneira de saber quem alguém é, onde ele está, nem o que fez ou está fazendo, o sistema jurídico – que é dependente dessas informações para exercer sua força coercitiva – parece perder sua efetividade”. O anonimato na rede torna cibercriminosos mais suscetíveis a praticar violações da privacidade. Esta consequência psicológica, de violações dos direitos alheios pela dificuldade de identificação do usuário, foi denominada por Drummond [19] de esquizofrenia cibernética.

A segunda característica é a irreversibilidade espaço-temporal, já que a violação da honra e da privacidade na internet tornam-se irreversíveis visto que as informações ficam permanentemente lá gravadas e alcançam inúmeros cidadãos. Há exceções, *verbi gratia*, o uso inapropriado de

entre pessoa jurídica e pessoa física, quando a primeira extrapola o contrato digital ou, em geral, os direitos de privacidade do usuário; e entre Estado e pessoas jurídicas ou físicas, quando os segundos invadem ilegalmente sistemas estatais. Em âmbito nacional, raramente se considera um ato primariamente estatal como cibercrime.

marca extinguido pela remoção da empresa plagiadora. Todavia, em redes sociais e ações cibercriminosas, a irreversibilidade é plenamente identificável. Qualquer ato é registrado e mesmo com remoção conteúdo, há a possibilidade de salvamento do conteúdo em algum hardware inacessível, permanecendo no servidor do provedor, além da incontável reprodução do mesmo. Essa particularidade torna perigosa a introdução dos atos ilícitos ou dos dados pessoais na internet, pois, após divulgada, a informação foge do controle de quem a publicou, ou seja, o dano causado pela violação da privacidade é imensuravelmente mais perigoso no ciberespaço.

A terceira característica é a permanência eterna da informação e do dano, pois uma vez inserida no mundo virtual, ela lá permanecerá até que alguém a retire. Deriva-se da Irreversibilidade Espaço-Temporal com consequências jurídicas mais específicas. Diferindo a informação virtual da produzida no mundo real pois neste a notícia acaba por desaparecer com o decurso do tempo, visto que os meios materiais de reprodução (revistas, jornais, livros, etc.) perdem sua atualidade. Na internet, devido à facilidade de acesso informativo e à virtualidade da rede, as informações tornam-se eternas. Para tanto, a violação de direitos na internet deveria ser tratada com mais severidade e celeridade. Esta singularidade restringe *lato sensu* a própria liberdade de expressão, pois os usuários, receosos das consequências eternas da rede, limitar-se-ão em comunicar no ciberespaço.

A quarta característica são os multiníves de responsabilidades. Há vários tipos de provedores, os prestadores de serviços na internet. São eles que fornecem ao usuário o acesso à internet, concedem a outros prestadores a plataforma necessária, garantem a armazenagem de mensagens e informações etc. As espécies de provedores se diferem de acordo com os tipos de serviços prestados, sendo eles os provedores de *backbone*, acesso, hospedagem, conteúdo, informação e correio eletrônico. Tendo o fornecedor cumprido com seus deveres, em casos de dano, verifica-se cada caso a fim de decidir pela incidência do dever de reparar, objetiva ou subjetivamente.

A perecibilidade das provas contra cibercriminosos é a quinta característica. As possíveis provas contra cibercriminosos são submetidas a mecanismos de criptografia pelo próprio e que, habitualmente, só podem ser averiguadas quando o equipamento está ligado, capaz de sofrer pequenas alterações e, logo, perda de provas cruciais. São necessários pouquíssimos segundos para que o cibercriminoso possa apagar todos seus rastros digitais ou submetê-los a rigorosos mecanismos de criptografia. Por isso, uma perícia rápida se faz mister.

E a última é a internacionalização das condutas. Os casos de litígios transnacionais englobando pessoas, físicas e jurídicas, de diferentes países ou de múltiplas jurisdições são bastante frequentes. Neste âmbito, houve o emblemático caso Garcia vs. Panasonic, em que o autor ganhou a ação pela aplicação do artigo 12 do CDC, com uma interpretação menos restritiva, conjugado com a teoria do risco e a chamada “teoria da integração” porque ‘‘as grandes corporações perderam a marca da nacionalidade para tornarem-se empresas mundiais’’ e se a globalização beneficiava a Panasonic, deveria, em contrapartida, também beneficiar o consumidor.[4] Em suma, era uma empresa grande

