EMAG
ESCOLA DE MAGISTRADOS
DA JUSTIÇA FEDERAL
DA 3ª REGIÃO

Cadernos de Estudos

Investigação e prova nos crimes cibernéticos

1

Cadernos de Estudos 1

Investigação e prova nos crimes cibernéticos

1ª edição

EMAG
ESCOLA DE MAGISTRADOS
DA JUSTIÇA FEDERAL
DA 3ª REGIÃO

TRF3

São Paulo
2017

TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO

CECÍLIA MARIA PIEDRA MARCONDES
Presidente

MAIRAN GONÇALVES MAIA JÚNIOR
Vice-Presidente

THEREZINHA ASTOLPHI CAZERTA
Corregedora-Regional

Desembargadores Federais
DIVA PRESTES MARCONDES MALERBI
PAULO OCTAVIO BAPTISTA PEREIRA
ANDRÉ NABARRETE NETO
MARLI MARQUES FERREIRA
NEWTON DE LUCCA
OTÁVIO PEIXOTO JÚNIOR
FÁBIO PRIETO DE SOUZA
NERY DA COSTA JÚNIOR
LUIS CARLOS HIROKI MUTA
CONSUELO YATSUDA MOROMIZATO YOSHIDA
MARISA FERREIRA DOS SANTOS
LUÍS ANTONIO JOHONSOM DI SALVO
NELTON AGNALDO MORAES DOS SANTOS
SÉRGIO DO NASCIMENTO
ANDRÉ CUSTÓDIO NEKATSCHALOW
LUIZ DE LIMA STEFANINI
LUÍS PAULO COTRIM GUIMARÃES
MARIA CECILIA PEREIRA DE MELLO
ANTONIO CARLOS CEDENHO
MARIA LUCIA LENCASTRE URSAIA
JOSÉ MARCOS LUNARDELLI
DALDICE MARIA SANTANA DE ALMEIDA
FAUSTO MARTIN DE SANCTIS
PAULO GUSTAVO GUEDES FONTES
NINO OLIVEIRA TOLDO
MÔNICA AUTRAN MACHADO NOBRE
TORU YAMAMOTO
MARCELO MESQUITA SARAIVA
TÂNIA REGINA MARANGONI
LUIZ ALBERTO DE SOUZA RIBEIRO
DAVID DINIZ DANTAS
MAURICIO YUKIKAZU KATO
GILBERTO RODRIGUES JORDAN
HÉLIO EGYDIO DE MATOS NOGUEIRA
PAULO SÉRGIO DOMINGUES
WILSON ZAUHY FILHO
ANA LÚCIA JORDÃO PEZARINI
NELSON DE FREITAS PORFIRIO JÚNIOR
VALDECI DOS SANTOS
CARLOS EDUARDO DELGADO

ESCOLA DE MAGISTRADOS
DA JUSTIÇA FEDERAL DA 3ª REGIÁO

Diretor

Desembargador Federal CARLOS MUTA

Membros da Diretoria

Desembargadora Federal CONSUELO YOSHIDA

Desembargador Federal NELTON DOS SANTOS

Desembargador Federal PAULO DOMINGUES

Equipe técnica EMAG

Assessora da Diretoria
Marta Fernandes Marinho Curia

Diretora da Divisão de Educação Corporativa, Publicação e Gestão de Acervo
Ana Mariza Vanzin

Revisão
João Rodrigues de Jesus
Vera Emidio

Colaboração
Ariane Rocha

Projeto gráfico e diagramação
Wladimir Wagner Rodrigues

Impressão
InPrima Soluções Gráficas - Unidade Paulista

Apoio
AJUFESP - Associação dos Juízes Federais de São Paulo e Mato Grosso do Sul

Catalogação na fonte

B83i

Brasil. Tribunal Regional Federal da 3ª Região. Escola de Magistrados

Investigação e prova nos crimes cibernéticos. São Paulo : EMAG, 2017.

352p. (Cadernos de estudos ; 1)

ISBN nº-978-85-98004-04-4

1.Crime de informática. 2. Investigação criminal. 3. Prova. 4. Internet. 5. Meio eletrônico. 6. Segurança de dados. 7. Crime contra a criança e o adolescente. I. Título.

CDU 343.14:34:681.3

Avenida Paulista, 1912 – 3º andar – Edifício Funcef Center – 01310-924 – São Paulo – SP
www.trf3.jus.br/emag | e-mail: emag@trf3.jus.br
Telefones: (011)3012-1781 e 3012-1785 – Fax: (011)3012-2050

Esta publicação não é comercializada.

Caros leitores

A atual Diretoria da Escola de Magistrados da Justiça Federal da 3ª Região tomou posse em março de 2016. Recebemos o legado deixado por magistrados vocacionados, que estiveram à frente dos trabalhos da instituição desde 1991. Tivemos e assumimos o compromisso de colaborar com o projeto institucional de formação e aperfeiçoamento dos magistrados, adotando, como norte diferencial, o modelo de gestão colegiada e participativa, de forma simples, porém efetiva e concreta.

Todas as ações da EMAG são, hoje, pensadas, aprovadas e realizadas por meio de decisões colegiadas da Diretoria. Antes disso, porém, instalou-se uma concepção de trabalho baseada na premissa de que a formulação de projetos de atuação institucional depende de consulta prévia e direta aos principais interessados na formação e aperfeiçoamento, de modo a identificar a linha de atuação da Escola com as necessidades e expectativas dos magistrados, enquanto principal público-alvo de nossas ações educacionais.

Dentre as primeiras iniciativas da Diretoria da EMAG, destacou-se a realização de visita técnica aos diversos fóruns da Capital, exatamente com o intento de permitir que a agenda educacional da Escola fosse não apenas adequada, como concretizada com o auxílio e participação direta e permanente dos

magistrados, num processo de formação construtiva não apenas do conhecimento em si, enquanto resultado, como do modelo decisório de concepção dos projetos de educação, formação e aperfeiçoamento.

Os resultados foram imediatos e não poderiam ter sido melhores. Apesar de todas as dificuldades orçamentárias e de trabalho, em razão do volume de processos em tramitação nas Varas e nos Gabinetes do Tribunal, os cursos da EMAG inovaram na temática e na metodologia. O mais importante, porém, é que tais cursos passaram a congregar, como nunca, magistrados que haviam deixado de ver a EMAG como órgão de referência, que deve ser, no ensino profissional voltado ao aprimoramento da atividade jurisdicional.

Não apenas novos cursos, mas novas temáticas e novo público foram agregados nas atividades da Escola a partir de tais iniciativas de trabalho, que, bem destacado, não foram mérito da Diretoria, mas de toda a equipe técnica e dos magistrados da nossa Região, com o apoio da Administração do Tribunal. Foram criados novos caminhos e instrumentos, e, sobretudo, diálogos inéditos, que primamos para que sejam permanentes e cada vez mais profundos. Esse é o meio que julgamos adequado para enfrentar o desafio de desenvolver ensino jurídico profissional em ambiente institucional e político, marcado por dificuldades não apenas de sustentar a necessidade do conhecimento como forma de aprimoramento da atividade jurisdicional, como de desenvolver os mecanismos necessários para atingir tais objetivos, em razão de tão severas restrições de recursos humanos, materiais e orçamentários.

Foram vários os eventos educacionais promovidos pela EMAG durante o ano acadêmico de 2016. “Investigação e prova nos crimes cibernéticos. Dificuldades técnicas e jurídicas – Questões práticas” foi um dos cursos implementados a partir de consulta direta aos magistrados do Fórum Criminal da Capital. Foi construído e coordenado pela Juíza Federal Adriana Delboni

Taricco, que conhece e vive, no dia a dia, os desafios do exercício da jurisdição criminal, com a colaboração de diversos órgãos que integram o sistema de Justiça Criminal: Ministério Público Federal, Departamento de Polícia Federal e Advocacia de Estado e Privada.

Não apenas foram inovadores os temas desenvolvidos. Contamos com a atuação e participação de palestrantes que, além de renomados, revelaram-se comprometidos com o projeto de compartilhar ciência e experiências para o desenvolvimento de uma Justiça mais eficiente em tempos de domínio do conhecimento digital. Foi-se mais longe: no âmbito das oficinas de trabalho, após palestras e exposições, seguindo a metodologia pedagógica da ENFAM, o conhecimento foi posto à prova e desafiado a produzir resultados práticos a favor do aprimoramento do sistema de Justiça Criminal.

Os dilemas, desafios, dúvidas, caminhos, soluções e resultados certamente vão permanecer vivos na lembrança dos participantes do evento. Todavia, mais do que lembranças, o conhecimento exige registro dos estudos do passado e do presente para a construção do conhecimento do futuro. O processo é complexo e permanente. Cabe à EMAG o dever de preservar a memória institucional das atividades desenvolvidas por seus magistrados em prol da Justiça.

Este registro histórico deve ser visto não como um ponto de chegada, mas como verdadeiro ponto de partida para novas discussões dentro do compromisso de construção contínua e dialogada do conhecimento. Além do material audiovisual e dos textos distribuídos e abordados no curso, a EMAG incentivou o projeto de elaboração, por parte dos magistrados, de enunciados acadêmicos e de textos com a síntese das discussões realizadas e das reflexões desenvolvidas no âmbito das exposições dos temas e nas oficinas práticas.

Tanto os enunciados como os textos têm natureza e objetivo acadêmico, ainda que relativos a temas vividos na jurisdição e ainda

que possam, como se espera, ter reflexos no aprimoramento da atividade jurisdicional. Sua institucionalização teve como objetivo central estimular a busca e a sede por conhecimento, destacando a importância do saber como meio e instrumento do ser para julgar, além de colaborar com a concepção da decisão como ato primordial de conhecimento e responsabilidade, e não de puro e mero voluntarismo.

O Caderno, que ora se apresenta, é apenas o registro histórico do processo, árduo, mas gratificante, de edificação do conhecimento, que não acaba na divulgação destes primeiros resultados, mas estimula novas e permanentes incursões não só no ambiente da EMAG, enquanto Escola de Formação e de Aperfeiçoamento de Magistrados, mas ainda no espaço intelectual, consciente e individual de cada julgador, diante da realidade própria e peculiar de cada processo, assim como, para além, no universo institucional da Justiça Federal da 3ª Região.

Ao ensejo da concretização deste importante projeto, a Diretoria da EMAG registra a valiosa colaboração de todos os que participaram do curso e elaboraram os trabalhos publicados, assim como, em especial, da AJUFESP, que ofertou, desde o primeiro momento, o indispensável apoio a esta iniciativa acadêmica.

Que a leitura possa ser tão proveitosa e estimulante como, certamente, foi, para os magistrados que participaram deste projeto, o desafio de construir conhecimento para distribuir justiça cada vez melhor, com serenidade, mas firmeza responsável, democrática e republicana.

Desembargador Federal CARLOS MUTA
Diretor da Escola de Magistrados
da Justiça Federal da 3ª Região

Sumário

Apresentação

Este Caderno de Estudos é fruto do encontro realizado, em novembro de 2016, no auditório da Escola de Magistrados da Justiça Federal da 3ª Região, entre juízes federais, procuradores da República, delegados federais, servidores da Justiça Federal, servidores do Ministério Público Federal e agentes da Polícia Federal.

O objeto de estudo desse encontro foi a investigação e a prova nos crimes cibernéticos, tendo, como ponto de partida, as dificuldades técnicas e jurídicas enfrentadas nas varas federais criminais que, por anos, vêm recebendo os resultados das operações nacionais deflagradas em relação a crimes ligados à pornografia infantil, praticada por meio da rede mundial de computadores.

Diante da importância do tema e de seus desdobramentos práticos, foi incorporada a sugestão do Exmo. Sr. Diretor da EMAG, Desembargador Federal Carlos Muta, no sentido de redigir e aprovar enunciados.

O caráter sigiloso do conteúdo, voltado às ferramentas modernas de investigação cibernética, às soluções disponíveis técnica e juridicamente na investigação e aos problemas e limitações na perícia informática, impôs a modalidade presencial.

Os sete enunciados, aprovados ao final, nasceram de debates entre os participantes, tendo sido discutidas questões sobre o cumprimento de mandados de busca e apreensão, a realização de ação controlada, a infiltração policial e a consideração de prova produzida integralmente em país estrangeiro.

A participação da Polícia Federal e do Ministério Público Federal foi imprescindível para que pudéssemos entender a dificuldade técnica na área da informática, às vezes tão distante das regras jurídicas existentes no Brasil.

Colegas e participantes do evento acabaram por sugerir outros temas igualmente pertinentes, trazendo dúvidas e questionamentos para além do conteúdo das palestras, demonstrando a conveniência de uma abordagem mais ampla do que a permitida pelo tempo destinado ao curso presencial.

Na medida em que eram apresentados a Deep Web, a Darknet, as peculiaridades de operações realizadas pela Polícia Federal em diversas subseções, os alvos de investigação e as ferramentas de trabalho na área de informática, outras temáticas surgiam, inclusive com questões transdisciplinares.

O plano de escrever sobre temas relacionados ao objeto do curso surgiu dessas discussões mais abrangentes, com o escopo de somar, no futuro, ideias e esforços visando facilitar o trabalho inerente aos processos que tratam de crimes cibernéticos em geral, e não só aos relacionados à pedofilia e à pornografia infantil.

A tecnologia não é apresentada, aqui, como um problema ou um empecilho à investigação de crimes e prova de autoria e dolo, mas como aliada da persecução penal, do mesmo modo que auxilia profissionais na área médica, na engenharia, e em outras tantas ciências.

Não há como entender de outra forma, já que a informática está cada vez mais impregnada em nossas vidas. Não saímos de casa sem aparelhos celulares, que são verdadeiros microcomputadores.

Adolescentes contam com *tablets* para estudar, crianças brincam em *iPads,* antes mesmo de falar ou andar, e assim por diante.

Contudo, em que pese nossa dependência com relação à tecnologia, são poucas as pessoas que realmente conhecem, a fundo, as diversas questões que envolvem a segurança relacionada a todos esses aparelhos modernos.

O déficit de conhecimento especializado tem reflexos no próprio trabalho desempenhado pelos magistrados: fazemos uso de computadores, gravamos e filmamos audiências, utilizamos videoconferência e teleaudiência, contamos com um sistema virtual nos Juizados Especiais Federais e nas Turmas Recursais, enviamos mensagens por *e-mail* funcional para agilizar a comunicação, mas não possuímos saber técnico, seguro e aprofundado, sobre o funcionamento de toda a tecnologia colocada a nossa disposição.

É certo também, que, em determinados casos, é necessário colocar de lado a investigação tradicional e considerar novos perfis de agentes na seara do crime cibernético, como provedores de conexão e de aplicação.

Pensando nessas modernas demandas voltadas à tecnologia e nas atuais dificuldades que circundam o crime cibernético, os artigos que seguem tratam das peculiaridades das buscas e apreensões de material referente a essa modalidade de crime, do documento digital, da coleta de vestígios digitais, da materialidade e da autoria delitiva, dos meios de comprovação do dolo.

Discorrem também sobre a maneira como o sujeito ativo desse tipo de crime costuma cooptar a vítima e sobre as dificuldades enfrentadas pelos juízes criminais, tais como os critérios ou a falta de parâmetros para a quantificação da pena e o poder geral de cautela do magistrado.

Além disso, os estudos contêm uma reflexão sobre a possibilidade de criação de um registro de identificação criminal de condenados pela prática desse tipo de delito, usando, como parâmetro, o sistema jurídico português.

Ao final de cada estudo, apresentamos a conclusão do trabalho em conjunto, necessário para construirmos uma linguagem comum, diminuindo o risco de depender da tecnologia sem conhecer seu mecanismo de atuação, e para nos atualizarmos e aprimorarmos em busca de uma eficaz prestação jurisdicional.

Ainda há muito que refletir, estudar e compartilhar sobre o tema, mas a interação entre Judiciário Federal, Ministério Público Federal e Polícia Federal é um início promissor.

ADRIANA DELBONI TARICCO*

* Mestre em Direito/Processo Civil pela PUC/SP. Juíza Federal Substituta da Justiça Federal de Primeiro Grau em São Paulo/SP. *E-mail*: ataricco@trf3.jus.br.

Cibercrime: quando a tecnologia é aliada da lei

Adriana Shimabukuro*

RESUMO

Este artigo compara as principais diferenças entre a investigação tradicional e a investigação de crimes que ocorrem por meio da Internet. São exploradas técnicas utilizadas por investigadores e introduzidos novos conceitos originários da tecnologia. São abordados conceitos de número IP[1], a importância dos registros de serviços e acessos, as novas características das evidências digitais, além das técnicas utilizadas por criminosos digitais para tentarem se manter anônimos.

Palavras-chave: Cibercrime. Logs de registro. Bitcoin. Darknet. Hash. Criptografia.

ABSTRACT

This article compares the main differences between traditional research and the investigation of crimes that occur through the Internet. Techniques used by researchers are explored and new concepts introduced from technology. IP number concepts, the importance of service and access records, the new characteristics of digital evidence, and the techniques used by digital criminals to try to remain anonymous are discussed.

***Keywords**: Cybercrime. Connection log. Bitcoin. Darknet. Hash. Encryption.*

* Pós-graduada em Redes de Computadores pela Escola Superior Aberta do Brasil (Esab). Assessora técnica do Grupo de Combate aos Crimes Cibernéticos da Procuradoria da República em São Paulo. *E-mail*: adrianashimabukuro@mpf.mp.br.

[1] O número IP é uma identificação que um dispositivo recebe ao acessar uma rede.

1 Introdução

Com a popularização do acesso à Internet nos últimos anos, os crimes digitais no Brasil alcançam números assustadores. De acordo com a SaferNet (2017), que controla a Central Nacional de Denúncias, mais de 115 mil denúncias envolvendo exclusivamente crimes contra direitos humanos foram recebidas e processadas no ano de 2016.

Os crimes envolvendo fraudes bancárias também não ficaram para trás. De acordo com TOZZETO (2010), a Federação Brasileira de Bancos (Febraban) divulgou que bancos brasileiros perderam R$ 1,8 bilhão só em 2015. Estes crimes englobam desde o roubo de senhas, via ataques de *phishing scam*, até os "*kits* boletos[2]", exclusividade do Brasil.

Os ataques não chegam a ser tão sofisticados, visto que os alvos, uma população que conhece pouco sobre segurança e que começou agora a ter acesso à Internet, não oferecem muita dificuldade ou riscos para o submundo criminoso.

Além desses crimes, podemos citar a pornografia infantil, o *bullying*, a violação de direitos autorais, racismo, até os recentes casos de ciberterrorismo, que começam a despontar em território brasileiro.

Especializar os legisladores e dar *expertise* à magistratura são medidas essenciais para combater esta nova onda de crimes tecnológicos, que infelizmente não parece diminuir a cada ano.

2 Saem as digitais e entram os números IPs

Identificar o criminoso cibernético é tão desafiador quanto identificar um criminoso por suas digitais. Se antes os policiais buscavam dados em bancos de digitais, agora estes dados estão em gigantescos arquivos que guardam o IP do usuário de Internet.

[2] *Softwares* que modificam arquivos de boletos bancários para que usuários façam depósitos em contas de criminosos.

O IP, ou *Internet Protocol*[3], é um número que um computador ou equipamento conectado à Internet recebe. Combinado a uma data e um horário, é possível localizar um usuário da Internet em qualquer parte do mundo. Temos duas versões de IP, a versão 4, utilizada desde 1981 e que está sendo migrada para a versão 6, disponível desde 1999. Veja, a seguir, exemplos de endereços IP nas duas versões.

IPv4: **201.199.244.101**

IPv6: **FEDC:2D9D:DC28:7654:3210:FC57:D4C8:1FFF**

3 Quando o local do crime está no ciberespaço[4]

Apesar de o conceito de ciberespaço não abranger um corpo físico ou espaço geográfico, ele representa uma construção social feita à imagem e semelhança do mundo físico. O ciberespaço conecta redes, equipamentos e principalmente pessoas. Uma representação clássica da Internet ou do ciberespaço é feita com a ilustração de um *iceberg*, como na figura 1.

É possível identificar basicamente três camadas: a Internet Pública, a Deep Web e a Dark Web.

Como o próprio nome sugere, a Internet Pública é de fácil acesso e não requer senhas ou *softwares* específicos para a navegação, ao contrário da Deep Web, que é composta de dados não indexados, isto é, não pode ser detectada por motores de busca como o Google ou Bing[5]. Na Deep Web também encontramos *sites* dinâmicos, criados como resultado de uma busca ou até páginas

[3] Protocolo de comunicação usado entre máquinas de uma rede.

[4] Espaço existente no mundo da comunicação, onde não é necessária a presença física dos interlocutores.

[5] Disponível em: <http://www.google.com> e <http://www.bing.com>. Acesso em: 23 mar. 2017.

que requerem acesso via *login* e senha, como, por exemplo, sua conta no Gmail.

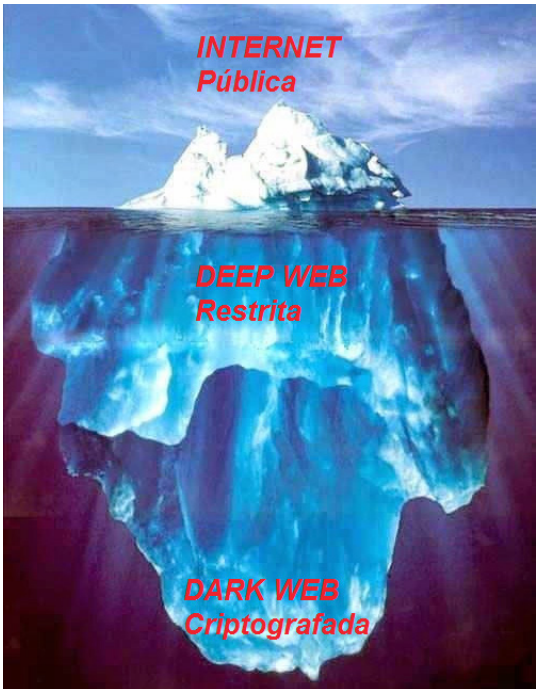

Figura 1: Representação didática das divisões da Internet.
Fonte: Figura elaborada pela Autora.

Diferente da Deep Web, a Dark Web ou Darknet é uma rede fechada, usada para compartilhar conteúdo de forma anônima. Seu acesso é permitido mediante o uso de *softwares* específicos, como o TOR Project, o Freenet e a rede I2P (2017) ou outras dezenas de redes secretas e criptografadas.

Conforme MERCÊS (2014), a Darknet é majoritariamente composta de *sites* de venda de produtos ilícitos, como armamento e drogas, além de *sites* que compartilham pornografia infantil.

A Polícia Federal do Rio Grande do Sul deflagrou as operações Darknet I (2014) e Darknet II (2016) para combater o compartilhamento de pornografia infantil no ambiente da Internet.

Supostamente protegidos pelas tecnologias que prometem privacidade, criminosos compartilhavam um grande volume de material abusivo de crianças e adolescentes. Utilizando técnicas de exploração de vulnerabilidades, dezenas de pedófilos foram identificados e presos. Além disso, crianças em situação de abuso sexual foram identificadas e resgatadas.

4 Rastros de criminosos passam a ficar armazenados em *logs* de provedores

A investigação cibernética traz novos agentes: os provedores de conexão[6] e provedores de aplicação[7]. O Marco Civil da Internet tornou obrigatório aos provedores guardar informações de usuários que utilizaram determinado serviço, bem como a data e a hora em que a conexão foi realizada.

Apesar de existirem questões quanto ao direito de privacidade, a obtenção destas informações é fundamental para a resolução de crimes. Os registros de acesso permitem rastrear e identificar onde surgiu determinada conduta ilícita; são fornecidos somente mediante ordem judicial. Os registros de serviço podem apontar a divulgação ou compartilhamento de conteúdo criminoso.

O Decreto n.º 8.771/2016, que regulamentou a Lei do Marco Civil da Internet, determina que os provedores de conexão e aplicação devem excluir os dados de usuários tão logo termine o prazo de retenção. Considerando que os prazos são exíguos, 6 (seis) meses para provedores de aplicação e 1 (um) ano para provedores

[6] Provedor de conexão é a pessoa jurídica fornecedora de serviços que possibilitam o acesso dos consumidores à Internet. Exemplo: Tim, Claro, Vivo, etc.

[7] Provedor de aplicação é a pessoa natural ou jurídica que se utiliza do acesso à Internet para prestar serviços. Exemplos: provedores de conteúdo, de *e-mail*, de hospedagem, etc.

de conexão, as autoridades passam a ter mais um desafio para o cumprimento da lei.

5 Provas voláteis, as novas evidências digitais

Enquanto no local de um crime tradicional se encontram informações essenciais para a investigação, como testemunhas, digitais, vestígios e indícios, o crime cibernético abriga suas principais evidências em inúmeros dispositivos, como computadores, telefones celulares, *pen drives*, máquinas fotográficas, provedores de Internet, registros de equipamentos de infraestrutura de rede (roteadores, *firewalls*, *web servers*, servidores de *e-mail*, etc.). As provas podem ser as mais diversas possíveis: arquivos digitais, registros de servidores, *cookies*[8], o histórico de navegadores, fotos ou vídeos, *e-mails* e registros de conversas *on-line*.

Pela característica da evidência digital, caso esta não seja prontamente preservada, pode ser rapidamente danificada ou alterada, impedindo qualquer investigação ou identificação de criminosos.

A coleta de vestígios digitais segue rigorosos mecanismos de preservação, além de controlar qualquer espécie de alteração.

Uma característica da evidência digital é que, na maioria dos casos, ela pode ser copiada inúmeras vezes. A cópia pode ser exatamente como a original e não invalida seu uso como prova.

Infelizmente, o mesmo princípio se aplica para um crime cibernético: quando uma imagem ou vídeo criminoso é removido da Internet, as cópias podem ser publicadas novamente, perpetuando o sofrimento e exposição da vítima.

[8] Arquivos gravados no computador do internauta, que registram os *sites* que ele visitou.

6 Confundindo o investigador: *proxies* e mascaramento de IP

Usar luvas para evitar que as digitais entreguem a identidade passa a ser ultrapassado quando falamos de crimes cibernéticos. Um criminoso mais habilidoso aprende desde cedo que ferramentas, quase sempre gratuitas e de fácil acesso, permitem esconder locais que um internauta visitou, comentários ou ações suspeitas.

Os números IPs, principal informação que identifica um usuário da Internet, podem ser escondidos ou até alterados por meio de ferramentas chamadas *proxies*. Os serviços de *proxy* são computadores intermediários entre o usuário e o destino a ser alcançado que possuem várias funções: desde manter a segurança do usuário que não se expõe diretamente na Internet até aumentar a velocidade da navegação usando recursos de *cache*[9].

Figura 2: Ferramentas permitem mascarar um endereço brasileiro, como se fosse um endereço alocado nos Estados Unidos.
Fonte: *PrintScreen* da aplicação *Real Hide IP.*

[9] Área que mantém dados armazenados de um local mais lento, com o objetivo de acelerar a recuperação de dados.

Com a possibilidade de manter sua privacidade atrás de um serviço de *proxy*, um criminoso pode utilizar o mesmo serviço para enganar um investigador e alocar seu endereço para um país remoto.

Serviços como o TOR (*The Onion Router*) podem utilizar até 3 (três) endereços falsos em países diferentes, tornando quase impossível o rastreamento.

7 Escondendo mensagens atrás da criptografia

Como explica SINGH (2010) em *O livro dos códigos*, esconder mensagens é uma necessidade que o homem tem desde que aprendeu a se comunicar. Criptografia é a técnica de cifrar mensagens para torná-las ininteligível. As primeiras técnicas se resumiam em substituir cada letra do alfabeto pela seguinte. Por exemplo, a palavra "amor" passaria a ser "bnps". Atualmente, as técnicas de criptografia utilizam complexos algoritmos matemáticos, protegendo desde transações bancárias até mensagens trocadas entre dois usuários.

Figura 3: Aplicando a criptografia para esconder mensagens.
Fonte: Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/hugo/Criptografia.html>. Acesso em: 23 mar 2017.

Em pouco tempo, a criptografia passará a estar presente em todos os dispositivos conectados, como carros autônomos, TVs inteligentes, câmeras, entre outros. Esta tecnologia é essencial para garantir a privacidade e a segurança dos seus consumidores.

A criptografia de ponta a ponta permite que somente os próprios usuários (remetente e destinatário) possam decodificar a informação compartilhada. Isto faz com que os provedores de aplicação sejam impedidos de fornecer qualquer informação para uma autoridade legal, trazendo grandes problemas para a resolução de crimes cibernéticos.

Recentemente, a Apple e o FBI travaram uma briga na Justiça americana, em virtude da apreensão de um iPhone 5c, pertencente a um dos atiradores do massacre em San Bernardino. Mesmo com o acesso físico ao aparelho, a polícia americana não poderia acessar seus dados, visto que a Apple passou a criptografar todo o conteúdo de seus equipamentos e somente a senha poderia dar acesso aos dados. A técnica da força bruta[10], usualmente empregada nestes casos era ineficiente, pois o equipamento poderia apagar todo o seu conteúdo quando da 11ª tentativa errada. Posteriormente, e sem explicações, o FBI informou que conseguiu acessar o conteúdo do aparelho sem o auxílio da Apple.

8 *Hash*, a identificação única dos arquivos

De acordo com a Microsoft, 1,8 bilhão de imagens são publicadas diariamente na Internet. A identificação de uma imagem criminosa neste ambiente é equivalente a procurar uma agulha no palheiro.

Para auxiliar nesta busca, é possível criar uma identificação única para cada tipo de arquivo que é disponibilizado na rede, o *hash*. Trata-se basicamente de uma sequência única de letras e números que, gerados por algoritmos matemáticos, servem para verificar a

[10] Técnica que gera todas as combinações de senha possíveis para tentar acesso a um sistema.

integridade de um arquivo, armazenar senhas e, neste caso, buscar um determinado arquivo em uma grande base de dados.

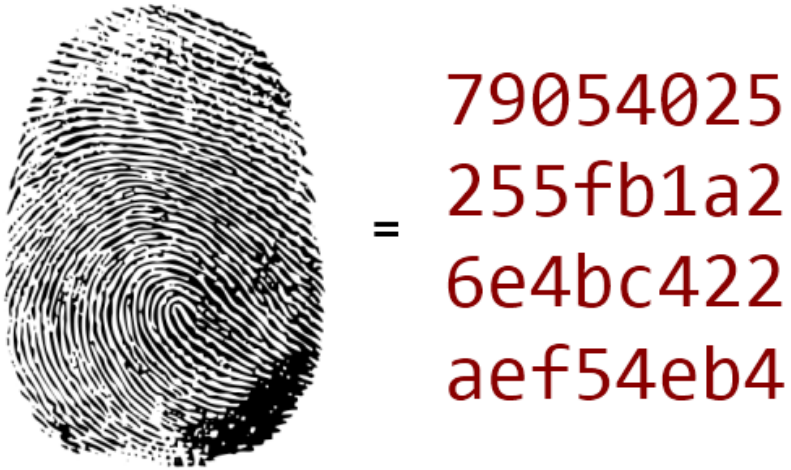

Figura 4: Algoritmos matemáticos geram a identificação única de qualquer arquivo digital.
Fonte: Disponível em: <https://blog.codinghorror.com/speed-hashing/>. Acesso em: 23 mar. 2017.

O *hash* é um importante método para rastrear informações criminosas na rede mundial de computadores, principalmente as imagens de pornografia infantil. Importantes operações da Polícia Federal foram deflagradas e permitiram localizar e identificar pedófilos que compartilhavam esse tipo de material na Internet.

9 A lavagem de dinheiro via *Bitcoins*

Transferir o dinheiro ilícito entre vários países como esquema simples de lavagem de dinheiro passa a ser um método antiquado no mundo obscuro da tecnologia.

Conforme explica ULRICH (2014), *Bitcoin* é uma moeda digital descentralizada, que permite efetuar transações financeiras sem intermediários, sem taxas, em qualquer parte do planeta, sem criar limites ou requisitos atrelados ao possuidor da moeda.

A principal característica do *Bitcoin* é a possibilidade de proteger a identidade do seu dono. Diferente da lavagem de dinheiro tradicional, que deixa rastros por onde as autoridades perseguem os criminosos, quando falamos em moedas digitais, temos interessados na aquisição de moeda procurando *sites* de câmbio que transformam o dinheiro ilícito em moeda legal, visto que o *Bitcoin* não tem meios de fiscalização ou supervisão por qualquer órgão regulamentador.

Após a aquisição dos *Bitcoins*, o dinheiro pode ser reinjetado em novas transações legais, sem qualquer suspeita de sua origem.

10 Internet das Coisas: trazendo o inimigo para dentro de casa

Conectar à Internet dispositivos eletrônicos utilizados no dia a dia parecia ser uma realidade distante há alguns anos. No entanto, hoje, muitos usuários podem otimizar e reduzir recursos valendo-se desta tecnologia.

Grandes empresas automobilísticas já desenvolvem tecnologias em câmeras e sensores que, instalados dentro dos carros, permitirão reconhecer o rosto do motorista, fornecer informações do cotidiano, além de recomendar músicas e acionar o Mapa GPS.

A linha branca dos produtos eletrodomésticos já anunciou a geladeira inteligente, que escaneia o que tem dentro e envia uma lista de compras para seu celular.

O que aconteceria se um criminoso conseguisse controlar o motor e o freio de um carro conectado à Internet?

E se um eletrodoméstico com falha de configuração se tornasse um meio favorável para disseminar *spams*[11] para outros usuários?

[11] Mensagens não solicitadas, comumente enviadas para um grande número de pessoas.

Um estudo da Hewlett Packard Enterprise (HPE, 2014) mostrou que 70% (setenta por cento) dos aparelhos ligados à Internet das Coisas têm falhas graves de segurança e estão sujeitos a ataques de criminosos. Problemas de privacidade e *softwares* inadequados também engrossam a fila dos novos desafios que as autoridades enfrentarão à medida que cada vez mais a Internet passa a fazer parte da vida das pessoas.

Só a união da indústria e dos fabricantes para trabalhar em um protocolo de segurança, bem como o uso de códigos abertos que permitam a detecção e correção dessas vulnerabilidades, poderá oferecer produtos mais seguros e confiáveis para serem usados na Internet das Coisas.

11 Conclusão

Outros desafios permeiam as investigações de crimes cibernéticos: os conceitos de Metadados, o aumento da capacidade de armazenamento e processamento dos equipamentos, milhares de novos aplicativos lançados diariamente, além da computação em nuvem e o Big Data[12].

As ferramentas atuais de investigação trabalham de maneira eficiente para buscar evidências em computadores. Listam as informações e filtram os dados baseados em campos específicos. Mas a tecnologia avança a cada minuto; consequentemente, as ferramentas que combatem os crimes precisam avançar.

Não será mais suficiente localizar a evidência de um crime. As novas ferramentas deverão criar novos padrões de pesquisa em ambientes gigantescos de informação. Modelos alternativos de análise deverão ser criados: a inteligência artificial poderá não só analisar perfis criminosos e auxiliar na identificação destes, mas atuar na prevenção de crimes e na proteção de vítimas.

[12] Termo usado para descrever um volume imenso de dados, que podem estar organizados ou não.

A educação será essencial: as crianças deverão saber usar a tecnologia desde pequenas. Além disso, investimentos deverão ser feitos para formar especialistas de segurança que possam atuar em situações críticas.

Os magistrados deverão conhecer o mínimo destes novos desafios tecnológicos para não ficarem à mercê de opiniões de advogados, promotores ou peritos, quando precisarem comprovar um delito.

Só assim a tecnologia será uma aliada da lei.

Referências bibliográficas

FREENET. Disponível em: <http://freenetproject.org>. Acesso em: 23 mar. 2017.

HPE. *HP IoT Research Study*. Disponível em: <https://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.U9exjfldXtt>. Acesso em: 14 dez. 2016.

HPE Security Research Cyber Risk Report 2016. Disponível em: <http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/>. Acesso em: 24 fev. 2017.

I2P. *The Invisible Internet Project*. Disponível em: <https://geti2p.net/en>. Acesso em: 22 fev. 2017.

MERCÊS, Fernando. *The Brazilian Underground Market.* Disponível em: <http://www.trendmicro.de/media/wp/the-brazilian-underground-market-wp-en.pdf>. Acesso em: 15 dez. 2016.

MICROSOFT Digital Crimes Unit. Palestra realizada por Andrés Rengifo, DCU Lead Latam. MPF/SP, dez. 2015.

SAFERNET. *Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos*. Disponível em: <http://indicadores.safernet.org.br/>. Acesso em: 10 fev. 2017.

SINGH, Simon. *O livro dos códigos*. São Paulo: Record, 2010.

TOR Project. Disponível em: <https://www.torproject.org/>. Acesso em: 13 jul. 2011.

TOZETTO, Claudia. *Cibercrime faz bancos perderem 1,8 bilhão*. Disponível em: <http://link.estadao.com.br/noticias/cultura-digital,cibercrime-faz-bancos-perderem-r-18-bilhao,10000028721>. Acesso em: 28 fev. 2017.

ULRICH, Fernando. *Bitcoin:* a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

Perícia de informática nos crimes cibernéticos

Márcio Rodrigo de Freitas Carneiro*

RESUMO

Neste artigo são explicados, de maneira breve, alguns dos procedimentos da perícia de informática, especificamente na realização dos exames de mídias de armazenamento digital, tanto em ações criminais, fora do mundo digital, como nos crimes cibernéticos.

Palavras-chave: Perícia. Computação. Cibernético. Federal. Criminal.

ABSTRACT

In this article, we briefly explain some of the computer forensic procedures, specially when examining digital storage devices, both in criminal offenses out the digital world as well as in cybercrimes.

***Keywords**: Forensic expertise. Computing. Cybernetic. Federal. Criminal.*

* Bacharel em Ciência da Computação pela Universidade de São Paulo. Perito Criminal Federal da Polícia Federal. *E-mail*: marcio.mrfc@dpf.gov.br.

1 Introdução

Nos processos criminais, é de suma importância a realização de exames periciais nos vestígios deixados por infrações e, consequentemente, a elaboração dos laudos assinados por peritos oficiais. Conforme o art. 5º da Lei n.º 12.030/2009, os peritos oficiais são os peritos criminais, médico-legistas e odontolegistas, cargos que compõem as polícias judiciárias ou órgãos com estrutura apartada, conforme legislação específica. Na esfera federal, os Peritos Criminais Federais (PCFs) compõem o quadro de cargos da Polícia Federal (PF).

No início dos anos 2000, houve um crescimento repentino na demanda pelas perícias de informática na PF, causado pela utilização de um maior número de computadores nas empresas e residências, bem como pelo aumento na deflagração de grandes operações. Em resposta, o quantitativo de PCFs com formação na área de informática aumentou, gradualmente, de 10 (dez) para 150 (cento e cinquenta) em pouco mais de dez anos. Mesmo assim, o efetivo ainda é insuficiente para soluções mais rápidas à grande demanda da Justiça.

Como se pode observar no gráfico 1, a apreensão de computadores e discos rígidos percebeu uma variação considerável dentro do período de dez anos. Melhorias nos procedimentos de busca e apreensão, bem como maior interação entre os cargos da PF, incluindo-se os PCFs de informática, podem explicar uma redução momentânea entre 2012 e 2014 na apreensão de itens que trazem grande volume de dados. Concomitantemente, a capacidade dos computadores e dispositivos de armazenamento só tem aumentado, mantendo o desafio do grande volume de dados a ser examinado todos os anos. Outro desafio que se torna evidente no gráfico são os dispositivos móveis, tais como celulares e *tablets*, cuja entrada dobrou nos últimos dois anos. O assunto será abordado posteriormente.