[4] DIREITO DO CONSUMIDOR. FILMADORA ADQUIRIDA NO EXTERIOR. DEFEITO DA MERCADORIA. RESPONSABILIDADE DA EMPRESA NACIONAL DA MESMA MARCA ("PANASONIC"). ECONOMIA GLOBALIZADA. PROPAGANDA. PROTEÇÃO AO CONSUMIDOR. PECULIARIDADES DA ESPÉCIE. SITUAÇÕES A PONDERAR NOS CASOS CONCRETOS. NULIDADE DO ACÓRDÃO ESTADUAL REJEITADA, PORQUE SUFICIENTEMENTE FUNDAMENTADO. RECURSO CONHECIDO E PROVIDO NO MÉRITO, POR MAIORIA. I - Se a economia globalizada não mais tem fronteiras rígidas e estimula e favorece a livre concorrência, imprescindível que as leis de proteção ao consumidor ganhem maior expressão em sua exegese, na busca do equilíbrio que deve reger as relações jurídicas, dimensionando-se, inclusive, o fator risco, inerente à competitividade do comércio e dos negócios mercantis, sobretudo quando em escala internacional, em que presentes empresas poderosas, multinacionais, com filiais em vários países, sem falar nas vendas hoje efetuadas pelo processo tecnológico

contendo a venda dos dois produtos em ambos países, um caso bastante específico. Inobstante, a maioria dos casos permanece sem solução: empresas com sede em um só país, comercialização por exportação/importação, compra e venda de produtos em outros países, disponibilização do produto num só país etc. Ademais, há a interação entre pessoas físicas de países distintos com litigâncias penais ou cíveis. Hoje, usuários podem difamar e discriminar cidadãos de outros países sem sansão legal, elucidando a seriedade deste problema, tampouco incidindo responsabilidades trabalhistas, ambientais, tributárias etc. Tal peculiaridade esclarece, até mesmo, a crise do conceito de cidadania e o fim do Estado-Nação [20]. Como solução, utopicamente, Marcelo Neves [21] leciona sobre as "aldeias jurídicas globais", uma *lex digitalis*, englobadas estruturalmente com sistemas mundiais através de Constituições civis [22].

5. Cibercrime como Crime Permanente

Consoante ao Código Penal, crime permanente é aquele de momento consumativo estendido temporalmente por domínio do criminoso acerca do momento de consumação do crime. *V.g*., o crime de possuir pornografia infantil tem caráter permanente, assim como o crime de lavagem de dinheiro por empresas. O grande benefício para a construção do Inquérito Policial desse tipo penal é a possibilidade da prisão em flagrante.[5] Renato Lima [23], doutrina que crimes plurilocais são aqueles de cunho penal com ação e resultado ocorrendo em locais diferentes. E crimes à distância são infrações penais as quais acontecem dentro do Brasil, mas o resultado se materializa no estrangeiro ou vice-versa. Para tanto, a determinação da competência prevista no artigo 70 do CPP, em caso de crime permanente, estará firmada pela prevenção, pelo art. 71 [24].

O crime permanente tem momento consumativo que se prolonga no tempo, a consumação continua ocorrendo enquanto perdurar o delito, como ao portar conteúdo digital ilícito, manter conteúdo postado em rede sem permissão dos envolvidos, privar alguém de seu direito de liberdade e privacidade ou ocultar conteúdo protegido por força de lei. Nisto, Guilherme Nucci [25] pondera que:

> Para identificação do crime permanente, oferece a doutrina duas regras: a) o bem jurídico afetado é imaterial (ex. saúde pública, liberdade individual etc.); b) normalmente é realizado em duas fases, a primeira, comissiva, e a segunda, omissiva (sequestra-se a pessoa através de uma ação, mantendo-a no cativeiro por omissão). Essas regras não são absolutas, comportando exceções.

Para o autor supramencionado, crimes permanentes seriam "aqueles que se consumam com uma única conduta, embora a situação antijurídica gerada se prolongue no tempo até quando queira o agente" [26]. Para Damásio Jesus [27], os crimes permanentes "são os que causam uma situação danosa ou perigosa que se prolonga no tempo. O momento consumativo se protrai no tempo, como diz a doutrina". Já para o professor Cézar Bitencourt [28], o "crime

da informática e no forte mercado consumidor que representa o nosso País. II - O mercado consumidor, não há como negar, vê-se hoje "bombardeado" diuturnamente por intensa e hábil propaganda, a induzir a aquisição de produtos, notadamente os sofisticados de procedência estrangeira, levando em linha de conta diversos fatores, dentre os quais, e com relevo, a respeitabilidade da marca. III - Se empresas nacionais se beneficiam de marcas mundialmente conhecidas, incumbe-lhes responder também pelas deficiências dos produtos que anunciam e comercializam, não sendo razoável destinar-se ao consumidor as consequências negativas dos negócios envolvendo objetos defeituosos. IV - Impõe-se, no entanto, nos casos concretos, ponderar as situações existentes. V - Rejeita-se a nulidade arguida quando sem lastro na lei ou nos autos (STJ - REsp: 63981 SP 1995/0018349-8, Relator: Ministro ALDIR PASSARINHO JUNIOR, Data de Julgamento: 11/04/2000, T4 - QUARTA TURMA, Data de Publicação: DJ 20.11.2000, "JusBrasil", 2000)

[5] Pelas características singulares da internet e alcance da conduta criminosa inclusive em nível internacional, ocorre a incidência pois, majoritariamente, é um crime plurilocal e à distância.

permanente é aquele crime cuja consumação se alonga no tempo, dependente da atividade do agente, que poderá cessar quando este quiser (cárcere privado e sequestro)".

Nesta interpretação, induz-se a possibilidade de incidência do cibercrime como crime permanente, principalmente em relação aos crimes puros. O bem jurídico, na maioria das vezes, será algum bem imaterial da pessoa, ferirá sua liberdade e majoritariamente sua privacidade. Outrossim, há também as duas fases, o crime se consolida através da ação do cibercriminoso – por exemplo, quando o sujeito ativo do delito virtual divulga e mantém conteúdo ilícito – e, em momento posterior, há a atuação permanente e ilícita pelo fulcro virtual até eventual descobrimento tardio da invasão ou extração de benefícios, como o vazamento de conteúdo privado.

A base conceitual do crime permanente é a execução do fato típico e não, simplesmente, sua consumação, pois nos crimes instantâneos de efeitos permanentes – como ensina a doutrina – a consumação também se prolonga no tempo. Ora, os crimes permanentes são aqueles que, quando consumados, sua execução é realizada permanentemente pela vontade do agente ativo, no caso o hacker ou uma empresa que invade privacidades ilicitamente, como se fosse um ciclo de novas condutas com novos resultados, chegando a novas consumações, de forma contínua. A distinção é importante pois haveria discussões acerca da aplicação da súmula 711 do Supremo Tribunal Federal, de aplicação da lei penal mais grave sobre o crime permanente.

Nesta mesma lógica, há o Projeto de Lei nº 5.463 de 2016 que visa acrescentar aos § 1º e 2º do art. 303 do CPP o denominado "flagrante digital", estabelecendo como infração permanente o delito cibernético de conteúdo permanente na internet [29]:

> § 1º. Considera-se, também, como infração permanente o crime cibernético cujo conteúdo permaneça na internet, ainda que excluída a publicação original, mas, em razão de sua disseminação ou de qualquer outro motivo determinante, tenha havido a replicação e a permanência do conteúdo delituoso na rede mundial de computadores.
> § 2º Entende-se o agente em flagrante delito enquanto houver a permanência do conteúdo delituoso na internet, nos termos do parágrafo anterior.

O deputado Roberto Alves, autor do referido projeto de lei, fê-lo a fim de combater a disseminação da violência em redes pelo compartilhamento de vídeos íntimos, após sensibilizar-se com o caso de uma menor de 16 anos cujas imagens de violência sexual foram transmitidas em redes sociais. Esta incidência do flagrante, supostamente, deve alertar usuários a terem mais cuidado com o compartilhamento de conteúdo, bastando a evidência de que o mesmo esteja disponível na internet. Consequentemente, coibir-se-ia praticamente todos cibercrimes.

6. Busca e Apreensão sem Mandado Judicial

Com a aprovação do Marco Civil, a necessidade de ordem judicial foi incluída no ordenamento. O MCI trouxe uma regra específica acerca da necessidade de ordem judicial para o Estado obter quaisquer tipos de informações privadas e o usuário ter conteúdo ofensivo retirado**:**

> Art. 7º. O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> (…) II – inviolabilidade e sigilo do fluxo de suas comunicações pela Internet, salvo por ordem judicial, na forma da lei;
> III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Mas qual a relevância jurídica da incidência de cibercrime como crime permanente? A Busca e Apreensão sem este mandado judicial é possível em flagrante permanente pela preocupação jurídica de cessá-lo imediatamente, engendrando um acometimento mais célere. Nesse caso, não se pode falar em ilicitude das provas obtidas porque o momento consumativo do delito está sempre em execução. O flagrante digital realizar-se-ia, assim, quando se descobrisse, por

investigação, a localização do suspeito pela identificação da localidade de perpetração do crime, bastando a evidência de que o conteúdo ou a ação delituosa ainda esteja disponível e em continuidade, de alguma forma, na internet. Logo, asseguraria suas vítimas em detrimento de certas garantias jurídicas do acusado. Ora, trata-se da mesma lógica dos cibercrimes, o momento consumativo da ilicitude de *hacking* ou divulgação de conteúdo indevido também está em contínua execução.