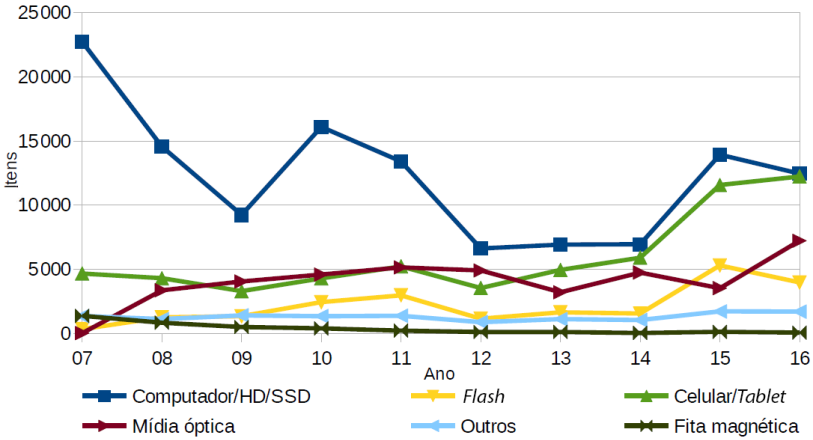

Gráfico 1: Entrada de material de informática por ano na perícia da PF, contabilização nacional.

Fonte: Gráfico elaborado pelo Autor a partir de dados do Sistema de Criminalística da Polícia Federal.

Graças ao desenvolvimento de interfaces mais intuitivas e simples para o usuário, bem como à popularização do acesso à Internet, os computadores (incluindo-se aqui os *smartphones* e *tablets*) tornaram-se ubíquos. Entretanto, pelo mesmo motivo da boa interface, a compreensão do funcionamento interno dessas máquinas torna-se desnecessária à maioria das pessoas. Mas, para as partes envolvidas num processo criminal, há que se compreender, em certo grau, alguns conceitos e procedimentos para melhor entendimento dos laudos periciais criminais de informática. A seguir, elaboram-se, no âmbito da Criminalística da PF, esses conceitos e procedimentos, sem prejuízo à sua aplicação nas esferas estaduais.

2 Crimes cibernéticos e perícias de informática

A perícia de informática é importante para praticamente todo tipo de investigação, haja vista a ubiquidade dos computadores citada anteriormente. Entretanto, para aqueles crimes cujos vestígios principais não são digitais, normalmente os vestígios

deixados em computadores e mídias de armazenamento não se tornam evidência do crime, mas sim indícios que auxiliam na investigação. Por exemplo, em crimes financeiros ou de tráfico de entorpecentes, mensagens de correio eletrônico, documentos digitais, entre outros elementos, são analisados pelos policiais dedicados ao caso para trazer informações e fatos circunstanciais que orientem o curso da investigação, bem como a obtenção de outros vestígios e, possivelmente, provas.

Para esses crimes, portanto, a perícia de informática realiza uma extração dos dados dos computadores e mídias, sempre que possível aplicando filtros objetivos para o contexto desejado. Pela limitação de efetivo e pelo desconhecimento do perito sobre o assunto, cabe aos policiais da investigação, bem como às partes durante o processo criminal, analisar efetivamente o conteúdo do material questionado.

Diferentemente, as investigações de crimes cibernéticos demandam a perícia de informática com vestígios efetivamente deixados pela ação criminosa. Os computadores e mídias, nesses casos, contêm arquivos, registros de sistema, entre outras informações, que são evidências do crime e podem servir de prova material. O exame pericial e o laudo produzido servirão de esclarecimento e convencimento para o juízo sobre o conteúdo ilícito, tal como sobre o meio e método utilizados para se cometer o crime denunciado.

3 Coleta de vestígios digitais

Computadores e outros dispositivos digitais armazenam dados que podem sustentar ou refutar um determinado crime, ou ainda apenas fornecer suporte para uma investigação. No contexto dos crimes cibernéticos, esses vestígios digitais tornar-se-ão evidências digitais que são essenciais para a comprovação da materialidade do crime, assim como, se possível, sua autoria.

No percurso de uma investigação de crime cibernético, após a identificação do endereço do imóvel do qual partiram os acessos à Internet identificados como ação criminosa, ou mesmo após a identificação de localidades por outras maneiras, cumprem-se os mandados de busca e apreensão (MBAs) emitidos pelos juízos competentes. O objetivo principal das buscas e apreensões, nesse contexto, é a coleta de vestígios digitais, além de quaisquer outros vestígios que possam esclarecer os fatos.

Apesar de o cumprimento de MBAs não requerer a presença de perito criminal, historicamente a perícia na PF tem um papel importante na capacitação técnica da equipe. De maneira geral, os procedimentos realizados na busca são:

a) Após convocação de testemunhas, ciência do morador ou responsável e entrada no imóvel, a equipe foca na busca por equipamentos que possam conter vestígios digitais. Esses itens são, não exaustivamente, computadores, *notebooks*, *smartphones*, *tablets*, dispositivos de armazenamento, tais como discos rígidos, discos de estado sólido ou *solid state drives* (SSDs), cartões de memória (normalmente utilizados em celulares e máquinas fotográficas digitais), memórias *flash* conhecidas como *pen drive* e mídias ópticas graváveis (CD-R, DVD-R, etc.). Desprezam-se assim mídias ópticas impressas, que normalmente contêm produtos comerciais.

b) Faz-se avaliação do conteúdo do material encontrado *in loco*, somente quando houver condições técnicas e táticas, com a utilização do *software* Localizador de Evidências Digitais (LED), desenvolvido pelo PCF Wladimir Leite, no Núcleo de Criminalística (Nucrim) do Setor Técnico Científico (Setec) da Superintendência de Polícia Federal em São Paulo. Essa avaliação será explanada na seção 3.1.

c) Faz-se a arrecadação ou apreensão do material que não foi excluído pela avaliação de conteúdo, com descrição detalhada dos materiais. Efetua-se uma explanação do procedimento executado para avaliação do conteúdo das mídias digitais, seja no auto circunstanciado da busca, seja em documento apartado. Em alguns

crimes, como dispõe o art. 241-B da Lei n.º 8.069/90, que trata da posse de material contendo cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, esse documento formaliza os procedimentos realizados na busca que trouxeram convicção à equipe e às testemunhas para a prisão em flagrante, se identificado o proprietário daquele material.

Cumpre ressaltar que, para a realização de uma busca com maior efetividade e qualidade, é importante o fornecimento de dados e informações sobre o investigado, tais como *usernames,* GUIDs*,* endereços de *e-mail* e outros identificadores do possível autor do delito, números de endereço IP, tanto de origem quanto de destino, que possibilitaram a emissão daquele MBA, dentre outros. Por vezes, a única informação que chega à equipe de busca vem do próprio MBA, e a equipe pode não ter conhecimento da investigação em curso.

Quando houver necessidade de delimitar o escopo da busca no documento do mandado, devem-se evitar restrições demasiadas como:

a) A determinação de que participe PCF na busca, haja vista que as atividades no local podem seguramente ser feitas por policiais treinados e a quantidade de peritos ainda é muito aquém do desejado para a demanda de exames periciais.

b) A determinação de que só seja apreendido material que contenha dados relacionados ao crime. Em muitas situações, não há condições táticas ou técnicas para realizar a avaliação do conteúdo das mídias, ou as limitações na avaliação de todo conteúdo e outros indícios que não estejam na mídia podem convencer a equipe de que se deve arrecadar o material que posteriormente será escrutinado no exame pericial.

3.1 Avaliação na busca e o Localizador de Evidências Digitais (LED)

Dada a intensa participação dos PCFs de informática em equipes de busca e apreensão referentes a crimes cibernéticos, o PCF Wladimir Leite, lotado no Nucrim/Setec/SR/PF/SP, desenvolveu uma ferramenta para agilizar a busca por arquivos de conteúdo ilícito, especificamente no contexto da pornografia infantil.

O processamento completo e detalhado das mídias de armazenamento digitais requer ferramentas dedicadas que normalmente tomam tempo considerável, portanto inviável de ser realizado no local de busca. Ao mesmo tempo, confiar apenas na navegação direta das pastas e arquivos da mídia suspeita deve ser o último recurso utilizado, por ser limitado e bastante sujeito a falhas.

Ainda que possa ser configurado para utilização em outros tipos de crime, a título de exemplo, para os locais de busca referentes à pornografia infantil, o LED executa:

a) Busca por arquivos conhecidos de uma base de dados da perícia, baseando-se no cálculo de uma função de *hash*[1] dos arquivos.

b) Busca por palavras tipicamente encontradas em nomes de arquivos, relacionadas ao tipo de crime ou ao caso.

c) Busca por palavras em arquivos de textos e de configuração dos programas mais utilizados para compartilhamento de arquivos na Internet.

d) Processamento de vídeos para geração de imagens contendo alguns quadros do vídeo, para rápida visualização.

e) Processamento dos arquivos de registro do sistema operacional Microsoft Windows, para obtenção de informações que podem ser úteis à avaliação do material no local de busca.

[1] Em computação, funções de *hash* são utilizadas para calcular um número de tamanho limitado, normalmente de 128 *bits* a 2 048 *bits* (16 a 256 *bytes*), a partir de qualquer arquivo de tamanho livre. Trata-se de uma função unidirecional, ou seja, não é possível deduzir o conteúdo do arquivo a partir do *hash*. No contexto das perícias, os *hashes* são úteis para a comparação rápida de arquivos e também para a autenticação de uma lista de arquivos (em cópias, relatórios e afins), pois qualquer alteração no conteúdo de um arquivo muda drasticamente o valor equivalente de seu *hash*. Também por isso costuma-se chamar o *hash* de "assinatura do arquivo".

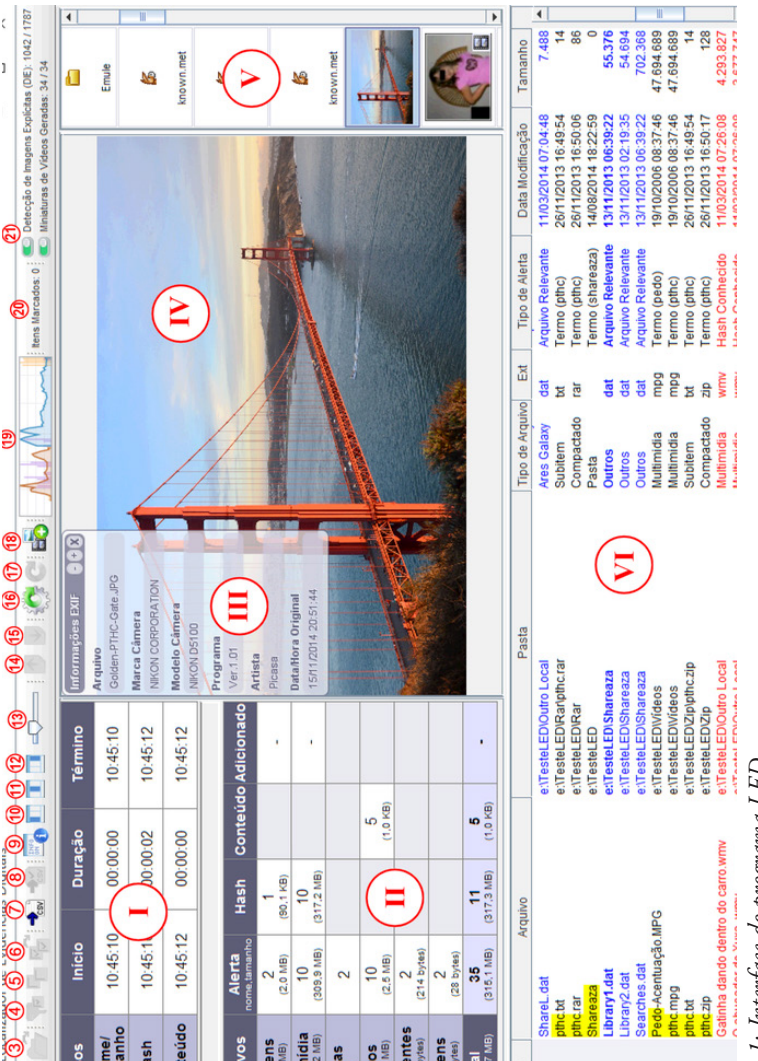

Figura 1: Interface do programa LED.
Fonte: Figura elaborada pelos Peritos Criminais Federais (PCFs).

Na figura 1 pode-se ver a tela de utilização do LED. Durante o processamento da mídia (ou de alguma pasta diretamente especificada), a seção I mostra o progresso e o tempo estimado de término. A seção II mostra a quantidade de arquivos em categorias de alerta, que indicam nomes ou tamanhos suspeitos, bem como a categoria *hash*, que indica arquivos presentes na base de dados de *hashes* utilizada pelo programa, e a categoria conteúdo, que indica arquivos cujo texto contém palavras configuradas para a busca. As seções III e IV mostram o conteúdo do arquivo. No exemplo da figura, a seção III mostra o conteúdo Exif (metadados gravados normalmente pela máquina fotográfica ou celular) encontrado dentro da foto. A seção V é composta de uma galeria de miniaturas das imagens, para rápida visualização. Já a seção VI lista os arquivos com indicação de tipo de alerta resultante do processamento, trecho suspeito do nome do arquivo em destaque amarelo, e arquivos cujo *hash* foi encontrado na base de dados na cor vermelha.

O menu superior ainda contém diversas funcionalidades de uso da interface, mas vale ressaltar os dois botões identificados com o número 21 que permitem a geração de miniaturas dos vídeos encontrados, para rápida visualização no local sem a necessidade de reproduzir individualmente cada arquivo, bem como a função de "Detecção de Imagens Explícitas (DIE)". A função DIE classifica as imagens encontradas num sistema de pontuação de 0 a 1 000, pelo uso de um algoritmo de *machine learning*, cujo treinamento foi realizado com mais de 500 mil imagens, sendo metade de pornografia infantil e metade não ilícitas. Essa classificação permite ordenar as imagens para agilizar a visualização de arquivos na busca por pornografia infantil.

3.2 Acesso às mídias suspeitas

Durante a busca, a avaliação de conteúdo das mídias pode ser realizada conectando-se a mídia suspeita em *notebook* preparado para o acesso às mídias externas, de modo que se minimizem os riscos de haver qualquer modificação dos dados presentes no

material questionado. É possível configurar os sistemas operacionais mais comuns, tais quais Microsoft Windows, distribuições diversas de Linux e Apple macOS, para que não haja escrita em mídias conectadas nas portas USB dos computadores. Também é possível utilizar equipamentos dedicados, que bloqueiem a escrita independentemente do computador utilizado.

Além das opções específicas citadas acima, também é possível utilizar mídias ópticas ou *pen drives* contendo sistemas Linux e que possam ser usados para iniciar um computador como seu sistema operacional. A perícia da PF tem se utilizado da distribuição C.A.IN.E (*Computer Aided Investigative Environment*), dedicada à computação forense, com a inclusão dos aplicativos LED e IPED, para treinamento e uso pelos policiais que executarão as avaliações de conteúdo em local de busca e apreensão. Na maior parte dos casos, é possível iniciar o computador suspeito pela mídia óptica ou pelo *pen drive*, e assim avaliar o conteúdo da mídia de armazenamento sem riscos de alteração, dentro das limitações técnicas de tempo e das condições táticas e logísticas impostas pelo local.

3.3 Aquisição de dados

Em alguns casos, incluindo investigações de crimes cibernéticos, é inviável a apreensão da mídia de armazenamento na qual se encontram os vestígios. Situações diversas, tais como dados armazenados em grandes servidores de empresas, interesse em registros de acesso de operadoras de telecomunicações ou mesmo de grandes corporações, ou ainda dados apenas acessíveis na nuvem, em serviços de armazenamento remoto sem algum indício de cópia local, não permitem apreensão de apenas um disco rígido ou mesmo um pequeno dispositivo contendo mídias de armazenamento.

Nessas situações, faz-se necessária a cópia dos dados de interesse para a investigação e posterior apreensão da mídia digital

destinatária daquele conteúdo. É importante descrever todo o procedimento, registrar o nome das pessoas envolvidas no apoio técnico e responsáveis legais, bem como, se possível, gerar os *hashes* dos arquivos copiados. O uso de embalagens de segurança numeradas, ou mesmo lacres para fechamento de embalagens comuns, é mais uma garantia da origem daqueles vestígios digitais, incluindo a formalização de todo o processo em auto de apreensão.

4 Cópia e preservação dos vestígios

Antes do processamento do conteúdo de uma mídia de armazenamento, deve-se copiá-la integralmente para outro suporte, para garantir a preservação da mídia original contra gravações indevidas e também o acesso aos dados em caso de possível falha da mídia. Utilizam-se ferramentas dedicadas à cópia forense, tais como "dcfldd", "FTK Imager" e "*ewfacquire*", com as quais se cria um arquivo em uma área de grande capacidade de armazenamento no computador do perito, ou em uma área de armazenamento na rede local. Esse arquivo contém os mesmos dados, sequencialmente e de forma integral, da mídia questionada. As ferramentas podem gerar números de *hashes* para trechos de tamanho determinado pelo perito, para posterior verificação da integridade dos dados copiados. O processo todo costuma ser chamado de "fazer uma imagem da mídia" ou "espelhar a mídia".

O procedimento descrito também é utilizado para fornecer cópia do material para a parte, normalmente após autorização judicial. Importante ressaltar que o local de destino da imagem forense da mídia deve ter espaço igual ou maior que a mídia original. É possível utilizar algoritmos de compressão para tentar diminuir o tamanho do arquivo destino, entretanto não é possível garantir uma eficiência mínima da compressão. Caso a mídia original esteja repleta de vídeos e imagens, por exemplo, que normalmente já são arquivos comprimidos, uma nova compressão não terá efeito.

5 Processamento dos vestígios

Dentre as ferramentas comerciais disponíveis para o processamento de mídias e imagens forenses, tais como AccessData FTK, Guidance EnCase, X-Ways Forensics, a primeira era a mais utilizada pela perícia da PF pelas funcionalidades disponíveis. Entretanto, há dois anos, o PCF Luis Nassif iniciou o desenvolvimento de uma ferramenta que facilitasse a visualização das mídias ópticas, as quais são parte integrante dos laudos de informática. O *software* evoluiu para uma ferramenta completa de processamento forense, chamada IPED (Indexador e Processador de Evidências Digitais), que utiliza outros programas de código aberto, tais como Sleuth Kit, Apache Tika, entre outras bibliotecas, processando os principais sistemas de arquivos encontrados nos computadores. O Microsoft NTFS é o mais comum nos dias de hoje. A ferramenta tem as seguintes funcionalidades, que, de certa maneira, refletem os principais passos dos exames realizados em mídias digitais:

a) **Cálculo de *hash* e consulta a bases de *hashes***: calcula os principais tipos de *hash* utilizados, tais como MD5, SHA-1, SHA-256, e-Donkey, etc.; pode utilizar bases de *hashes* para alertar a presença de arquivos conhecidos ou ignorar arquivos comuns de sistema.

b) **Categorização e indexação**: categorização dos arquivos baseada principalmente nos formatos comumente utilizados, bem como indexação dos textos extraídos de dezenas de tipos de arquivos.

c) **Galeria de imagens e vídeos**: disponibilização de miniaturas das imagens e seleção de quadros dos vídeos para agilizar a visualização e análise.

d) **Arquivos apagados e *data carving***: recuperação de arquivos apagados do sistema, que pode ainda conter referências das remoções, assim como extração de arquivos em espaços não alocados no disco, arquivos de sistema como *pagefile*, entre outros de *cache* (armazenagem temporária), para diversos tipos de arquivos.

e) **Detecção de imagens explícitas**: implementada pelo PCF Wladimir, em seu programa LED, é também utilizada no IPED para categorização de imagens possivelmente contendo pornografia, para auxílio dos exames de pornografia infantil.

f) **Visualização integrada**: é possível visualizar dezenas de tipos de arquivos integradamente ao programa, para agilidade e independência do sistema. Também se pode visualizar o conteúdo hexadecimal, útil para análise de alguns tipos de arquivos, bem como texto puro extraído do arquivo, se presente.

g) **Marcação de itens e geração de relatórios**: permite a marcação dos itens, a criação de categorias, a geração de relatórios com a exportação dos arquivos e a inclusão do próprio IPED para rápida visualização do conteúdo extraído, com busca por palavras-chave e galeria de imagens.

Outros peritos ajudam na implementação de funcionalidades específicas e na resolução de problemas do IPED, o que torna a ferramenta bastante dinâmica e moderna, quando comparada com outras opções. Na figura 2, pode-se ver uma tela da interface de uso do IPED.

Certamente uma ferramenta única não atende a todas as demandas dos peritos de informática. Sempre que necessário, a imagem forense ou os arquivos extraídos dela podem ser processados separadamente por outras ferramentas específicas. Os resultados obtidos podem ser adicionados ao caso processado no IPED. Também, se necessário e viável, ferramentas externas podem ser integradas ao IPED, para automatização dos passos executados pelo perito.

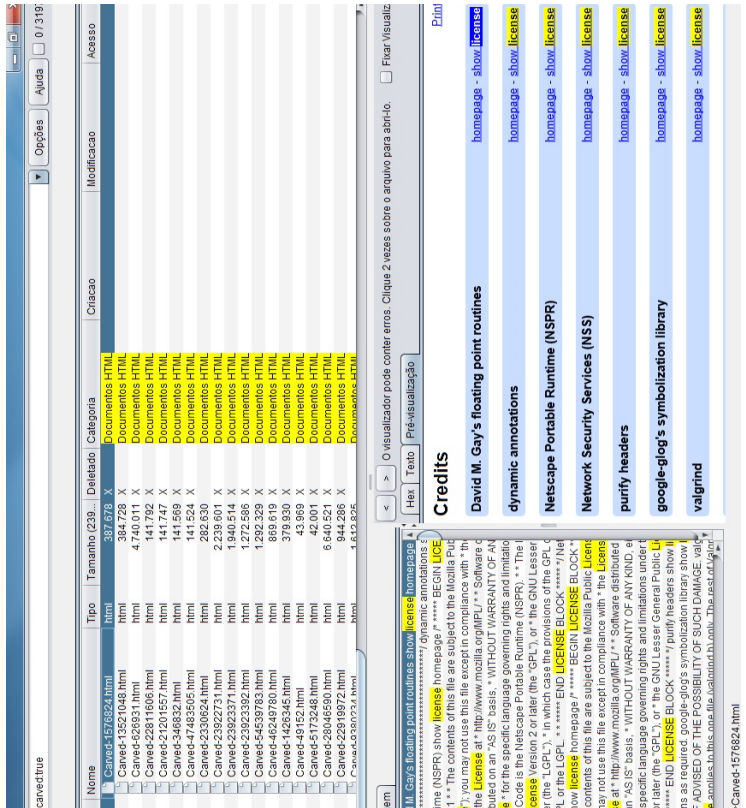

Figura 2: Interface de análise do IPED.
Fonte: Figura elaborada pelos PCFs.

5.1 Vestígios digitais em crimes cibernéticos

Em outros tipos de investigações, nas quais os computadores normalmente não contêm evidências digitais de materialidade e/ou autoria, mas sim indícios ou dados correlatos aos fatos investigados, a extração ampla dos dados para posterior análise é a principal demanda à perícia de informática. Já nos crimes cibernéticos, o contrário disso é regra, e espera-se que a perícia traga luz às evidências digitais e a prova material para o processo criminal.

Cada tipo de crime cibernético pode trazer desafios específicos ao perito, como mostram os exemplos a seguir.

5.1.1 Clonagem de cartões

Nos computadores e mídias apreendidos no combate à clonagem de cartões, principalmente nos computadores de investigados mais atuantes na obtenção de dados e na utilização dos números clonados, é praxe a pesquisa por expressões que remetam a arquivos contendo dados em formatos típicos, lidos da tarja magnética do cartão.

Dependendo do grupo investigado, pode-se pesquisar por programas indevidamente instalados em terminais de transação eletrônica de lojas, ou programas conhecidos como *malwares*, enviados por *e-mail* ou outros métodos de mala direta, na tentativa de "infectar" computadores alheios para obtenção de dados bancários. Há, ainda, aplicativos utilizados para gravação e impressão de cartões de tarja magnética.

Finalmente, também se podem obter outros indícios importantes para a investigação e o processo criminal, tais como mensagens de correio eletrônico, mensagens de comunicação instantânea, histórico do navegador e outros tipos de documentos.

5.1.2 Pornografia envolvendo crianças ou adolescentes

Nos exames periciais de informática em mídias de armazenamento e computadores apreendidos em locais de busca

relacionados a investigações de pornografia infantil, cabe ao perito extrair arquivos que possam conter cenas de nudez ou sexo envolvendo crianças ou adolescentes, além de verificar o compartilhamento dos arquivos e a utilização de aplicativos que permitam transmitir dados pela Internet. O primeiro objetivo do perito é encontrar as imagens e vídeos cujo conteúdo seja claramente ilegal. A busca por *hashes* conhecidos, além da utilização da função de Detecção de Imagens Explícitas do IPED, auxilia o perito na classificação das imagens que devem ser consideradas armazenamento de pornografia infantil.

Posteriormente, buscam-se evidências que possam confirmar o compartilhamento de parte ou de todos esses arquivos, seja com a utilização de programas de compartilhamento de arquivos ponto a ponto, tais como eDonkey, eMule, Shareaza, entre outros, seja por mensageiros instantâneos, correio eletrônico ou sítios na *www*. Também se utilizam ferramentas que busquem palavras-chave normalmente utilizadas pelos criminosos, como "pthc" (*Pre Teen HardCore*), "*teen*", "*pedo*", entre outras. Além disso, procuram-se outros registros que indiquem o comportamento do usuário, bem como conversas com outros criminosos em diversos tipos de programas mensageiros.

Vale ressaltar que a comprovação do efetivo compartilhamento de arquivos nem sempre é viável, mas evidências digitais no computador, tais como arquivos idênticos aos encontrados nas investigações, disponíveis em pastas compartilhadas pelos programas de troca utilizados, corroboram as ações de compartilhamento investigadas anteriormente e que levaram àquela busca e apreensão.

Outro ponto a destacar é o critério de classificação do conteúdo como ilegal ou não. A seleção desses arquivos, feita no exame de informática, tem apenas o intuito de reduzir o volume de dados a ser visto pelos operadores do Direito no processo e facilitar a compreensão do laudo. Não se trata de fato de uma avaliação técnica. Considerando uma grande quantidade de arquivos, é possível destacar imagens e vídeos nitidamente contendo crianças,

bem como descartar material que apenas contém claramente adultos. Entretanto, há cenas nas quais é inviável determinar se os indivíduos são adolescentes ou jovens adultos. Nos exames periciais, esses arquivos duvidosos podem eventualmente ser adicionados ao laudo com ressalvas, por não se tratar de conteúdo claramente infantojuvenil. Nesses casos, resta somente a tentativa de localizar os indivíduos retratados, para a verificação da idade deles à época da realização das fotografias ou vídeos.

Finalmente, pode ser necessária, em alguns casos, a utilização de técnicas adequadas de amostragem, para a contabilização das imagens de nudez ou sexo envolvendo crianças ou adolescentes num conjunto demasiadamente grande de arquivos de pornografia. Considerando que a lei não quantifica o crime, a análise do comportamento do usuário do computador, com as diversas evidências digitais, bem como a confirmação de posse ou provável compartilhamento de um número expressivo de arquivos de pornografia infantil, forma a prova material que traz convicção sobre o crime ao processo.

6 Aparelhos celulares, *smartphones* e *tablets*

Os equipamentos portáteis, hoje utilizados em massa, tais como celulares, *smartphones* e *tablets*, são, na prática, computadores compactados na palma da mão. Como vimos no gráfico 1, houve um grande salto na entrada desses equipamentos na perícia, nos últimos dois anos, o que mostra que cada vez mais pessoas carregam um aparelho portátil consigo e, portanto, cada vez mais são apreendidas em investigações e procedimentos criminais.

Apesar de se tratar de computadores, algumas particularidades nesses itens trazem dificuldades à perícia:

a) Comumente, utilizam-se senhas de bloqueio ao aparelho, que por padrão bloqueiam automaticamente em pouco tempo de inatividade do equipamento. São muitos os modelos que impossibilitam o acesso aos dados sem a senha e não há métodos de

quebra conhecidos. Por isso, é importante que a equipe, durante o mandado de busca ou na prisão em flagrante, consiga obter a senha diretamente com o proprietário do dispositivo.

b) O acesso à mídia de armazenamento interno não é simples e direto como nos computadores e *notebooks*. As memórias *flash* internas aos celulares são soldadas ao circuito impresso do aparelho, e todo acesso é limitado à porta USB de comunicação. Utilizando-se de equipamentos dedicados, como o Cellebrite UFED, pode-se realizar a extração de dados do sistema instalado (a grande maioria, hoje, utiliza sistema Android ou iOS); ou ainda, em alguns casos, realizar o que é chamado de extração física, que se assemelha ao espelhamento de uma mídia de armazenamento. Posteriormente, esse arquivo extraído poderá ser analisado com o próprio *software* da Cellebrite ou ainda com o IPED.

c) Alguns aplicativos criptografam os dados com chaves armazenadas em áreas especiais do sistema operacional, que só podem ser acessadas alterando o dispositivo, de um modo impossível ao usuário normal, com credenciais de administrador do sistema (vulgo "*root*", de onde vem a expressão "rootar o aparelho"). Essas condições trazem nova luz aos procedimentos periciais, que anteriormente evitavam a qualquer custo alterações aos vestígios digitais. Nesses casos, deve-se documentar todo o procedimento realizado, mesmo que minimamente invasivo, para embasamento da obtenção das evidências digitais.

Dada a quantidade de marcas e modelos disponíveis no mercado, bem como a variedade de configurações tanto dos sistemas instalados como das maneiras de acesso aos dados internos, os equipamentos portáteis constituem enorme desafio aos fabricantes de extratores de dados, bem como à perícia, que, em determinados casos, pode ver esgotadas as alternativas de acesso aos dados, quando certa versão de sistema ou de *software* não é suportada pelos equipamentos e técnicas forenses disponíveis.

7 Conclusão

Como se pode verificar, a perícia de informática enfrenta constantemente o problema da demanda excessiva, frente a um diminuto quadro de peritos formados na área. Paralelamente, os procedimentos envolvidos nos exames de informática são extensos e, adicionalmente, mais complexos e demorados quando a análise minuciosa das mídias é imprescindível, como nos casos em que os vestígios digitais são essenciais à comprovação do crime. Também, quesitos pouco objetivos, ou que tragam conjecturas vagas demais, atrasam o exame e podem diminuir a clareza do laudo.

Cada vez mais se faz necessária a capacitação dos policiais de todos os cargos para melhor conhecimento de conceitos de informática, bem como dos procedimentos a serem realizados em investigações e buscas e apreensões. Deve-se reduzir o volume de computadores, mídias e telefones apreendidos, sem que isso cause prejuízo para o caso ou operação, e assim trazer mais foco nos alvos específicos e concisão ao volume de dados trazido à perícia.

No curso de uma operação ou investigação, em especial nos crimes que não ocorrem realmente em ações cibernéticas, a perícia de informática tem um papel importante na extração e disponibilização dos dados, com aplicação de alguns filtros objetivos, para que sejam analisados pelo corpo de policiais com conhecimento aprofundado dos fatos e elementos envolvidos nas ações criminosas. Esses exames normalmente são requeridos em milhares de mídias e computadores, nacionalmente, e espera-se rápida resposta para continuidade das investigações.

Já nas investigações de crimes cibernéticos, como aqueles envolvendo pornografia infantil, a perícia tem um papel crucial mais ao fim da investigação, com o exame minucioso dos vestígios eletrônicos, que trarão as evidências digitais e serão formalizados como prova material, se possível de autoria do delito. São exames pontuais, o mais normal é que sejam realizados em poucas mídias apreendidas de um indivíduo, mas que muitas vezes requerem

urgência por tratar-se de investigado preso. A utilização de técnicas de amostragem para avaliação de quantidades demasiadamente grandes de arquivos de pornografia não pode ser descartada para viabilização dos exames em tempo hábil.

Os desafios de novas tecnologias, como os equipamentos portáteis, tais como celulares, *smartphones* e *tablets*, podem causar, em um certo momento, um gargalo na capacidade de atendimento da perícia. Entretanto, o desenvolvimento e a compra de novas ferramentas, bem como a capacitação de todos os policiais, inclusive os peritos, trarão sem dúvida soluções para responder de modo satisfatório à demanda.

Finalmente, considerando o desafio constante do aumento do volume de dados, da complexidade dos dispositivos apreendidos e da conhecida escassez de recursos humanos do Poder Executivo, há que se esperar compreensão da Justiça, da defesa e da acusação, para que os limitados recursos da polícia judiciária sejam usados com parcimônia, melhorando, assim, a resposta que todo o sistema persecutório dá à sociedade.

Referências bibliográficas

CASEY, Eoghan. *Digital Evidence and Computer Crime*: Forensic Science, Computers, and the Internet. 3rd. ed. Academic Press, 2011.

VELHO, Jesus Antonio (Org). *Tratado de computação forense.* Campinas: Millennium, 2016.

Obtenção de provas digitais e jurisdição na Internet

Fernanda Teixeira Souza Domingos*

Priscila Costa Schreiner Röder**

RESUMO

Este artigo pretende investigar a obtenção, pelos agentes de investigação no Brasil e no mundo, das provas digitais de delitos, sejam eles cibernéticos ou não, em poder de provedores de Internet, face às diferentes tecnologias que permitem o armazenamento dessas informações nos mais diferentes locais do planeta. Tal modalidade de crime desafia os tradicionais conceitos de soberania, territorialidade e jurisdição.

Palavras-chave: Jurisdição. Internet. Territorialidade. Provas. Digital.

ABSTRACT

This article intends to investigate possible solutions to difficulties faced, in Brazil and in the world, by law enforcement agents in obtaining cybercrime or real crime digital evidence from Internet providors, considering different technologies that allow this information to be

* Graduada pela Faculdade de Direito da Universidade de São Paulo. Procuradora da República em São Paulo, nas áreas cível e criminal. Coordenadora do Grupo de Combate aos Crimes Cibernéticos da Procuradoria da República em São Paulo e Vice-coordenadora do Grupo Nacional de Combate aos Crimes Cibernéticos da 2ª CCR/PGR. *E-mail*: fernandadomingos@mpf.mp.br.

** Graduada pela Faculdade de Direito da Universidade de São Paulo. Procuradora da República em São Paulo, nas áreas cível e criminal. Coordenadora Substituta do Grupo de Combate aos Crimes Cibernéticos da Procuradoria da República em São Paulo e Membro do Grupo Nacional de Combate aos Crimes Cibernéticos da 2ª CCR/PGR. *E-mail*: priscillaschreiner@mpf.mp.br.

stored in many different places in the world. This type of crime challenges the traditional concepts of sovereignty, territoriality and jurisdiction.

***Keywords**: Jurisdiction. Internet. Territoriality. Evidence. Digital.*

1 Introdução

O advento de novas tecnologias revolucionou a guarda e o armazenamento de documentos. A tecnologia digital possibilitou que quantidade imensa de informações pudesse ser trocada e passasse a ser armazenada, principalmente em face do incremento na comunicação e transações na comunidade global que migraram para o mundo digital, representando facilidade e rapidez para a mobilidade de dados.

Documentos virtuais passam a fazer parte das relações sociais, tanto com referência às transações reais quanto às transações plenamente virtuais. Acompanhando essa tendência, a investigação dos ilícitos do mundo atual depende de evidências digitais, independentemente de terem ocorrido, total ou parcialmente, no mundo real ou no mundo virtual.

Atualmente, a obtenção de provas digitais torna-se crucial para elucidar delitos, deparando-se esta questão, porém, com as diferentes jurisdições nas quais as evidências digitais estão armazenadas.

É de fato possível saber onde tais evidências se encontram armazenadas? É possível ater-se aos tradicionais conceitos de soberania e jurisdição quando as relações ocorreram na Internet? Qual a solução para as relações do mundo real, que dependem de evidências deixadas na Internet?

Pretendemos neste artigo debater as principais questões que afligem a elucidação de delitos que dependem da obtenção da prova digital produzida na Internet, bem como discorrer sobre algumas soluções existentes.

2 Soberania, jurisdição e territorialidade

Extremamente importante para a elucidação das questões acima propostas a definição e análise dos conceitos de soberania e jurisdição, pois estão intrinsecamente ligados às respostas encontra-

das na legislação pátria sobre o tema, que culminaram na redação do art. 11 da Lei n.º 12.965/2014, conhecida como Marco Civil da Internet (MCI), a ser comentada adiante.

Para DALLARI (2016), o conceito de soberania tem evoluído desde a Antiguidade, alcançando o auge, com as características que hoje conhecemos como um poder absoluto, perpétuo e inalienável, a partir do século XVI, com a obra *Les six livres de la République*, de Jean Bodin[1].

DALLARI explica que dentre os autores há diferentes concepções a respeito do *conceito de soberania*. Alguns se referem a ela como "poder do Estado"; outros, como "qualidade essencial do Estado"; e outros, ainda, como "a expressão da unidade de uma ordem". Porém, na síntese de todas as teorias, observa o autor que a noção de soberania está sempre ligada à concepção de poder, seja quando concebida em termos puramente políticos como *poder incontrastável de querer coercitivamente e verificar competências*, seja na evolução para uma concepção puramente jurídica, vista como o *poder de decidir em última instância sobre a atributividade das normas*, isto é, *sobre a eficácia do Direito*.

No entanto, considerando-se que o Estado compreende fenômenos sociais, jurídicos e políticos, o conceito de soberania para REALE (1960, p. 127) deve integrar todos eles, definindo-a assim como "o poder de organizar-se juridicamente e de fazer valer dentro do seu território a universalidade de suas decisões nos limites dos fins éticos de convivência".

A soberania possui como características o ato de ser *una* (inadmissível a convivência num mesmo Estado de duas soberanias), *indivisível* (aplica-se à universalidade dos atos ocorridos no Estado, sendo inadmissível a existência de partes separadas da mesma soberania), *inalienável* (seu detentor desaparece quando

[1] Para BODIN, "*soberania* é o poder absoluto e perpétuo de uma República, palavra que se usa tanto em relação aos particulares quanto em relação aos que manipulam todos os negócios de Estado de uma República". (Expressão *República* no significado moderno de *Estado*.)

fica sem ela) e *imprescritível* (não possui prazo certo de duração, aspira à existência permanente). Desse modo, atentando-se às características da soberania, é inadmissível que uma empresa estrangeira que possua filial, ou venha a prestar serviços no Brasil, se submeta a apenas parte da soberania nacional: concorda com a submissão à legislação comercial ou tributária brasileira, porém descumpre ou não atende de maneira correta as decisões emanadas do Poder Judiciário brasileiro para o fornecimento de informações telemáticas, sob o equivocado argumento de necessidade de cooperação jurídica internacional com o país onde estão suas sedes ou servidores.

Observe-se que não há qualquer entrave a que empresas estrangeiras operem no Brasil. A nossa própria Constituição Federal, no seu art. 170, parágrafo único, assegura a todos "o livre exercício de qualquer atividade econômica, independentemente de autorização de órgãos públicos", porém estas devem se submeter igualmente à soberania do Estado brasileiro, consoante dispõe o inciso I do mesmo art. 170, ao prever que

> o exercício de atividade econômica por empresa ou corporação sediada em outro país está necessariamente condicionado ao respeito à soberania nacional, princípio conformador de toda a ordem econômica [grifo nosso].