Tratando das ressalvas dessa possibilidade, em 2015, a decisão do STF no RE 603.616 discutiu se e quando policiais podem adentrar domicílios sem mandado judicial com o fito de buscar e apreender droga. Em síntese, o STF estabeleceu que o ingresso forçado em domicílios sem mandado judicial é apenas legítimo quando amparar-se em razões devidamente justificadas pelas circunstâncias indicadoras que no interior da residência esteja a ocorrer situação de flagrante delito. A ilicitude do ingresso forçado na esfera domiciliar tem sido afastada pelo fato de que o tráfico de drogas (ou a posse de arma) configuram crime permanente, no indício do estado de flagrância. A princípio, estas razões devidamente justificadas têm de ser legitimamente constatadas. Por não enxergar esses requisitos no HC 138.565 em 2017, a 2ª Turma do Supremo Tribunal Federal concedeu *Habeas Corpus* para trancar a ação penal contra um homem que teve sua residência vasculhada por policiais civis sem ordem da Justiça, encontrando drogas na residência. Ou seja, é uma incidência de flagrante a ser aplicada com a devida diligência.

A expressão ambígua que autoriza a realização do ato, qual seja, as “fundadas razões”, oferece à autoridade judicial certa discricionariedade e subjetividade. Entende-se, contudo, que para o seu deferimento, deverão estar presentes a urgência, necessidade e “fortes indícios da existência de elementos de convicção” devidamente interligado ao processo legal a que a busca subordina, não sendo suficiente a simples suspeita como bem aduz Pitombo [30].

Jéssica Picolo [31] bem elenca outras características juridicamente relevantes do meio cibernético: a transnacionalidade, a deslocalização e a repetição automática. Esta a última é importante para julgarmos ser essa característica que torna o ato criminoso pela internet permanente, pois uma vez que instalado um programa malicioso ou alterados os dados ou compartilhado conteúdo ilícito, a cada novo acesso ou compartilhamento a ação criminosa é reiterada.

A Busca e Apreensão é medida institucionalizada que, naturalmente, viola certos direitos conforme limitações da Constituição Federal e de legislações infraconstitucionais. Por atingir a liberdade individual do investigado, o emprego há de ser com especial cautela, devendo a autoridade violar os direitos do indivíduo o mínimo possível, no momento do cumprimento da diligência, para alcançar os fins perseguidos na persecução penal. Nesta acepção, Cleunice Pitombo [32] explicita que “[...] o direito fundamental apenas poderá sofrer diminuição dentro da estrita legalidade”, com fins legítimos e justificativa socialmente relevante. Para que não desapareçam as provas do crime, a autoridade policial deve apreender todos os itens que tiverem correlação com o delito (art. 6º, II, do CPP). O art. 240 do mesmo diploma legal relaciona ainda pessoas e objetos sujeitos à Busca e Apreensão tanto pela autoridade policial como pelo juiz, quando fundadas razões a autorizarem. Apesar da Busca e a Apreensão estarem incertas no capítulo das provas, a doutrina as considera mais como medida acautelatória, liminar, destinada a evitar o perecimento das coisas e das pessoas.

Destarte, cada órgão público deveria fornecer meios os quais o cidadão possa conferir tanto os acessos aos seus dados pessoais, como a motivação do ato administrativo materializado pelo agente público que os acessou, efetivando o princípio da publicidade como preceito geral e do sigilo como exceção, conforme o inciso I do artigo 3 da Lei de Acesso à Informação (Lei n.º 12.527/2011). Portanto, caso o cidadão discorde com a motivação do acesso e perceba distorções quanto aos seus fins, poderá contestá-lo através de um processo administrativo ou ação judicial, como a Ação de Indenização contra a Administração Pública, *v.g*. Em caso da comprovação dos fatos ilícitos, deve o suspeito ser autuado; no caso de inocência, deve o Estado

"prestar contas"[6] a este cidadão, apresentando documentos ao mesmo de como fora extraído e analisado seus dados. Essa *accountability* é de responsabilidade do Estado e das empresas com seus usuários-consumidores. Atualmente, os provedores ferem este direito do usuário ao utilizar seus dados – como localização, padrão de imagens etc. – sem prévia autorização, como as reportagens de BBC News [33], Nichols [34] e Hill [35] exemplificam; já o Estado, ao investigar estes delitos e não oferecer mecanismos para eludir excessos desse próprio Estado. A título exemplificativo, nos Estados Unidos, há interceptações e violações de privacidade sem nunca o cidadão – de qualquer país – ter o conhecimento. A Regra 41 [36] dos Procedimentos Especiais concede poderes ao FBI para interceptar qualquer computador suspeito sem reportar-se ao judiciário, isto é, "deram-se" permissão para invadir qualquer computador do mundo.