Como expressão da soberania nacional, a *jurisdição* é a atividade tendente à declaração do direito no caso concreto, que pode ser definida como o poder do Estado de aplicar a lei e administrar a Justiça, nos limites da sua soberania e no alcance do território nacional. Para DINAMARCO (2006, p. 145), jurisdição "é uma das funções do Estado, mediante a qual este se substitui aos titulares dos interesses em conflito para, imparcialmente, buscar a pacificação do conflito que os envolve, com justiça".

A soberania nacional, e, consequentemente a jurisdição, será exercida dentro dos limites do território de cada Estado, não sendo possível a existência de Estado sem território. Dentro dos

seus limites territoriais, a ordem jurídica do Estado prevalece, pois é a única dotada de soberania.

O Brasil adotou como regra, conforme art. 5º, *caput*, do Código Penal, o Princípio da Territorialidade, segundo o qual aplica-se a lei penal brasileira aos crimes cometidos no território nacional, ressalvados os casos do art. 7º, II, do mesmo diploma legal.

Nos dizeres de TOLEDO (1991, p. 45),

> são submetidos à lei brasileira os crimes cometidos dentro da área terrestre, do espaço aéreo, e das águas fluviais e marítimas, sobre as quais o Estado brasileiro exerce sua soberania, pouco importando a nacionalidade do agente. Porém, nos dias atuais, o conceito de território para fins de aplicação da jurisdição deve englobar também o espaço virtual, com todos os serviços de Internet prestados no Brasil.

Portanto, uma empresa estrangeira que possui filial e presta serviços de Internet no Brasil está constituída sob as leis brasileiras, sem o que não poderia operar no país. Negar-se a cumprir decisão válida emanada de juiz brasileiro, para que sejam fornecidos os dados telemáticos armazenados em seus servidores, exigindo para tanto pedido de cooperação jurídica internacional, traduz-se em desrespeito à jurisdição brasileira como expressão da soberania nacional.

Esta ideia deve ficar bem clara, pois haverá ainda casos em que obviamente será necessário o pedido de cooperação internacional, sobretudo com os avanços e facilidades trazidos pela Internet e o aumento do volume das provas produzidas ou armazenadas em meio cibernético. Nessas circunstâncias é bastante comum o atributo da transnacionalidade.

BECHARA (2011, p. 37-38) explica que prova transnacional

> é aquela cujo meio de prova se encontra num Estado distinto ao da autoridade judicial competente, ou ainda

> quando os meios de prova de um mesmo fato se encontram em Estados diversos.
>
> E continua:
>
> Em outras palavras, a prova transnacional é aquela cuja fonte de prova encontra-se dentro dos limites da soberania de outro Estado, e que, portanto, requer a cooperação e o auxílio deste para a obtenção do dado ou elemento probatório.

É preciso aclarar essa afirmação, para que não dê margem a dúvidas quanto à jurisdição do Estado brasileiro sobre o fornecimento de documentos e informações constituídos a partir do território nacional.

Assim, uma conta corrente bancária, aberta numa instituição financeira estabelecida em território nacional e, portanto, constituída sob as leis brasileiras (nos termos do Decreto-Lei n.º 4.657, de 4 de setembro de 1942, Lei de Introdução às Normas do Direito Brasileiro – LINDB)[2], está sujeita a ter seus documentos e informações apresentados ao juiz brasileiro, mesmo que tais informações estejam arquivadas junto a uma filial ou à matriz da instituição financeira situadas no exterior.

Por outro lado, uma conta corrente bancária aberta no exterior, isto é, sob a soberania e jurisdição de outro Estado, somente terá seus dados e informações disponibilizados ao Judiciário brasileiro mediante pedido de cooperação internacional, mesmo que tal instituição financeira possua congênere no território brasileiro, pois neste último caso o serviço, ou seja, a abertura da conta corrente e sua manutenção, não foi prestado em território nacional, mas sim no Estado estrangeiro. Exemplo claro disso foi citado por ARAS (apud ROCHA et al., 2006): o caso Banestado – Banco do Estado do Paraná, no qual houve evasão de divisas e lavagem de dinheiro

[2] "Art. 9º Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituírem.

§ 1º Destinando-se a obrigação a ser executada no Brasil e dependendo de forma essencial, será esta observada, admitidas as peculiaridades da lei estrangeira quanto aos requisitos extrínsecos do ato."

através de contas CC5, contas de não residentes, abertas na praça de Foz do Iguaçu em alguns bancos brasileiros, inclusive o Banestado, mediante autorização especial do Banco Central do Brasil, e que foram utilizadas de forma fraudulenta, já que os titulares das contas correntes eram "laranjas". Grande parte dos valores foi destinada a contas abertas na agência do Banestado de Nova York e, a partir delas, os valores foram distribuídos para outros bancos.

No que toca às contas abertas no Brasil, a documentação e movimentação financeira foram obtidas sem problemas, mediante decisão judicial de quebra do sigilo bancário do Juízo brasileiro. No entanto, para obtenção da documentação relativa às contas do Banestado de Nova York, foi imprescindível a cooperação internacional da Promotoria de Nova York (*District Attorney of the New York County*) e de outros órgãos americanos, já que nesse caso o serviço de abertura e manutenção das contas ocorreu no exterior.

3 Jurisdição na Internet

A Internet não possui fronteiras e assim foi arquitetada para que seja, a princípio, acessada de qualquer parte do globo. Isto significa a criação de uma realidade virtual sem as barreiras físicas das delimitações territoriais dos Estados.

As relações humanas multiplicaram-se com essa ferramenta, que, embora criada para ser global, esbarra nas diferenças culturais refletidas nas diversas legislações. O mesmo conteúdo pode ter tratamento diverso em países diferentes e ser tratado como legal ou ilegal.

No que toca aos delitos reais ou virtuais que deixaram evidências digitais, a sua investigação torna-se mais complexa, uma vez que aumenta a dificuldade em precisar o local onde estão as provas a serem coletadas.

Embora a Internet pareça uma rede etérea, seu funcionamento depende de uma infraestrutura real. Assim, para acessar essa comunidade virtual, são necessários provedores de

conexão à rede, que atribuem ao usuário um número IP (*Internet Protocol*) através do qual ele passa a navegar no ciberespaço. O conteúdo a ser acessado ou as plataformas que possibilitam a produção de conteúdo pelo próprio usuário, incluindo-se aí as mensagens de *e-mail*, ou outras formas de comunicação via Internet, dependem de estrutura disponibilizada pelos provedores de aplicações de Internet.

O funcionamento correto dessa rede obedece a critérios organizacionais matemáticos, que permitem a fluidez dessa estrutura. Isto significa que as empresas provedoras de Internet detêm as informações referentes aos passos que os usuários percorrem na rede: acessos, postagens e comunicações.

São essas informações que em geral permitem, de forma precisa, desvendar um crime cibernético ou obter uma prova digital para elucidar um crime real. O que tem aturdido o mundo jurídico é a obtenção dessas informações, desses dados que consubstanciam a prova digital.

As empresas provedoras de Internet, englobando todos os tipos envolvidos nessa atividade, passaram a ser assoberbadas de pedidos de informações sobre os dados, recebendo solicitações e ordens de toda parte do mundo.

Uma vez que tais empresas podem possuir sede física em um país, mas armazenar suas informações em servidores em qualquer local do planeta, os operadores do Direito depararam-se com a perplexidade de não saber qual local teria jurisdição para decidir acerca do fornecimento de tais dados. Além disso, cada país possui uma percepção peculiar acerca da proteção da privacidade, o que se reflete nas diferenças legislativas sobre requisitos para fornecimento de dados e conteúdo. Some-se a isso a volatilidade da prova digital, pois a enorme quantidade de informações em circulação no mundo faz com que a sua manutenção pelas empresas

seja a menor possível, ditada pelos custos que o armazenamento de dados gera.

A necessidade das próprias empresas de armazenar essa grande quantidade de informações por questões internas gerenciais, ou por determinação das legislações às quais se consideram submetidas, resultou em que o armazenamento de dados ocorresse em servidores nos mais diversos países, seguindo critérios econômicos e fiscais. Também, por razões de segurança, há servidores replicados em locais diferentes do globo e informações armazenadas de forma fracionada.

Segundo LA CHAPELLE e FEHLINGER (2016), os possíveis critérios aventados para definir qual a lei aplicável na obtenção de dados digitais são:

a) a lei do local em que está o usuário, do qual se pretende obter os dados;

b) a lei do local onde estão os servidores que armazenam os dados;

c) a lei do local de incorporação da empresa que presta o serviço;

d) a lei do local dos registradores de onde o domínio foi registrado.

Todas as possíveis soluções apresentam dificuldades e podem conflitar com as regras de aplicação da lei penal de cada país. A primeira opção, que sujeitaria os provedores de Internet a fornecerem dados nos termos da legislação do local onde está o usuário, pode se deparar com a situação em que o usuário esteja em um determinado país cometendo uma ação criminosa pela Internet e produzindo resultado criminoso no país que necessita dos seus dados para investigação e processo, utilizando-se de provedor de Internet com sede em um terceiro país!

A opção que pretende que se utilizem as leis do local onde estão os servidores que armazenam os dados, e que tem sido advogada pelas grandes empresas provedoras de Internet, sob o argumento de precisarem cumprir as leis de proteção de dados

e privacidade, impõe uma tarefa ingrata ao operador do Direito que necessita da prova digital. Isso porque, como exposto acima, os dados podem estar duplicados em vários servidores espalhados simultaneamente pelo mundo, ou até fragmentados, guardados em diferentes locais. Ou seja, não haveria nem mesmo certeza absoluta a respeito do local exato em que determinado dado imprescindível a uma investigação estaria armazenado. A opção sobre a utilização da lei da região em que a empresa foi incorporada também soa estranha, quando o local onde o serviço está sendo prestado não coincide com aquele da incorporação, já que estariam sendo aplicadas leis estrangeiras no território nacional. A opção sobre a aplicação da legislação do Estado de origem do registrador também implica a aplicação de leis estrangeiras a fatos que possuem impacto no território nacional.

Todas essas opções, ao assumirem que, para fornecimento de dados digitais, as empresas provedoras de Internet devem obedecer aos parâmetros legais de jurisdições diversas do local onde os fatos ocorreram ou o serviço foi prestado, implicam a necessidade de pedidos de cooperação internacional.

Tais pedidos, conhecidos como *Mutual Legal Agreement Treaties* (MLATs) – Acordos de Assistência Mútua em Matéria Penal, tradicionalmente têm um processamento muito lento, pois dependem de que os pedidos sejam feitos de forma correta, de que sejam traduzidos e enviados pelas autoridades competentes, para que uma autoridade no país requerido dê início à execução do pedido.

Esse procedimento protocolar, que já se apresentava por demais demorado para os pedidos tradicionais, é no mais das vezes inócuo face à volatilidade das provas digitais e da necessidade de investigação célere, não estando adequado às novas tecnologias.

Assim, os pedidos dos operadores do Direito para obtenção de provas digitais, direcionados às empresas provedoras de Internet,

têm proliferado, principalmente quando tais empresas possuem algum vínculo com o local onde os efeitos da ação criminosa são sentidos e onde o caso está sendo investigado ou processado.

Muitas vezes, também, as empresas que proporcionam serviços de Internet, os quais acabam sendo utilizados para uma ação criminosa e, portanto, detêm provas digitais, não possuem vínculo com o local onde o caso está sendo investigado, complicando ainda mais a obtenção das informações digitais.

3.1 Jurisdição e Internet: Convenção de Budapeste

A Convenção de Budapeste é o tratado internacional sobre crimes cibernéticos, firmado no âmbito do Conselho da Europa, que procura harmonizar as legislações penal e processual penal, a fim de permitir a cooperação para obtenção de provas digitais. Foi assinada em 23 de novembro de 2001 e aberta para adesão e ratificação dos demais países, tendo sido homologada por 52 signatários.

O Brasil não é signatário da Convenção de Budapeste, mas por ser o único tratado sobre crimes cibernéticos existente, acaba sendo o modelo e parâmetro para as demais legislações.

No que toca à preservação e obtenção das provas digitais, a Convenção de Budapeste determina que haja preservação de dados, quando requerido, pelo prazo de 90 (noventa) dias, prorrogável por igual período. Também fala em auxílio mútuo para fornecimento de dados de tráfego e para interceptação de conteúdo.

Quanto ao acesso a dados armazenados fora do território de cada Estado-parte da Convenção, a previsão disposta no art. 32 é tímida:

> Art. 32. Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público.
>
> Uma Parte pode, sem autorização de outra Parte:

> a) aceder a dados informáticos armazenados, acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou
>
> b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados, situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

Assim, há a possibilidade de obtenção dos dados digitais armazenados fora do território nacional de cada Parte, sendo válidos para o processo, quando esses dados são públicos, isto é, podem livremente ser acessados de qualquer localização (fonte aberta), ou quando há o consentimento voluntário de quem estaria legalmente autorizado a fornecê-los. Logo, ou o próprio criminoso teria que voluntariamente concordar em fornecer esses dados, ou a empresa provedora de Internet, detentora desses dados, teria que possuir uma autorização expressa nesse sentido, o que não parece facilitar o trabalho dos agentes investigadores.

No entanto, há casos decididos por Cortes europeias, americanas e também brasileiras, que têm servido de norte para solucionar essa necessidade de obtenção de provas digitais, que não seriam alcançadas pela jurisdição do país onde a investigação e/ou processo se desenvolvem.

3.2 Jurisdição e Internet no Código Penal brasileiro

Para a aplicação da Lei Penal, o Estado brasileiro titular do *jus puniendi* adotou, como regra, o princípio da territorialidade, conforme já citado no art. 5º do Código Penal, sem prejuízo da incidência de outros princípios nos casos dispostos no art. 7º, inciso II, do mesmo diploma legal. E, para a definição do lugar do delito, optou o legislador penal pela adoção do Princípio da Ubiquidade (art. 6º do CP), estabelecendo que se considera praticado o crime "no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde produziu ou deveria produzir-se o resultado".

Da análise dos artigos acima mencionados, infere-se que, na prática de crimes por meio da Internet, ocorrida no território nacional, torna-se completamente irrelevante para a aplicação da lei penal o local em que fica a sede da empresa provedora do serviço de Internet ou onde estão armazenadas as informações telemáticas.

Portanto, se um crime cibernético ocorreu no Brasil, estará sujeito à jurisdição brasileira, sendo dever do Estado investigar e reprimir as condutas delituosas praticadas e fazer cumprir as decisões emanadas de juiz brasileiro para a efetiva apuração do delito, sem a necessidade de cooperação internacional para o cumprimento da decisão.

3.3 Jurisdição e Internet no Código de Processo Civil brasileiro

O Código de Processo Civil de 1973 disciplinava os limites da jurisdição nacional no art. 88. No novo CPC, instituído pela Lei n.º 13.105/2015, a matéria encontra-se disciplinada no Título II ("Dos Limites da Jurisdição Nacional e da Cooperação Internacional"), Capítulo I ("Dos Limites da Jurisdição Nacional"), inaugurado pelo art. 21, abaixo transcrito:

> Art. 21. Compete à autoridade judiciária brasileira processar e julgar as ações em que:
>
> I – o réu, qualquer que seja a sua nacionalidade, estiver domiciliado no Brasil;
>
> II – no Brasil tiver de ser cumprida a obrigação;
>
> III – o fundamento seja fato ocorrido ou ato praticado no Brasil.
>
> Parágrafo único. Para o fim do disposto no inciso I, considera-se domiciliada no Brasil a pessoa jurídica estrangeira que nele tiver agência, filial ou sucursal [grifos nossos].

Ao comentar o artigo acima, MILLER (apud CABRAL; CRAMER, 2016, p. 73), relata que este guarda estreita correspondência com o art. 88 do CPC de 1973, na sua estrutura e

nos seus termos, ao definir o alcance da jurisdição brasileira, vista como desdobramento lógico-jurídico do atributo da soberania estatal. MILLER chama a atenção para o parágrafo único do citado art. 21 que, ao se reportar ao inciso I do mesmo dispositivo legal, acabou por alargar, para fins processuais, o conceito de domicílio da pessoa jurídica.

Sabe-se que várias das empresas provedoras de Internet, que prestam serviços no Brasil, principalmente os grandes provedores, atuam sob a forma de um único grupo econômico transnacional, composto de empresas controladoras e controladas[3], muitas das quais com filiais ou representação no Brasil. Pois bem, por força do antigo art. 88 e atual art. 21 do CPC, tanto a pessoa jurídica aqui instalada, como toda a corporação estrangeira possuirão como domicílio o Brasil nas demandas originadas de serviço prestado neste país.

3.4 Jurisdição e Internet no Código de Defesa do Consumidor

Os serviços prestados através da *web* são considerados relações de consumo, assim como o usuário dos serviços de Internet enquadra-se na definição de "consumidor", e os provedores de serviços e conexão de Internet, no conceito de "fornecedor", consoante os termos dos arts. 2º e 3º, do Código de Defesa do Consumidor.

Desse modo, nas relações de consumo derivadas de serviços de Internet prestados por empresas nacionais ou estrangeiras no Brasil, há *responsabilidade subsidiária* entre as sociedades

[3] "É controlada:
I - a sociedade de cujo capital outra sociedade possua a maioria dos votos nas deliberações dos cotistas ou da assembleia geral e o poder de eleger a maioria dos administradores;
II - a sociedade cujo controle, referido no inciso antecedente, esteja em poder de outra, mediante ações ou cotas possuídas por sociedades ou sociedades por esta já controladas." (Art. 1.098 do Código Civil.)

controladoras e controladas, para fins de proteção aos direitos do consumidor, usuário da Internet (art. 28, § 2º, CDC).

Os tribunais têm aplicado cada vez mais o entendimento de que há responsabilidade subsidiária, e mesmo solidária, entre as empresas controladoras e controladas, nos casos de responsabilidade civil das empresas provedoras de serviços de Internet, quando há dano causado pela má prestação do serviço ou dano causado a outrem através da Internet.

A doutrina e a jurisprudência reconhecem a necessidade de proteger o jurisdicionado contra práticas comerciais abusivas, exercidas em economias globalizadas, como demonstram vários julgados[4].

4 Decisões judiciais acerca da jurisdição na Internet

4.1 Caso Yahoo! Inc., na Bélgica

Em 18 de janeiro de 2011, a Suprema Corte belga decidiu[5] que o provedor de aplicações Yahoo! preenchia os requisitos do Código de Processo Penal belga, sendo considerado um provedor de serviços de comunicações eletrônicas e, portanto, nos termos da legislação belga (art. 46 bis do Código de Processo Penal), obrigado a cooperar com as investigações criminais, sob pena de multas altíssimas. No caso, a Yahoo! foi condenada a pagar uma multa de

[4] Jurisprudência: STJ, REsp n.º 1021987/RN, Rel. Min. Fernando Gonçalves, julg. 7 out. 2008; STJ, REsp n.º 566468/RJ, Rel. Min. Jorge Scartezzini, julg. 23 nov. 2004; TJDFT, ApCiv n.º 20060110068265ACJ, julg. 31 out. 2006; STJ, REsp n.º 1117633/RO, Rel. Min. Herman Benjamin, julg. 9 mar. 2010; TJRJ, Ap n.º 0035977-12.2009.8.19.0203, Rel. Roberto Guimarães, julg. 8. fev. 2012 (MARQUES, BENJAMIN e MIRAGEM, 2012, p. 191 e p. 214-216).

[5] Disponível em: <https://www.wsgr.com/attorneys/BIOS/PDFs/burton-yahoo-0411.pdf>; <http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters> e <http://www.stibbe.com/en/news/2014/july/court-of-appeal-of-antwerp-confirms-yahoos-obligation-to-cooperate-with-law-enforcement-agencies>. Acesso em: 10 mar. 2017.

55 (cinquenta e cinco) mil euros, equivalentes a 80 260 (oitenta mil, duzentos e sessenta) dólares americanos e mais uma multa diária, por não fornecer os dados correspondentes a uma conta de *e-mail* do serviço Yahoo!, aptos a permitir a identificação do usuário no bojo de uma investigação criminal de fraude numa compra e venda, e não pagamento por aquisição de equipamento eletrônico, em uma loja em Dendermonde, na Bélgica.

O promotor belga havia intimado a empresa em seus escritórios na Califórnia, Estados Unidos, que alegou a ilegalidade do procedimento, o qual deveria ter obedecido os trâmites do MLAT através dos respectivos Departamentos de Justiça de ambos os países. A Suprema Corte belga decidiu que, embora a Yahoo! não tivesse um escritório na Bélgica, ela estava presente virtualmente no território belga, submetendo-se, portanto, de modo voluntário à jurisdição belga, já que participava da economia do país, disponibilizando o domínio http://www.yahoo.be, utilizava as línguas locais em seu *website*, com *pop-ups* de propaganda baseados na localização dos usuários e era acessível a partir do território belga com foco nos consumidores belgas[6].

Este caso foi o primeiro a ser decidido no sentido de haver jurisdição de um Estado sobre uma empresa, com base na oferta de serviços direcionados ao público de determinado Estado, mesmo sem a presença física da empresa no território desse Estado.

4.2 Caso Microsoft Irlanda X USA (The North Ireland Case)[7]

Numa investigação sobre tráfico de drogas, os promotores americanos conseguiram uma ordem de busca e apreensão para que a Microsoft Inc., empresa baseada nos Estados Unidos da América,

[6] Disponível em: <https://gavclaw.com/2015/12/07/its-true-belgian-supreme-court-confirms-order-for-yahoo-to-hand-over-ip-addresses/>. Acesso em: 11 mar. 2017.

[7] Disponível em: <https://www.lawfareblog.com/microsoft-ireland-case-brief-summary>. Acesso em: 11 mar. 2017.

entregasse os dados de IP e o conteúdo de *e-mails* de um usuário do serviço de correio eletrônico da empresa.

A Microsoft recusou-se a entregar as informações, dizendo que seria necessário o procedimento de cooperação internacional conhecido como MLAT, uma vez que os dados estavam armazenados em seu servidor localizado na Irlanda.

O Departamento de Justiça Norte-Americano alegou que o mandado de busca e apreensão poderia ter efeitos de uma intimação e que, portanto, não se tratava de efeito extraterritorial da ordem, pois a Microsoft Inc. poderia trazer os dados requisitados de volta ao território americano apenas acionando um terminal situado no próprio território americano e entregá-los aos promotores. Os argumentos utilizados para a obtenção de dados localizados fora do território americano baseiam-se na "tese do controle" sobre os dados. Assim, se a empresa possui controle, isto é, acesso aos dados requisitados, não importa onde esses dados estão armazenados, deve entregá-los (SILVA, 2016).

No entanto, o 2º Circuito de Nova York[8], em sede recursal, decidiu que, segundo a lei americana, um mandado de busca e apreensão não pode ter efeitos de intimação (*subpoena*) e que a entrega de conteúdo implica a necessidade de um mandado de busca e apreensão (*search warrant*), o qual não pode ter efeitos além do território americano. A decisão foi objeto de recurso pelo Departamento de Justiça Americano.

4.3 O Caso Google: fundamentos precursores do art. 11 do MCI

Em 2006, foi proposta a Ação Civil Pública[9], promovida pelo Ministério Público Federal em face da empresa Google Brasil

[8] *In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation*, United States Court of Appeals for the Second Circuit, Docket no. 14-2985, julg. 14 jul. 2016.

[9] Autos n.º 2006.61.00.018332-8, 17ª Vara Cível da Subseção Judiciária de São Paulo.

Internet Ltda., que findou em 2 de julho de 2008 com a assinatura de Termo de Ajustamento de Conduta (TAC) entre as partes, no bojo da Comissão Parlamentar de Inquérito do Senado Federal, a chamada CPI da Pedofilia. Conhecido como "Caso Google", este foi um dos casos de maior repercussão sobre a obrigação de as empresas provedoras de Internet colaborarem com a Justiça brasileira na persecução penal de crimes cibernéticos ocorridos no país.

Resumidamente, o Caso Google surgiu em razão das dificuldades na apuração, pelas autoridades brasileiras, dos crimes de distribuição de pornografia infantil e delitos de discurso do ódio, que vinham sendo largamente cometidos na extinta rede social Orkut, serviço pertencente ao grupo Google[10]. Com efeito, a empresa vinha desrespeitando a jurisdição brasileira ante o não atendimento das ordens emanadas dos juízes brasileiros para o fornecimento dos dados telemáticos, imprescindíveis à apuração desses crimes. Argumentava a empresa ré, Google Brasil Internet Ltda., que os dados requisitados estariam hospedados em servidores localizados nos Estados Unidos, cujo gerenciamento caberia à empresa Google Inc., o que demandaria pedido de cooperação jurídica internacional.

Importante mencionar que os fundamentos jurídicos trazidos pelo Ministério Público Federal no caso Google, que propiciaram a concessão da decisão liminar requerida à época e posterior realização do Termo de Ajustamento de Conduta, com várias cláusulas que impunham obrigações à empresa quanto à guarda e fornecimento de dados telemáticos, foram os precursores no reconhecimento do dever de uma empresa estrangeira provedora de Internet submeter-se à jurisdição brasileira e colaborar com a Justiça do país na investigação dos crimes cibernéticos ocorridos no território nacional.

[10] A Google Brasil Internet Ltda., constituída sob as leis brasileiras, é uma sociedade controlada pelas *holdings* transnacionais Google Internacional LLC e Google Inc., constituindo-se em um único grupo econômico transnacional.

Assim, quase uma década antes da entrada em vigor do Marco Civil da Internet, a questão da aplicação da lei brasileira aos crimes praticados através da rede mundial de computadores já demandava a atenção – e preocupação – dos aplicadores do Direito, principalmente em razão das dificuldades enfrentadas pela Justiça brasileira na obtenção de dados e elementos de prova a serem fornecidos pelas empresas provedoras de serviço de Internet que operavam no Brasil.

Da leitura do art. 11 do MCI, observa-se que sua redação resultou do que já estabelecia de maneira esparsa a legislação brasileira, em uma interpretação sistemática e lógica do ordenamento jurídico pátrio. Tais fundamentos podem ainda hoje ser empregados para desconstruir alegações utilizadas por alguns provedores de Internet na tentativa de se esquivar do cumprimento de decisões emanadas do Poder Judiciário brasileiro, sob a equivocada alegação da necessidade de cooperação jurídica internacional.

5 Solução da legislação brasileira: art. 11 do Marco Civil da Internet (Lei n.º 12.965/2014)

No Brasil, tanto para a obtenção de dados de IP, data e hora, quanto para a obtenção de conteúdo estático de comunicação, isto é, conteúdo de comunicações armazenadas nos servidores das empresas, é necessária a quebra de sigilo telemático e a autorização judicial, para que os provedores de aplicações de Internet os forneçam. Para a obtenção do conteúdo dinâmico da comunicação, é necessária ordem judicial que autorize a interceptação telemática, observando-se os rigores da Lei n.º 9.296/96.

Para o acesso pelas autoridades previstas pelo art. 10, § 3º, do MCI, aos dados cadastrais do usuário de determinada conexão de Internet, não há necessidade de ordem judicial, estando os dados cadastrais definidos no Regulamento do Marco Civil da Internet, Decreto n.º 8.771, de 11 de maio de 2016, em seu art. 11, § 2º,

como a filiação, o endereço e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

É importante notar que os registros de conexão à Internet, bem como os registros de acesso a aplicações de Internet, podem ser obtidos mediante ordem judicial para formação de conjunto probatório em processo judicial cível ou penal, nos termos do art. 22 do MCI. Já as comunicações telemáticas somente podem ser obtidas para formação de conjunto probatório em investigação criminal ou instrução processual penal, a exemplo das comunicações telefônicas, nos termos do parágrafo único do art. 1º da Lei n.º 9.296/96, de 24 de julho de 1996, que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal.

Face à perplexidade que a rede mundial de computadores causou para a obtenção de provas digitais, ao ensejar dúvidas quanto à jurisdição do Estado requisitante sobre as empresas detentoras desses dados, o legislador brasileiro editou o Marco Civil da Internet.

Conforme explanado, o sistema jurídico brasileiro já apresentava preceitos claros quanto aos limites de sua jurisdição no Código Penal, no Código de Processo Civil e no Código de Defesa do Consumidor. A estes acrescentaram-se as normas trazidas com a entrada em vigor do Marco Civil da Internet, especialmente no seu art. 11:

> Art. 11 Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet, em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

> § 2º O disposto no *caput* aplica-se, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de Internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

O art. 11, § 1º, do MCI, explicita que a todos os dados coletados no território nacional por provedores de conexão e de aplicações de Internet, bem como ao conteúdo das comunicações, aplica-se o *caput* do artigo, isto é, deve ser respeitada a legislação brasileira nas operações de coleta, armazenamento, guarda e tratamento, observados os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Resta claro que, para o afastamento desses direitos, proteção e sigilo, os requisitos a serem observados são os da legislação brasileira. O § 1º ainda destaca que pelo menos um dos terminais deve estar localizado no Brasil. Porém, o § 2º mitiga essa exigência ao estabelecer que o disposto no *caput*, isto é, a aplicação da legislação brasileira ocorre, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

Assim, as dúvidas são suscitadas em relação aos provedores estrangeiros de Internet. A legislação é clara ao dizer que, se a empresa possui filial no Brasil, esta filial se sujeita à jurisdição nacional, já que está situada fisicamente no país, onde somente poderá operar se os seus atos constitutivos forem aprovados pelo governo brasileiro.

Fica, portanto, sujeita à legislação brasileira, nos termos dos arts. 11 e 12 da Lei de Introdução às Normas do Direito Brasileiro – LINDB (BRANT, 2014), que estabelece ser competente a autoridade judiciária brasileira, quando o réu for domiciliado no Brasil ou aqui tiver de ser cumprida a obrigação. Dessa forma, a filial da empresa estrangeira integra o grupo econômico estrangeiro, mas as atividades da empresa estrangeira em relação aos serviços prestados no território nacional estão submetidas à legislação brasileira. Consequentemente, não importa à autoridade requisitante onde os dados digitais foram armazenados, pois esta é uma decisão gerencial da empresa, e, como vimos, podem estar armazenados em qualquer local do planeta. O que importa, conforme foi aventado no caso Microsoft Irlanda X USA, é que a empresa provedora de Internet tem o domínio, o controle dos dados digitais (SILVA, 2016), sendo possível a ela fornecê-los e, por integrar grupo econômico com presença física no país, prestando serviços em seu território, está submetida à jurisdição nacional, tendo o dever de cumprir as ordens judiciais que lhe determinam a entrega das informações consubstanciadas em provas digitais.

A segunda hipótese do § 2º do art. 11 diz respeito à pessoa jurídica sediada no exterior, que oferta serviços ao público brasileiro e, interpretando o parágrafo *a contrario sensu*, não possui filial no território brasileiro. Mesmo nesses casos aplica-se a jurisdição brasileira, restando determinar em que situações pode-se dizer que os serviços estão sendo ofertados ao público brasileiro, já que na Internet as ofertas são, em princípio, globais.

Para melhor entendimento da terminologia *serviço ao público brasileiro,* trazemos a seguir a definição esclarecedora constante de texto de OLIVEIRA (apud SENADO FEDERAL, 2014):

> Por oferta de serviço ao público brasileiro, há de compreender-se o comportamento da empresa estrangeira em que vem, de forma direcionada e específica, promover *marketing* ao mercado de consumo brasileiro. O simples

> fato de determinados *sites* estrangeiros disponibilizarem textos em português não é suficiente para caracterizar oferta ao público brasileiro, pois, em uma era globalizada, é comum os *sites* estrangeiros vazarem seus textos em vários idiomas.

Assim, seguindo-se o exemplo do texto, se um brasileiro acessa um *site* de compras norte-americano com *marketing* direcionado ao mercado nacional, ainda que não haja filial no Brasil, haveria duas observações:

a) não será aplicada a legislação brasileira quanto à disciplina do contrato de compra e venda, e sim a norte-americana, por força do art. 9º, § 2º, da LINDB[11] e jurisprudência à época;

b) será aplicada a legislação brasileira quanto à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações, por força do art. 11 do Marco Civil da Internet.

Esclarecendo-se o real alcance da norma prevista no art. 11, § 2º, do MCI, observe-se a posição sistemática do § 2º em relação ao *caput* do art. 11, além de referência expressa a ele, do que se conclui que, para qualquer operação de coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações telemáticas (art. 11, *caput*, MCI), será aplicada a legislação brasileira à empresa provedora nacional ou estrangeira, com filial ou não no Brasil. Desde que ofereça seus serviços de Internet ao público brasileiro, deverá submeter-se à jurisdição brasileira.

Assim, qualquer provedor estrangeiro que *ofertar serviço ao público brasileiro*, ainda que não tenha filial no Brasil, deve respeitar a legislação brasileira relativamente aos dados pessoais, aos registros de conexão e de acessos a aplicações, o que abrange as normas para que a privacidade seja afastada mediante a quebra do sigilo telemático com a entrega de dados que são prova digital.

[11] Decreto-lei n.º 4.657, de 4 de setembro de 1942.

Observe-se que o Marco Civil da Internet, *salvo no tocante à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações telemáticas*, não cuida de definir a legislação que disciplinará, por exemplo, o contrato celebrado por um brasileiro que adquire um produto em *site* estrangeiro. Para isso será observada a LINDB e a jurisprudência. Assim, se um brasileiro acessou *site* de compra estrangeiro pertencente a uma multinacional *com filial no Brasil* e com oferta de serviço voltado ao mercado de consumo brasileiro, o Código de Defesa do Consumidor disciplinará o contrato. Se o *site* pertencer a empresa sem filial no Brasil e cujo serviço não seja voltado ao público brasileiro, é aplicável a lei estrangeira para a disciplina do contrato (art. 9º, § 2º, da LINDB); mas, se a empresa estrangeira oferecer serviços ao público brasileiro, com ou sem filial no Brasil, será aplicada a legislação brasileira e o MCI para as hipóteses constantes do *caput* do art. 11.

Desse modo, de acordo com a legislação brasileira após o advento do MCI, em nosso entendimento a cooperação internacional somente será acionada em duas hipóteses:

a) a primeira, nos casos em que seja necessário transmitir uma ordem judicial a provedor de Internet que não tenha presença física no território nacional. Ou seja, embora o serviço tenha sido prestado ou oferecido ao público brasileiro, não há sede ou filial da empresa no Brasil e, para se dar *efetividade* às decisões judiciais, é preciso valer-se da cooperação com o país onde seja possível alcançar o provedor de Internet. Note-se que, no caso Yahoo! X Bélgica, a Corte belga entendeu ser válida a intimação da empresa Yahoo!, com endereço nos Estados Unidos da América, para que apresentasse os *logs* do *e-mail* investigado, isto é, informação do IP, data e hora, formulada diretamente pelo promotor do caso, sem necessidade de cooperação internacional por meio dos departamentos de Justiça de ambos os países. No caso do Brasil, essas informações de IP, data e hora, que possibilitam a identificação do endereço de onde o usuário enviou o *e-mail*, somente podem ser prestadas com autorização judicial, nos termos do art. 15, § 3º, do MCI, de forma que o correto

seria a utilização da cooperação internacional, com a remessa da ordem judicial pelas vias diplomáticas para cumprimento. Porém, entendemos que seria válida a prova fornecida diretamente pela empresa estrangeira sem sede no país, que prestasse as informações requeridas na forma da lei brasileira;

b) a segunda hipótese para utilização da cooperação jurídica internacional é aquela em que as empresas provedoras de Internet não ofertam seus serviços ao público brasileiro, mas o acesso foi feito a partir de conexão iniciada no território nacional. Nesses casos, a empresa não possui filial ou representação no Brasil e o público-alvo para utilizar os seus serviços não se encontra no território brasileiro. Se utilizado um serviço desse provedor estrangeiro de Internet com consequências criminais ou cíveis no Brasil, será necessária a realização de cooperação internacional para a obtenção de uma ordem judicial que determine ao provedor estrangeiro a entrega das informações telemáticas.

6 Sanções pelo descumprimento dos arts. 10 e 11 do Marco Civil da Internet – art. 12 MCI

A fim de garantir efetividade à jurisdição brasileira na matéria regulada pelo MCI, o seu art. 12 prevê, sem prejuízo da aplicação de outras sanções de natureza cível, criminal ou administrativa, as sanções de advertência, multa de até 10% do faturamento do grupo econômico no Brasil no seu último exercício, a suspensão temporária das atividades e a proibição de exercê-las quando envolverem os atos previstos no art. 11. Tratando-se de empresa estrangeira, a filial, sucursal, escritório ou estabelecimento situado no país, responderá solidariamente pela multa.

Entendemos que, quando o MCI se refere à possibilidade de aplicação de sanções pelo descumprimento dos arts. 10 e 11 precedentes, resta claro que as atividades mencionadas devem estar de acordo com a legislação brasileira, inclusive no que se refere ao cumprimento de ordens judiciais que, nos termos da legislação

pátria, afastam a proteção e o sigilo de dados e determinam o seu fornecimento.

Dessa maneira, quaisquer dos provedores de Internet, nacionais ou estrangeiros, podem estar sujeitos às sanções do art. 12. Dentre elas, pensamos que a medida mais efetiva é sem dúvida a sanção prevista no inciso II do artigo que se refere à multa que pode chegar a 10% do faturamento do grupo econômico no Brasil, no seu último exercício. Haverá de fato um problema se a empresa estrangeira não possuir nenhuma filial, sucursal ou representação no país, nem esteja presente no país empresa que integre o mesmo grupo econômico, de forma que não possa ser alcançada pela multa. Nesse caso, pode-se aplicar a suspensão temporária ou mesmo a proibição do exercício das atividades. Estas modalidades de sanção, sendo mais gravosas, já que inibem a prestação do serviço, devem ser aplicadas somente em relação a descumprimentos graves e quando não for possível alcançar os provedores com multa ou outras sanções de natureza econômica.

7 Conclusão

No que concerne à obtenção de provas digitais produzidas a partir da Internet, o legislador brasileiro foi sensível à natureza dessas provas, que, por serem em essência voláteis, necessitam chegar rapidamente às mãos dos agentes de investigação e Justiça do Estado brasileiro, a fim de propiciar a rápida e efetiva investigação e processamento judicial dos delitos e ilícitos cibernéticos, ou não, mas que dependam das provas digitais para sua elucidação.

Assim, o legislador optou, nessa seara, por firmar a jurisdição brasileira a partir do conceito de serviço ofertado ou prestado em território nacional, pois, embora a Internet se revele como espaço virtual sem fronteiras, o seu ponto de ligação com o mundo real ocorre em um território existente e delimitado de um Estado.

Desse modo, embora provedores de Internet possam vir a confrontar-se com legislações diferentes, ao se verem compelidos a cumprir diretamente ordens judiciais de entrega de provas digitais, não há no presente momento outro modo de garantir a efetividade das investigações e dos processos que não pela afirmação da soberania do Estado em que as atividades dos provedores ocorreram.

Resta claro que o melhor caminho a ser seguido é o do entendimento entre os Estados, para que harmonizem suas legislações com o fim de possibilitar uma investigação mais célere e efetiva. Entendemos que a legislação brasileira apresenta uma solução razoável, até porque não inova desmedidamente, baseando-se em conceitos, princípios e práticas sempre utilizados pelo direito pátrio, apenas se adaptando à nova realidade.

Porém, enquanto não se obtém um tratado internacional único, cabe às empresas provedoras de Internet, detentoras das provas digitais, cumprirem a lei dos locais onde prestam serviços, colaborando para a solução dos conflitos e a manutenção da paz social.