A alteração institucional do MCI diminuiu o tempo de resposta do Estado, não trazendo efetivamente maior segurança ao indivíduo, pois um requerimento de busca leva, em média, 30 dias para ser apreciado pelo juiz competente, enquanto minutos é o suficiente para o cibercriminoso, sabendo do requerimento, apagar seus rastros. Não olvidando que se o Delegado de Polícia estiver imbuído de más intenções, certamente induzirá a erro o Magistrado; por outro lado, também, o Juiz de Direito é passível de cometer abusos. Desta forma, a alteração constitucional aumentou a burocracia e postergou a prestação da tutela jurisdicional. *Exempli gratia*, a Lei Carolina Dieckmann não diminuiu invasões a aparelhos de terceiros e a obtenção de fotos com nudez alheia; inobstante, sem os devidos meios de efetivação, chegou a atrapalhar [37]. Nos Estados Unidos, as agências fiscalizadoras podem renunciar à permissão de um juiz se o agente federal acredita que provas criminais estão prestes a serem destruídas. É justamente o caso do hacker ou empresa cibercriminosa, já que as evidências estão sempre na iminência de serem destruídas pelos mesmos.

Toda vez que o Estado deixa de dar uma resposta célere, fere o direito fundamental dos indivíduos, pois diminui o acesso à segurança do usuário e mal administra recursos pela ineficácia investigativa. As instituições policiais são uma das mais vigiadas por organismos do Estado e da sociedade civil, sujeita a controle externo do Poder Judiciário, Ministério Público, Ouvidorias, órgãos fiscalizadores não-oficiais tais como ONGs, imprensa etc. Em termos práticos, a assertiva democrática diz que "cada indivíduo possui direito igual à mais ampla liberdade possível, compatível com a igual liberdade dos outros". Com efeito, o direito à privacidade configura, além de um direito fundamental, um direito de personalidade, essencial e inerente à pessoa. Isso significa que a tutela do direito à privacidade visa proteger a sociedade como todo. A falta de regulamentação e tecnologia adequada para combater os casos de violação deste direito dificultam a sua prevenção e repressão, ocasionados, na dicção de Leonardi [38], "pelas mesmas características e peculiaridades que tornam a Internet tão atraente, a tremenda facilidade de disseminação, de busca e de reprodução de informações em tempo real, sem limitações geográficas aparente".

Como academia, analisemos concretamente ante a jurisprudência do tribunal brasileiro. Em 2016, a Justiça do Rio mandou *Yahoo* e *Microsoft* revelarem o autor de e-mails ofensivos que enviara mensagens difamatórias a um casal.[7] A

[6] No termo mais comum, *accountability* é primordial para a existência de qualquer regime democrático transparente. Em síntese, Johnson e Wayland doutrinam que esta transparência e visibilidade das tecnologias não possuem, ao contrário da transparência democrática, uma conotação positiva porque "a transparência sugere a operação da democracia, dos poderosos sendo responsabilizados" (JOHNSON, Deborah. WAYLAND, K. Surveillance and transparency as sociotechnical systems of accountability. In: HAGGERTY, K.; SAMATAS, M. "Surveillance and democracy**"**. London: Routledge, 2010. p. 19-33).

[7] APELAÇÃO. AÇÃO CAUTELAR DE EXIBIÇÃO DE DOCUMENTOS. RELATÓRIO DE 'LOGS DE IP' DOS ACESSOS EFETUADOS À CONTA DE CORREIO ELETRÔNICO. LEGITIMIDADE PASSIVA. Embora a apelante-ré, Microsoft Informática Ltda., seja pessoa jurídica distinta da sociedade empresária Microsoft Corporation, mantenedora do serviço de correio eletrônico Hotmail, vê-se do contrato social que aquela é por esta controlada, devendo então ser rejeitada a

vítima, então, ingressou com uma Ação de Exibição de Documentos. Ao conceder a liminar, o juiz afirmou que houve desrespeito ao artigo 5º, inciso IV, da CF, que afirma ser livre a manifestação do pensar, sendo vedado o anonimato. “A manifestação do ofensor, através de e-mail, contrariou a Constituição Federal, tendo em vista que, anonimamente, denegriu e agrediu o patrimônio moral do autor”, afirmou.