8 Referências bibliográficas

ARAS, Vladimir. Direito Probatório e Cooperação Jurídica Internacional. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). *A prova no enfrentamento à macrocriminalidade.* Salvador: *Jus*Podivm, 2015.

___. Lavagem de dinheiro, evasão de divisas e cooperação internacional: o Caso Banestado. In: ROCHA, João Carlos de Carvalho; HENRIQUES FILHO, Tarcísio Humberto Parreiras; CAZETTA, Ubiratan (Coord.). *Crimes contra o Sistema Financeiro Nacional*: 20 anos da Lei n. 7.492/1986. Belo Horizonte: Del Rey, 2006.

BECHARA, Fábio Ramazzini. *Cooperação jurídica internacional em matéria penal*: eficácia da prova produzida no exterior. São Paulo: Saraiva, 2011. p. 37-38.

BRANT, Cássio Augusto Barros. *Marco Civil da Internet:* comentários sobre a Lei 12.965/2014. Belo Horizonte: D´Placido, 2014.

CABRAL, Antonio do Passo; CRAMER, Ronaldo. *Comentários ao Novo Código de Processo Civil.* 2. ed. Rio de Janeiro: Forense, 2016.

DALLARI, Dalmo de Abreu. *Elementos de Teoria Geral do Estado*. São Paulo: Saraiva, 2016.

DINAMARCO, Cândido Rangel; GRINOVER, Ada Pellegrini; CINTRA, Antonio Carlos de Araújo. *Teoria Geral do Processo.* São Paulo: Malheiros, 2006.

DOMINGOS, Fernanda Teixeira Souza. A obtenção das provas digitais na investigação dos delitos de violência e exploração sexual online. In: SILVA, Ângelo Roberto Ilha da (Org.). *Crimes cibernéticos.* Porto Alegre: Liv. do Advogado Ed., 2017.

___. As provas digitais nos delitos de pornografia infantil na Internet. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). *A prova no enfrentamento à macrocriminalidade.* Salvador: *Jus*Podivm, 2015.

LA CHAPELLE, Bertrand; FEHLINGER, Paul. *Jurisdiction on the Internet: from legal arms race to transnational cooperation.* Internet & Jurisdiction. Paper Series, n. 28, April 2016. Disponível em: <www.internetjurisdiction.net>. Acesso em: 11 mar. 2017.

MARQUES, Claudia Lima; BENJAMIN, Antonio Herman V.; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. São Paulo: Revista dos Tribunais, 2013.

OLIVEIRA, Carlos Eduardo Elias de. *Aspectos principais da Lei n.º 12.965, de 2014*, *o Marco Civil da Internet*: subsídios à comunidade jurídica. Brasília/DF, Senado Federal, Núcleo de Estudos e Pesquisas da Consultoria Legislativa, abr. 2014.

RAMOS, André de Carvalho; GRAMSTRUP, Erik Frederico. *Comentários à Lei de Introdução às Normas do Direito Brasileiro – LINDB.* São Paulo: Saraiva, 2015.

REALE, Miguel. *Teoria do Direito e do Estado.* São Paulo: Martins, 1960.

SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). *A prova no enfrentamento à macrocriminalidade*. 2. ed. Salvador: *Jus*Podivm, 2016.

SILVA, Ângelo Roberto Ilha da (Org.). *Crimes cibernéticos*. Porto Alegre: Liv. do Advogado Ed., 2017.

SILVA, Melissa Garcia Blagitz de Abreu e. *The Microsoft Ireland Case and access to Data: an international perspective*. Trabalho apresentado durante o curso de Mestrado em Direito na Universidade de Chicago, Estados Unidos, na matéria *Computer Crime*, ministrada pelo Professor William Ridgway, jun. 2016.

TOLEDO, Francisco de Assis. *Princípios básicos de Direito Penal.* São Paulo: Saraiva, 1991.

A dificuldade de acesso ao conteúdo das mensagens ilícitas trocadas via WhatsApp para uso em procedimento de investigação e ação penal

Adriana Galvão Starr*

RESUMO

O presente artigo pretende investigar a recusa do maior aplicativo de mensagens instantâneas em número de usuários no Brasil quanto ao atendimento de decisões judiciais que determinam a interceptação das mensagens trocadas por tal via, diante da alegação de impossibilidade técnica, decorrente da criptografia de ponta a ponta. Também são objeto de investigação a legislação atual acerca do tema e as possíveis soluções diante da recusa de fornecimento do conteúdo das mensagens.

Palavras-chave: WhatsApp. Interceptação de mensagens. Decisões judiciais. Impossibilidade técnica. Criptografia de ponta a ponta.

ABSTRACT

This article intends to investigate the refusal of the largest Brazilian instant messaging application in users to comply with court decisions that determine the interception of messages exchanged thereby, based on the allegation of technical impossibility due to end to end encryption. Likewise the current legislation on the subject and the possible solutions to the refusal of providing the content of the messages are also under investigation.

* Pós-graduada em Direito Público pela Escola Superior do Ministério Público de São Paulo e pós-graduada em Direito Privado pela Escola Paulista da Magistratura. Juíza Federal da 1ª Vara Federal com JEF Adjunto Cível e Criminal de Assis/SP. *E-mail*: agstarr@jfsp.jus.br.

***Keywords**: WhatsApp. Interception of messages. Court decisions. Technical impossibility. End to end encryption.*

1 Introdução

No início de abril de 2016, o aplicativo de mensagens WhatsApp anunciou a implementação de criptografia de ponta a ponta nas comunicações trocadas entre seus usuários.

A privacidade quase absoluta é um dos pilares dos criadores do aplicativo, desde o início de suas atividades, conforme se observa nas diversas entrevistas concedidas pelos criadores do WhatsApp Brian Acton e Jan Koum, assim como no trecho da "Política de Privacidade"[1]:

> Política de privacidade do WhatsApp
>
> Última modificação: 25 de agosto de 2016
>
> O respeito que temos por sua privacidade é como um código em nosso DNA. Desde que começamos o WhatsApp, construímos nossos Serviços nos baseando em sólidos princípios de segurança.

Antes disso, as mensagens enviadas via iMessage, Telegram e outros aplicativos de comunicação instantânea já eram criptografadas, fato que enseja o argumento de que não possuem os dados necessários ao atendimento de determinações judiciais proferidas em inquéritos ou ações penais no sentido de determinar a interceptação das conversas mantidas nos ambientes virtuais em referência.

Em decorrência da elevada quantidade de usuários – mais de 100 (cem) milhões –, que fazem do Brasil o segundo país que mais utiliza o aplicativo no mundo, a questão do WhatsApp assume especial relevância e uma possível solução aplicável ao WhatsApp pode ser estendida aos programas similares, razão pela qual o aplicativo em questão consta do título do presente artigo e será mencionado diversas vezes.

[1] Disponível em: <https://www.whatsapp.com/legal/?l=pt_br#privacy-policy-information-we-collect>. Acesso em: 1 mar. 2017.

Ademais, o WhatsApp tem sido o protagonista de todos os descumprimentos de decisões judiciais que levaram às polêmicas decisões de suspensão do aplicativo.

Não obstante o foco do presente artigo no WhatsApp, é importante que se adote solução uniforme para todos os aplicativos de trocas de mensagens instantâneas, caso contrário, aqueles que os utilizam para a prática de crimes apenas migrarão de programa, sem que se solucione o principal problema, qual seja a transformação do mundo virtual em esfera imune ao controle dos órgãos estatais voltados ao combate ao crime.

Cumpre ressaltar, ainda, que não há nada de ilegal na utilização de aplicativos de mensagens criptografadas, ao contrário, são amplamente recomendados pela Anistia Internacional, a fim de impedir o monitoramento político-ideológico de conteúdos por regimes que não prezam pela liberdade de expressão.

Contudo, o que se nota pelo que afirmam autoridades de quase todos os territórios do mundo – inclusive Estados Unidos e União Europeia – é que aplicativos de mensagens vêm alegando o direito à privacidade e ao sigilo das comunicações como pilar inabalável. Essa atitude pode amparar a utilização para o cometimento de crimes graves, como tráfico de drogas, armas e de pessoas, divulgação de imagens e vídeos de pedofilia, sequestro, fraudes, homicídios, atentados terroristas e estupros. Desse modo, finge-se ignorar que não existe direito absoluto, bem como que a maioria dos usuários de tais aplicativos, na qualidade de não criminosos, não possuem interesse na proteção incondicional das mensagens trocadas com fins delituosos.

O compartilhamento de dados criminosos por meio dos aplicativos, como imagens de atos sexuais violentos ou de atos de pedofilia, possui o agravante da impossibilidade de bloqueio da informação, ou seja, ao contrário da página da Internet, que pode ser retirada do ar, a informação, fotografia ou vídeo encaminhada via aplicativo de troca de mensagens atinge um sem número de

usuários. Além disso, a depender das configurações do destinatário, tal conteúdo fica armazenado na memória dos aparelhos e, por vezes, nas nuvens, de modo que se torna impossível apagá-lo, bloqueá-lo ou, de qualquer modo, impedir seu acesso em larga escala.

Importa ressaltar que a questão do afastamento do sigilo das comunicações voltadas ao crime já fora há muito superada e não há sentido em retomá-la cada vez que surgir novo recurso tecnológico destinado a facilitar a comunicação.

Por tais razões, o presente artigo tem como objetivo analisar as possíveis soluções para o problema, considerando o preenchimento dos requisitos previstos na Lei n.º 9.296/1996 para a interceptação das mensagens trocadas via aplicativos.

2 Solução legislativa

Evidentemente, a forma mais fácil e rápida de solucionar a questão da ausência de fornecimento de dados pelos aplicativos de mensagens seria pela via legislativa.

Aplicando-se os requisitos previstos na Lei n.º 9.296/1996, que versa sobre a quebra de sigilo telefônico, por exemplo, poderia ser editada lei que previsse que somente aplicativos que tivessem condições de atender às determinações judiciais de fornecimento de conteúdo das comunicações poderiam funcionar em território nacional. Tal lei também poderia definir os procedimentos e prazos para o atendimento da decisão judicial que determinasse a interceptação.

O problema da solução legislativa reside no fato de o controle da utilização de aplicativo de mensagens vir acompanhado da tentativa de restrição de sua utilização, com a finalidade comercial. Trata-se de uma questão complexa, vez que as operadoras de telefonia sentem-se prejudicadas pelos aplicativos em questão e trabalham para que sua utilização seja mais restrita ou que haja contraprestação pela utilização do número de telefone para a instalação dos aplicativos em comento.

Nesse aspecto, destaca-se o fato de que tais aplicativos, por não serem regulados, de forma direta, pela Anatel, não se submetem, por exemplo, à Resolução n.º 426 editada pela Agência Reguladora referida, cujo art. 24, *caput*, prevê a obrigatoriedade de implementação dos recursos tecnológicos necessários ao cumprimento das decisões judiciais, nos seguintes termos:

> Art. 24. A prestadora deve tornar disponíveis os recursos tecnológicos e facilidades necessários à suspensão de sigilo de telecomunicações, determinada por autoridade judiciária ou legalmente investida desses poderes, e manter controle permanente de todos os casos, acompanhando a efetivação dessas determinações, e zelando para que elas sejam cumpridas, dentro dos estritos limites autorizados.

A regulamentação pela Anatel provavelmente viria acompanhada da imposição de pagamento de tributos, além de eventual contraprestação à operadora de telefonia móvel pela utilização da linha telefônica para a instalação e utilização do aplicativo, retirando, portanto, a gratuidade da comunicação pela via dos aplicativos de mensagem instantânea, razão pela qual a medida é controversa e a ela se opõem os usuários.

Nota-se, ademais, a falta de vontade política para implementar solução legislativa efetiva para os contumazes descumprimentos de decisões judiciais pelos administradores do WhatsApp.

O Marco Civil da Internet, introduzido por meio da Lei n.º 12.965/2014, é insuficiente para tal finalidade.

A mera leitura da lei em referência deixa clara a preocupação com o direito à privacidade do usuário e a outros aspectos relevantes como a neutralidade da rede, a garantia de manutenção do acesso à Internet e à guarda e procedimentos para a obtenção de registros de utilização de usuários. Basicamente, a Lei n.º 12.965/2014 versa sobre os direitos dos usuários em relação aos provedores de Internet, assim como aos direitos e obrigações desses perante o Poder Público com vistas ao fornecimento de dados cadastrais e de acesso.

Contudo, a legislação em comento não teve qualquer preocupação com a utilização da Internet para fins ilícitos, note-se que o Capítulo II é intitulado "Dos Direitos e Garantias dos Usuários". Em momento algum, a lei prevê deveres dos usuários, tal como o dever de não utilizar a Internet para o cometimento de crimes ou ilícitos civis.

Tanto assim o é que, após a entrada em vigor do Marco Civil da Internet, em 23 de junho de 2014 (60 dias após a publicação ocorrida em 24 de abril de 2014), os aplicativos de trocas de mensagens continuam a ser utilizados para a prática dos mais diversos crimes e as decisões judiciais de interceptação do conteúdo das mensagens permanecem sistematicamente descumpridas.

Tais descumprimentos levaram às decisões de suspensão temporária do funcionamento do WhatsApp, cominação de multa e até mesmo à prisão do vice-presidente do Facebook na América Latina, Diego Dzodan, todas com fundamento legal no art. 10, §§ 1º e 2º, da Lei n.º 12.965/2014, combinado com o art. 12 da mesma lei:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
>
> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos

> arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
>
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o *caput* sua filial, sucursal, escritório ou estabelecimento situado no país.

Conforme se depreende da situação fática de repetida desídia no atendimento às determinações judiciais, as medidas trazidas pela Lei n.º 12.965/2014 são claramente ineficazes para compelir os aplicativos de mensagens instantâneas a colaborar com a persecução penal daqueles que fazem uso ilícito de seus serviços.

Isso se deve, em especial, ao fato de os administradores alegarem que não possuem registro das conversas travadas entre seus usuários, razão pela qual não poderiam fornecer os dados requisitados.

Parece evidente a existência de falhas na regulamentação legislativa referente à possibilidade de introdução de aplicativos de mensagens instantâneas em território nacional, pois não se afigura razoável que empresa que não esteja apta ao atendimento de determinações judiciais voltadas ao combate de crimes graves seja autorizada a funcionar livremente no país, atendendo mais de 100 (cem) milhões de brasileiros.

Antes da edição do Marco Civil da Internet, o Congresso Nacional já havia se deparado com a necessidade de regulamentação penal da invasão de dispositivos para coleta e divulgação de

dados telemáticos, por meio da edição da Lei n.º 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, por ter decorrido diretamente da invasão da caixa de *e-mails* da atriz, mediante a atuação de *hackers* que utilizaram as fotos íntimas para extorsão e posterior divulgação na Internet.

Tal fato criminoso ocorreu em maio de 2012 e culminou com a edição da Lei n.º 12.737/2012, publicada em 3 de dezembro de 2012, que alterou o Código Penal para introduzir o art. 154-A e B, assim como os §§ 1º e 2º do art. 266 e o parágrafo único do art. 298 do aludido diploma.

A alteração do art. 154 do Código Penal, denominada "invasão de dispositivo informático", visa punir, basicamente, a atuação do *hacker*, visto que a figura inserta no dispositivo 154-A tipificou a invasão de dispositivo informático para obter, alterar ou destruir informação alheia ou instalar *software* de vulnerabilidade para obter vantagem ilícita. O art. 154-B apenas dispõe que, em regra, será necessária a representação para a ação penal tipificada no artigo anterior, salvo se o crime for praticado contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios, ou empresas concessionárias de serviços públicos.

Ao art. 266 foram acrescentados o § 1º, que cria o crime de "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública" e o § 2º, que majora a pena daquele na hipótese de cometimento em ocasião de calamidade pública.

A Lei n.º 12.737/2012 alterou, ainda, o art. 298 do Código Penal, introduzindo ao dispositivo em referência o parágrafo único, que equipara a falsificação de cartão de crédito ou débito ao documento particular para fins penais.

Salta aos olhos a ausência de preocupação do Poder Legislativo com o tema da necessidade de acesso às comunicações

realizadas por meio de aplicativos para fins de investigação criminal e combate ao crime. A Lei n.º 12.737/2012 foi publicada em dezembro de 2012, em resposta a um fato ocorrido em maio do mesmo ano, após lapso temporal de cerca de 7 (sete) meses, apenas posteriormente foi editado o Marco Civil da Internet – Lei n.º 12.965/2014. Contudo, até o presente momento não há regulamentação relativa aos aplicativos, utilizados livremente para a prática de crimes.

Não obstante, é certo que o mero fato de não haver regulamentação específica acerca da necessidade de fornecimento de dados pelos administradores dos aplicativos de mensagens às autoridades judiciais certamente não os exime do atendimento de decisões judiciais.

Nesse passo, na ausência de previsão legislativa expressa e específica sobre o tema, é preciso analisar os meios possíveis para se lidar com a ausência de fornecimento do conteúdo das conversas trocadas por meio do WhatsApp e aplicativos correlatos.

3 Termo de Ajustamento de Conduta

Poder-se-ia cogitar a realização de Termo de Ajustamento de Conduta, introduzido no ordenamento jurídico nacional pelo art. 211 da Lei n.º 8.069/1990 – Estatuto da Criança e do Adolescente e, posteriormente, previsto no art. 13 da Lei n.º 8.078/1998 – Código de Defesa do Consumidor, que acrescentou o § 6º ao art. 5º da Lei n.º 7.347/1985 – Lei da Ação Civil Pública, que consiste, nos dizeres de MAZZILI (2006):

> Tal como está previsto no art. 5º, § 6º, da Lei n.º 7.347/85, o compromisso de ajustamento de conduta é lavrado em termo, e nele se contém uma obrigação de fazer ou não fazer; é ele tomado por um dos órgãos públicos legitimados à propositura da ação civil pública ou coletiva, e mediante esse instrumento, o causador do dano a interesses transindividuais (meio ambiente, consumidor, patrimônio cultural, ordem urbanística, etc.) se obriga a adequar sua conduta às exigências da lei, sob

> pena de cominações já pactuadas no próprio instrumento, o qual terá força de título executivo extrajudicial.
>
> O objeto do compromisso de ajustamento pode versar qualquer obrigação de fazer ou não fazer, no zelo de quaisquer interesses difusos, coletivos ou individuais homogêneos, o que inclui, basicamente, a proteção a danos efetivos ou potenciais aos seguintes interesses: a) meio ambiente; b) consumidor; c) ordem urbanística; d) patrimônio cultural (bens e valores artísticos, estéticos, turísticos, paisagísticos, arqueológicos, históricos); e) ordem econômica e a economia popular; f) crianças e adolescentes; g) idosos; h) pessoas portadoras de deficiência; i) investidores no mercado de valores mobiliários; j) quaisquer outros interesses transindividuais.
>
> [...]
>
> Ressalvada, pois, a questão da impossibilidade de transigência efetiva de direitos, no mais, o compromisso de ajustamento de conduta pode versar qualquer obrigação de fazer ou não fazer relacionada com a defesa de quaisquer interesses transindividuais (difusos, coletivos ou individuais homogêneos), como, por exemplo, questões ligadas ao meio ambiente, ao consumidor, ao patrimônio cultural, à ordem econômica e à economia popular, à ordem urbanística, etc.

Importa ressaltar que se está diante de interesse difuso, cuja definição contida no parágrafo único do art. 81 da Lei n.º 8.078/1990, inciso I, preceitua serem aqueles "transindividuais, de natureza indivisível, de que sejam titulares pessoas indeterminadas e ligadas por circunstâncias de fato", pois toda a sociedade é prejudicada pela ausência de colaboração dos aplicativos de mensagens instantâneas na prática de crimes realizados por tal via, em decorrência do fato de não atenderem às determinações judiciais que lhes são dirigidas.

Assim, caracterizando-se a negativa ao cumprimento de decisões judiciais que determinam o acesso aos dados de aplicativos de mensagens instantâneas como clara violação a direito coletivo, seria possível a realização de termo de ajustamento de conduta entre os legitimados para a propositura da ação coletiva e os administradores dos aplicativos em referência.

Tal medida possui a vantagem da agilidade. Afora a solução legislativa, constitui forma rápida e segura de resolução, ao menos parcial, do problema.

Contudo, não se pode ignorar a dificuldade de implementação, vez que os criadores e administradores do WhatsApp e Facebook, que adquiriu o primeiro em outubro de 2014, não parecem dispostos a transigir na questão da redução da privacidade dos usuários de seus programas, não obstante seus comunicados oficiais no sentido da prontidão para a colaboração com as autoridades segundo suas limitações técnicas, em nada condizentes com suas atitudes.

Ademais, o aplicativo tem sido beneficiado por decisões proferidas por Tribunais de Segundo Grau, assim como pelo Supremo Tribunal Federal quanto à reforma das determinações de suspensão dos serviços, colocando-os na cômoda situação de não precisarem sujeitarem-se ao fornecimento de informações sem que qualquer consequência os atinja.

4 Ações judiciais

Cuidando-se de direito difuso, a solução para a negativa de atendimento das determinações judiciais poderia ensejar o ajuizamento de Ação Civil Pública, uma vez que o art. 1º, inciso IV, da Lei n.º 7.347/1985 contém previsão residual de tutela dos direitos difusos ou coletivos não previstos nos incisos anteriores, como é o caso ora em análise.

Nessa hipótese, o legitimado para a propositura poderia pedir a condenação das empresas à implantação de tecnologia que possibilitasse o fornecimento de dados necessários ao atendimento de decisões judiciais.

A principal desvantagem da utilização da Ação Civil Pública na busca pelo cumprimento das decisões judiciais pelos administradores dos aplicativos de mensagens instantâneas reside

no fato de não constituir solução rápida, dado que tais ações possam perdurar por vários anos até o trânsito em julgado.

Ademais, a matéria já se encontra submetida ao Supremo Tribunal Federal, por meio da ADI n.º 5527/DF, de relatoria da Ministra Rosa Weber, e da ADPF n.º 403/SE, relatada pelo Ministro Edson Fachin.

A ADI n.º 5527/DF foi ajuizada em 16 de maio de 2016, pelo Partido da República (PR), e tem por objeto a declaração de inconstitucionalidade do art. 12, incisos III e IV, da Lei n.º 12.965/2014, assim como seja conferida interpretação conforme a Constituição ao art. 10, § 2º, de modo a limitar o seu alcance aos casos de persecução criminal.

Subsidiariamente, o partido autor requer seja declarada a nulidade parcial, sem redução de texto, do art. 12, incisos III e IV, da Lei n.º 12.965/2014, para que seja afastada a sua aplicação às ferramentas de "troca de mensagens", ou, ainda, para que seja condicionada a aplicação das sanções de suspensão temporária e de proibição do exercício das atividades à prévia frustração das sanções previstas nos incisos I e II.

A ação foi ajuizada em razão da utilização dos dispositivos impugnados a fim de justificar decisões judiciais determinando "a suspensão das atividades dos serviços de troca de mensagens pela Internet, sob o fundamento de que a empresa responsável pelo aplicativo se nega a disponibilizar à autoridade judiciária o conteúdo de mensagens privadas trocadas por usuários submetidos a investigação criminal".

No tocante ao pedido de interpretação conforme a Constituição, no art. 10, § 2º, da Lei n. 12.965/2014, de modo a limitar o seu alcance aos casos de persecução criminal, entendemos ser evidente que, uma vez que a disponibilização do conteúdo deve ocorrer "na forma que a lei estabelecer", impõe-se a aplicação da Lei n.º 9.296/1996, seja pela previsão contida no art. 1º, *caput*,

deste último diploma legal, que faz referência à interceptação de comunicações telefônicas, de qualquer natureza, seja em decorrência do parágrafo único, ao dispor que a legislação em comento aplica-se às comunicações em sistema de informática ou telemática.

> Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo único. O disposto nesta lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Ademais, não vislumbramos qualquer inconstitucionalidade no art. 12 da Lei n.º 12.965/2014. Consoante já referido no presente texto, a relativização, ou o afastamento do sigilo das comunicações voltadas ao crime, já tinha sido superada décadas atrás e não há sentido em retomá-la a cada vez que surgir novo recurso tecnológico destinado a facilitar a comunicação. Em última análise, é isso que se pretende com a ADI n.º 5527/DF.

Pende de julgamento, ainda, a Arguição de Descumprimento de Preceito Fundamental – ADPF nº 403/SE, ajuizada pelo Partido Popular Socialista (PPS) em face do Juiz de Direito da Vara Criminal da Comarca de Lagarto/SE, em decorrência da prolação de decisão que determinou a suspensão do aplicativo WhatsApp, em todo o território nacional, após a recusa do fornecimento de conteúdo de comunicações determinada nos autos do Processo n.º 201655000183.

A ADPF em questão possui como pedidos:

> nos termos do art. 5º, § 1º, da Lei n.º 9.882/99, diante da grave violação ao direito à comunicação livre e irrestrita, seja deferida a liminar pelo relator de plano, *ad referendum* do Tribunal Pleno, para suspender os efeitos da decisão do Juiz da Vara Criminal de Lagarto, Marcel Maia Montalvão, [que,] nos autos do Processo n.º 201655000183, bloqueou o aplicativo de comunicação WhatsApp por 72 horas, de forma que o mesmo volte a operar imediatamente;

> b) EM PROVIMENTO FINAL E DEFINITIVO, que seja julgado o presente pedido de arguição de descumprimento de preceito fundamental, para reconhecer a existência de violação ao preceito fundamental à comunicação, nos termos do art. 5º, inciso IX, com a finalidade de não mais haver suspensão do aplicativo de mensagens WhatsApp por qualquer decisão judicial (fl. 9 do documento eletrônico 1).

O então presidente do Supremo Tribunal Federal, Ministro Ricardo Lewandowski concedeu a medida liminar nos seguintes termos:

> [...]
>
> Sem adentrar no mérito do uso do aplicativo para fins ilícitos, é preciso destacar a importância desse tipo de comunicação até mesmo para intimação de despachos ou decisões judiciais, conforme noticiado pelo sítio eletrônico http://www.conjur.com.br/2016-fev-27/klaus-koplin-urgente-intimacao-feita-whatsapp.
>
> Ressalto, de resto, que não se ingressa aqui na discussão sobre a obrigatoriedade de a empresa responsável pelo serviço revelar o conteúdo das mensagens, conforme determinado pelo Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias/RJ e supostamente descumprido pelo WhatsApp, eis que isso constitui matéria de alta complexidade técnica, a ser resolvida no julgamento do mérito da própria ação.
>
> Assim, nessa análise perfunctória, própria das medidas cautelares, entendo que não se mostra razoável permitir que o ato impugnado prospere, quando mais não seja por gerar insegurança jurídica entre os usuários do serviço, ao deixar milhões de brasileiros sem comunicação entre si.
>
> Cito, por oportuno, a decisão proferida pelo Ministro Marco Aurélio na ADPF n.º 309/DF, cujo acórdão de julgamento foi assim ementado:
>
> "PODER DE CAUTELA – JUDICIÁRIO. Além de resultar da cláusula de acesso para evitar lesão a direito – parte final do inciso XXXV do art. 5º da Constituição Federal –, o poder de cautela, mediante o implemento de liminar, é ínsito ao Judiciário.
>
> POLÍTICA PÚBLICA DE ACESSIBILIDADE – REGULAMENTAÇÃO – MINISTÉRIO DAS COMUNICAÇÕES – AFASTAMENTO POR DECISÃO DE TRIBUNAL REGIONAL FEDERAL – ARGUIÇÃO NO SUPREMO – PENDÊNCIA

> DE APRECIAÇÃO – SEPARAÇÃO DE PODERES – INSEGURANÇA JURÍDICA – LIMINAR REFERENDADA. Envolvida matéria de alta complexidade técnica e pendente de solução em outra arguição formalizada, cumpre suspender decisão judicial a se sobrepor a futuro pronunciamento do Supremo" [grifos nossos].
>
> Isso posto, com base no poder geral de cautela, defiro a liminar para suspender a decisão proferida pelo Juízo da 2ª Vara Criminal da Comarca de Duque de Caxias/RJ, nos autos do IP 062-00164/2016, restabelecendo imediatamente o serviço de mensagens do aplicativo WhatsApp, sem prejuízo de novo exame da matéria pelo relator sorteado.

Distribuída a ação ao Ministro Edson Fachin, foram admitidos *amici curiae* e determinada a realização de audiência pública, visto que as questões extrapolam os limites estritamente jurídicos e exigem conhecimento transdisciplinar a respeito do tema, por meio de decisão prolatada em 27 de outubro de 2016, que também delimita o objeto da ADPF e as questões a serem dirimidas por meio da audiência pública:

> A presente ADPF n.º 403/SE traz, entre outras, discussões como (i) a possibilidade técnica ou não de interceptação de conversas realizadas por meio do aplicativo WhatsApp; (ii) a possibilidade ou não de suspensão temporária das atividades do aplicativo WhatsApp; (iii) a possibilidade ou não de colaboração do WhatsApp com as requisições judiciais baseadas no art. 5º, XII CRFB, Lei n.º 9.296/1996 e na Lei n.º 12.965/2014.
>
> [...]
>
> Assento que, aqueles que forem habilitados a participar da referida audiência pública deverão, como pré-requisito para sua atuação, trazer respostas a perguntas por ora preambulares abaixo elencadas, à luz da área específica de competência, sem prejuízo das demais contribuições que queiram trazer ao debate.
>
> 1. Em que consiste a criptografia de ponta a ponta (*end to end*) utilizada por aplicativos de troca de mensagens como o WhatsApp?
>
> 2. Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia de ponta a ponta (*end to end*)?

> 3. Seria possível desabilitar a criptografia de ponta a ponta (*end to end*) de um ou mais usuários específicos para que, dessa forma, se possa operar interceptação juridicamente legítima?
>
> 4. Tendo em vista que a utilização do aplicativo WhatsApp não se limita a apenas uma plataforma (aparelhos celulares/*smartphones*), mas permite acesso e utilização também em outros meios, como, por exemplo, computadores (no caso do WhatsApp mediante o WhatsApp Web/Desktop), ainda que a criptografia de ponta a ponta (*end to end*) esteja habilitada, seria possível "espelhar" as conversas travadas no aplicativo para outro celular/*smartphone* ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?

A audiência pública da ADPF 403/SE será aproveitada para o julgamento da ADI n.º 5527/DF.

Além dos aspectos técnicos mencionados pelo Ministro Edson Fachin, juridicamente, a questão que se coloca é: se, de fato, se concluir pela impossibilidade de quebra da criptografia do WhatsApp e aplicativos correlatos – fato que reputamos pouco provável, diante dos recursos tecnológicos atuais – simplesmente se decidirá no sentido da proibição de suspensão do aplicativo, de modo a perpetuar a atuação virtual voltada à prática do crime como verdadeiro território sem lei?

A propósito, é preciso ponderar que a lei sem o preceito secundário (sanção) torna-se mera sugestão de conduta, sem a coercibilidade que dela se espera.

Como se não bastasse, questiona-se, igualmente: como se pretende a persecução penal eficiente sem os instrumentos que permitam o monitoramento de ações criminosas de máxima gravidade?

Tais questões merecem ser ponderadas no julgamento das ações constitucionais aludidas.

Também não pode ser ignorado o fato de o próprio *site* do aplicativo prever, dentre as Políticas de Privacidade, a possibilidade

de coleta de dados quando seus administradores acreditam na necessidade da medida:

> Proteção jurídica
>
> Podemos coletar, usar, reter e compartilhar dados quando acreditarmos em boa-fé que isso se faz necessário para: (a) atuar conforme exigido pela legislação aplicável ou em processos judiciais ou administrativos; (b) impor nossos termos e outros termos e políticas aplicáveis, inclusive investigações sobre possíveis violações; (c) detectar, investigar, prevenir e resolver atividades fraudulentas e ilícitas ou questões de segurança ou técnicas; ou (d) proteger os direitos, a propriedade e a segurança de nossos usuários, do WhatsApp, da família de empresas do Facebook ou de terceiros[2].

Embora o texto não especifique quais dados seriam objeto de compartilhamento, questiona-se se as determinações judiciais são descumpridas mais por razões ideológicas dos criadores do aplicativo do que pelas alegadas impossibilidades técnicas, conduta altamente reprovável.

Ademais, o *site* do aplicativo prevê a possibilidade de não utilização da criptografia de ponta a ponta em aplicativos em versões desatualizadas:

> É possível que você toque em criptografia na tela de dados do contato ou dados do grupo e receba uma notificação dizendo que as mensagens que você enviar não são criptografadas de ponta a ponta. Nesse caso, é provável que você ou a pessoa com quem você está conversando precise atualizar para a versão mais recente do WhatsApp. Uma vez que todos os participantes de um grupo ou o seu contato em uma conversa individual tiverem atualizado para a versão mais recente do WhatsApp, um pequeno indicador irá aparecer na conversa lhes informando que as mensagens na sua conversa são criptografadas de ponta a ponta[3].

Não se tem notícias de o WhatsApp ter efetivamente comprovado a criptografia de ponta a ponta nos processos em que

[2] Disponível em: <https://www.whatsapp.com/legal/?l=pt_br#privacy-policy-information-we-collect>. Acesso em: 1 mar. 2017.

[3] Disponível em: <https://www.whatsapp.com/faq/pt_br/general/28030015>. Acesso em: 1 mar. 2017.

foram proferidas as decisões de interceptação das comunicações, limitando-se a alegar o descumprimento por impossibilidade técnica de obtenção das mensagens.

5 Possível medida incidental

Por fim, resta comentar as possíveis medidas a serem adotadas nas hipóteses de descumprimento de decisões judiciais no bojo de procedimento investigatório ou ação penal.

Partindo da premissa de que não serão cumpridas as determinações de fornecimento do conteúdo da comunicação ilícita travada entre os investigados ou réus, independentemente das sanções adotadas em face do WhatsApp ou aplicativos correlatos, segundo as informações prestadas até o momento por seus administradores em todo o mundo, é preciso buscar alternativas para auxiliar na prova dos delitos perpetrados por tal via, assim como para desestimular a utilização dos aplicativos para fins ilícitos.

Consoante já referido no presente texto, o art. 12 da Lei n.º 12.965/2014 prevê as seguintes sanções, sem prejuízo de outras de natureza cível, criminal ou administrativa:

a) advertência, com indicação de prazo para adoção de medidas coercitivas;

b) multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil, excluídos os tributos;

c) suspensão temporária das atividades;

d) proibição de exercício das atividades.

O Facebook Brasil chegou a ter milhões de reais bloqueados (apenas em um processo foram bloqueados 38 milhões de reais) pela Justiça Federal de Manaus – e ainda assim não cumpriu as determinações que lhe haviam sido direcionadas.

A suspensão temporária das atividades também não encontrou respaldo nos Tribunais, consoante já exposto.

Assim, há pouca – para não dizer nenhuma – efetividade nas medidas passíveis de adoção pelas autoridades responsáveis pela investigação e julgamento dos crimes praticados com a utilização do WhatsApp.

Não obstante, além das medidas previstas no art. 12 da Lei n.º 12.965/2014, há outra possibilidade prevista na Política de Privacidade do aplicativo, divulgada por meio de sua página na Internet, que prevê a possibilidade de desativar a conta utilizada para fins ilícitos:

> Uso aceitável de nossos serviços
>
> Nossos termos e políticas. Nossos serviços têm que ser utilizados de acordo com os nossos termos e políticas publicados. Se desativarmos a sua conta em decorrência de violação dos nossos termos, você não criará outra conta sem a nossa permissão.
>
> Uso lícito e aceitável. Os nossos serviços têm que ser acessados e utilizados somente para fins lícitos, autorizados e aceitáveis. Você não usará (ou ajudará outras pessoas a usar) nossos serviços: (a) de forma a violar, apropriar-se indevidamente ou infringir direitos do WhatsApp, dos nossos usuários ou de terceiros, inclusive direitos de privacidade, de publicidade, de propriedade intelectual ou outros direitos de propriedade; (b) de forma ilícita, obscena, difamatória, ameaçadora, intimidadora, assediante, odiosa, ofensiva em termos raciais ou étnicos, ou instigue ou encoraje condutas que sejam ilícitas ou inadequadas, inclusive a incitação a crimes violentos; (c) envolvendo declarações falsas, incorretas ou enganosas; (d) para se passar por outrem; (e) para enviar comunicações ilícitas ou não permitidas, mensagens em massa, mensagens automáticas, ligações automáticas e afins; ou (f) de forma a envolver o uso não pessoal dos nossos serviços, a menos que esteja autorizado por nós.

É certo que não se pode comparar a utilidade de tal medida com a interceptação das conversas em tempo real, nos moldes da Lei n.º 9.296/1996, para fins de investigação, contudo constitui medida que impõe algum tipo de limite à utilização de tais aplicativos como meio seguro para a prática de crimes.

Ademais, sem tais aplicativos, o criminoso pode ver-se forçado a utilizar as chamadas telefônicas regulares, passíveis de interceptação.

É certo que tal medida teria que ser permanente e extensível àqueles que emprestassem seus CPFs e números de telefone ao criminoso.

Não se tem notícia de qualquer determinação de desativação de conta do WhatsApp, assim também não se conhece qual seria a reação de seus administradores em face da determinação. É certo, porém, que não caberia a alegação de impossibilidade técnica de cumprimento, tampouco geraria a comoção social verificada com as suspensões.

6 Conclusão

Em decorrência do baixo custo ao consumidor em relação aos serviços prestados pelas operadoras de telefonia móvel, são cada vez mais utilizados em todo o mundo aplicativos de troca de mensagens instantâneas, por meio dos quais é possível realizar chamadas de voz e enviar mensagens de texto, imagens e vídeos.

No Brasil, segundo os dados da Anatel, em janeiro de 2017 havia 243 (duzentos e quarenta e três) milhões de linhas móveis ativas[4] e cerca de 25% (vinte e cinco por cento) delas é utilizada também para WhatsApp.

Em razão da utilização em larga escala pelos detentores de linhas móveis, praticidade e baixo custo, o aplicativo em questão já teve seu uso regulamentado por diversos órgãos do Poder Judiciário, denotando sua relevância e utilidade.

Em que pesem as vantagens que levam à utilização de tal aplicativo, há lacuna legislativa acerca da óbvia obrigatoriedade

[4] Disponível em: <http://agenciabrasil.ebc.com.br/economia/noticia/2017-03/numero-de-linhas-de-celulares-ativas-no-pais-registra-nova-queda-em-janeiro>. Acesso em: 28 fev. 2017.

de cumprimento às leis e decisões judiciais do país para que um aplicativo seja utilizado em território nacional.

Em decorrência de tal lacuna, bem como da recusa de fornecimento do conteúdo das comunicações, os aplicativos de mensagem instantânea têm sido utilizados livremente para o cometimento de crimes graves, como tráfico de drogas, armas e de pessoas, divulgação de imagens e vídeos de pedofilia, sequestro, fraudes, preparação de homicídios, atentados terroristas e estupros.

O Marco Civil da Internet, instituído pela Lei n.º 12.965/2014, prevê, em seu art. 10, § 2º, combinado com os arts. 11 e 12, incisos III e IV, a possiblidade de suspensão temporária das atividades e a proibição de exercício das atividades da empresa responsável pela prestação do serviço.

Discute-se a aplicabilidade das sanções de suspensão temporária do WhatsApp em decorrência do descumprimento de decisões judiciais de fornecimento do conteúdo de mensagens, por tal razão, aliada à comoção social gerada com as suspensões determinadas, todas as decisões judiciais que aplicaram a medida foram duramente criticadas pela mídia e reformadas pelos Tribunais.