Em 2003, houve a propositura de um “método de verificação” para verificar qual direito tem peso maior em cada caso. Trata-se de uma decisão prolatada pelo STJ, em sede do Recurso Ordinário em Mandato de Segurança,[8] interposto para contestar o acórdão o qual autorizou a quebra de sigilo bancário requerida pelo Ministério Público. Na época, tal decisão fora conturbada. O relator do acórdão, o ministro Luiz Fux, entendeu que a quebra para fins de investigação de suspeita de crime financeiro não viola a privacidade do impetrante, porque o sigilo bancário não é um direito absoluto. Noutras palavras, o colegiado do STJ sentenciou pela sobreposição do direito à informação ao direito à privacidade, determinando a quebra do sigilo bancário do autor do mandato. O interesse público envolvido e a licitude dos meios de obtenção da informação são de monta essencial para a dissolução do embate. Em relação ao interesse público, a própria ementa regula a importância da fiscalização de suspeita de crime financeiro. Para o ministro-relator, Luiz Fux, tal valor é digno *per si* de determinar a quebra do sigilo bancário. Averígua-se, isto posto, a legitimidade e necessidade pública do Estado utilizar seu direito de verificação da informação em detrimento da privacidade de alguns de seus cidadãos. Para isto, conta-se com a conformidade, a idoneidade, a necessidade, a exigibilidade e a proporcionalidade em sentido estrito.

Em síntese, há uma propensão lógica à consideração do princípio da liberdade de informação em preferência ao direito à privacidade do indivíduo suspeito de fraude. Essa inclinação ocorre porque as vantagens da supressão do direito à privacidade são maiores do que se o contrário acontecesse, como prega o princípio da ponderação de Alexy [39]. Existe uma crescente tendência recente nos tribunais de adotar o meio de dissolução proposto por Alexy na ocorrência de conflito de princípios fundamentais. Para esse exame, deverá o operador do direito,

---

tese de ilegitimidade passiva ad causam, não só porque ambas integram o mesmo conglomerado econômico, mas sobretudo em razão da aplicação da teoria da aparência, à luz do princípio da facilitação da defesa do consumidor, porquanto a diferenciação das pessoas jurídicas que compõem a holding Microsoft não é de fácil percepção à parte vulnerável da referida relação. Ocorre que o art. 1.194 do CC/02, aplicável por analogia ao caso, dispõe que “o empresário e a sociedade empresária são obrigados a conservar em boa guarda toda a escrituração, correspondência e mais papéis concernentes à sua atividade, enquanto não ocorrer prescrição ou decadência no tocante aos atos neles consignados”. Demais disso, em havendo relação de consumo, o art. 6º, III, do CDC consagra o princípio da transparência e estabelece o dever de informação clara e adequada ao consumidor em todas as fases contratuais, razão pela qual deve o servidor/provedor de correio eletrônico ter o cuidado de propiciar meios de identificar todos os acessos feitos à conta de e-mail do próprio consumidor, haja vista o dever de segurança que o sigilo das comunicações impõe. Parcial provimento do recurso. (TJ – RJ, Processo n.º: 0450891-64.2014.8.19.0001, Relator: Des. Maria Luiza de Freitas Carvalho, Data de Julgamento: 26/10/2016, TJ-RJ – 48ª Vara Cível, Data de Publicação: DJ 18/07/2016, “JusBrasil**”**, 2016)

[8] EMENTA. RECURSO ORDINÁRIO. MINISTÉRIO PÚBLICO. SIGILO BANCÁRIO. DIREITO RELATIVO. SUSPEITA DE CRIME FINANCEIRO. 1. A suspeita de crime financeiro, calcado em prova de lesividade manifesta, autoriza a obtenção de informações preliminares acerca de movimentação bancária de pessoa física ou jurídica determinada por autoridade judicial com o escopo de instruir inquérito instaurado por órgão competente. 2. A quebra de sigilo bancário encerra um procedimento administrativo investigatório de natureza inquisitiva, diverso da natureza do Processo, o que afasta a alegação de violação dos Princípios do Devido Processo Legal, do Contraditório, e da Ampla Defesa. 3. O sigilo bancário não é um direito absoluto, deparando-se ele com uma série de exceções previstas em lei ou impostas pela necessidade de defesa ou salvaguarda de interesses sociais mais relevantes (Vide §§ 3º e 4º do art. 1º e art. 7º da Lei Complementar 105/2001) 4. Recurso ordinário improvido. (STJ-SC, RMS 15146 SC 2002/0087609-7, Rel. Min. Luiz Fux, Data de Julgamento: 18/03/2003, Data de Publicação: DJ 07.04.2003, “JusBrasil”, 2003)

antes de qualquer medida, realizar um diagnóstico dos possíveis efeitos adversos que a medida restritiva-limitativa poderá gerar, avaliando sua efetiva e real necessidade para solução da matéria. Alexy adverte que “quanto mais grave é a intervenção em um direito fundamental, tanto mais graves devem ser as razões que o justifiquem”. A tutela da averiguação de informações e a restrição de conteúdo, no fulcro digital, devem ser feitas com a maior cautela possível e só quando necessário. De qualquer maneira, não deve haver outra opção a não ser a restrição para evitar o dano maior de lesão a outros direitos fundamentais alheios, mediante até do art. 20 do Código Civil. Em síntese, deve-se buscar a solução menos excessiva ou drástica. Em todas as dimensões de adequação, necessidade e ponderação em sentido estrito, imperiosa é a análise completa dos fatos e, perante o dimensionamento preciso, contextualizar a via de exercício da liberdade de expressão e se esta posição pode afrontar outros princípios constitucionais, como a dignidade humana, a honra, a privacidade ou a intimidade.