A questão relativa à possibilidade de suspender temporariamente os serviços do aplicativo encontra-se submetida ao Supremo Tribunal Federal, por meio da ADI n.º 5527/DF e da ADPF n.º 403/SE. Está prevista a realização de uma audiência pública, vez que o julgamento depende de conhecimentos técnicos e transdisciplinares que extrapolam os limites estritamente jurídicos.

No presente trabalho, após o estudo dos termos de uso do próprio aplicativo, ficou evidente a possibilidade de coleta de dados quando os administradores do aplicativo acreditam necessário. A página do aplicativo não especifica, contudo, quais os dados passíveis de coleta e compartilhamento.

Os mesmos termos de uso preveem a possibilidade de não incidir a criptografia de ponta a ponta na hipótese de utilização de versão desatualizada do aplicativo.

Não obstante, não se tem notícia de os descumprimentos judiciais virem acompanhados de efetiva comprovação de impossibilidade técnica de obtenção do conteúdo das mensagens.

Ainda de acordo com os termos de uso do aplicativo, verificou-se a possibilidade de bloqueio na hipótese de ativação da conta que venha a ser utilizada para a incitação de crimes violentos ou para o envio de comunicações ilícitas.

É evidente que a medida não possui resultado investigativo, tal como a interceptação. Todavia, serviria para impor algum tipo de limite à utilização do aplicativo como meio seguro para a prática de crimes, além de, eventualmente, forçar o criminoso a utilizar a linha telefônica passível de interceptação.

Referências bibliográficas

BRASIL. Agência Nacional de Telecomunicações. Conselho Diretor da Anatel. Resolução n.º 426, de 9 de dezembro de 2005. Aprova o Regulamento do Serviço Telefônico Fixo Comutado (STFC). *Portal da Legislação*, Brasília, dez. 2005. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/20-2005/7-resolucao-426>. Acesso em: 26 fev. 2017.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei n.º 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. *Portal da Legislação*, Brasília, jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 25 fev. 2017.

___. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Portal da Legislação*, Brasília, abr. 2014. Disponível em: < http://www.

planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 25 fev. 2017.

____. Lei n.º 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. *Portal da Legislação*, Brasília, nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm >. Acesso em: 26 fev. 2017.

BRASIL. Supremo Tribunal Federal. Ação de Descumprimento de Preceito Fundamental n.º 403/SE. Rel. Min. Edson Fachin. Consulta Processual, Decisões da Presidência, 19 jul. 2016. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28ADPF%24%2ESCLA%2E+E+403%2ENUME%2E%29+E+S%2EPRES%2E&base=basePresidencia&url=http://tinyurl.com/zm94psj >. Acesso em: 28 fev. 2017.

____. Ação de Descumprimento de Preceito Fundamental nº 403/SE. Rel. Min. Edson Fachin. Consulta Processual, Decisões Monocráticas, 27 out. 2016. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28ADPF%24%2ESCLA%2E+E+403%2ENUME%2E%29+NAO+S%2EPRES%2E&base=baseMonocraticas&url=http://tinyurl.com/zm94psj>. Acesso em: 28 fev. 2017.

CRAIDE, Sabrina. Número de linhas de celulares ativas no país registra nova queda em janeiro. *Agência Brasil*, Brasília, 2 mar. 2017. Disponível em: <http://agenciabrasil.ebc.com.br/economia/noticia/2017-03/numero-de-linhas-de-celulares-ativas-no-pais-registra-nova-queda-em-janeiro>. Acesso em: 28 fev. 2017.

MAZZILLI, Hugo Nigro. Compromisso de ajustamento de conduta: evolução e fragilidades; atuação do Ministério Público. *Revista de Direito Ambiental*, v. 41, p. 93, jan. 2006. Disponível em: <http://www.mazzilli.com.br/pages/artigos/evolcac.pdf>. Acesso em: 27 fev. 2017.

WHATSAPP. Informação Legal do WhatsApp. *Termos de Serviço do WhatsApp*. Disponível em: <https://www.whatsapp.com/legal/?l=pt_br#key-updates>. Acesso em: 1 mar 2017.

WHATSAPP FAQGeral. *Criptografia de ponta a ponta*. Disponível em: <https://www.whatsapp.com/faq/pt_br/general/28030015>. Acesso em: 1 mar. 2017.

Operações da Polícia Federal na área cibernética

Valdemar Latance Neto*

RESUMO

Este trabalho tem a finalidade de compartilhar as experiências de três investigações na área cibernética, desenvolvidas pela Unidade de Inteligência Policial de Sorocaba/SP entre os anos de 2014 e 2016. A *Operação Moikano* investigou o compartilhamento por *e-mail* de arquivos contendo abuso sexual contra crianças e adolescentes. Além da identificação de dezenas de pessoas envolvidas nessa prática, foram descobertos alguns casos de estupro contra crianças. A *Operação Proteção Integral* também apurou o intercâmbio pela Internet de vídeos e fotos dessa natureza, mas os investigados utilizavam redes *peer-to-peer* em vez de *e-mails*. Por fim, a *Operação Barba Negra* cuidou de descobrir os responsáveis pela prática reiterada, na Internet, de crimes de violação de direitos autorais por meio da exibição pública de filmes, séries e programas de televisão em *sites*, sem a devida autorização.

Palavras-chave: Crimes cibernéticos. Pornografia infantil. Internet. Violação. Direitos autorais. Inquérito policial. Polícia Federal.

ABSTRACT

The present work intends to share the experience of three operations on cybercrime developed by the Intelligence Police Unit of Brazilian Federal Police from Sorocaba/SP between 2014 and 2016. The Operation Moikano investigated the sharing of child abuse material in the Internet by e-mail messages. Dozens of suspects were identified

* Bacharel em Direito pela Universidade de Sorocaba/SP (UNISO). Especialista em Inteligência Policial pela Academia Nacional de Polícia. Delegado de Polícia Federal, responsável pela Unidade de Inteligência Policial da Delegacia de Polícia Federal em Sorocaba/SP. *E-mail*: valdemar.vln@dpf.gov.br.

and the Brazilian Federal Police gathered proof of some rapes against children. The Operation Proteção Integral investigated the sharing of child abuse material in the internet by peer-to-peer networks. At last, the Operation Barba Negra discovered a criminal group behind daily crimes against copyright by sharing, in a website, movies, series and TV shows, without the authors' authorization.

***Keywords**: Cybercrime. Child pornography. Internet. Violation. Copyright. Police investigation. Federal Police.*

1 Introdução

Entre os anos de 2014 e 2016, a Unidade de Inteligência Policial da Delegacia de Polícia Federal de Sorocaba desenvolveu três investigações policiais que tinham como objeto condutas criminosas cometidas via Internet. Diante dos bons resultados alcançados nas operações *Moikano*, *Proteção Integral* e *Barba Negra*, esses trabalhos acabaram se tornando, em alguns aspectos, exemplos de boas práticas em investigações de crimes cibernéticos.

Seguindo a mesma linha da apresentação pessoal realizada nas instalações da Escola de Magistrados da Justiça Federal da 3ª Região (EMAG), este artigo tem a finalidade de relatar fatos ocorridos no curso dessas investigações e convidar o leitor a refletir sobre alguns pontos relevantes. Sem a pretensão de dar resposta definitiva às difíceis questões enfrentadas, procura-se adiante dividir essas experiências, narrando o que houve, as soluções adotadas e os resultados alcançados.

Em vez de longas discussões sobre temas controvertidos da área do Direito, pretende-se fazer um breve estudo de caso para cada uma dessas operações policiais, abordando temas nelas surgidos como cooperação de Google e Microsoft, afastamento do sigilo de dados telemáticos, compartilhamento de arquivos contendo abuso sexual de crianças e adolescentes, estupros contra crianças, violação de direitos autorais na Internet, cooperação de entidades privadas na investigação criminal, entre outros.

2 Operação Moikano

A Constituição da República impôs, no *caput* do seu art. 227, um dever à família, à sociedade e ao Estado de assegurar os direitos individuais à criança e ao adolescente, com "absoluta prioridade", protegendo-os de "toda forma de negligência, discriminação, exploração, violência, crueldade e opressão". As ideias que levaram à *Operação Moikano* emanam fundamentalmente desse dispositivo constitucional, que, infelizmente, não tem sido lembrado

como deveria nas investigações sobre fatos criminosos tipificados nos arts. 240 e seguintes do Estatuto da Criança e do Adolescente (Lei n.º 8.069/1990), em trâmite na Justiça Federal.

Este primeiro capítulo tem o fim de fazer um breve estudo de caso da investigação formalizada nos autos do Inquérito Policial n.º 225/2014-DPF/SOD/SP, levado a efeito na Delegacia de Polícia Federal da cidade de Sorocaba, entre 28 de abril de 2014 e 4 de julho de 2015. Resumidamente, a partir da prisão em flagrante do usuário da conta de *e-mail* moikano_br@hotmail.com, iniciou-se apuração com a finalidade de identificar os suspeitos que com ele compartilhavam, pela Internet, arquivos contendo exploração sexual de crianças e adolescentes[1].

Porém, os resultados obtidos foram além das expectativas iniciais. Ao fim do trabalho, tinham sido presos um contumaz estuprador de meninos entre 7 e 13 anos, um animador de festas infantis que narrava ter participado de orgias com crianças, um pai que abusava dos próprios filhos, entre outras histórias não menos relevantes que não cabem neste artigo. Ademais, no curso da investigação, um suspeito foi preso enquanto ainda planejava abusar sexualmente de uma vizinha de 9 anos, graças à célere decisão judicial da 1ª Vara Federal de Sorocaba/SP, após pedidos formulados em caráter de urgência pela Polícia Federal.

[1] A legislação consagrou a expressão "pornografia infantil", um eufemismo para o que os arquivos produzidos, compartilhados ou possuídos pelos investigados realmente retratam: ou estupros ou exploração sexual de crianças e adolescentes. Quem já teve a árdua tarefa de analisar incontáveis arquivos nesse tipo de investigação sabe que essa expressão ameniza demais o que deveria retratar. A título de comparação, a Interpol padronizou o uso da expressão genérica "exploração sexual de crianças e adolescentes" (*child sexual exploitation*), que nos parece mais adequada a retratar o teor desses arquivos. "*It is worth noting that we avoid using the term 'child pornography' when describing images of sexual abuse of children. Other, more appropriate terminology includes the term 'child sexual abuse material'*." (Disponível em: <https://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children>. Acesso em: 5 mar. 2017. A despeito disso, como "pornografia infantil" consta da lei brasileira, será utilizada no texto.

Antes de detalhar essas histórias, contudo, convém voltar ao início. Nos últimos meses do ano de 2013, após retornar a Sorocaba/SP de um período de trabalhos em investigações que tramitaram na cidade de São Paulo/SP, expus à chefia da delegacia minha disposição pessoal de ficar responsável por todas as investigações que cuidassem de condutas criminosas que envolvessem a distribuição pela Internet ou posse de arquivos contendo abuso ou exploração sexual de crianças e adolescentes. Fiz isso movido, basicamente, pelo sentimento protetivo que a paternidade me trouxe, bem como por uma dose de frustração de realizar trabalhos policiais para uma vítima abstrata, a União, de resultados praticamente invisíveis no mundo real. Imaginava que teria mais motivação em atuar em casos cujo resultado pudesse efetivamente trazer alguma proteção a crianças.

Acabei contemplado com essas investigações, mesmo porque nunca foi tarefa fácil recrutar interessados em atuar nessa área. O primeiro problema, porém, apresentou-se imediatamente. Não havia uma investigação promissora sequer. Naquele momento, todos os inquéritos policiais da delegacia versavam sobre fatos antigos. A maioria deles dizia respeito a possíveis crimes cometidos, cerca de 2 (dois) anos antes, pela rede social Orkut[2], que, àquela altura, era pouquíssimo utilizada e estava prestes a ser extinta.

Um trabalho investigativo da Polícia Federal mudaria esse panorama. Nos últimos meses de 2013, policiais federais do Paraná coordenaram a deflagração, em âmbito nacional, da *Operação Glasnost*, cuja finalidade era identificar suspeitos que

[2] Essas investigações tinham sido iniciadas pelo Ministério Público Federal em São Paulo/SP, a partir de informações encaminhadas pelo Google. Basicamente, eram feitos pedidos de afastamento do sigilo dos dados ao Poder Judiciário que, após deferidos, ensejavam o envio de ofícios judiciais às operadoras. Com os dados cadastrais do contratante, incluindo o local de onde a conexão à Internet suspeita tinha sido feita, pedia-se a declinação da competência e a Justiça Federal de São Paulo/SP encaminhava o caso ao juiz territorialmente competente. Nos casos mencionados no texto, o Ministério Público Federal em Sorocaba requisitava a instauração de inquérito policial, na chegada do caso. Isso tudo, porém, demorava meses para ocorrer, o que prejudicava a obtenção de bons resultados.

compartilhavam arquivos contendo exploração sexual de crianças e adolescentes por meio de um *site* russo. Um dos locais de busca domiciliar era na cidade de Itu/SP, dentro da circunscrição da Delegacia de Polícia Federal de Sorocaba/SP, onde acabou sendo preso em flagrante, na posse de arquivos ilícitos, o investigado que utilizava a conta de *e-mail* moikano_br@hotmail.com.

Era o início da *Operação Moikano*. Juntamente com o pedido de autorização para busca domiciliar, a Polícia Federal solicitou à 1ª Vara Federal de Sorocaba/SP o afastamento do sigilo dos dados dessa conta de *e-mail*, com a finalidade de obter todo o material telemático nela armazenado. Instada pelo Poder Judiciário, a Microsoft encaminhou à Polícia Federal os dados contidos nessa conta a partir dos quais se descobriu uma enorme rede internacional de compartilhamento de arquivos contendo violência sexual contra crianças e adolescentes.

Partindo da conta moikano_br@hotmail.com, foram atentamente analisadas as mensagens e identificados os interlocutores que trocaram arquivos ilícitos com o suspeito. Em seguida, a Polícia Federal apresentou ao Poder Judiciário outros pedidos de afastamento do sigilo dos dados das novas contas descobertas, utilizadas pelos comparsas. No decorrer da investigação, 176 (cento e setenta e seis) contas tiveram o sigilo afastado por decisão da 1ª Vara Federal de Sorocaba/SP. Como o material ilícito e as informações que podiam levar à identificação dos suspeitos estavam armazenados nessas contas, não haveria outro meio de obter a prova necessária à demonstração dos crimes senão pela cooperação das empresas que detinham os dados. Em outras palavras, ou se obtinha o conteúdo das mensagens de *e-mail* ou não seria obtida a materialidade necessária para comprovar os crimes.

Google e Microsoft, portanto, foram fundamentais para o sucesso da investigação. A *Operação Moikano* marca uma louvável mudança de postura dessas empresas quanto à cooperação com o

Estado brasileiro. Anteriormente, no curso da *Operação Durkheim*[3], deflagrada pela Polícia Federal em São Paulo/SP, no final de 2012, Google e Microsoft haviam se negado a cumprir decisões judiciais que afastavam o sigilo de contas de *e-mail*, usando, em resumo, o frágil argumento de que não estavam sujeitas à legislação brasileira, porque seus servidores ficavam nos Estados Unidos. Foram necessárias corajosas decisões judiciais da 5ª Vara Criminal Federal de São Paulo/SP[4], atendendo a pedidos da Polícia Federal, impondo pesadas multas diárias na hipótese de descumprimento para, finalmente, essas empresas entregarem o que tinham armazenado nas contas que foram objeto da medida.

De outro lado, na *Operação Moikano*, nenhum confronto foi necessário. Em vez de conflito, cooperação. Os bons resultados obtidos na investigação vieram do apoio do Google e, principalmente, da Microsoft, responsável por gerenciar a maioria das contas que foram identificadas na grande rede de distribuição de arquivos contendo violência sexual contra crianças e adolescentes.

Ainda nesse tema, cumpre ressaltar que a técnica de investigação utilizada não foi a interceptação telemática, mas o afastamento do sigilo dos dados armazenados. No curso da *Operação Moikano*, os sucessivos pedidos apresentados pela Polícia Federal eram para que o Poder Judiciário, diante de robustos indícios de condutas criminosas tipificadas no art. 241-A do Estatuto da Criança e do Adolescente (Lei n.º 8.069/90), determinasse ao Google e à Microsoft que encaminhassem todo o material armazenado na conta do suspeito. Em alguns casos, isso significava mensagens armazenadas há anos.

[3] Inquérito Policial n.º 004/2010-COR/SR/DPF/SP.

[4] O Google chegou a impetrar no TRF3 mandado de segurança tentando evitar a entrega dos dados. Após o indeferimento do pedido de liminar nesse mandado de segurança, os advogados da empresa procuraram a Polícia Federal para viabilizar a entrega das mensagens armazenadas nas contas que tiveram o sigilo afastado pela Justiça Federal em São Paulo.

Não cabe confundir, portanto, com a interceptação telemática, sujeita aos requisitos da Lei n.º 9.296/96, que consiste em acompanhar, concomitantemente, pelo prazo de 15 (quinze) dias todo o fluxo de dados telemáticos. Para demonstrar a atividade criminosa dos vários suspeitos na *Operação Moikano*, a interceptação telemática não seria suficiente. O planejamento era demonstrar que alguns deles praticavam o mesmo crime há anos, trocando material ilícito por *e-mail*, e, além disso, armazenando esses arquivos na Internet. Se fosse utilizada a interceptação telemática, o material armazenado antes da decisão judicial nunca seria descoberto, já que os 15 (quinze) dias passariam a valer dela em diante.

Usando a técnica adequada, foi possível identificar com segurança boa parte dos usuários das contas suspeitas, ou, pelo menos, descobrir o local de onde o suspeito estabeleceu a conexão com a Internet para praticar o crime com indícios suficientes a justificar uma busca domiciliar, no curso da qual a autoria poderia ser descoberta.

Com efeito, a partir dos dados contidos na conta moikano_br@hotmail.com e nas de seus interlocutores, uma grande quantidade de material telemático foi encaminhada à Polícia Federal por Google e Microsoft. Foram necessários meses de intenso e árido[5] trabalho pela equipe de investigação da Unidade de Inteligência Policial da Delegacia de Polícia Federal de Sorocaba/SP para analisar todos esses arquivos. Ao todo, 176 (cento e setenta e seis) contas tiveram o sigilo constitucional afastado. Ao fim do exame de todas elas, colheram-se evidências de que 75 (setenta e cinco) eram utilizadas por pessoas que agiam em território estrangeiro, circunstância apta a afastar qualquer dúvida quanto à competência da Justiça Federal.

[5] A análise das imagens contendo exploração sexual de crianças é uma atividade extremamente desgastante com alto risco de causar sintomas como ansiedade, pesadelos, desinteresse sexual, exaustão, depressão, desesperança, insônia, obesidade, intolerância, entre outros.

De fato, a troca de material ilícito veiculado em mensagens de *e-mail* entre dois interlocutores no Brasil não seria suficiente para configurar hipótese de competência federal, conforme jurisprudência consolidada do Superior Tribunal de Justiça[6]. No caso, porém, havia um grande número de suspeitos trocando arquivos contendo abuso sexual de crianças e adolescentes entre si e boa parte deles estava em outros países, como Chile, Paraguai, Colômbia, Estados Unidos, Espanha, entre outros. As informações obtidas, portanto, traziam indícios concretos da transnacionalidade das condutas criminosas sob apuração.

Feita essa breve digressão para tratar rapidamente da competência, voltemos à análise do material encaminhado por Google e Microsoft. Para cada uma das contas foi elaborado um relatório de análise de polícia judiciária, com o fim de identificar o usuário da conta e verificar se havia arquivos contendo pornografia infantojuvenil nas mensagens. A estratégia mostrava-se trabalhosa desde quando foi vislumbrada, mas não havia outra saída senão a leitura de cada mensagem, ainda que rapidamente. Um deslize do suspeito, em uma mensagem escondida entre milhares, podia ensejar sua identificação, o que de fato aconteceu em alguns casos.

As vantagens dessa técnica de investigação foram a identificação segura de boa parte dos suspeitos, a produção da prova

[6] "CONFLITO DE COMPETÊNCIA. DIREITO PROCESSUAL PENAL. ART. 241, *CAPUT*, DA LEI N.º 8.069/90. DIVULGAÇÃO. CRIME PRATICADO NO TERRITÓRIO NACIONAL POR MEIO DE PROGRAMA DE COMUNICAÇÃO ELETRÔNICA ENTRE DUAS PESSOAS. COMPETÊNCIA DA JUSTIÇA ESTADUAL. 1. " 'Aos juízes federais compete processar e julgar: os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no país, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente.' (Constituição Federal, art. 109, inciso V.) 2. Em se evidenciando que os crimes de divulgação de fotografias e filmes pornográficos, ou de cenas de sexo explícito envolvendo crianças e adolescentes, não se deram além das fronteiras nacionais, restringindo-se a uma comunicação eletrônica entre duas pessoas residentes no Brasil, não há como afirmar a competência da Justiça Federal para o processo e julgamento do feito. 3. Conflito conhecido, para declarar competente o Juízo Estadual suscitante." (STJ, CC 57411/RJ, Terceira Seção, Rel. Min. Hamilton Carvalhido, julg. 13 fev. 2008, DJ 30 jun. 2008.)

antes mesmo da realização de busca domiciliar e, por consequência, a extraordinária diminuição do risco de equívocos no momento mais invasivo das buscas nas residências suspeitas, evitando a indesejável atribuição do rótulo social de "pedófilo" a alguém que nenhuma relação tinha com as condutas suspeitas.

Algumas desvantagens (ou dificuldades) também se revelaram no curso da análise de milhares de mensagens examinadas. A primeira e mais óbvia era justamente a quantidade extraordinária de material para analisar. Como a maioria dos investigados evitava mencionar informações pessoais nas mensagens de *e-mail*, era preciso examinar detalhadamente cada uma em busca de uma pista que levasse à identificação do suspeito.

Apesar de a fartura de material probatório garantir o sucesso do trabalho de investigação, isso causou de pronto a angústia decorrente da possibilidade de haver, em meio a tanta informação, situações urgentes que demandassem resposta imediata da Polícia Federal. O desafio era identificá-las e, eventualmente, neutralizá-las sem comprometer o imprescindível sigilo da primeira fase da investigação, antes das buscas domiciliares.

Outra dificuldade era descobrir se havia alguma investigação anterior sobre o mesmo suspeito. Como a rede de compartilhamento de arquivos era internacional e integrada também por pessoas que estavam em diferentes cidades brasileiras, era muito provável a existência de investigações anteriores, em outras unidades policiais, que tivessem como objeto os mesmos suspeitos. Uma vez que havia material demais para analisar, a equipe de investigação não podia se dar ao luxo de fazer um trabalho que já estava sendo feito por outros policiais, em alguma outra unidade (da Polícia Federal ou mesmo das Polícias Civis).

Essas vantagens e desvantagens serão abordadas, novamente, nos casos que serão relatados adiante. Antes, porém, cabe registrar que a *Operação Moikano* foi deflagrada no dia 30 de junho de 2015, quando a Polícia Federal deu cumprimento a

50 (cinquenta) mandados de busca domiciliar e 31 (trinta e um) mandados de prisão preventiva expedidos pela 1ª Vara Federal de Sorocaba/SP, que deferiu integralmente os pedidos feitos na representação policial. Nesse dia, 13 (treze) suspeitos foram presos em flagrante, por armazenar arquivos contendo exploração sexual infantil. Das várias histórias ocorridas no curso do trabalho foram escolhidas quatro cujo relato tem o escopo de desconstruir dois mitos equivocados sobre o compartilhamento de pornografia infantil pela Internet. O primeiro é o de que os autores desse tipo de crime não representam qualquer risco à sociedade, por serem meros coitados, desajustados, que passam a vida em frente ao computador se masturbando. O segundo diz respeito à falsa ideia de que se trata apenas de "arquivos de computador", numa visão desfocada do que eles realmente retratam: estupros de crianças.

2.1 A vizinha

A análise das dezenas de *gigabytes* não estava na metade ainda, quando, ao chegar ao trabalho, um dos policiais federais da UIP/DPF/SOD/SP me chamou para ver algo que demandaria ação urgente. Era uma mensagem de *e-mail*, que continha uma conversa por escrito entre dois suspeitos, na qual um deles, morador da cidade de Joinville/SC, contava que tinha conseguido "passar a mão" no corpo de uma menina "loirinha", "linda", de "9 anos", que morava nas redondezas. Ele lamentava não ter sido capaz de levá-la para dentro de sua casa, onde poderia estuprá-la. Então, pedia a seu interlocutor, que anteriormente narrara algumas aventuras sexuais com crianças, dicas de como convencer a menina a entrar na casa dele. Prometia, por fim, enviar-lhe fotos das cenas de sexo com a criança se obtivesse sucesso.

Embora pudesse se tratar de uma conversa fantasiosa, utilizada apenas para provocar o imaginário sexual do interlocutor, a hipótese de ocorrer efetivamente a violência sexual contra essa criança não poderia ser descartada, nem, portanto, ignorada.

Imediatamente, todas as atividades da unidade policial tiveram que ficar em segundo plano para cuidarmos, prioritariamente, deste caso.

O primeiro passo foi requisitar, com urgência, os dados cadastrais do usuário do IP, na data e horário da mensagem em questão. Com a rapidez necessária, a operadora respondeu fornecendo o nome e a qualificação do responsável pelo contrato de Internet, bem como o endereço de onde foi feita a conexão.

Este caso, aliás, é excelente para ilustrar a relevância do disposto no art. 15 da Lei n.º 12.850/2013:

> O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de Internet e administradoras de cartão de crédito.

Isso porque, antes da vigência da lei, havia diferentes entendimentos sobre o tema; houve um tempo em que prevalecia a necessidade de autorização judicial para a obtenção de meros dados cadastrais do responsável pela Internet. Era necessário, então, formular representação pedindo o encaminhamento de ofício judicial às operadoras para conseguir obter o nome, a qualificação e o endereço do responsável pelo contrato. Obviamente, isso levava muito mais tempo do que a requisição direta e era uma das razões do insucesso das investigações do passado. Em vez de meses, o dispositivo possibilitou que os dados fossem obtidos no mesmo dia.

Com o endereço de conexão à Internet, solicitou-se à Delegacia de Polícia Federal em Joinville/SC a realização de diligências nas proximidades. Duas policiais federais diligentemente estiveram no bairro e conseguiram identificar uma menina cujas características correspondiam à descrição feita na mensagem acima mencionada. Aos 9 anos, ela ia à escola de manhã e passava todas as tardes aos cuidados de seu irmão de cerca de 14 anos, enquanto sua

mãe trabalhava. Não havia mais dúvida da existência e da grande vulnerabilidade da menina.

Quanto ao investigado, ele foi identificado na rede social Facebook. Tomando como parâmetro de pesquisa o *e-mail* que ele usava para trocar material ilícito, foi possível encontrar seu perfil, no qual ele utilizava o apelido "Maneca", o mesmo usado para assinar algumas das mensagens de *e-mail* que continham arquivos com cenas de estupro de crianças.

Uma circunstância, porém, colocava em dúvida essa identificação. Todas as conexões à Internet tinham sido feitas na residência ao lado da do suspeito. O responsável pelo contrato era um policial militar, pai de duas filhas que tinham entre 8 e 11 anos. Embora remota, havia a possibilidade de o policial militar estar se passando pelo vizinho para realizar atividades criminosas na Internet. O mais provável, no entanto, era que o suspeito estivesse usando clandestinamente a Internet do vizinho.

Nessas circunstâncias excepcionais, em meio a uma grande quantidade de informações e de fatos diferentes, pediu-se autorização judicial para desmembrar esse caso específico do inquérito policial da *Operação Moikano* para instauração de um novo inquérito e, assim, cuidar separadamente das possíveis condutas criminosas do suspeito de Joinville/SC. Ao mesmo tempo, formulou-se representação solicitando autorização para realizar busca domiciliar na residência do suspeito e na casa do seu vizinho policial, local de instalação da Internet, apontado pela operadora.

O Poder Judiciário autorizou a busca domiciliar nos dois locais e decretou a prisão preventiva do suspeito, diante do comprovado planejamento de estuprar a criança que morava nas redondezas. As equipes policiais foram devidamente instruídas da situação peculiar e orientadas a tomar cautela extraordinária na busca domiciliar que seria realizada na casa do policial militar cujo nome constava como responsável pela Internet. Na verdade, se não houvesse uma incrível surpresa, a finalidade dessa busca na casa do

policial limitar-se-ia a esclarecer o porquê do uso da sua Internet para distribuição de pornografia infantil.

No dia do cumprimento dos mandados judiciais, o usuário da conta manecasilva@hotmail.com foi preso em flagrante, em sua casa, na posse de material contendo abuso sexual de crianças e adolescentes. Sem qualquer incidente, esclareceu-se, na casa do policial militar, que este autorizara o suspeito a utilizar a Internet, em retribuição a um favor que o vizinho lhe tinha feito anteriormente. Na verdade, o suspeito tinha se separado recentemente e estava sem Internet instalada em sua própria residência e acabou apelando ao policial militar, que o autorizou a instalar um cabo que levasse a Internet até a casa ao lado. Não imaginava o policial que o suspeito utilizaria a rede mundial para a prática de crime dessa natureza.

Embora não seja possível afirmar com certeza que o usuário da conta manecasilva@hotmail.com reuniria coragem suficiente para estuprar a menina, o fato é que, em algum momento, ele, no mínimo, imaginou fazê-lo. Tudo indica, na verdade, que fantasiava isso a cada vez que a via na rua de sua casa. Foi além, ao verbalizar esse desejo ao seu interlocutor e pedir dicas para convencer a vítima a entrar em sua casa, onde se tornaria uma presa fácil.

As provas colhidas após as buscas domiciliares e prisão em flagrante do suspeito apontam que o estupro não ocorreu. Pode ser que a ação policial, tomada após imprescindível e rápida autorização judicial, tenha impedido esse estupro. Ou que não, obviamente. Talvez o suspeito nunca encontrasse a oportunidade perfeita para atacar a vítima de apenas 9 anos.

De qualquer forma, persiste a boa sensação de ter protegido a criança desse possível ataque, talvez evitando um evento que poderia causar-lhe efeitos deletérios, físicos e psicológicos para o resto da vida. O caso mostra o peso da responsabilidade de atuar em investigações que envolvem o compartilhamento de exploração sexual infantil pela Internet. A dignidade sexual de crianças pode,

sim, estar em risco efetivo, real, e o estupro de uma criança pode ocorrer caso a atuação do Estado demore.

Se de um lado a responsabilidade se mostra gigantesca, de outro o caso retrata o quão gratificante é ter evitado uma violência que traria cicatrizes permanentes na criança, uma vítima que motivou os policiais federais, tão acostumados a proteger apenas a irreal União, a atuar ainda com mais afinco, por nos lembrar das razões fundamentais, primárias, que, em algum momento, nas brincadeiras inocentes da infância, tiveram influência na escolha da nossa arriscada, penosa e apaixonante profissão.

2.2 O palhaço

O meticuloso trabalho de analisar, uma a uma, todas as mensagens da conta de *e-mail* utilizada para compartilhar arquivos contendo abuso sexual de crianças traz a vantagem de possibilitar, em alguns casos, a identificação irrefutável do suspeito. Na *Operação Moikano*, isso aconteceu no caso do palhaço *Ricocó*, o usuário da conta multishowricoco@hotmail.com que trabalhava como animador de festas infantis, na cidade de Salvador/BA.

Em conversas por *e-mail* com outro comparsa, *Ricocó* trocou arquivos contendo abuso sexual de crianças e adolescentes e, em um desses diálogos, mencionou que tinha um perfil na rede social Facebook, oferecendo algumas informações que possibilitavam encontrar sua página pessoal. Com elas não foi difícil obter diversas fotos do suspeito, imagens de propaganda do seu personagem contendo um número de telefone celular para contratação de *show*s, nome e sobrenome, entre outras informações que não deixavam dúvida quanto à identificação do usuário do *e-mail* multishowricoco@hotmail.com.

O exame do perfil do palhaço *Ricocó* no Facebook era extremamente perturbador. Após a descoberta das preferências sexuais do suspeito, pela análise do material contido na conta de *e-mail*, não foi fácil evitar essa sensação ruim ao constatar que na

página dele havia dezenas de fotos em que o palhaço estava rodeado de inúmeras crianças, nas mais diversas situações. Em algumas, provavelmente no mundialmente conhecido carnaval de Salvador/BA, o palhaço dançava alegremente com crianças pequenas, vestidas em trajes mínimos, aparentemente da mesma idade das várias vítimas que figuravam nos vídeos e fotos compartilhados pelo suspeito na Internet.

Como se não bastasse o que foi obtido na rede social, nas próprias mensagens de *e-mail* analisadas havia arquivos de divulgação do trabalho de animador de festa infantil, com as informações necessárias para a contratação do palhaço *Ricocó*. Havia, também, fotos pessoais do suspeito, que ele encaminhara para amigos e familiares. As informações não deixavam dúvida alguma sobre a identidade do usuário da conta multishowricoco@hotmail.com, a qual integrava a grande rede de distribuição pela Internet de arquivos contendo abuso sexual de crianças e adolescentes.

Foram requisitados os dados cadastrais do responsável pelo telefone informado na página de Facebook para a contratação dos *shows* do palhaço *Ricocó*. Na resposta, como esperado, vieram justamente os dados do suspeito.

O caso retrata duas vantagens do afastamento de sigilo dos dados telemáticos de contas de *e-mail*: identificar pessoalmente o responsável pelo compartilhamento de arquivos ilícitos na Internet (autoria) e obter, antes da busca domiciliar, esses arquivos (materialidade), com informações precisas de data e horário das condutas criminosas.

Definida com segurança a autoria dos crimes cometidos por meio da conta multishowricoco@hotmail.com, cuja materialidade já se encontrava disponível pela cooperação da Microsoft, uma outra circunstância, narrada no próximo tópico, foi fundamental para que a Polícia Federal postulasse o desmembramento dessa parte da investigação, que se mostrava mais bem instruída que os outros casos e não poderia esperar o desfecho destes.

2.3 O amigo dos pais

Um dos interlocutores do palhaço *Ricocó* compartilhou com ele arquivos contendo abuso sexual de uma criança de aparentemente 8 anos, sexo masculino, por meio da conta leo_oliveira_santoandre@live.com. O primeiro exame das imagens, porém, já indicava que se tratava de material inédito, recentemente produzido.

Realizou-se, então, uma análise detalhada de todas as informações contidas nos arquivos de imagem enviados ao palhaço *Ricocó*. Descobriu-se que as fotos tinham sido tiradas no dia 10 de janeiro de 2015, uma semana antes do envio, por meio de um telefone da marca Samsung. Infelizmente, porém, não havia as coordenadas geográficas nos arquivos, que podiam apontar seguramente o local exato do estupro do menino.

Foram extraídas as informações de IP, data, horário e fuso das mensagens encaminhadas por meio da conta leo_oliveira_santoandre@live.com e, com isso, foram requisitados os dados cadastrais do responsável pelo contrato de Internet. Na resposta, a operadora informou que todas as conexões tinham sido feitas por um cliente, morador da cidade de Santo André/SP, que tinha na composição de seu nome tanto "Leonardo" quanto "Oliveira", referências empregadas para formar o endereço de *e-mail* utilizado para a prática dos crimes.

Foram feitas diligências no local de onde partiram as conexões à Internet e policiais federais confirmaram que o suspeito continuava a residir ali.

A Polícia Federal pediu a prisão preventiva dos usuários das contas multishowricoco@hotmail.com e leo_oliveira_santoandre@live.com e autorização para busca domiciliar nos seus endereços. Os requerimentos foram integralmente deferidos pela 1ª Vara Federal de Sorocaba/SP.

No dia 30 de junho de 2015, foram cumpridos os mandados judiciais. Infelizmente, quando da realização da busca domiciliar, o palhaço *Ricocó* não foi encontrado em sua residência, de onde aparentemente tinha acabado de se mudar. Ele ficou foragido por algum tempo, mas acabou preso alguns meses depois. Em 9 de agosto de 2016, o palhaço *Ricocó* foi condenado, em Primeira Instância, a cumprir 9 (nove) anos e 10 (dez) meses de reclusão, com início de cumprimento em regime fechado, pela prática de crimes de posse e compartilhamento de arquivos contendo abuso sexual infantojuvenil.

Embora a busca domiciliar tenha sido infrutífera, ele armazenava em sua conta de *e-mail* esses arquivos (art. 241-B do ECA) e, em algumas mensagens, também compartilhou com alguns comparsas (art. 241-A do ECA). A prova obtida antes da realização da busca domiciliar, por meio da técnica adequada, possibilitou essa condenação.

De outro lado, no cumprimento do mandado judicial de busca domiciliar na casa do usuário da conta leo_oliveira_santoandre@live.com, ele foi preso em flagrante por possuir arquivos contendo abuso sexual de crianças. O celular Samsung, utilizado para tirar as fotos antes mencionadas, foi apreendido nesse dia e nele foram encontrados novos arquivos registrando abuso sexual de outras vítimas, todos meninos entre 7 e 13 anos.

Esses meninos foram identificados e ouvidos com o auxílio de uma psicóloga, na Superintendência da Polícia Federal em São Paulo/SP. Os pais ficaram surpresos com a notícia, uma vez que consideravam o suspeito, que morava no mesmo bairro de todas as vítimas, um amigo.

Posteriormente, examinando algumas conversas que o suspeito teve com outros comparsas por aplicativos de comunicação, constatou-se que a dica principal, em sua opinião, para conseguir ter acesso às crianças que potencialmente se tornariam vítimas de estupro, era justamente ficar amigo dos pais. "Fique amigo dos

pais", disse a um comparsa que, maravilhado com as aventuras sexuais com crianças que lhe foram narradas, indagara como ele conseguia ficar sozinho com as vítimas.

Efetivamente, na esmagadora maioria dos casos de abuso sexual, o agressor é alguém muito próximo da criança. A dica de ouro do usuário da conta leo_oliveira_santoandre@live.com tem embasamento em números e estudos internacionais. Sem angariar a simpatia e a confiança dos pais, dificilmente o agressor sexual terá a oportunidade de ficar sozinho com a criança.

Leonardo foi condenado pela 1ª Vara Federal de Sorocaba/SP à pena de 74 (setenta e quatro) anos, 6 (seis) meses e 5 (cinco) dias de reclusão pela prática dos crimes tipificados no ECA e pelo estupro de 5 (cinco) crianças, identificadas no curso da *Operação Moikano*. Essa sentença foi proferida em 9 de dezembro de 2015, pouco mais de 5 (cinco) meses após a deflagração da operação policial.

Com o investigado preso, o laudo pericial contendo o exame do material apreendido foi formulado em menos de 30 (trinta) dias. Apresentado o relatório do inquérito policial, o Ministério Público Federal promoveu a ação penal, munido de fartas provas, e, ao final do processo penal em Primeira Instância, o Poder Judiciário impôs a pena de reclusão com celeridade louvável.

Eis outro caso que sempre deixará a agradável sensação de dever cumprido. As conversas que Leonardo travara com outros comparsas, pelo computador, mostram que ele não pararia de abusar sexualmente dessas crianças. Ao contrário, ele buscava claramente meios de justificar para si mesmo que o que fazia não era errado, não lesava as crianças que, afinal, consentiam e gostavam de ganhar presentes, sorvetes e passeios no *shopping*, em troca de estupros. Se não estivesse preso, os abusos às 5 (cinco) vítimas identificadas continuariam, sem dúvida alguma. Outras crianças, certamente, também seriam abusadas, assim que ele conseguisse conquistar a confiança dos pais.

2.4 O pai catequista

Dentre as centenas de contas de *e-mail* examinadas no curso da *Operação Moikano*, o endereço quero-sexo_2013@hotmail.com chamou a atenção por ter encaminhado, em um pacote com diversos arquivos contendo violência sexual contra crianças, uma foto de um menino de sunga, em uma praia. Essa imagem parecia ter sido tirada pelo próprio suspeito, diferentemente dos outros arquivos, já conhecidos de investigações anteriores. Como a conexão à Internet utilizada apontava que o usuário dessa conta estava na cidade de Santos/SP, surgiu a hipótese de o menino ser vítima de abuso sexual. Outra possibilidade era que o investigado tirasse fotos de crianças de sunga na praia, sem que ninguém percebesse, e as utilizasse posteriormente como moeda de troca na rede de compartilhamento de pornografia infantil da qual fazia parte.

Diferentemente, por exemplo, do caso do palhaço *Ricocó*, narrado acima, as informações disponíveis nas mensagens da conta quero-sexo_2013@hotmail.com não foram suficientes para identificar o seu usuário. Serviram apenas para apontar o endereço de onde foram feitas as conexões à Internet. Tratava-se de uma casa situada nos fundos de um imóvel, em cuja parte da frente funcionava uma creche para as crianças, ligada à igreja, na cidade de Santos/SP.

Em diligências feitas por policiais federais no local, diante da imperiosa necessidade de manter o sigilo até aquele ponto da investigação, não foram obtidas informações capazes de apontar um possível suspeito. Havia apenas o nome do responsável pelo contrato de Internet com a operadora. Diante das circunstâncias, havia a possibilidade de tratar-se de um computador utilizado por diversas pessoas, o que dificultaria (ou até inviabilizaria) a identificação do suspeito.

Pediu-se autorização judicial para busca domiciliar no local, única diligência capaz de levar à identificação do usuário

da conta quero-sexo_2013@hotmail.com. Era necessário, porém, extrema cautela na execução da ordem judicial, proferida pela 1ª Vara Federal de Sorocaba, por se tratar de um imóvel com ligação à igreja, sem um suspeito clara e previamente apontado pelas informações até então disponíveis. Uma grande preocupação na deflagração da *Operação Moikano* era impedir que algum inocente tivesse a honra manchada, em seu círculo social, com uma injusta e indelével atribuição do rótulo de "pedófilo".

Em casos como este, em que o endereço estava claramente identificado, mas o suspeito ainda não, as equipes policiais foram instruídas a agir com uma dose extra de cautela e utilizar vestimentas e viaturas descaracterizadas, desde que as circunstâncias locais permitissem fazê-lo com segurança.

Não houve qualquer incidente. No dia da deflagração da *Operação Moikano*, o usuário da conta quero-sexo_2013@hotmail.com não só foi identificado como acabou preso em flagrante na posse de fotos e vídeos contendo abuso sexual de crianças.

Contrariando uma orientação geral da coordenação da operação policial de pedir a prisão preventiva dos suspeitos que fossem identificados, a autoridade policial que presidiu o auto de prisão em flagrante entendeu, com base nas informações disponíveis naquele momento, arbitrar fiança, colocando o investigado em liberdade imediatamente.

Com isso o caso não tinha prioridade para a realização de perícia no material apreendido. Surgiu o problema da demora na elaboração do laudo em material de informática, tema de outra apresentação no evento da EMAG. Em virtude da elevada sobrecarga de requisições de perícia dessa natureza, 2 (dois) anos era, aproximadamente, a média de demora para a elaboração de laudo em um caso sem prioridade.

No inquérito policial do usuário da conta quero-sexo_2013@hotmail.com, o laudo ficou pronto em janeiro de

2017, cerca de 18 (dezoito) meses depois da deflagração da *Operação Moikano*. O teor do laudo pericial escancarou o equívoco de ter libertado o investigado, sob fiança. A suspeita inicial de que ele poderia ser um agressor sexual de crianças se confirmou. O pior é que, dentre suas vítimas, estavam os próprios filhos, um menino de aproximadamente 11 anos e uma menina de 3.

Vieram à tona conversas perturbadoras em que o suspeito relatava ter abusado do próprio filho, exibia o desejo de presenciar seu menino ser penetrado por alguém, em um barco, no meio do mar, onde os gritos da criança não seriam ouvidos por ninguém. Havia, também, diálogos em que o investigado encaminhou fotos da própria filha nua, ainda bebê, dizendo que só não a penetrava porque iria machucá-la e não teria como explicar à esposa.

Diante das novas informações, a Polícia Federal formulou outros pedidos, que foram deferidos pela Justiça Federal de Santos/SP. No dia 21 de janeiro de 2017, em nova busca domiciliar feita em sua casa, o suspeito foi, mais uma vez, preso em flagrante na posse de arquivos contendo estupro de crianças.

Ouvido, o filho do suspeito confirmou que já tinha sido vítima de abuso sexual praticado pelo pai. Disse que este o obrigava a ficar em frente à *webcam*, exibindo-se nu a estranhos, com os quais o pai batia papo pela Internet. Contou, ainda, que ao mexer no *tablet* do pai, viu fotos da própria irmã nua, então com 3 anos de idade, entre outros absurdos.

Em meio a farto material contendo abuso sexual de crianças, também foram encontradas várias fotos do suspeito na igreja, rodeado de crianças, onde exercia a nobre função de catequista. Ao contrário do que se imagina, os envolvidos nesse tipo de crime comumente têm ligação intensa com a igreja (independentemente de qual), buscando na religião expiar a culpa pelos atos cometidos contra as crianças.

O caso mostra a relevância da prisão processual de prováveis agressores sexuais. Obviamente, em uma prisão em flagrante, nem sempre há todas as informações necessárias para identificar indícios de que se trata de um estuprador de crianças. Mas o que houve com o catequista de Santos/SP lembra a relevância de analisar com maior cautela as investigações que envolvem o compartilhamento pela Internet de arquivos com exploração sexual infantil. Eventual equívoco nessa decisão pode significar devolver o estuprador às vítimas.

De toda forma, trata-se de mais um abusador de crianças que, com algum atraso, foi afastado da sociedade graças às informações colhidas no decurso da *Operação Moikano*. O caso continua em andamento, circunstância que trouxe sensível limitação para a redação deste tópico. Certamente, as provas colhidas pela Polícia Federal serão suficientes para o Poder Judiciário aplicar a pena merecida pelo estuprador dos próprios filhos.

3 Operação Proteção Integral

O intercâmbio de arquivos por *e-mail* traz grande limitação na quantidade de dados a serem compartilhados entre os interlocutores. O modo de agir utilizado pelos investigados durante a *Operação Moikano* não serve, por exemplo, para a troca de arquivos muito grandes, como vídeos em alta definição ou grande quantidade de fotos.

Há alguns anos os interessados em obter grande quantidade de arquivos na Internet utilizam as denominadas redes *peer-to-peer* (ponto a ponto), cuja característica peculiar é possibilitar o compartilhamento direto de arquivos entre os computadores dos usuários, sem a existência de um servidor centralizado. Vários aplicativos como eMule, Shareaza, Ares Galaxy, LimeWire, etc., que utilizam essa tecnologia, estão disponíveis gratuitamente na rede mundial para quem quiser utilizar.

Por meio de qualquer deles, uma pessoa que disponibiliza arquivos para compartilhamento em seu computador possibilita, em tempo real, que qualquer outro usuário do mesmo aplicativo os acesse, em qualquer lugar do mundo, desde que conectado à Internet. Essas transferências de arquivos ocorrem inclusive por fragmentos de dados provenientes de vários usuários da rede, simultaneamente. Ao fazer um *download*, portanto, o usuário consegue pegar partes do arquivo de diferentes pessoas. Esses fragmentos são armazenados em diretório temporário do computador até que todas as partes do arquivo sejam obtidas, complementando-o. Até mesmo esses fragmentos baixados já ficam, automaticamente, à disposição para *download* por parte dos outros usuários (ainda que o arquivo não esteja completo na pasta compartilhada).

Ao instalar um programa de compartilhamento dessa natureza, o usuário, livremente, aceita compartilhar uma pasta de seu computador (ou *smartphone*, *tablet*, etc.) com os outros usuários do aplicativo. Todos os arquivos contidos nessa pasta (ainda que parciais) podem ser visualizados e obtidos, livremente, pelos outros usuários do programa, por *download*.

Por serem fáceis de usar e possibilitarem o compartilhamento de uma grande quantidade de dados, os programas acima mencionados são muito populares, no mundo inteiro. São usados, por exemplo, para baixar da Internet música, vídeos, livros e jogos. Após instalados, basta o usuário inserir expressões de seu interesse nos mecanismos de busca, avaliar os resultados e clicar nos arquivos que lhe interessam obter.

O problema é que os compartilhadores de pornografia infantil encontram a mesma facilidade nesses aplicativos. Inserindo nos mecanismos de busca expressões comumente utilizadas, como "*pedo*", "*pthc*", "*incest*", "*hussyfan*", etc., aparecem inúmeros arquivos dessa natureza para escolha do usuário.

Nesse contexto, para coibir a disseminação de arquivos contendo abuso sexual de crianças e adolescentes pela Internet, e

para possibilitar a responsabilização penal de seus autores, foram criadas técnicas de identificação de atividades criminosas nas redes *peer-to-peer*.

Como as pastas compartilhadas de todos os usuários têm as suas informações abertas livremente a qualquer outro usuário do mesmo programa, é possível identificar por meio do chamado *hash*[7], uma espécie de "DNA" do arquivo, se determinado usuário possui nessa pasta algum arquivo que contenha pornografia infanto-juvenil.

A partir de um catálogo de arquivos de pornografia infantil, cujos códigos de identificação única (*hash*) são conhecidos graças a investigações anteriores, torna-se possível identificá-los nas pastas compartilhadas pelos usuários desses aplicativos. Por consequência, é possível determinar quais usuários estão distribuindo-os na Internet.

Assim, utilizando informações disponibilizadas pelos próprios usuários desses aplicativos de compartilhamento em redes *peer-to-peer*, a Polícia Federal, nos primeiros meses de 2016, identificou 15 (quinze) locais, nas cidades de São Paulo, Sorocaba e Itapetininga, de onde se distribuía grande quantidade de arquivos contendo abuso sexual de crianças.

Foram instaurados inquéritos policiais separados para apurar a conduta de cada um dos investigados. Todos foram instruídos com uma informação de polícia judiciária explicando o funcionamento básico desses aplicativos e a forma como foram obtidas as informações sobre as condutas suspeitas. Distribuídos livremente, os 8 (oito) inquéritos da Delegacia de Sorocaba/SP[8]

[7] *Hash* é uma sequência alfanumérica que identifica unicamente uma informação computacional como um arquivo. Se um arquivo possui o mesmo valor *hash* que outro, pode-se afirmar com certeza que ambos possuem exatamente o mesmo conteúdo, ainda que tenham nomes diferentes entre si.

[8] Os demais foram instaurados na cidade de São Paulo pelo GRCC/SR/PF/SP, que trabalhou em conjunto com a UIP/DPF/SOD/SP durante a investigação e deflagração da *Operação Proteção Integral*.

espalharam-se pelas 4 (quatro) varas da Justiça Federal da cidade. Todas receberam pedidos da Polícia Federal de autorização para realização de busca domiciliar nos endereços identificados e deferiram.

Neste tipo de investigação dificilmente se identifica o suspeito antes da busca domiciliar. Diferentemente do que foi relatado antes, quanto à *Operação Moikano*, em que as informações contidas nas mensagens de *e-mail* possibilitaram determinar o suspeito previamente, a descoberta de atividades ilícitas em redes *peer-to-peer* permite a identificação segura do local de onde são feitas as conexões à Internet. Em regra, a autoria é esclarecida durante a busca domiciliar e nos atos subsequentes da investigação.

A vantagem da técnica de investigação utilizada na *Operação Proteção Integral* é que foram obtidas informações recentíssimas das conexões à Internet utilizadas pelos suspeitos. Se na *Operação Moikano* costumávamos requisitar dados cadastrais com informações mais antigas (de meses ou anos atrás, a depender da data da mensagem), na *Operação Proteção Integral* dispúnhamos algumas vezes de informações de 2 (dois) minutos atrás. Com dados muito mais recentes era extraordinariamente maior a chance de prender os suspeitos em flagrante delito, na posse dos arquivos ilícitos.

Nas cidades de Sorocaba e Itapetininga, foram realizadas 8 (oito) buscas domiciliares autorizadas pelas 4 (quatro) varas da Justiça Federal de Sorocaba/SP, no dia 31 de março de 2016, quando foi deflagrada a *Operação Proteção Integral*. Sete suspeitos foram identificados como usuários dos programas de compartilhamento e presos em flagrante delito, na posse de arquivos contendo abuso sexual de crianças e adolescentes.

Em um dos endereços, o suspeito não foi preso em flagrante porque tinha o costume de baixar os arquivos e, imediatamente, apagá-los. Ainda assim, a busca domiciliar serviu para apu-

rar a autoria do crime de distribuição desses arquivos, por meio de aplicativo de compartilhamento em rede *peer-to-peer*.

No total, dos 15 (quinze) suspeitos cujos endereços foram objeto de busca domiciliar no dia 31 de março de 2016, durante a deflagração da *Operação Proteção Integral*, 13 (treze) foram presos em flagrante. Para se ter uma ideia, na *Operação Moikano*, foram 13 (treze) prisões em flagrante num universo de 50 (cinquenta) locais de busca[9].

As informações mais recentes da *Operação Proteção Integral* provaram ser mais efetivas para a prisão em flagrante do suspeito, confirmando a hipótese de que a rapidez da investigação em crimes cibernéticos é fundamental para a obtenção de bons resultados.

Falando em celeridade, um dos casos pode ser adotado como exemplo de boas práticas para a Polícia Federal, o Ministério Público Federal e o Poder Judiciário. Diz respeito a um dos presos em flagrante, que teve a prisão preventiva decretada pela 3ª Vara Federal de Sorocaba/SP, no dia da deflagração da *Operação Proteção Integral*, 31 de março de 2016. Diante da prioridade, o laudo pericial no material de informática apreendido não demorou nem 30 (trinta) dias, o que possibilitou a conclusão do inquérito policial. O suspeito foi denunciado, o processo penal transcorreu e, em 15 de julho de 2016, pouco mais de 3 (três) meses depois, ele foi condenado à pena de reclusão de 10 (dez) anos e 11 (onze) meses pela prática dos crimes tipificados nos arts. 241-A e 241-B do ECA.

Diferentemente desse caso, porém, os inquéritos que cuidam das condutas praticadas pelos suspeitos que não tiveram a prisão preventiva decretada continuam em curso, aguardando

[9] Isso não significa que nos demais locais a busca domiciliar foi inútil. Como registrado em tópico próprio, na maioria dos casos da *Operação Moikano*, o investigado estava identificado antes da busca. Mas como as informações eram mais antigas, extraídas de mensagens de *e-mail* armazenadas, era muito maior a chance de o suspeito ter apagado os dados, trocado de computador, etc.

a elaboração do laudo pericial, principal motivo da demora desse tipo de investigação.

Por fim, cumpre registrar que, na *Operação Proteção Integral*, um dos investigados também foi identificado como estuprador de crianças. Quando da deflagração, não havia qualquer informação nesse sentido ainda. Ele foi preso, denunciado e, enquanto estava em curso o processo penal, um cidadão apareceu na Delegacia de Polícia Federal em Sorocaba/SP para relatar que seu filho, frequentador da mesma igreja do preso, tinha sido vítima de abuso sexual.

Apurou-se que o investigado era membro de confiança da banda de uma igreja situada no centro de Sorocaba/SP. Frequentador do local há muitos anos, ele possuía livre acesso, inclusive quando não havia ninguém ali. Valendo-se da sua posição proeminente como membro da igreja, o suspeito atraía as vítimas com ensaios fora de hora e com presentes (instrumentos musicais, comida, dinheiro, etc.), abusando de, pelo menos, 4 (quatro) meninos. Um deles foi vítima dos 6 aos 15 anos de constantes abusos sexuais, ocorridos majoritariamente na própria igreja, segundo seu próprio relato, agora aos 18 anos.

O caso continua em andamento, o que impede maiores detalhes. Reforça, porém, o argumento de que o compartilhamento de pornografia infantil pela Internet e o abuso sexual de crianças e adolescentes são faces da mesma moeda.

4 Operação Barba Negra

Em setembro de 2015, a *Motion Picture Association America Latina* (MPA Latin America), representante dos maiores estúdios de produção de filmes do mundo, apresentou à Polícia Federal representação das vítimas, nos termos do disposto no art. 186, IV, do Código de Processo Penal, na qual pedia o início de investigação com o fim de apurar quem eram os responsáveis pelo

site Mega Filmes HD, então o maior *site* da América Latina de exibição de filmes e seriados, sem a devida autorização.

Na época o megafilmeshd.net tinha cerca de 60 (sessenta) milhões de visitantes por mês e estava na 39ª posição entre os *sites* mais visitados do país. O acervo de vídeos era extenso e incluía filmes que ainda estavam em exibição nos cinemas. O sucesso de audiência, porém, também decorria da praticidade e funcionalidade do próprio *site*. Para assistir sem gastar nada a qualquer dos títulos, a única exigência era o aborrecimento de clicar em algumas propagandas que apareciam antes do início da execução do vídeo.

Essas informações já foram trazidas pela própria representante das vítimas ao pedir o início da investigação para a Polícia Federal. Uma das novidades deste caso foi justamente dispor, no inquérito policial, desde o início, de um razoável conjunto de provas documentais apresentado pelo ilustre advogado.

O funcionamento do *site*, por exemplo, foi registrado em uma ata notarial passo a passo. Diversas pesquisas em fontes abertas, disponíveis na Internet, também já foram apresentadas apontando os autores dos possíveis crimes de violação de direitos autorais. Como na polícia se costuma começar a maioria das investigações com meros fragmentos de informações, que devem ser meticulosamente trabalhados para tentar esclarecer as suspeitas iniciais, a *Operação Barba Negra* fugiu ao padrão nesse quesito. O competente trabalho da associação e do seu advogado facilitou de maneira extraordinária o desenvolvimento da investigação policial desde o início.

O primeiro tema relevante deste caso já apareceu no pedido de início de investigação quanto à dúvida se seria mesmo hipótese de atuação da Polícia Federal e, por conseguinte, de competência da Justiça Federal.

Utilizando ferramentas de medição de audiência que verificam a localização aproximada dos visitantes do *site*, o advogado

da associação demonstrou que, aproximadamente, 15% (quinze por cento) dos cerca de 60 (sessenta) milhões de visitantes mensais estavam em território estrangeiro, mormente em países com grande número de brasileiros, como Portugal, Estados Unidos e Japão.

Presentes indícios concretos de transnacionalidade, restava verificar se nos crimes sob investigação estavam previstos tratado ou convenção internacional para atrair a aplicação do disposto no art. 109, V, da Constituição da República. Indo além da boa argumentação apresentada pelo advogado da associação, a exemplar decisão judicial que apreciou os pedidos feitos pela Polícia Federal, ao cuidar amplamente da questão da competência, reconheceu a existência de várias convenções promulgadas pelo Brasil a proteger o direito autoral como a Convenção de Berna para a Proteção das Obras Literárias e Artísticas (Decreto n.º 75.699/75); a Convenção Universal sobre Direito de Autor (Decreto n.º 76.905/75), na qual se assume o compromisso de assegurar a proteção suficiente e eficaz dos direitos dos autores de obras cinematográficas; a Convenção de Roma (Decreto n.º 57.125/1965), bem como a Convenção Interamericana sobre os Direitos de Autor em Obras Literárias, Científicas e Artísticas, firmada em Washington, no ano de 1946, e promulgada no Brasil pelo Decreto n.º 26.675, de 18 de maio de 1949.

Em resumo, em vista de indícios concretos de transnacionalidade decorrente da audiência internacional, bem como da circunstância de haver convenções internacionais firmadas pelo Brasil para a proteção aos direitos autorais, a 1ª Vara Federal de Sorocaba/SP reconheceu sua competência para a apreciação dos pedidos da Polícia Federal, comentados adiante, seguindo, *mutatis mutandis*, o entendimento então pacificado do Superior Tribunal de Justiça quanto ao delito tipificado no art. 241-A do Estatuto da Criança e do Adolescente.

Feita essa breve digressão para expor a questão da competência, cabe rememorar que foi apresentada pelo advogado

boa parte das pesquisas necessárias para chegar aos responsáveis pelo esquema criminoso. Coube à Polícia Federal, em um primeiro momento, apenas confirmar todos os elementos de convicção trazidos logo na representação da vítima.

No mesmo passo, requisitou-se ao setor de perícias a preservação do *site* megafilmeshd.net para que os dados ficassem armazenados e disponíveis posteriormente ao Poder Judiciário.

Ainda com o fim de instruir os pedidos que seriam feitos à 1ª Vara Federal de Sorocaba/SP, foram produzidos alguns vídeos de curta duração, que registravam cenas da tela do computador utilizado para acessar o *site* megafilmeshd.net. Nesses vídeos, ficaram registrados o grande acervo de filmes e seriados, a existência de títulos que ainda estavam no cinema e o procedimento necessário para assistir às obras disponíveis. Foi um meio encontrado de mostrar, de forma fiel e dinâmica, o funcionamento do *site*.

Como antecipado, a única exigência para assistir de graça a qualquer um dos títulos disponíveis no megafilmeshd.net era o aborrecimento de clicar em alguns anúncios, antes do início da execução do filme. O usuário selecionava o título e, em seguida, era obrigado a fechar as novas janelas ou visualizar cerca de 3 (três) anúncios publicitários. Essa era a forma de pagamento utilizada pelos milhares de usuários do *site*.

Com a grande audiência de cerca de 60 (sessenta) milhões de visitas mensais, ocupando a 39ª colocação entre os *sites* mais visitados do Brasil, e com uma página no Facebook que possuía mais de 5 (cinco) milhões de seguidores, o megafilmeshd.net atraiu a atenção do mercado publicitário, que se tornou a fonte de renda do esquema criminoso de violação de direitos autorais. Variando um pouco no modo de pagamento, cada visualização de anúncio e cada clique em propaganda que gerasse uma visita ao *site* do anunciante rendia algum valor às pessoas por trás do *site*.

Isso tornou muito lucrativa a atividade ilícita e fez com que alguns dos principais responsáveis pela organização criminosa passassem a exibir, orgulhosamente, no seu círculo social, real e virtual, o fruto desse trabalho: carros de luxo, bolsas e roupas de *grife*, etc. Diligências policiais nas redondezas das casas dos suspeitos confirmaram as informações iniciais trazidas pela associação, indicando incompatibilidade entre o patrimônio aparente que possuíam e determinadas circunstâncias pessoais como desemprego, endereço, falta de explicação para sinais de riqueza repentina, etc.

Aliando os documentos trazidos pela associação na representação que pediu o início do inquérito policial às diligências policiais, mencionadas acima, descobriu-se que os filmes e seriados eram obtidos na própria Internet, armazenados em serviços gratuitos ilimitados da rede mundial, e os *links* eram disponibilizados de maneira bem organizada e visualmente amigável na página do megafilmeshd.net.

Para executar o esquema, alguns dos envolvidos trabalhavam na gerência do *site*, outros no desenvolvimento técnico da página, assegurando a consistência e funcionalidade necessárias para manter e cativar a audiência, e alguns na obtenção e colocação dos títulos em serviços de armazenamento gratuito na Internet.

Formou-se, assim, um robusto conjunto de indícios da existência de uma organização criminosa montada com a finalidade de obter considerável lucro mensal por meio da constante violação de direitos autorais, que consistia em disponibilizar na Internet um enorme acervo de títulos de filmes, seriados e programas de televisão, sem a devida autorização.

Com fundamento nesses indícios, a Polícia Federal pediu à 1ª Vara Federal de Sorocaba/SP a prisão temporária de um casal suspeito de chefiar a organização criminosa, a condução coercitiva de 5 (cinco) possíveis auxiliares, a realização de busca domiciliar em 4 (quatro) locais (nos estados de São Paulo e Minas Gerais), o bloqueio das contas bancárias, o afastamento do sigilo das contas

de *e-mail* e, por fim, a suspensão do uso do domínio megafilmeshd.net. Todos os pedidos foram deferidos.

Uma novidade foi justamente a última medida apontada no parágrafo anterior. Tendo em vista o enorme número de acessos ao *site* megafilmeshd.net e, portanto, as constantes violações aos direitos autorais, era urgente tornar indisponível os *links* disponibilizados de modo organizado a partir do domínio megafilmeshd.net, o qual tinha angariado considerável valor financeiro.

Assim, já se vislumbrava que, logo que os investigados deixassem de administrar o domínio, alguém passaria a fazê-lo (ou ao menos tentaria). Pretendia-se, pois, deixar o endereço eletrônico indisponível na tentativa de evitar que o Poder Judiciário fosse novamente acionado para retirar a página do ar. Então, a ordem judicial determinou à empresa responsável pelo domínio que, em vez da página com conteúdo ilícito, fosse exibido o comunicado: "O domínio megafilmeshd.net está indisponível por ordem da 1ª Vara Federal de Sorocaba".

Cumpre destacar, de outro lado, o relevantíssimo papel da prisão temporária para a boa instrução do inquérito policial e para a retirada imediata do *site* do ar. De fato, levando em conta os elementos indiciários então presentes, o Poder Judiciário reconheceu a possível existência de uma organização criminosa voltada à prática reiterada de crimes de violação de sigilo funcional (art. 184, § 3º, do Código Penal, e art. 2º da Lei n.º 12.850/13) e decretou a prisão temporária dos dois investigados que exerciam a coordenação das atividades criminosas, conforme requerido pela Polícia Federal.

Nessa decisão, o eminente juiz federal determinou que, enquanto não fosse implementada a suspensão do uso do domínio megafilmeshd.net, a prisão processual iria persistir. Em outras palavras, enquanto o *site* estivesse no ar, acessível para a violação do direito dos autores, a continuação da prática criminosa justificaria

a continuação da prisão temporária e, eventualmente, a decretação da prisão preventiva com o fim de resguardar a ordem pública.

Neste ponto, cabe destacar que os investigados utilizavam um serviço de privacidade para tornar anônimos os responsáveis pelo *site*. Havia a possibilidade de a empresa estrangeira contratada para tal mister colocar empecilhos para o cumprimento da ordem judicial. No entanto, a combinação da medida de suspensão com a decretação da prisão temporária evitou qualquer problema. Cientes de que ficariam presos provisoriamente enquanto os crimes estivessem acontecendo com o *site* no ar, os próprios investigados viram-se motivados a cooperar fornecendo as senhas de acesso para gerenciar o megafilmeshd.net. Isso possibilitou que a Polícia Federal conseguisse de imediato dar cumprimento à ordem judicial, tirando o *site* do ar no mesmo dia das buscas domiciliares, ocorridas em 18 de novembro de 2015, quando da deflagração da *Operação Barba Negra*. Foram apreendidos computadores, telefones celulares, mídias, joias, dinheiro e 4 (quatro) automóveis.

A retirada do *site* megafilmeshd.net provocou uma enxurrada de reclamações na Internet de milhares de pessoas que compunham a sua incrível audiência. No dia da deflagração e no seguinte, a expressão #prayformegafilmeshd foi uma das líderes no *ranking* do Twitter, tanto nacional como mundial. Eram reclamações sérias de alguns, a maioria alegando que a Polícia Federal deveria se preocupar com outros crimes mais graves e com a prisão do ex-presidente Lula, em vez de acabar com a diversão do povo e prender seus supostos benfeitores. A maior parte dos textos, porém, era composta de manifestações bem-humoradas de internautas que lamentavam o fim do *site* megafilmeshd.net.

A repercussão da deflagração acabou gerando interesse da CPI dos crimes cibernéticos, que estava em curso no Congresso Nacional na época. A Polícia Federal foi convidada a tratar da *Operação Barba Negra* em sessão desta CPI, no dia 17 de dezembro de 2015.

Na oportunidade, um resumo semelhante a este foi apresentado aos ilustres parlamentares. Destacou-se a relevância da verba publicitária para financiamento dos crimes descobertos durante a *Operação Barba Negra*, circunstância que coincidia com algo que a própria CPI constatara: havia até comerciais do Governo Federal sendo veiculados em *sites* semelhantes ao megafilmeshd.net.

Ao final dos trabalhos da Comissão Parlamentar de Inquérito, a *Operação Barba Negra* influenciou em algumas partes da redação final do relatório, como neste trecho que trata da verba publicitária como forma de financiamento da pirataria digital:

> Com base em denúncia apresentada nesta CPI pelo Sub-relator da área, em Audiência Pública no dia 8 de outubro de 2015, com a presença do Sr. Edinho Silva, Ministro da Secretaria de Comunicação Social da Presidência da República, foi verificado que as entidades contratantes de serviços de publicidade e as agências de propaganda, em se tratando de veiculação de publicidade na Internet, não possuem o controle final sobre quais sítios efetivamente veiculam os anúncios contratados. Isso se deve a que algoritmos verificam quais sítios de Internet possuem maior quantidade de acessos e automaticamente a essas páginas são direcionados os anúncios contratados. Assim, como apresentado na denúncia, propagandas de empresas tradicionais e até do governo podem terminar sendo veiculadas em sítios utilizados para a prática de crimes cibernéticos, neste caso o *streaming* ilegal de filmes e séries de televisão. Pouco tempo após a denúncia apresentada, foi deflagrada a Operação Barba Negra, da Polícia Federal, que resultou em prisões e na suspensão dos serviços do maior sítio de compartilhamento ilegal de filmes, o sítio Mega Filmes HD [grifo nosso].
>
> Dessa forma, esse tipo de derivação automática de publicidade nos leva a propor a criação de um Código de Boas Práticas a ser adotado pelas entidades envolvidas com a publicidade no meio digital, para evitar a comercialização de espaço para anúncios publicitários em plataformas digitais que disponibilizem conteúdos ilícitos, pratiquem condutas ilegais e/ou fomentem a prática de tais condutas pelos seus usuários. Esse Código de Boas Práticas poderá ensejar posterior assinatura de Termo de Ajustamento de Conduta entre os principais sítios de Internet, Conar,

> associações de mídia digital e Ministério Público Federal. (Parte III, 5, "e") [10]

Posteriormente, a *Operação Barba Negra* foi considerada a maior operação policial de combate à pirataria em *sites* da América Latina do ano de 2015. A Polícia Federal inclusive teve a honra de receber prêmio internacional no evento denominado *Show East*, realizado na cidade de Miami, estado da Flórida, nos Estados Unidos, no final de 2016.

Nada disso, porém, impediu que outras pessoas tentassem se aproveitar da fama conseguida pelo megafilmeshd.net para ganhar dinheiro facilmente, por meio de condutas criminosas semelhantes às narradas acima. Por incrível que pareça, alguns dias depois da deflagração da *Operação Barba Negra*, um usuário do Facebook, utilizando um perfil real, prometeu que em breve estaria no ar o MegaFilmesHD 2.0.

As circunstâncias indicavam que aquilo não passava de uma mentira, mas o fato é que a promessa se concretizou alguns meses depois. Aos poucos, o *site* MegaFilmesHD 2.0 passou a crescer e conquistar audiência, valendo-se da notoriedade do nome. Na página oficial no Facebook, os gerenciadores do novo *site*, em resposta a questionamento de um internauta, alegaram que tinham a permissão dos criadores do megafilmeshd.net para a nova página na Internet.

Embora isso provavelmente não fosse verdade, as circunstâncias impunham novos esclarecimentos na investigação. A associação representante das produtoras apresentou nova representação solicitando investigação sobre os responsáveis pelo MegaFilmesHD 2.0. Apesar de os suspeitos não estarem agindo no território da circunscrição da Delegacia de Polícia Federal de Sorocaba/SP, foram convincentes os argumentos de que os fatos deveriam ser apurados no mesmo inquérito policial, pelas regras de conexão.

[10] Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1447125>. Acesso em: 27 fev. 2017.

Paralelamente, a mesma associação apresentou nova representação, desta vez pedindo apuração quanto aos *sites* FilmesOnline e ArmagedomFilmes, líderes de audiência na Internet desde a queda do megafilmeshd.net. O eminente advogado da associação, mais uma vez de forma convincente, demonstrou que havia um elo entre esses dois *sites* e o megafilmeshd.net: todos receberam verbas publicitárias de uma mesma fonte, a maior empresa de Internet do Brasil. Em outras palavras, havia elementos indiciários no inquérito policial de que um funcionário dessa empresa convenceu um dos responsáveis pelo megafilmeshd.net a veicular seus anúncios, dizendo abertamente que já tinha acertos semelhantes, extremamente lucrativos, com outros *sites* do "mesmo ramo": FilmesOnline e ArmagedomFilmes.

Reconhecendo a conexão probatória e considerando que o modo de agir era o mesmo do originalmente apurado no *site* megafilmeshd.net, foram apresentados novos pedidos ao Poder Judiciário com o fim de esclarecer de forma cabal os fatos criminosos, inclusive quanto a uma possível relação entre os responsáveis por todos esses *sites*. Mais uma vez, a 1ª Vara Federal de Sorocaba/SP deferiu todos os pedidos apresentados pela Polícia Federal e, no dia 13 de outubro de 2016, foram efetuadas 7 (sete) prisões temporárias e retirados do ar o MegaFilmesHD 2.0, FilmesOnline e ArmagedomFilmes, na segunda fase da *Operação Barba Negra*.

Novamente, as medidas de suspensão de uso de domínio e prisão temporária serviram para possibilitar a retirada imediata das páginas ilícitas da Internet. Após a cooperação dos presos temporários, a própria Polícia Federal postulou ao Poder Judiciário a soltura deles.

Essa nova ação policial teve uma curiosa (e certamente provisória) medida preventiva. Em levantamento feito na Internet pouco depois da deflagração da 2ª fase da *Operação Barba Negra*, constatou-se que dezenas de *sites* menores, mas que também exibiam, sem autorização, conteúdo protegido por direitos autorais,

saíram do ar espontaneamente, por medo de serem responsabilizados na esfera criminal. Alguns deixaram notas de esclarecimento nas páginas iniciais, avisando aos seus visitantes que estavam encerrando as atividades porque podiam ser mal interpretados pelo "governo" e, talvez, presos, apesar de não lucrarem nem perto do que lucravam os grandes *sites* piratas tirados do ar.

A investigação continua, o que, por enquanto, impede a revelação de determinadas circunstâncias. Nos limites impostos por isso, ficam essas linhas sobre a *Operação Barba Negra*, a primeira a retirar do ar *sites* piratas de incrível audiência e desvendar os principais responsáveis pelas ações criminosas, contando com o imprescindível apoio, na investigação, da associação representante das produtoras e, consequentemente, do excelente trabalho do seu advogado.

5 Conclusão

Os inquéritos policiais que apuram o compartilhamento internacional, pela Internet, de arquivos contendo exploração sexual de crianças e adolescentes devem ser tratados com prioridade pelas instituições envolvidas na persecução penal, em atendimento ao disposto no art. 227 da Constituição da República. A rapidez no trâmite de investigações dessa natureza é fundamental para a obtenção de bons resultados.

O afastamento do sigilo dos dados armazenados em contas de *e-mail* pelo Poder Judiciário é uma técnica de investigação eficaz para a identificação do suspeito e a obtenção da materialidade delitiva nesses casos.

Não são todos os autores de crimes tipificados nos arts. 241-A e 241-B do ECA uns coitados, desajustados, que passam a vida em frente ao computador se masturbando, sem fazer mal a ninguém. Dentre eles há os que abusam sexualmente de crianças e adolescentes, circunstância que justifica a celeridade nesses casos em respeito às vítimas. Não se trata de investigações que versam

sobre arquivos de computador, mas de cenas de estupro de crianças reais, registradas em vídeo ou foto pelos seus algozes.

A apuração desses crimes cibernéticos pode levar à obtenção da prova do crime de estupro de vulnerável, normalmente difícil de ser obtida em virtude do silêncio da vítima, que não costuma reportar o fato nem à própria família. O abusador, em regra, é alguém muito próximo à criança ou ao adolescente, outra circunstância a dificultar a descoberta do crime pelo Estado.

Referências bibliográficas

BALTAZAR JUNIOR, José Paulo. *Crimes federais*. 5. ed. rev. e atual. Porto Alegre: Liv. do Advogado Ed., 2010.

BOURKE, Michael. *The 'Butner Study' Redux:* A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders. Disponível em: <http://www.olemiss.edu/depts/ncjrl/pdf/I%20C%20A%20C/2013%20-%20April%2018-19/09f%20-%20BUTNER%20STUDY.pdf>. Acesso em: 5 mar. 2017.

_____. *The use of tactical polygraph with sex offenders*. Disponível em: <http://www.protect.org/sites/default/files/tactical_polygraph_study.pdf>. Acesso em: 5 mar. 2017.

FERREIRA, Aurélio Buarque de Holanda. *Novo Dicionário da Língua Portuguesa.* 2. ed. rev. Rio de Janeiro: Nova Fronteira, 1986.

LOPES JÚNIOR, Aury; GLOECKNER, Ricardo Jacobsen. *Investigação preliminar no Processo Penal.* 5. ed. rev., atual. e ampl. São Paulo: Saraiva, 2013.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data*: a revolution that will transform how we live, work, and think. New York: Houghton Mifflin Harcourt, 2013.

NUCCI, Guilherme de Souza. *Código de Processo Penal comentado*. 11 ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2012.

_____. *Leis penais e processuais penais comentadas.* São Paulo: Revista dos Tribunais, 2006.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo.* 17. ed. rev. e atual. São Paulo: Malheiros, 2000.

O poder geral de cautela do juiz e a efetividade das decisões nos procedimentos que versam sobre crimes cibernéticos

Ricardo Uberto Rodrigues*

RESUMO

Estudo realizado sobre a existência do poder geral de cautela do juiz criminal e a possibilidade de aplicação analógica para integração do sistema processual penal, mediante a utilização de medidas cautelares e executivas, típicas e atípicas. É objeto do estudo a ampliação das medidas possíveis de serem adotadas pelo juiz criminal para efetividade das decisões que tenham por finalidade a obtenção de dados para a identificação de autores de crimes cibernéticos e apuração de sua materialidade.

Palavras-chave: Poder. Geral. Cautela. Analogia. Crimes cibernéticos.

ABSTRACT

A study on the existence of judge's general power of caution and the possibility of the application by analogy to the integration of the criminal procedure system, through the use of precautionary and executive measures, typical and atypical ones. It is focused on the expansion of possible measures to be adopted by the criminal judge for the effectiveness of decisions to obtain data for the identification of cybercrimes' perpetrators and the investigation of its materiality.

***Keywords**: Power. General. Caution. Analogy. CyberCrimes.*

* Especialista em Direito Público pela Universidade Newton de Paiva e Especialista em Direito Penal Econômico e Europeu pela Faculdade de Direito da Universidade de Coimbra. Juiz Federal da 1ª Vara Federal de São Carlos/SP. *E-mail*: rudrigue@trf3.jus.br.

1 Introdução

A proliferação dos denominados "crimes cibernéticos" tem exigido dos agentes envolvidos em sua repressão a adoção de medidas compatíveis com a instantaneidade e com a peculiar característica nômade destes delitos, as quais, muitas vezes, não se demonstram suficientemente previstas no arcabouço das medidas processuais penais típicas, vazadas na legislação vigente.

A atual quadra de desenvolvimento tecnológico da humanidade impõe aos órgãos de repressão penal das condutas veiculadas pela rede mundial de computadores que sejam dotados de instrumentos eficazes ao combate dos "crimes cibernéticos".

Hodiernamente, constitui-se em desafio aos órgãos de repressão penal a obtenção de informações e dados existentes em provedores, em tempo mínimo, para que possam ser adotadas providências no sentido de identificar os autores do delito e colher provas atinentes à sua "materialidade".