O artigo 2º do Marco Civil define que o uso da Internet no Brasil tem como princípio básico o respeito à liberdade de expressão, todavia, não significa que uma lei infraconstitucional possa modificar o equilíbrio dado pela Constituição. A CF não coloca nenhum direito fundamental como absoluto e o Marco Civil não poderia ter a pretensão de fazê-lo. Para o Direito, seria utópico solucionar os problemas advindos da internet sem atingir a liberdade e privacidade individual.

7. Considerações Finais

O estudo problematizou a matriz jurídica tradicional e deduziu ser legitimado ao Estado proteger os direitos das vítimas de cibercrimes. Todavia, é também seu dever preservar a internet como uma plataforma aberta, sem engessamentos pelo excesso de normas, com interferências mínimas e pontualmente eficazes, remediando os cibercrimes. Neste enquadramento, políticas públicas e regulamentação estatal são indispensáveis, pautadas em profissionalização, organização de ações contra *hackers*, melhores agências e sistematização de atores públicos no combate ao cibercrime. Enseja-se aos cibercrimes os benefícios de um crime permanente, já que o bem jurídico na maioria das vezes será algum bem imaterial da pessoa, ferirá sua liberdade e, em muitas vezes, sua privacidade. Ademais, se carece de melhores diretrizes doutrinárias para que a jurisprudência interna possa embasar, complementarmente à lei.

Pelas características singulares dos fulcros tecnológicos, mais especificamente da internet, nota-se a necessidade de uma efetiva coercibilidade de normas visando a diminuição de práticas lesivas ao usuário. Com transparência, finalidade legítima e proporcionalidade, o problema central fora esmiuçado e a solução proposta maximiza os efeitos positivos da liberdade de expressão e privacidade dos usuários e minimiza os efeitos negativos de violações dos cibercriminosos. Logo, a hipótese da legitimidade e necessidade desta adaptação legal fora corroborada. Por isto, consoante às características singulares da internet, com diferença paradigmática da realidade virtual e não-virtual, certos direitos do cibercriminoso devem e podem ser afetados, como bem permite intrinsicamente o flagrante delito pelo bem do direito à informação pelo Estado.

Referências

[1] ELASTICA CLOUD THREAT LABS. “1H 2016 Shadow Data Report”. 2016. p. 5, 10 e 11.

[2] NORTON. “Norton Cyber Security 2012”. 2013.

[3] ZAHARIA, Andra. “10 Alarming Cyber Security Facts that Threaten Your Data [Updated]”. Disponível em: <https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/>. Acesso em: 10 out. 2019.

[4] SYMANTEC CORPORATION WORLD HEADQUARTERS. “Internet Security Threat Report 2015”. Volume 20, 2015. p. 5.

[5] HPE SECURITY RESEARCH. “Hewlett Packard Enterprise (HPE) Cyber Risk Report 2016”. 2016. p. 30-33.

[6] SYMANTEC CORPORATION WORLD HEADQUARTERS. “Underground black market:

Thriving trade in stolen data, malware, and attack services". 2015. Disponível em: <https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>. Acesso em: 10 out. 2019.

[7] TRENDMICRO. "A Global Black Market for Stolen Personal Data". Disponível em: <http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/>. Acesso em: 10 out. 2019.

[8] SECUREWORKS. "2016 Underground Hacker Marketplace Report". 2016.

[9] CONVENÇÃO SOBRE O CIBERCRIME. Budapeste, 23.XI.2001.

[10] MATTEUCCI, Nicola. "Estado Contemporâneo". In: BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. "Dicionário de Política". 11 ed. Brasília: Editora Universidade de Brasília, 1998, v. 1. p. 401.

[11] OFFE, Claus. "Contradictions of the Welfare State". Londres: Hutchinson & Co. ltd., 1984.

[12] MATTEUCCI, *op. cit.*, p. 703-705.

[13] ARANHA, Márcio Iorio. "Manual de Direito Regulatório: Fundamentos de Direito Regulatório". 2ª ed. Coleford: Laccademia Publishing, 2014. p. 88.