Este texto objetiva contribuir para a definição de medidas processuais subsidiárias à legislação processual penal em vigor, fundadas no poder geral de cautela do juiz e alcançadas pela aplicação analógica (art. 3º, Código de Processo Penal – CPP), com a finalidade de ampliar o arcabouço de medidas disponíveis ao magistrado para a apuração dos crimes em testilha e a obtenção de dados e informações essenciais à sua prova.

Desse modo, por primeiro, será fundamentada a existência do poder geral de cautela do juiz criminal. Na sequência, far-se-á o estudo a respeito da possibilidade de aplicação analógica de medidas cautelares e executivas existentes em outros ramos do Direito, com vistas à efetividade das decisões proferidas no Juízo Criminal. Em passo seguinte, colhem-se elementos para a afirmação da aplicação de medidas cautelares e executivas atípicas no Processo Penal, sob a inspiração do novel Código de Processo Civil – CPC. Por fim, serão delineadas algumas medidas passíveis de adoção pelo Juízo

Criminal que podem contribuir para a maior eficácia das decisões proferidas em procedimentos que apurem crimes cibernéticos, notadamente quanto à obtenção de dados indispensáveis à prova da "materialidade" e autoria delitivas.

2 O poder geral de cautela do juiz criminal: argumentos pelo não reconhecimento

Há muito se discute sobre a existência do poder geral de cautela do magistrado com competência criminal.

Os opositores ao seu reconhecimento fundamentam a negativa nos princípios da legalidade e tipicidade (taxatividade) das medidas cautelares processuais penais, bem como da presunção de inocência, refutando, assim, a possibilidade de o juiz criminal utilizar-se de mecanismos processuais que não estejam expressa e exaustivamente definidos na legislação processual penal. Nessa esteira, a lição de BADARÓ (2015, p. 944-945):

> O princípio da legalidade também se aplica às medidas cautelares. No processo penal, mormente em tema de prisão processual, não existem medidas cautelares atípicas. Não há, como no processo civil, a previsão de um poder geral de cautela do juiz que o autorize a decretar medidas cautelares não previstas em lei.
>
> [...]
>
> As prisões cautelares são apenas aquelas previstas em lei e nas hipóteses estritas que a lei autoriza. Há, pois, um princípio de taxatividade das medidas cautelares pessoais, que implica admitir somente aquelas medidas previstas no ordenamento jurídico. A vedação das medidas cautelares atípicas no processo penal sempre esteve ligada à ideia de legalidade da persecução penal. Ou seja, as medidas cautelares processuais penais são somente aquelas previstas em lei e nas hipóteses estritas que a lei autoriza. Somente assim será possível evitar a arbitrariedade e o casuísmo, dando-se total transparência às "regras do jogo".

O entendimento sobre a taxatividade das medidas cautelares penais também já foi adotado pelo Superior Tribunal de Justiça, notadamente em medidas cautelares pessoais, que restringem

a liberdade do investigado ou do réu. A propósito, confiram-se os seguintes precedentes:

> *HABEAS CORPUS*. IMPETRAÇÃO ORIGINÁRIA. SUBSTITUIÇÃO AO RECURSO ORDINÁRIO. IMPOSSIBILIDADE. RESPEITO AO SISTEMA RECURSAL PREVISTO NA CARTA MAGNA. NÃO CONHECIMENTO. 1. A Primeira Turma do Supremo Tribunal Federal, buscando dar efetividade às normas previstas na Constituição Federal e na Lei n.º 8.038/90, passou a não mais admitir o manejo do *habeas corpus* originário em substituição ao recurso ordinário cabível, entendimento que foi adotado por este Superior Tribunal de Justiça. 2. Tratando-se de *Writ Impetrado* antes da alteração do entendimento jurisprudencial, o alegado constrangimento ilegal será enfrentado para que se analise a possibilidade de eventual concessão de *habeas corpus* de ofício. TENTATIVA DE HOMICÍDIO QUALIFICADO. PRISÃO PREVENTIVA. REVOGAÇÃO PELA CORTE ORIGINÁRIA. CRIME COMETIDO CONTRA A ESPOSA. IMPOSIÇÃO DE MEDIDAS PROTETIVAS DE URGÊNCIA. PROIBIÇÃO DE AUSENTAR-SE DE CASA, EXCETO PARA O TRABALHO. AUSÊNCIA DE PREVISÃO NO ORDENAMENTO JURÍDICO. OFENSA AO PRINCÍPIO DA LEGALIDADE. PODER GERAL DE CAUTELA DOS JUÍZES CRIMINAIS PARA FINS RESTRITIVOS. INEXISTÊNCIA. ILEGALIDADE E DESPROPORCIONALIDADE DA CAUTELAR ATÍPICA. SUFICIÊNCIA DAS DEMAIS RESTRIÇÕES IMPOSTAS. CONSTRANGIMENTO EVIDENCIADO. ORDEM CONCEDIDA DE OFÍCIO. 1. As medidas protetivas de urgência, assim como as cautelares diversas da prisão, quando afetarem o *status libertatis*, obrigatoriamente devem observar o princípio da legalidade. 2. A cumulação de providências cautelares deve sempre atentar para o binômio proporcionalidade e adequação, aqui incluída a necessidade da medida restritiva à liberdade. 3. O juiz criminal não é dotado de poder geral de cautela para fins restritivos, tendo em vista os estritos limites da legalidade penal e o princípio da presunção de não culpabilidade. 4. Verificando-se que as demais medidas impostas pela Corte originária em substituição à prisão se mostram suficientes para os fins a que se propõem e que visam alcançar – garantir a segurança da vítima e evitar novas investidas violentas por parte do agente –, mostra-se flagrantemente ilegal e desproporcional a aplicação de medida não expressamente prevista no ordenamento jurídico, como a que proibiu o paciente de sair de casa, exceto para trabalhar. 5. *Habeas corpus* não conhecido, concedendo-se a ordem de ofício, para afastar a medida protetiva de proibição de sair de casa, exceto para o trabalho. (HC n.º 222.298/SE, Quarta

> Turma, Rel. Min. Jorge Mussi, julg. 17 out. 2013, DJe 30 out. 2013.)
>
> PROCESSO PENAL. *HABEAS CORPUS*. CRIMES CONTRA A ORDEM TRIBUTÁRIA E CONTRA A ADMINISTRAÇÃO PÚBLICA. PRISÃO PREVENTIVA REVOGADA COM DETERMINAÇÃO DE AFASTAMENTO DO CARGO. ART. 20. PARÁGRAFO ÚNICO DA LEI N.º 8.429/92. APLICAÇÃO NO PROCESSO PENAL. INVIABILIDADE. PODER GERAL DE CAUTELA. INVIABILIDADE. PODER GERAL DE CAUTELA NO PROCESSO PENAL PARA FINS RESTRITIVOS. INEXISTÊNCIA. 1. É inviável, no seio do processo penal, determinar-se, quando da revogação da prisão preventiva, o afastamento do cargo disciplinando no art. 20, parágrafo único, da Lei n.º 8.429/92, previsto para casos de improbidade administrativa. 2. Não há falar, para fins restritivos, de poder geral de cautela no processo penal. Tal concepção esbarra nos princípios da legalidade e da presunção de inocência. 3. Ordem concedida para revogar a providência do art. 20, parágrafo único, da Lei n.º 8.429/92, determinada pelo Tribunal *a quo*, no seio da Ação Penal n.º 2007.70.09.001531-6, da 1.ª Vara Federal de Ponta Grossa/PR. (HC n.º 128.599/PR, Sexta Turma, Rel.ª Min.ª Maria Thereza de Assis Moura, julg. 7 dez. 2010, DJe 17 dez. 2010.)

Sem embargo do entendimento exposto, o qual se restringe às *medidas de caráter pessoal*, que afetam a liberdade do indivíduo, demonstrar-se-á não somente a existência do poder geral de cautela do juiz criminal, como também a possibilidade de adoção de medidas atípicas, mesmo as de cunho eminentemente restritivo, com fundamento na aplicação analógica.

3 A aplicação analógica e o poder geral de cautela criminal

É cediço na doutrina a possibilidade de aplicação analógica no Processo Penal. Ademais, tal possibilidade encontra suporte no art. 3º do Código de Processo Penal: "A lei processual penal admitirá interpretação extensiva e aplicação analógica, bem como o suplemento dos princípios gerais de direito". Sobre o tema, com a propriedade que lhe é inerente, vejamos a seguir o que ensina MAGALHÃES NORONHA (1997, p. 17-18).

> A lei processual, como toda lei, está sujeita a interpretação, que é o processo lógico que busca mostrar a vontade

> contida na norma jurídica. Interpretar é desvendar o conteúdo desta.
>
> [...]
>
> O art. 3º admite expressamente a interpretação extensiva e a aplicação analógica, o que bem se compreende, pois no próprio Direito Penal Substantivo, aquela é admissível, desde que considere como tal a ampliação do sentido ou alcance das palavras da lei, para que elas correspondam à vontade desta; como admissível é também a analogia *in bonam partem*, quando se trata de evitar decisões iníquas, que não condizem com as finalidades de uma justiça substancial, tratando-se, em regra, de exclusão de crime, isenção ou atenuação de pena e extinção da punibilidade.
>
> Enquanto nesse Direito a analogia sofre essa restrição, isto é, só se admite a favorável ao acusado, no Processual é ampla. Não é ela, aliás, processo de interpretação, não busca a vontade da lei, porém procura supri-la. Não tem, pois, função interpretativa e sim integrante da norma. Com ela amplia-se a vontade da lei para que compreenda um caso não previsto, mas semelhante ao que considera.
>
> [...]
>
> O art. 3º invoca ainda a suplementação dos princípios gerais de direito. Também com eles se podem suprir ou preencher as lacunas da lei. Não é pacífico o que se deve entender por ditos princípios. Sem a preocupação de expor a divergência reinante, diremos que são eles os do direito pátrio, os emanados do sistema da legislação do país, nada impedindo, entretanto, que quando eles não solucionem a dúvida se lance mão dos princípios gerais do direito universal.
>
> Dito isto, claro está que os princípios mais invocados serão os do Direito Processual Civil, não só por serem de Direito Processual como também porque múltiplos são os institutos comuns a ambos.

Na mesma linha, os ensinamentos de XAVIER DE AQUINO e NALINI (2005, p. 81-82):

> No processo penal, a analogia é muito ampla. Não se limita apenas ao Direito Processual Penal, podendo ultrapassá-lo. Por óbvio, a disposição do processo civil é aplicável, analogicamente, ao processo penal. Porém, pode-se recorrer também a uma analogia mais abrangente, quando não existir norma regulamentadora de casos similares ou matérias análogas – *analogia legis*. É a hipótese de utilização da *analogia juris*, propiciadora de se recorrer ao sistema

> jurídico inteiro, a partir da norma constitucional, para resolver o caso concreto. Pode-se conceituar a *analogia juris* como procedimento pelo qual se extrai a norma para o caso concreto, não de outra norma, mas do conjunto inteiro das normas disciplinadoras de todo um setor de relações.
>
> Quando insuficiente a interpretação, em todas as suas modalidades, e o recurso à analogia, o intérprete pode procurar a solução nos princípios gerais de direito.

Como bem explicitado pelos ilustres doutrinadores, o art. 3º do CPP constitui-se na "ponte de ouro", na "janela" que possibilita a integração do Direito Processual Penal pelos demais ramos jurídicos, notadamente o Direito Processual Civil, donde poderão ser extraídas medidas cautelares e executivas que complementarão os instrumentos disponibilizados ao juiz criminal para a efetividade de seus provimentos jurisdicionais.

Impende ressaltar, no ponto, que a doutrina reconhece, ao contrário do que ocorre com o Direito Penal, a possibilidade de se aplicar a analogia *in malam partem* na seara do Direito Processual Penal. A propósito, a lição de NUCCI (2012, p. 74):

> O Código de Processo Penal admite, expressamente, que haja interpretação extensiva, pouco importando se para beneficiar ou prejudicar o réu, o mesmo valendo no tocante à analogia. Pode-se, pois, concluir que, admitido o mais – que é a analogia –, cabe também a aplicação da interpretação analógica, que é o menos.

Na mesma esteira, assevera MARQUES (2009, p. 29) que:

> O art. 3º, do Código de Processo Penal, diz claramente que "a lei processual penal admitirá interpretação extensiva e aplicação analógica". Assim o fez para evitar que se procurasse impor, no domínio do processo, a série de restrições pertinentes ao Direito Penal sobre a analogia.

Desse modo, ainda que se cogite da aplicação de medidas restritivas, por seu caráter instrumental e não punitivo, deve ser admitida a aplicação de medidas cautelares e executivas no âmbito do Processo Penal, mediante a utilização de analogia.

Nesse passo, destacam-se da jurisprudência do Superior Tribunal de Justiça e do Supremo Tribunal Federal inúmeros precedentes em que é reconhecida a aplicação da analogia e a existência do poder geral de cautela do juiz criminal.

São exemplos de decisões que reconhecem a aplicação analógica das normas do Código de Processo Civil:

a) possibilidade de o relator decidir monocraticamente para não conhecer de recurso inadmissível, prejudicado ou que não tenha impugnado especificamente os fundamentos da decisão recorrida, sem ofensa ao princípio da colegialidade, com espeque no art. 932, III e IV, do CPC[1];

b) definição do conceito de testemunha mediante a aplicação do art. 415 do CPC 1973 e do art. 288 do Código Civil[2];

c) aplicação do art. 87 do CPC 1973, por analogia, aos processos penais, na definição da competência territorial do juiz[3];

d) mitigação do princípio da identidade física do juiz, mediante aplicação, por analogia, do art. 132 do CPC 1973[4];

e) possibilidade de substituição de testemunhas, mesmo após a revogação do art. 397 do CPP, mediante a aplicação, por analogia, das hipóteses previstas no art. 408 do CPC 1973;

f) aplicação do princípio geral da sucumbência previsto no art. 20, § 3º, do CPC 1973, por analogia, ao Processo Penal, quando se tratar de ação penal privada[5];

---

[1] STJ, AgRg no REsp n.º 1558471/RS, Quinta Turma, Rel. Min. Jorge Mussi, julg. 25 out. 2016, DJe 7 nov. 2016; STJ, AgRg no AREsp n.º 826.153/PR, Sexta Turma, Rel. Min. Nefi Cordeiro, julg. 11 out. 2016, DJe 4 nov. 2016.

[2] STJ, REsp n.º 1549417/MG, Sexta Turma, Rel. Min. Sebastião Reis Júnior, julg. 23 ago. 2016, DJe 8 set. 2016.

[3] STJ, REsp n.º 1558124/MT, Sexta Turma, Rel. Min. Sebastião Reis Júnior, julg. 23 ago. 2016, DJe 8 set. 2016.

[4] STJ, Rcl n.º 19.873/RJ, Terceira Seção, Rel. Min. Nefi Cordeiro, julg. 22 jun. 2016, DJe 1 jul. 2016.

[5] STJ, AgRg n.º REsp n.º 1206311/SP, Quinta Turma, Rel. Min. Jorge Mussi, julg. 5 jun. 2014, DJe 11 jun. 2014.

g) impossibilidade de retificação de voto proferido em julgamento por órgão jurisdicional colegiado após a proclamação do resultado do julgamento pelo presidente, mediante a aplicação, por analogia, do art. 556 do CPC 1973[6].

E como exemplos do reconhecimento da existência do poder geral de cautela do juiz criminal:

a) antecipação da produção de provas, com fundamento no poder geral de cautela do juiz, nas hipóteses de suspensão do Processo Penal com fundamento no art. 366 do CPP[7];

b) suspensão do livramento condicional, por intermédio de interpretação conjugada do art. 87 do Código Penal e do art. 145 da Lei de Execução Penal, com fundamento no poder geral de cautela do juiz da execução penal[8];

c) remoção de preso para outro estabelecimento prisional, com fundamento no poder geral de cautela do juiz das execuções penais[9];

d) requisição prévia de folhas de antecedentes criminais e ficha de término de pena pelo juiz antes de decidir sobre a concessão da liberdade provisória, com fundamento no poder geral de cautela[10];

e) possibilidade de concessão de efeito suspensivo ao agravo previsto no art. 197 da Lei de Execução Penal, com fundamento no poder geral de cautela do juiz[11].

---

[6] STJ, REsp n.º 1370651/MG, Quinta Turma, Rel. Min. Moura Ribeiro, julg. 11 mar. 2014, DJe 19 mar. 2014.

[7] STF, HC n.º 109728, Segunda Turma, Rel. Min. Ricardo Lewandowski, julg. 15 maio 2012, processo eletrônico DJe-109, divulg. 4 jun. 2012, public. 5 jun. 2012.

[8] STJ, HC n.º 202.844/RJ, Sexta Turma, Rel.ª Min.ª Maria Thereza de Assis Moura, julg. 6 fev. 2014, DJe 26 fev. 2014.

[9] STJ, HC n.º 232.203/RO, Quinta Turma, Rel. Min. Marco Aurélio Bellizze, julg. 17 abr. 2012, DJe 20 jun. 2012.

[10] STJ, HC n.º 102.124/RJ, Quinta Turma, Rel. Min. Napoleão Nunes Maia Filho, julg. 4 fev. 2010, DJe 15 mar. 2010.

[11] STJ, HC n.º 66.604/SP, Quinta Turma, Rel. Min. Napoleão Nunes Maia Filho, julg. 9 ago. 2007, DJ 10 set. 2007, p. 258.

Consoante se infere dos exemplos elencados, não há como negar a aplicação da analogia no Processo Penal, ainda que esta implique medidas restritivas.

Por igual, o poder geral de cautela no Processo Penal também é amplamente reconhecido e se aplica, ainda que acarrete medidas de restrição de direitos, como se verificou nas hipóteses de execução da pena.

Ressalta POLASTRI (2014, p. 82-84) que, malgrado nos casos de prisão cautelar, só devam ser aceitas medidas previstas em lei:

> [...] Em relação a outras espécies de medidas cautelares processuais penais, não haverá o mesmo óbice. Queremos crer, inclusive, que também em outras modalidades de cautelares pessoais, desde que não prisionais, se poderá exercer o Poder Geral de Cautela [...]

E sublinha que:

> Não identificamos impedimento nesses casos, como vislumbram Rogério Lauri Tucci et al., nas previsões dos incisos II e XV do art. 5º da Constituição Federal, pois, se o primeiro veda o fazer ou deixar de fazer algo em virtude de lei, é de se considerar que o Poder Geral de Cautela, como já visto, é previsto na lei processual civil, e o Código de Processo Penal admite a aplicação da analogia e dos princípios gerais do Direito (art. 3º do CPP). E quanto ao inciso XV, a livre locomoção das pessoas encontra limite no fato de ser necessária a decretação da medida cautelar para assegurar os fins do processo contra o transgressor da lei.

Apesar de amplamente reconhecida a aplicação da analogia, impende ressaltar que há julgado do Superior Tribunal de Justiça[12] que estabeleceu a impossibilidade de aplicação da pena de litigância de má-fé no âmbito do Processo Penal, por considerar inviável a aplicação da analogia *in malam partem*.

Todavia, como já asseverado anteriormente com referência à doutrina abalizada, a analogia *in malam partem* somente é

[12] STJ, AgRg nos EDcl nos EAREsp 316.129/SC, Terceira Seção, Rel. Min. Reynaldo Soares da Fonseca, julg. 25 maio 2016, DJe 1 jun. 2016.

vedada no âmbito do Direito Material, não em relação ao Direito Processual. Desse modo, o julgado referido vai de encontro não somente à doutrina como também à própria jurisprudência, que sinaliza em sentido contrário, conforme se extrai dos exemplos declinados acima.

Em arremate, para que não pairem dúvidas a respeito da possibilidade da aplicação analógica no Processo Penal, bem como da existência do poder geral de cautela do juiz criminal, o qual pode ser extraído de normas do Processo Civil ou demais ramos do Direito, colhe-se o seguinte julgado do Supremo Tribunal Federal:

> PROCESSUAL PENAL. IMPOSIÇÃO DE CONDIÇÕES JUDICIAIS (ALTERNATIVAS À PRISÃO PROCESSUAL). POSSIBILIDADE. PODER GERAL DE CAUTELA. PONDERAÇÃO DE INTERESSES. ART. 798, CPC; ART. 3º, CPC. 1. A questão jurídica debatida neste *habeas corpus* consiste na possibilidade (ou não) da imposição de condições ao paciente com a revogação da decisão que decretou sua prisão preventiva 2. Houve a observância dos princípios e regras constitucionais aplicáveis à matéria na decisão que condicionou a revogação do decreto prisional ao cumprimento de certas condições judiciais. 3. Não há direito absoluto à liberdade de ir e vir (CF, art. 5º, XV) e, portanto, existem situações em que se faz necessária a ponderação dos interesses em conflito na apreciação do caso concreto. 4. A medida adotada na decisão impugnada tem clara natureza acautelatória, inserindo-se no poder geral de cautela (CPC, art. 798; CPP, art. 3º). 5. As condições impostas não maculam o princípio constitucional da não culpabilidade, como também não o fazem as prisões cautelares (ou processuais). 6. Cuida-se de medida adotada com base no Poder Geral de Cautela, perfeitamente inserido no Direito brasileiro, não havendo violação ao princípio da independência dos poderes (CF, art. 2º), tampouco malferimento à regra de competência privativa da União para legislar sobre Direito Processual (CF, art. 22, I). 7. Ordem denegada. (STF, HC n.º 94147, Segunda Turma, Rel.ª Min.ª Ellen Grace, julg. 27 maio 2008, DJe-107, divulg. 12 jun. 2008, public. 13 jun. 2008. EMENT VOL-02323-05 PP-00921 LEX STF, v. 30, n. 360, 2008, p. 451-459.)

Destarte, fica definitivamente fulminada a afirmação doutrinária, e até jurisprudencial, no sentido da inexistência do poder geral de cautela do juiz criminal, bem como da impossibilidade de utilização da analogia. Rechaça-se, também, a afirmação no sentido de que não poderão resultar do exercício do poder geral de cautela medidas de cunho restritivo ao investigado, réu ou a terceiro sobre o qual devam recair os efeitos da decisão judicial.

Registre-se, em conclusão, que sendo a aplicação analógica permitida pelo ordenamento jurídico e havendo arcabouço normativo para buscar as medidas adotadas com fundamento no poder geral de cautela, não há que se afirmar a violação ao princípio da legalidade.

De igual modo, o argumento sobre a violação do Princípio da Presunção de Inocência (não culpabilidade) não se sustenta. Com efeito, mesmo a decretação da prisão cautelar (o mais), por ter fundamentos e pressupostos diversos da prisão pena, não vulnera o princípio da presunção de inocência[13], não havendo que se sustentar que outras medidas (o menos), diversas e menos invasivas que a prisão, violariam tal princípio.

4 A superação do princípio da tipicidade ou taxatividade das medidas cautelares e executivas

Firmado o entendimento no sentido da existência do poder geral de cautela no Juízo Criminal, bem como da possibilidade de utilização da analogia para a integração do sistema processual penal, cumpre verificar, na atual quadra, a superação do princípio da tipicidade ou taxatividade das medidas cautelares e executivas, com fundamento nos princípios estabelecidos pelo novel Código

[13] "Não há que se falar, em hipóteses como esta, de ofensa ao princípio constitucional da presunção de inocência, haja vista a natureza cautelar da prisão, existente para assegurar o regular andamento do feito de origem." (TRF 3ª Região, HC n.º 64533-0023660-76.2015.4.03.0000, Décima Primeira Turma, Rel.ª Des.ª Fed. Cecilia Mello, julg. 10 nov. 2015, e-DJF3 Judicial 1 17 nov. 2015.)

de Processo Civil, os quais podem ser, por analogia, reportados ao Processo Penal.

Nessa esteira, o Código de Processo Civil de 2015 prevê, expressamente, a existência do poder geral de cautela do juiz em seu art. 139, IV, o qual estabelece que incumbe ao juiz

> determinar todas as medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias para assegurar o cumprimento de ordem judicial, inclusive nas ações que tenham por objeto prestação pecuniária.

Para além de contemplar o poder geral de cautela, segundo o qual se admite que o juiz possa conceder a tutela cautelar quando, no curso do processo, surja uma situação de risco, o mesmo dispositivo legal também contempla o "princípio da atipicidade das medidas executivas". Conforme elucida MEDINA (2016, p. 256): "Esse princípio já vinha, cada vez com mais veemência, ocupando o espaço do princípio que lhe é oposto, o da tipicidade das medidas executivas".

A opção do legislador pela adoção do princípio da atipicidade das medidas executivas e cautelares é revelada pela letra dos arts. 139, IV; 772, III; e 773 do CPC 2015. Nessa esteira, preleciona MEDINA (2016, p. 1 070-1 071):

> Na medida em que, no sistema jurídico, se dá primazia ao princípio da atipicidade, (a) a participação do juiz na elaboração da solução jurídica dos litígios passa a ser mais intensa, ante o abrandamento da tendência – veemente no Estado Liberal de outrora – de se reduzirem ao máximo os poderes do juiz; (b) a atividade jurisdicional deve proporcionar aos demandantes respostas capazes de propiciar uma tutela mais aproximada possível da pretensão violada, bem como impedir que a violação ocorra (cf., p. ex., art. 497 do CPC 2015), o que impõe sejam criados instrumentos capazes de proporcionar à jurisdição o alcance de tal desiderato; (c) ante a multiplicidade e a complexidade das situações litigiosas que podem ser levadas a juízo, tais mecanismos não podem ser previstos num rol taxativo, *numerus clausus*, pois há o risco de se excluírem direitos igualmente merecedores de tutela; (d) as medidas executivas que podem ser postas em prática podem não ser aquelas requeridas pelas partes, necessariamente,

> porque o juiz pode constatar a viabilidade de um meio executivo mais adequado à satisfação (fim) da pretensão do exequente.

Ressalta o ilustre processualista, contudo, que, no sistema brasileiro, deve prevalecer um "sistema típico temperado pelo atípico":

> O modelo baseado na tipicidade das medidas executivas tende a alcançar resultados satisfatórios na medida em que as situações de Direito Material e os problemas que emergem da sociedade sejam parecidos. Nesses casos, é até mesmo conveniente a previsão de medidas similares para os casos em que problemas parecidos se reproduzem, a fim de que se observe em relação àqueles que estejam em uma mesma situação de Direito Material um procedimento também similar. Quando, porém, o modelo típico de medidas executivas mostra-se insuficiente, diante de pormenores do caso, o sistema típico acaba tornando-se ineficiente. Faz-se necessário realizar um ajuste tendente a especificar o procedimento, ajustando-o ao problema a ser resolvido. Para tanto, é de todo conveniente que o sistema preveja um modelo atípico ou flexível de medidas executivas. Assim, diante de modelos típicos de medidas executivas, havendo déficit procedimental, deverá ser necessário que o juiz estabeleça medida executiva adequada ao caso. É, a nosso ver, o que sucede, no caso referido no art. 139, IV, do CPC 2015.

E adverte que:

> Essa regra não pode, como é intuitivo, tornar despiciendas as medidas executivas típicas previstas na lei processual. Fosse assim, bastaria a existência de tal disposição, e todo regramento restante previsto na lei processual quanto às medidas executivas poderia ser desprezado.

Por conseguinte, reconhecida a possibilidade da aplicação analógica ao Processo Penal, bem como a existência do *poder geral de cautela*, nada obsta que o juiz, valendo-se do arcabouço de medidas cautelares e executivas expressamente previstas no Código de Processo Civil, possa integrar sua atuação jurisdicional com as normas vigentes. Por exemplo, com a aplicação de multa na hipótese de descumprimento da ordem judicial, medida já

chancelada pela jurisprudência do Superior Tribunal de Justiça[14], mediante o reconhecimento da aplicação analógica dos dispositivos dos arts. 461, § 5º, e 461-A do CPC 1973.

De igual modo, como dito alhures, a aplicação analógica e a utilização do poder geral de cautela também sustentam a possibilidade de o juiz determinar medidas cautelares e executivas não previstas expressamente em lei (atípicas), utilizando-se para tanto dos arts. 139, IV; 772, III; e 773 do CPC 2015. Tais normas nada mais expressam do que um dos poderes inerentes à jurisdição. É dizer, o *Poder de Coerção do Juiz*. Segundo GRECO (2015, p. 107):

> O poder de coerção é o poder do juiz de impor *aos sujeitos do processo ou a terceiros* o respeito e a obediência às suas ordens, determinações e decisões. Esse poder faculta, inclusive, se necessário, o emprego da força física ou da força policial, e exercita-se através de sanções e restrições à liberdade individual, pessoal e patrimonial [grifo nosso].

Ainda, conforme preleciona o ilustre processualista (2015, p. 276), decorrem do poder de coerção os *atos de coação* ou *de coerção*, "que são atos de autoridade, de invasão da esfera de interesses ou da esfera patrimonial de uma das partes, ou até de terceiros, para impor-lhes, pela força, o respeito a ordens ou determinações judiciais".

As medidas cautelares e executivas, típicas e atípicas, amoldam-se, portanto, ao poder de coerção do juiz, inerente ao exercício da jurisdição.

Sublinhe-se, outrossim, que as medidas atípicas seriam subsidiárias às medidas típicas, funcionariam como "soldado de reserva", e como tal estariam sujeitas aos predicados da instrumentalidade, acessoriedade, referibilidade e proporcionalidade, de modo a não se permitir o arbítrio.

[14] STJ, REsp n.º 1455000/PR, Sexta Turma, Rel.ª Min.ª Maria Thereza de Assis Moura, Rel. p/ o acórdão Min. Rogerio Schietti Cruz, julg. 19 mar. 2015, DJe 9 abr. 2015.

5 A possibilidade de adoção de medidas típicas e atípicas para garantir a eficácia das decisões nos crimes cibernéticos

No âmbito da repressão aos crimes cibernéticos, é inegável que o principal obstáculo enfrentado pelo Juízo Criminal é a obtenção de dados e informações das empresas (provedores, etc.) acerca dos usuários que potencialmente estejam envolvidos com a prática de tais crimes.

Cumpre mencionar que, com o advento da Lei n.º 12.965, de 23 de abril de 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria, foi previsto, em seus arts. 10 e 11, que o provedor responsável pela guarda dos registros de conexão e de acesso à Internet está obrigado a disponibilizar tais informações mediante requisição judicial. Isso deve ocorrer notadamente quando tais informações puderem contribuir para a identificação de usuário que esteja relacionado, mediante a presença de indícios mínimos, à prática de crimes, como, por exemplo, o armazenamento ou compartilhamento de material que contenha abuso sexual de menores, conhecido popularmente como "pornografia infantil".

Note-se que a legislação brasileira adotou, no art. 11 do diploma legal mencionado, o critério da territorialidade, ao estabelecer que, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet, em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Ficou também estabelecido que a lei brasileira é aplicável aos "dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil" e "mesmo que as

atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil" (§ 2º).

A fim de emprestar maior efetividade aos comandos legais mencionados, o art. 12 da Lei n.º 12.965/2014 estabelece que, *sem prejuízo das demais sanções cíveis*, *criminais* ou *administrativas*, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III – suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV – proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Em seu parágrafo único, o dispositivo legal mencionado preceitua que, "tratando-se de empresa estrangeira, respondem solidariamente pelo pagamento da multa de que trata o *caput* sua filial, sucursal, escritório ou estabelecimento situado no país".

Desse modo, pela incidência da legislação especial, tem-se a possibilidade de se infligirem as sanções mencionadas, as quais se recomenda a aplicação de forma gradual e sucessiva.

No entanto, como a própria legislação estabelece e como vimos de sustentar, o juiz não está adstrito apenas às medidas e sanções previstas na lei especial, na hipótese de descumprimento do

comando para o fornecimento de dados essenciais à investigação ou instrução processual.

É importante assinalar que, para além da previsão da legislação específica, por aplicação analógica, com fundamento no art. 3º do Código de Processo Penal e por força dos arts. 139, IV; 772, III; e 773 do CPC 2015, para a execução da medida, o juiz poderá determinar, de ofício ou a requerimento das partes, as *medidas necessárias ao seu cumprimento*, notadamente quanto à entrega de documentos e fornecimento de dados. Tal medida abrange tanto ordens instrumentais como ordens finais. As primeiras para permitir a decisão final; e as subsequentes, para a tutela ou satisfação da pretensão punitiva.

Assim, pela aplicação analógica dos dispositivos previstos no Código de Processo Civil, notadamente o que permite a adoção de medidas atípicas, caso as típicas não se afigurem suficientes, possibilita-se a imposição de medidas que não estejam expressamente estabelecidas no art. 12 da Lei n.º 12.965/2014, dentre as quais podem ser citadas, *como sugestão*:

a) vedação ou suspensão de emissão de títulos ou valores mobiliários;

b) suspensão do registro no Bacen para a distribuição dos valores mobiliários no mercado;

c) proibição às sociedades anônimas de pagar dividendos, bonificações em dinheiro, amortizações, reembolsos ou resgate de ações endossáveis, com o consequente arresto dos valores para pagamento de multas;

d) suspensão temporária do direito de participar de licitações e contratações com o Poder Público;

e) vedação ou suspensão de obtenção de subsídios, subvenções ou doações do Poder Público;

f) suspensão da veiculação de publicidade nos *sites* respectivos, dentre outras.

No que tange às medidas possíveis, não é demais lembrar que a razoabilidade e proporcionalidade devem se fazer presentes, a fim de que a afetação dos direitos envolvidos não ultrapasse o estritamente necessário e adequado para se coibir a omissão ou modorra verificada. Nesse passo, colhe-se, por oportuno, excerto da decisão proferida pelo Min. Ricardo Lewandowski na ADPF n.º 403-MC/SE[15], que versou sobre a suspensão do aplicativo WhatsApp no território nacional:

> Ora, a suspensão do serviço do aplicativo WhatsApp, que permite a troca de mensagens instantâneas pela rede mundial de computadores, da forma abrangente como foi determinada, parece-me violar o preceito fundamental da liberdade de expressão aqui indicado, bem como a legislação de regência sobre o tema. Ademais, a extensão do bloqueio a todo o território nacional afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa.

Mutatis mutandis, a determinação de suspensão da prestação dos serviços seria equiparável à própria prisão cautelar, se vista sob o prisma do indivíduo e não da empresa responsável pelo fornecimento dos dados.

Daí, a toda evidência, a necessidade de se obtemperar o rol de medidas possíveis de serem adotadas pelo juiz mediante a aplicação da analogia e do poder geral de cautela, valendo reportar, no ponto, a lição de POLASTRI (2014, p. 85):

> Isso se pode conceder ainda mais facilmente no Processo Penal, onde o principal instrumento cautelar é a prisão provisória. Ora, existem casos em que, em vista da gravidade dos efeitos da restrição de liberdade cautelar, e ainda da necessidade de estrito atendimento aos requisitos legais, faltará razoabilidade e proporcionalidade na sua aplicação.
>
> [...]
>
> Assim, conforme defendemos, ao fazer uso do Poder Geral de Cautela, o juiz poderá ter uma alternativa não prevista em lei para evitar uma desproporcional decretação da prisão cautelar que, assim, passa inclusive a ser de aplicação mais benéfica ao acusado.

[15] Disponível em: <http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=4975500>. Acesso em: 29 dez. 2016.

Sinaliza-se, portanto, que a suspensão da prestação do serviço constitui-se em medida excepcional, somente adotada em derradeira hipótese, sendo antes viável que o juiz se utilize de medidas cautelares ou executivas, *atípicas se o caso*, como alternativas à suspensão da prestação dos serviços.

6 Conclusão

Em conclusão, pode-se asseverar o seguinte:

a) Afirma-se a existência de um poder geral de cautela no Juízo Criminal, o qual já tem sido consagrado pela doutrina e jurisprudência, mesmo no que tange à adoção de medidas restritivas das liberdades individuais.

b) O art. 3.º do Código de Processo Penal permite a aplicação analógica, e a consequente integração das normas processuais penais, por normas existentes em outros ramos do Direito, notadamente o Direito Processual Civil.

c) As normas previstas nos arts. 139, IV; 772, III; e 773 do CPC 2015 sinalizam para a possibilidade de o magistrado com competência criminal adotar medidas cautelares e executivas, típicas e atípicas, com a finalidade de efetivar as ordens judiciais.

d) Considerando que a obtenção de dados e informações dos provedores e demais empresas, que têm a Internet como plataforma de atuação, constitui o principal obstáculo à apuração dos crimes cibernéticos, o juiz poderá, mediante a utilização do poder geral de cautela e da analogia, determinar as medidas típicas e atípicas necessárias à obtenção dos dados pretendidos pela investigação ou instrução processual.

e) No âmbito das medidas cautelares ou executivas a serem adotadas para a obtenção dos dados necessários à investigação ou instrução processual, o juiz preferirá medidas alternativas à suspensão das atividades da empresa em relação à qual se dirige a ordem de fornecimento de dados, ainda que se trate de medidas atípicas.

f) As medidas cautelares e executivas atípicas serão adotadas subsidiariamente às típicas e se sujeitarão aos predicados da instrumentalidade, acessoriedade, referibilidade e proporcionalidade.

7 Referências bibliográficas

BADARÓ, Gustavo Henrique. *Processo Penal.* 3. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2015.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, 24 abr. 2014.

CÓDIGO de Processo Penal. In: *VADE MECUM Saraiva.* 21. ed. São Paulo: Saraiva, 2016.

GRECO, Leonardo. *Instituições de Processo Civil*: introdução ao Direito Processual Civil. 5. ed. Rio de Janeiro: Forense, 2015. v. 1.

MAGALHÃES NORONHA, Edgard. *Curso de Direito Processual Penal.* 25. ed. São Paulo: Saraiva, 1997.

MARQUES, José Frederico. *Elementos de Direito Processual Penal.* 3. ed. atual. Campinas: Millennium, 2009. v. 1.

MEDINA, José Miguel Garcia de. *Novo Código de Processo Civil comentado*. 4. ed. São Paulo: Revista dos Tribunais, 2016.

NOVO CÓDIGO de Processo Civil e Constituição Federal. 45. ed. São Paulo: Saraiva, 2017.

NUCCI, Guilherme de Souza. *Código de Processo Penal comentado.* 11. ed. São Paulo: Revista dos Tribunais, 2012.

POLASTRI, Marcellus. *A tutela cautelar no Processo Penal.* 3. ed. São Paulo: Atlas, 2014.

XAVIER DE AQUINO, José Carlos Gonçalves; NALINI, José Renato. *Manual de Processo Penal*. 2. ed. São Paulo: Revista dos Tribunais, 2005.

A prova da materialidade delitiva nos crimes cibernéticos

Rodiner Roncada*

RESUMO

O presente trabalho aborda algumas questões processuais relevantes relacionadas à prova da materialidade delitiva nos crimes cibernéticos. Expõe o conceito doutrinário de crimes cibernéticos e justifica a necessidade de prova técnica para a comprovação da existência da infração penal. Discute a imprescindibilidade do laudo pericial para a espécie e as hipóteses legais de dispensa, expondo as consequências processuais advindas da ausência injustificada da prova técnica.

Palavras-chave: Crimes cibernéticos. Prova pericial. Exame de corpo de delito.

ABSTRACT

This work approaches some relevant processual questions involving the materiality criminal evidence to cybercrimes. It explains the doctrinaire concept of cybercrime and justifies the need of technical evidence to prove the existence of criminal offense. It discusses the indispensability of expert evidence for the type of crime and legal hypotheses of exemption, demonstrating the processual consequences that come from unjustified lack of technical evidence.