[14] *ibidem*, p. 22.

[15] *ibidem*, p. 88.

[16] VENOSA, Sílvio de Salvo. "Direito Civil – Responsabilidade Civil". 6ª ed. São Paulo: Atlas, 2006. p. 263.

[16] LEONARDI, Marcel. "Responsabilidade Civil dos Provedores de Serviços de Internet". São Paulo: Juarez de Oliveira, 2005. p. 270.

[18] *idem*. "Responsabilidade Civil dos Provedores de Serviços de Internet". São Paulo: Juarez de Oliveira, 2012. p. 157.

[19] DRUMMOND, Victor. "Internet, privacidade e dados pessoais". Rio de Janeiro: Lumen Juris, 2003. p. 1.

[20] LIMBERGER, Têmis. BUNCHAFT, Maria Eugênia. "Novas tecnologias e direitos humanos: uma reflexão à luz da concepção de esfera pública". In: "Espaço Jurídico Journal of Law [EJJL]", Joaçaba-SC, v. 17, n. 3, p. 843-868, set./dez. 2016. p. 848.

[21] NEVES, Marcelo. "Transconstitucionalismo". São Paulo: Editora WMF Martins Fontes, 2009. p. 111.

[22] TEUBNER, Gunther. "Globale Zivilverfassunge: Alternativen zur staatszentrierten Verfassungstheorie, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht". 63 (1), 2005. p. 4.

[23] LIMA, Renato Brasileiro de. "Curso de Processo Penal". Niterói: Impetus, 2013. p. 496.

[24] CAPEZ, Fernando. "Curso de Processo Penal". 19 ed. São Paulo: Saraiva, 2012. p. 277

[25] NUCCI, Guilherme de Souza. "Código Penal Comentado". 14 ed. São Paulo: Editora Revista dos Tribunais, 2014. p. 117.

[26] *idem.* "Manual de Direito Penal". 6 ed. São Paulo: Revista dos Tribunais, 2009.

[27] JESUS, Damásio de. "Direito Penal". 1 v. São Paulo: Saraiva, 2009. p. 189-190.

[28] BITENCOURT, Cézar Roberto. "Tratado de Direito Penal". São Paulo: Saraiva, 2010. p. 253-254.

[29] ALVES, Roberto. "Projeto de Lei nº 5463 de 2016. 01/06/2016". Acrescenta ao Código de Processo Penal o denominado "flagrante digital", que estabelece como infração permanente o delito cibernético. "Diário do Congresso Nacional", Brasília, DF, 1 jun. 2016. p. 1.

[30] PITOMBO, Cleunice A. "Da Busca e da Apreensão no Processo Penal". 2. ed. São Paulo: Revista dos Tribunais, 2005. p. 128.

[31] PICOLO, Jessica de Freitas. "Criminologia em torno do crime cibernético". In: "Âmbito Jurídico", Rio Grande, XIX, n. 154, nov. 2016. Disponível em: <http://www.ambitojuridico.com.br/site/index.php/Paulo%20Leandro%20Maia?n_link=revista_artigos_leitura&artigo_id=18112>. Acesso em: 10 out. 2019.

[32] PITOMBO, *op. cit*., p. 91.

[33] BBC NEWS. "Is your phone listening in? Your stories". 2017. Disponível em: <https://www.bbc.com/news/technology-41802282>. Acesso em: 10 out. 2019.

[34] NICHOLS, Sam. "Your Phone Is Listening and it's Not Paranoia". 2018. Disponível em: <https://www.vice.com/en_au/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia>. Acesso em: 10 out. 2019.

[35] HILL, Kashmir. MATTU, Surya Mattu. "Facebook Knows How to Track You Using the Dust on Your Camera Lens". 2018. Disponível em: <https://gizmodo.com/facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620>. Acesso em: 10 out. 2019.

[36] Rule 41. "Search and Seizure". 2016. Disponível em: <https://www.law.cornell.edu/rules/frcrmp/rule_41>. Acesso em: 10 out. 2019.

[37] BERETTA, Pedro. “Sem meios eficazes, Lei Carolina Dieckmann até atrapalha”. In: “Consultor Jurídico”. 2014. Disponível em: <https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha>. Acesso em: 10 out. 2019.

[38] LEONARDI, Marciel. “Responsabilidade Civil dos Provedores de Serviços de Internet”. São Paulo: Juarez de Oliveira, 2012. p. 42.

[39] ALEXY, Robert. “Teoria dos Direitos Fundamentis”. Tradução de Viroílio Afonso da Silva da 5ª edição de “*Theorie der Grundrechte*” (2006). São Paulo: Malheiros Editores LTDA, 2009. p. 91.