***Keywords**: Cybercrimes. Expert evidence. Corpus delict examination.*

* Mestre em Direitos Humanos Fundamentais pelo Centro Universitário FIEO (UNIFIEO/SP). Juiz Federal Substituto da Justiça Federal de Primeiro Grau em São Paulo. *E-mail*: rroncada@jfsp.jus.br.

1 Introdução

Recentemente, noticiou-se que o Brasil fechou o ano de 2015 com 102,1 (cento e dois vírgula um) milhões de pessoas conectadas à Internet, espalhadas em 27,5 (vinte e sete e meio) milhões de domicílios brasileiros, conforme levantamento do IBGE na Pesquisa Nacional por Amostra de Domicílios – PNAD. Isso representa a metade da população brasileira com acesso à rede mundial de computadores.

Diante desse contingente expressivo de internautas, surgem ao menos duas constatações. A primeira é positiva, pois o número demonstra que a maioria da população possui condições materiais para ingressar na rede e está disposta a enfrentar os desafios do mundo tecnológico para obter informações e facilidades, ou apenas para fins recreativos. A segunda é sombria: na medida em que cresce o número de internautas operando na rede, também cresce a quantidade de infratores que, aproveitando-se das facilidades de um suposto anonimato e fazendo uso de aparatos tecnológicos, buscam obter alguma vantagem ilícita e/ou imoral, de ordem material, psicológica ou emocional, causando prejuízos patrimoniais e morais a outros usuários individuais e a instituições públicas e privadas.

Notoriamente, os órgãos estatais incumbidos da repressão à prática de ilícitos penais têm investido recursos humanos e materiais para a adequada apuração deste tipo de delito, criando delegacias especializadas em crimes de informática e grupos especiais de perícia criminal digital, além de firmar convênios com entidades nacionais e internacionais voltadas ao aperfeiçoamento técnico das equipes. Todavia, como é previsível, dada a expansão da tecnologia nos meios sociais, dificilmente se logrará uma resposta estatal rápida e efetiva ao problema da criminalidade digital. Haverá de se incrementarem os mecanismos automáticos de localização e inibição imediata das práticas virtuais ilícitas, de forma a tornar certa a identificação do criminoso e sua persecução penal.

A par das questões criminológicas, uma vez ocorrida a infração penal com uso da informática, surge o problema jurídico da sua adequada demonstração, de modo a fornecer aos agentes do Estado a prova dos elementos técnicos vinculados diretamente à infração, de todo indispensável ao início da atividade persecutória.

O problema em destaque é designado no foro processual como *prova da materialidade delitiva*, pressuposto lógico-jurídico indispensável para a afirmação da culpa do acusado, sem o qual não se prossegue no exame prático da subsunção dos fatos à norma penal.

No presente trabalho, pretendemos abordar alguns aspectos processuais relevantes a respeito da prova da materialidade delitiva nos crimes cibernéticos, revendo alguns conceitos doutrinários sobre o assunto e delimitando a importância dessa prova para fins de regularidade processual e de legitimidade da sentença como resposta penal.

2 A definição de "crime cibernético"

É penosa a conceituação do que seja um "crime cibernético" ou um "delito de informática", por se tratar de expressão que transita entre a técnica e o mundo vulgar. Afinal, ao mesmo tempo que a cibernética é uma ciência bastante ampla, que estuda os sistemas e mecanismos de automação, regulação e comunicação nos seres vivos e nas máquinas (HOUAISS, 2009), o substantivo "crime" é mal aplicado, pois seu uso pretende abranger qualquer conduta ilícita prevista em tipo penal, inclusive eventual contravenção penal (que não é "crime" na acepção técnica) praticada em ambiente virtual. Melhor seria adotar a expressão "infração penal com uso da informática", já que, para a prática do delito da espécie, em regra não se exige que o tipo penal descreva elemento técnico-objetivo pertencente à cibernética, bastando que incidentalmente haja o emprego de algum equipamento apto a processar dados. Caso, *v.g.*, da prática de calúnia, difamação ou injúria pela Internet, em que o

uso de dispositivo informático é meio de execução do crime, e não elemento do tipo penal.

De todo modo, são consagradas nos meios jurídicos as expressões "crimes cibernéticos", "delitos de informática" ou "crimes virtuais" (PINHEIRO, 2006, p. 14), voltadas a definir aquelas infrações penais (crimes ou contravenções penais) praticadas em ambiente virtual – por exemplo, em redes sociais, em sítios eletrônicos, em redes de compartilhamento ou através de caixa postal eletrônica – ou mesmo as praticadas fora desse ambiente, porém mediante o uso de dispositivo de informática – caso, por exemplo, do furto de numerário em caixa automático mediante a captura fraudulenta de dados pessoais do correntista por dispositivo eletrônico.

A doutrina nacional costuma dividir os crimes de informática entre "puro", "misto" e "comum" (FIORILLO; CONTE, 2016, p. 187).

O crime virtual puro é aquele em que a conduta recai sobre o próprio computador físico e seus componentes (*hardware*) ou sobre o sistema operacional ou programas (*software*), prejudicando o seu funcionamento. O bem jurídico protegido é a própria informação digital, independentemente de quem seja o seu titular. A Lei n.º 12.737/12 inaugurou no Direito brasileiro a figura típica, prevista no art. 154-A do Código Penal, sob a rubrica "invasão de dispositivo informático".

O crime virtual misto é aquele em que o tipo penal também exige o emprego da informática na realização da conduta, mas o objetivo do agente é obter alguma vantagem ilícita com a prática. Ex.: inserção de dados falsos em sistema de informações da administração pública (art. 313-A do Código Penal).

Já o crime virtual comum é aquele em que a norma penal não exige como condição para a sua ocorrência o emprego de dispositivo de informática, que surge acidentalmente, apenas como um meio de execução do delito. É a espécie mais comum

observada na prática, como se vê em certos crimes de estelionato, furto mediante fraude, injúria qualificada pelo preconceito, posse de pornografia infantil, etc.

Constata-se, portanto, a possibilidade da ocorrência das mais variadas espécies de infrações penais envolvendo o ambiente virtual, impondo ao Estado e à sociedade desenvolver técnicas de inibição e repressão a tais condutas ilícitas, incentivando inclusive a criação de grupos privados e especializados no combate a delitos digitais, com conhecimentos específicos e cada vez mais profundos de informática, até mesmo para auxiliar adequadamente as instituições públicas incumbidas da persecução e da punição de infrações penais.

3 A prova da materialidade nos crimes cibernéticos

Uma vez constatada a ocorrência de infração penal com uso de informática, diante das características da espécie, envolvendo sensíveis aspectos técnicos e quase sempre uma identidade camuflada, desde já nasce a problemática da comprovação, pelos meios admitidos em Direito, da sua existência e de quem foi o seu autor.

Nesse intento, cabe aos órgãos encarregados da persecução penal – mais especificamente à Polícia Judiciária e ao Ministério Público – colacionar as provas hábeis a demonstrar a materialidade e a autoria do delito, revelando pelos meios legítimos todos os elementos e circunstâncias fáticas e jurídicas descritas no tipo penal.

Trata-se de uma exigência do *sistema penal acusatório*, adotado pela Constituição Federal de 1988, pelo qual incumbe ao órgão acusador do Estado (ou excepcionalmente ao particular, quando titular da ação penal) a demonstração cabal do ato infracional praticado, quebrando o presuntivo estado de inocência gravado na Carta em favor de toda pessoa humana ou entidade personalizada.

A prova da materialidade delitiva exige especial atenção dos órgãos persecutórios, já que os meios utilizados na, ou para, a

infração penal não são comuns, de conhecimento geral, mas técnicos, a impor uma demonstração científica da forma de execução do delito.

O meio de prova mais adequado para a demonstração da prática criminosa é o *exame de corpo de delito*, materializado em um laudo pericial emitido por técnico habilitado na área de conhecimento científico, de acordo com o previsto nos arts. 158 a 184 do Código de Processo Penal brasileiro. Define-se como *corpo de delito* o conjunto dos vestígios deixados pela infração penal; já o *exame de corpo de delito* é a análise e o registro feito por peritos acerca desses vestígios, com as conclusões técnicas derivadas do material observado. Esse exame pode ser direto ou indireto, a depender se recai sobre o próprio corpo de delito (objetos vinculados diretamente à infração penal) ou sobre elementos obtidos por outras fontes (dados ou informes que não compõem o corpo de delito, mas podem elucidar o ocorrido).

Várias questões podem surgir a partir da assertiva de que a prova da materialidade do crime de informática depende do exame de corpo de delito: o laudo pericial é mesmo imprescindível para a prova da materialidade em infrações penais de informática? Pode ele ser substituído validamente por outros meios legítimos de prova? Se o corpo de delito desapareceu, por destruição ou ocultação, o laudo pericial fica prejudicado? Qual é o momento mais oportuno para a realização do exame?

Com este breve trabalho, pretendemos jogar alguma luz sobre tal ordem de indagações, partindo das normas positivadas de Direito Processual que regulam a proposição e a produção das provas no ambiente acusatório.

3.1 A imprescindibilidade do laudo pericial para a prova da materialidade nos delitos de informática: mito ou verdade?

Parece-nos intuitivo que não se faz prova da existência do crime cibernético sem o *exame de corpo de delito*, formalizado em

laudo técnico pericial. Isto porque a execução do delito envolve aspectos técnicos específicos, a exigir conhecimento científico da informática para atestar a existência da infração penal. Não é dado ao juiz, ainda que possua conhecimento da área, suprir a ausência do exame pericial pelo seu próprio conhecimento científico, pois isso arranharia a sua imparcialidade e isenção para o julgamento da causa, colocando-se na posição de produtor de prova, além de subtrair das partes a possibilidade de contraditar, no curso do processo, a exposição científica dos fatos e suas consequências jurídicas.

Para evitar erros técnicos de julgamento e garantir a dialética processual, o nosso Código de Processo Penal impõe como regra a realização de exame de corpo de delito para comprovar a materialidade delitiva, desde que a infração penal não seja transeunte. Assim está disposto na redação do art. 158: "Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado".

Por outro lado, há interferência do postulado processual da inexistência de hierarquia das provas, pelo qual o juiz fundamenta sua decisão pela livre apreciação do conjunto probatório, não havendo preferência entre as fontes de conhecimento, nem vinculação às conclusões periciais, cujo laudo tem valor apenas relativo, como, aliás, deixa explícito o art. 182 do CPP[1]. Assim, sendo o juiz o principal destinatário da prova, pode motivadamente afastar-se do exame pericial (não propriamente dispensá-lo) e acolher, como razão de decidir, outros elementos de prova em sentido oposto ao laudo técnico. Neste sentido, basta rememorar o item VII da Exposição de Motivos do Código de Processo Penal:

> [...] nem é prefixada uma hierarquia de provas: na livre apreciação destas, o juiz formará, honesta e lealmente, a sua convicção. [...] Todas as provas são relativas; nenhuma

[1] "Art. 182. O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte."

> delas terá, *ex vi legis*, valor decisivo, ou necessariamente maior prestígio que outra.

Em face de tal postulado, parte da jurisprudência inclinou-se pela dispensabilidade do exame pericial quando houver outros elementos de prova suficientes para atestar a materialidade do crime, relativizando completamente o comando do citado art. 158 do CPP. Confiram-se dois julgados dos tribunais superiores sobre a questão:

> I – Ausência do exame necroscópico da vítima: irrelevância, dado que a sua morte resultou demonstrada por outras provas. Exame de balística: desnecessidade. II – [...]. III – HC indeferido. (STF, HC n.º 70118-3/SP, Rel. Min. Carlos Velloso, julg. 6 abr. 1993.)

> [...] O princípio do livre convencimento motivado, vigente em qualquer processo brasileiro, faz com que seja o art. 158 do Código de Processo Penal (quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado) interpretado de modo a definir regra geral de necessidade de prova, e não de sua exclusividade, salvo diante de confissão, assim permitindo ao julgador valorar a existência de quaisquer fatos controversos, inclusive quanto aos vestígios do crime, por quaisquer meios de prova. (STJ, AgRg no REsp n.º 1.257.007/SC, Rel. Min. Sebastião Reis Júnior, julg. 11 nov. 2014.)

A doutrina adverte, contudo, que a ocorrência da infração penal deve ser objetivamente comprovada no processo, mediante a colheita direta ou indireta dos vestígios materiais, deles extraindo-se uma conclusão segura sobre a existência do crime, por meio de exame pericial, conforme determina o art. 158 do CPP (NUCCI, 2015, p. 68). Somente em caso de desaparecimento dos vestígios materiais, a lei processual autoriza a dispensa do exame de corpo de delito, podendo ser substituído pela prova testemunhal (art. 167 do CPP[2]).

Eugênio Pacelli anota não se tratar de questão alusiva à hierarquia de provas, mantendo-se o regime processual do livre

[2] "Art. 167. Não sendo possível o exame de corpo de delito, por haverem desparecido os vestígios, a prova testemunhal poderá suprir-lhe a falta."

convencimento motivado do juiz, mas sim à *especificidade de meio de prova*, tendo o legislador eleito um meio específico para a comprovação da existência do delito, garantindo ao acusado um sistema probatório criterioso para a afirmação da certeza e do convencimento (OLIVEIRA, 2012, p. 331-332).

Para alguns, a norma do art. 158 do CPP tangencia, excepcionalmente, o *sistema de apreciação da prova legal* ou *prova tarifada*, pelo qual o magistrado é obrigado a observar as regras preestabelecidas em lei sobre o valor de cada prova (CAPEZ, 2010, p. 381; NUCCI, 2015, p. 23). Entendemos, no entanto, que essa aproximação é apenas aparente, pois o juiz não fica vinculado ao conteúdo do laudo técnico, podendo rechaçá-lo em vista de outros elementos de prova que, combinados, refutem as conclusões periciais. Vigora, portanto, em sua plenitude, o *sistema do livre convencimento motivado* ou *da persuasão racional*, cabendo ao juiz, ao examinar o conjunto probatório, apontar as contradições porventura existentes na prova e decidir conforme a verdade preponderante – a chamada *verdade processual* (NUCCI, 2015, p. 21).

Mesmo não havendo hierarquia entre os meios de prova, o art. 158 do diploma processual penal não deixa margem a dúvidas: quando a infração penal deixar vestígios materiais, o exame de corpo de delito é indispensável à regularidade do processo, não podendo ser substituído por qualquer outra prova, nem mesmo pela confissão do acusado. A penalidade processual é expressa: a ausência do exame pericial acarreta a nulidade absoluta do processo, insanável pela mera preclusão (art. 564, III, "b"[3]). Almeja o legislador, assim, garantir ao acusado a formação da culpa pelos meios que melhor possam representar a certeza dos fatos, mitigando a possibilidade de prevalecer algum subjetivismo exacerbado do julgador.

[3] "Art. 564. A nulidade ocorrerá nos seguintes casos: [...] III – por falta das fórmulas ou dos termos seguintes: [...] b) o exame do corpo de delito nos crimes que deixam vestígios, ressalvado o disposto no art. 167; [...]."

É certo que não há como escapar a alguma dose de subjetividade, mesmo por parte do perito, já que, conforme observado por Luís Fernando Manzano, "toda perícia resulta da interpretação de um técnico ou profissional sobre alguma coisa ou alguém por ele examinado" (apud EBERHARDT, 2016, p. 65-66). Não obstante, cabe considerar que o exame de corpo de delito é o caminho científico mais próximo entre a verdade e o devido processo legal, constituindo a prova mais segura para a afirmação da existência ou não do crime.

Nas infrações penais de informática, o exame de corpo de delito é inevitável: não há como confirmar de modo seguro a sua existência e a sua extensão sem constatar o caminho lógico percorrido pelo agente criminoso dentro do ambiente virtual, até mesmo determinando a origem dos atos executórios, fundamental para circunscrever a autoria do crime. Isso só pode ser feito por exame técnico, em que os vestígios são analisados e classificados por profissional habilitado em informática, que vai elaborar uma opinião crítica e abalizada sobre os fatos científicos observados.

Somente sob circunstâncias muito especiais dispensa-se o exame de corpo de delito, aplicável, como regra, a qualquer infração penal, inclusive a cibernética.

Em primeiro lugar, por mais evidente, dispensa-se o exame pericial em caso de desaparecimento dos vestígios, por destruição ou ocultação total dos objetos que compõem o cenário do crime. Sem objeto a examinar, impossível qualquer verificação técnica, ficando autorizada a substituição da prova pericial pela prova testemunhal (art. 167 do CPP). Ressalva-se que, nas infrações cibernéticas, vários vestígios são virtuais (incorpóreos), cujos dados não raras vezes independem da máquina desaparecida e que podem ser úteis na elucidação da materialidade e da autoria (a exemplo de dados gravados em servidor de rede), impondo-se então a realização do exame pericial indireto.

Segundo, os fatos evidentes, decorrentes de um silogismo simples, e os fatos notórios, de conhecimento geral do povo, não precisam ser provados, prescindindo do exame pericial. Por exemplo, num crime de posse de material pornográfico infantil envolvendo criança de tenra idade (art. 241-B do ECA – Lei n.º 8.069/90), não é necessário prova técnica para confirmar a qualidade de "criança", evidenciada pelas imagens apreendidas. Aqui é preciso bastante cuidado para não confundir fato notório ou evidente, que pressupõe a certeza do conhecimento, com presunção comum, retirada do raciocínio dedutivo mais complexo, insuficiente para comprovar a materialidade delitiva. Por exemplo, um determinado *site* é conhecido pela venda de *softwares* piratas; alguém adquiriu, para revender, programas de informática naquele *site*; há grande chance de esses programas serem piratas, violadores de direitos autorais, mas há de ser comprovada tal circunstância.

Por fim, os fatos de conhecimento comum – aquém dos fatos notórios, que fazem parte da cultura geral do povo – não necessitam de exame pericial, pois estão ao alcance de qualquer cidadão, podendo ser provados por qualquer meio. Nas palavras de Eugênio Pacelli de Oliveira:

> Se houver um fato, qualquer fato, cuja existência, a senso comum, ao alcance do conhecimento dito *vulgar*, pode ser comprovada por outro meio de prova, qualquer prova, não haverá de se falar na prova específica. O *específico* que fizemos acompanhar o vocábulo *prova* estará sempre na dependência da natureza do delito e dos fatos a serem provados, como ocorre, por exemplo, no exame cadavérico, na identificação de arcada dentária, etc." (OLIVEIRA, 2012, p. 420). [Grifos do original]

Entram nesta categoria, em nosso sentir, diversos fatos do conhecimento vulgar relacionados aos crimes cibernéticos, como, por exemplo, o funcionamento prático da Internet, o acesso público a manifestações individuais em redes sociais, a utilidade de um determinado *software*, etc., que não demandam análise pericial. No crime de compartilhamento de pornografia infantil (art. 241-A do ECA), tem sido comum a alegação da defesa de inexistência

de prova da materialidade delitiva em vista de o laudo pericial ter omitido a efetiva troca de arquivos digitais de conteúdo pedófilo. Entendemos que basta para comprovar a materialidade delitiva a simples informação de que o autor do crime instalou em seu dispositivo digital um determinado programa de compartilhamento automático de arquivos (chamado, em linguagem técnica, de compartilhamento em rede *peer-to-peer*, par a par ou P2P). Isso justamente em face do conhecimento vulgar, ao alcance de todos, de que o programa em questão, uma vez instalado, já disponibiliza na rede os arquivos ilícitos armazenados pelo agente. O *software* mais comum utilizado para o compartilhamento de arquivos digitais é o denominado "eMule", recorrente em crimes de pedofilia infantojuvenil pela Internet (MPF, 2016, p. 230-231).

Afora estes casos, a ausência do laudo pericial acarreta a nulidade absoluta do processo (art. 564, III, "b", do CPP), dada a inexistência de prova adequada da materialidade delitiva. O defeito pode ser sanado antes da sentença, requisitando o juiz a realização do exame pericial e, após a juntada do respectivo laudo, reabrindo nova instrução, caso haja questionamentos de pelo menos uma das partes a respeito do conteúdo do laudo (art. 573 do CPP[4]). Não sendo possível obter a prova da materialidade, nem sequer por testemunhas, impõe-se a absolvição do réu (EBERHARDT, 2016, p. 79).

4 Aspectos formais e procedimentais relevantes

As infrações penais com emprego de informática não possuem normas próprias de ordem processual dispostas em lei. Neste aspecto, são aplicáveis as normas processuais previstas genericamente no Código de Processo Penal e em leis especiais, quando incidentes na espécie (a exemplo da lei de combate à organização

[4] "Art. 573. Os atos, cuja nulidade não tiver sido sanada, na forma dos artigos anteriores, serão renovados ou retificados. § 1º A nulidade de um ato, uma vez declarada, causará a dos atos que dele diretamente dependam ou sejam consequência. § 2º O juiz que pronunciar a nulidade declarará os atos a que ela se estende."

criminosa – Lei n.º 12.850/13). Como exceção, ressalte-se que o Marco Civil da Internet no Brasil – Lei n.º 12.965/15 – possui importantes instrumentos de apuração de infrações penais cibernéticas, determinando em seus arts. 13, 15 e 22 que o servidor de conexão ou de aplicações da Internet atenda à ordem judicial de acesso ao conteúdo dos registros.

As autoridades policiais e o Ministério Público não estão inibidos de expedir atos administrativos disciplinando certas formalidades na obtenção e na produção da prova técnica, respeitadas a Constituição Federal e as leis em vigor.

No que toca ao *exame de corpo de delito*, sua disciplina genérica encontra-se nos arts. 158 a 184 do CPP, alguns dos quais já foram mencionados.

No aspecto formal da prova, destacamos que o art. 159, *caput*, do CPP[5], impõe que o exame seja feito por um perito oficial,

[5] "Art. 159. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior. (Redação dada pela Lei n.º 11.690, de 2008.) § 1º Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior, preferencialmente na área específica, dentre as que tiverem habilitação técnica relacionada com a natureza do exame. (Redação dada pela Lei nº 11.690, de 2008.) § 2º Os peritos não oficiais prestarão o compromisso de bem e fielmente desempenhar o encargo. (Redação dada pela Lei n.º 11.690, de 2008.) § 3º Serão facultadas ao Ministério Público, ao assistente de acusação, ao ofendido, ao querelante e ao acusado a formulação de quesitos e indicação de assistente técnico. (Incluído pela Lei n.º 11.690, de 2008.) § 4ºO assistente técnico atuará a partir de sua admissão pelo juiz e após a conclusão dos exames e elaboração do laudo pelos peritos oficiais, sendo as partes intimadas desta decisão. (Incluído pela Lei n.º 11.690, de 2008.) § 5º Durante o curso do processo judicial, é permitido às partes, quanto à perícia (incluído pela Lei n.º 11.690, de 2008): I – requerer a oitiva dos peritos para esclarecerem a prova ou para responderem a quesitos, desde que o mandado de intimação e os quesitos ou questões a serem esclarecidas sejam encaminhados com antecedência mínima de 10 (dez) dias, podendo apresentar as respostas em laudo complementar (incluído pela Lei n.º 11.690, de 2008); II – indicar assistentes técnicos que poderão apresentar pareceres em prazo a ser fixado pelo juiz ou ser inquiridos em audiência. (Incluído pela Lei n.º 11.690, de 2008.) § 6º Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes,

isto é, aquele vinculado permanentemente a uma instituição pública e investido no cargo de perito. É indispensável que possua diploma de curso superior, não necessariamente em sua área de atuação, embora a especialização dê mais credibilidade à prova.

Não havendo perito oficial na localidade, o exame poderá ser realizado por duas pessoas idôneas, com diploma em curso superior, preferencialmente na área do exame. Por não serem peritos oficiais, prestarão compromisso em juízo de bem desempenhar o encargo (art. 159, §§ 1º e 2º. O exame realizado por apenas um perito não oficial acarreta a nulidade da prova (Súmula 361 do STF[6]). A jurisprudência considera relativa essa nulidade, cabendo à parte demonstrar o prejuízo e argui-la em tempo oportuno (STF, HC n.º 75.793/RS, Rel. Min. Sepúlveda Pertence, julg. 31 mar. 1998).

Quanto ao momento de realização da prova técnica, pode ser feita logo no início da instrução processual, caso em que o contraditório será imediato, facultando-se às partes a indicação de assistente técnico e a formulação de quesitos. Os assistentes atuarão após a apresentação do laudo pericial, apresentando seus pareceres no prazo fixado pelo juiz e garantindo-se a eles o acesso ao material probatório (art. 159, §§ 3º, 4º e 6º).

Contudo, assim como ocorre com outras infrações penais, na grande maioria dos casos envolvendo o emprego de informática, o laudo pericial é confeccionado ainda na fase inquisitiva, até mesmo para viabilizar o indiciamento do investigado e auxiliar na

salvo se for impossível a sua conservação. (Incluído pela Lei n.º 11.690, de 2008.) § 7º Tratando-se de perícia complexa, que abranja mais de uma área de conhecimento especializado, poder-se-á designar a atuação de mais de um perito oficial, e a parte indicar mais de um assistente técnico. (Incluído pela Lei n.º 11.690, de 2008.)"

[6] STF, Súmula 361: "No Processo Penal, é nulo o exame realizado por um só perito, considerando-se impedido o que tiver funcionado anteriormente na diligência de apreensão". Oportuno lembrar que, com o advento da Lei n.º 11.690/2008, modificando a redação do art. 159 e parágrafos do CPP, remanesce o entendimento sumulado somente aos exames realizados por peritos não oficiais.

formação da *opinio delicti* do órgão acusatório, sinalizando com a necessária segurança a existência ou não da materialidade delitiva.

De fato, o art. 6º, VII, do CPP[7], determina que a autoridade policial providencie tão logo quanto possível o exame de corpo de delito, demonstrando o legislador preocupação com o potencial desaparecimento dos vestígios com o passar do tempo. Trata-se de medida de antecipação de prova, de natureza cautelar, em que o contraditório será diferido ou postergado para após o recebimento da denúncia ou queixa, quando então terá início o Processo Penal. Assim, as partes não ficarão inibidas de contraditar a prova pericial e requerer novos esclarecimentos, até mesmo indicando seus assistentes técnicos (art. 159, § 5º), cabendo ao magistrado julgar a pertinência das diligências requeridas e deferir o prazo adequado para serem atendidas.

O laudo pericial deve ser elaborado em até 10 (dez) dias, contados da ciência da requisição pelo perito (art. 160, parágrafo único, do CPP[8]). Tal prazo é considerado *impróprio*, não havendo sanção processual prevista para o caso de entrega fora do tempo (NUCCI, 2015, p. 80). Se houver abuso desta faculdade, caberá ao juiz ou ao delegado de polícia requisitar a apresentação do laudo no prazo que assinalar, sob pena de apuração de responsabilidade administrativa e criminal do perito oficial desidioso. Quanto aos peritos nomeados (não oficiais ou louvados), poderão ser destituídos e substituídos por outros.

[7] "Art. 6º. Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: [...] VII – determinar, se for o caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;"

[8] "Art. 160. Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem e responderão aos quesitos formulados. Parágrafo único. O laudo pericial será elaborado no prazo máximo de 10 (dez) dias, podendo este prazo ser prorrogado, em casos excepcionais, a requerimento dos peritos." (Redação dada pela Lei n.º 8.862, de 28 de março de 1994.)

5 Conclusão

As infrações penais cibernéticas são aquelas previstas em tipo penal que recaem sobre um dispositivo de informática, cujas informações digitais são protegidas pela norma. Há também aquelas em que se verifica o uso de equipamento informático para obtenção de alguma vantagem ilícita pelo agente, ainda que o emprego de meio tecnológico não esteja previsto no tipo penal.

Por se tratar de infração penal envolvendo a ciência da informática, a prova da materialidade delitiva deve ser feita por exame de corpo de delito, aquilatando-se o caminho técnico percorrido pelo agente para a prática da infração digital.

Somente o exame de corpo de delito, formalizado em laudo pericial, trará a necessária segurança jurídica para a afirmação da existência ou não da infração penal cibernética, de modo a atender adequadamente aos postulados constitucionais do estado de inocência e do sistema penal acusatório.

Em hipóteses excepcionais, previstas em lei ou em razão da qualidade do fato, estará dispensado o exame de corpo de delito. Entram nesta categoria o desaparecimento total dos vestígios do crime (art. 167 do CPP), os fatos evidentes, os fatos notórios e os de conhecimento vulgar.

Afora tais casos, a ausência de laudo pericial acarreta a nulidade absoluta do processo (art. 564, III, "b", do CPP), presumindo-se o prejuízo causado ao réu em razão da inexistência de prova específica determinada em lei para a demonstração da materialidade delitiva (art. 158 do CPP). Não obstante, a nulidade poderá ser sanada pela oportuna realização do exame técnico, reabrindo-se a instrução processual, se necessário, em caso de discussão das partes sobre o conteúdo do laudo técnico (art. 573 do CPP).

Referências bibliográficas

BRASIL. Instituto Brasileiro de Geografia e Estatística. *Pesquisa Nacional por Amostra de Domicílios – PNAD 2015*. Disponível em: <http://www.ibge.gov.br/home/presidencia/noticias/imprensa/ppts/00000028012211102016222725469 85.pdf>. Acesso em: 19 jan. 2017.

____. Ministério Público Federal. Câmara de Coordenação e Revisão. *Roteiro de atuação sobre crimes cibernéticos*. 3. ed. Brasília/DF, 2016.

CAPEZ, Fernando. *Curso de Processo Penal*. 17. ed. São Paulo: Saraiva, 2010.

DICIONÁRIO Houaiss da Língua Portuguesa. Rio de Janeiro: Objetiva, 2009.

EBERHARDT, Marcos. *Provas no Processo Penal*: análise crítica, doutrinária e jurisprudencial. Porto Alegre: Liv. do Advogado, 2016.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. *Crimes no meio ambiente digital e a sociedade de informação.* 2. ed. São Paulo: Saraiva, 2016.

NUCCI, Guilherme de Souza. *Provas no Processo Penal*. 4. ed. Rio de Janeiro: Forense, 2015.

OLIVEIRA, Eugênio Pacelli de. *Curso de Processo Penal*. 16. ed. São Paulo: Atlas, 2012.

PINHEIRO, Emeline Piva. *Crimes virtuais: uma análise da criminalidade informática e da resposta estatal*. Santa Catarina: UFSC, 2006. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/29397-29415-1-PB.pdf>. Acesso em: 16 jan. 2017.

A busca e apreensão na investigação e prova dos crimes cibernéticos

Márcio Satalino Mesquita*

RESUMO

Este artigo analisa, do ponto de vista do exercício da jurisdição, os problemas e respectivas soluções, decorrentes das inovações tecnológicas na documentação digital, no trabalho de investigação e prova de crimes cibernéticos com uso da busca e apreensão.

Palavras-chave: Direito. Processo Penal. Busca. Apreensão.

ABSTRACT

This paper analyzes, from the point of view of the exercise of jurisdiction, the problems, and their solutions, arising from the technological innovations in digital documentation in the investigation and proof of cybercrimes, using search and seizure.

***Keywords**: Law. Criminal procedure. Search and Seizure.*

* Graduado em Engenharia Mecânica pelo Instituto de Ensino de Engenharia Paulista e em Direito pela Universidade de São Paulo. Mestre em Educação pela Universidade Federal de São Carlos. Juiz Federal da 2ª Vara de Taubaté/SP. *E-mail*: msmesqui@trf3.jus.br.

1 Introdução

Este trabalho é fruto da reflexão sobre temas debatidos durante o curso "Investigação e prova nos crimes cibernéticos. Dificuldades técnicas e jurídicas – Questões práticas", promovido, na primavera de 2016, pela Escola de Magistrados da Justiça Federal da 3ª Região (EMAG), do TRF3, sob a direção do Desembargador Federal Carlos Muta e a coordenação da Juíza Federal Substituta Adriana Delboni Taricco. A ambos agradeço a oportunidade de ter participado do curso e o convite para a elaboração deste trabalho.

Registro que os temas que ligam Direito e Informática são especialmente caros para mim. Tenho formação em Ciências Exatas, sempre gostei de computador e já atingi idade suficiente para ter uma visão retrospectiva sobre esse assunto. Lembro-me de quando vi, pela primeira vez, trazida do exterior por um parente, uma calculadora; aprendi no colégio a fazer cálculos em régua de cálculo; ainda jovem, tive meu primeiro contato com um computador quando eram máquinas sem teclado e sem vídeo: as informações eram introduzidas por meio de cartões perfurados e as respostas saíam em uma impressora. Mudei de área, mas o interesse permaneceu.

O próprio tema do curso remete à ideia de que vivemos uma época de transformação, que cria dificuldades para o mundo jurídico. Sabemos que o Direito sempre corre atrás dos fatos sociais, que ele é na verdade muito mais resultado do que agente das transformações sociais.

Há sempre uma ideia recorrente de que a época em que vivemos é de profundas transformações, que jamais foram vividas anteriormente. Parafraseando um ilustre político, poderíamos dizer que "nunca antes na história desse país, ou do mundo", ocorreram tantas mudanças em tão pouco tempo.

Não discordo, evidentemente, da avaliação de que a velocidade das mudanças sociais na atualidade não tem paralelo na

história. Mas penso que todos nós temos a tendência a acreditar que a época em que vivemos é ímpar, na qual tudo está sendo modificado. Acredito que as pessoas que estavam na exposição mundial de tecnologia em Paris, em 1900, admirando a Torre Eiffel – a maravilha da engenharia de então –, também tinham essa mesma sensação. Estavam presenciando a invenção do automóvel e outras maravilhas.

E o que há de novo, que nos espanta tanto e, sem dúvida, provoca tantas dificuldades como as mencionadas no título do curso que inspira esse trabalho? Indubitavelmente, a novidade é o desenvolvimento da tecnologia de processamento e transmissão das informações.

Do ponto de vista teórico, os computadores são basicamente o resultado de tecnologia aplicada aos semicondutores, na construção de circuitos integrados, capazes de realizar operações lógicas. A teoria é antiga: os semicondutores foram descobertos no século XIX, e as operações lógicas foram descritas pelo matemático britânico George Boole, também no século XIX.

Contudo, em meados do século XX, o desenvolvimento da teoria dos semicondutores, a invenção do *chip* e a construção dos primeiros computadores iniciaram um período de intenso aprimoramento tecnológico.

Os computadores trabalham apenas com os dígitos 0 e 1 (sistema binário ou de base 2), porque nesse sistema é fácil a representação (com corrente, 1; sem corrente, 0; ou ainda polarizado, 1; não polarizado, 0), embora toda a transmissão de dados, por meios físicos (cabos ou fibras ópticas) ou pelo espaço (por ondas de rádio), seja feita analogicamente, já que os meios de transmissão de dados são sinais elétricos, ou eletromagnéticos, ou luminosos, contínuos, e não discretos. Daí a expressão mundo digital, aquele em que todo tipo de informação – um texto, uma imagem, uma fotografia, uma música, um vídeo – é registrado em forma digital ou numérica.

Logo se percebeu que os computadores seriam muito mais úteis se pudessem se comunicar entre si. Surgiu, então, a rede mundial, que é na verdade uma interligação de redes de computadores, a Internet, criada inicialmente para fins militares. Isso acabou resultando no que hoje é conhecido como *cyberspace*, também chamado de mundo virtual, em oposição ao mundo real. Interessante notar que o termo virtual é aqui usado no mesmo sentido que os programadores de computador utilizam: algo que simula a realidade; uma impressora virtual é uma impressora que não existe na realidade, mas apenas logicamente; o sistema opera como se ela realmente existisse.

Portanto, é esse novo mundo digital e virtual que cria dificuldades para o velho mundo jurídico. Essas dificuldades ocorrem no campo do Direito Penal, uma vez que, enquanto algumas das novas condutas que surgem no mundo virtual podem ser enquadradas nos crimes atualmente existentes, outras condutas lesivas não encontram tipificação legal correspondente.

Também ocorrem no campo do Direito Processual Penal, pois alguns de seus institutos clássicos – como a busca e apreensão, objeto deste trabalho – foram criados e desenvolvidos em um ambiente no qual os conceitos de local do crime, de domicílio e de documento eram tais que não mais se conformam com a realidade digital e virtual.

Resultado esperado dessas mudanças tecnológicas, tais dificuldades são ainda mais agravadas pelo perfil conservador dos operadores do Direito, em especial dos juízes, decorrente, a meu ver, de um arraigado idealismo, no sentido platônico do termo. Tudo o que existe deve ser enquadrado nas categorias de pensamento já existentes; não se admite uma novidade: é o que se chama, no jargão jurídico, de descobrir ou "revelar" a natureza jurídica de determinado instituto, negócio, contrato, situação, etc.

Exemplo disso é a discussão, anterior à alteração do ECA (Estatuto da Criança e do Adolescente), sobre a configuração ou

não do crime quando da divulgação das imagens pornográficas pela Internet, sendo digno de nota o acórdão do Supremo Tribunal Federal no Recurso em *Habeas Corpus* – RHC n.º 76689[1], no sentido de que "a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo". Nessa mesma linha, não custa lembrar que houve discussão sobre a validade, ou não, de petições datilografadas, e não manuscritas, quando da invenção da máquina de escrever.

O tema desse trabalho, portanto, é analisar, não do ponto de vista da teoria do Direito Processual Penal, mas do ponto de vista prático do exercício da jurisdição, quais são as dificuldades – e as soluções – do emprego da busca e apreensão na investigação e prova dos crimes cibernéticos.

2 Crimes cibernéticos

Várias denominações são utilizadas para essa nova categoria de crimes: *computer crimes*, abuso de computador, crime de computação, criminalidade mediante computador, delito informático, crime informático, delinquência informática, fraude informática, delinquência econômica, crimes por meio de informática, crimes cibernéticos.

Talvez a expressão mais corrente, no Brasil de hoje, seja *crimes cibernéticos*. Mas isso não é muito relevante. Embora existam várias definições, creio que a maioria dos doutrinadores concorda com que os crimes cibernéticos, ou crimes de informática, são aqueles que têm como próprio objeto os sistemas informatizados (também chamados de *crimes de informática puros* ou *próprios*)

[1] STF, HC n.º 76689/PB, Primeira Turma, Rel. Min. Sepúlveda Pertence, julg. 22 set. 1998, DJ 6 nov. 1998 PP-00003 EMENT VOL-01930-01 PP-00070. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%2876689%2ENUME%2E+OU+76689%2EACMS%2E%29&base=baseAcordaos&url=http://tinyurl.com/h683uk3>. Acesso em: 5 mar. 2017.

ou crimes em que os sistemas informatizados são o meio para a execução de quaisquer outros crimes (também chamados *crimes de informática impuros* ou *impróprios*).

No que diz respeito à busca e apreensão, não há diferença relevante entre crimes cibernéticos próprios ou impróprios, uma vez que é cabível busca e apreensão tanto nos crimes que tenham por objeto os sistemas informatizados, quanto naqueles em que tais sistemas são apenas empregados como meio de execução.

Se aceita essa conceituação, é grande o número de crimes cibernéticos, próprios e impróprios, atualmente tipificados na legislação, com relação aos quais pode ser eventualmente decretada busca e apreensão: racismo, furto, dano, estelionato, crimes contra o sistema financeiro, pornografia infantil, crimes contra a honra, ameaça, interceptação do fluxo de dados em serviço de telecomunicações, crimes contra a inviolabilidade dos segredos, crimes contra a ordem tributária, crimes eleitorais, violação de correspondência, incitação ao crime, apologia de crime ou criminoso, violação de direito autoral, induzimento, instigação ou auxílio ao suicídio, favorecimento da prostituição, rufianismo, tráfico de drogas, crimes contra o consumidor, invasão de dispositivo informático.

Merecem especial destaque, no âmbito deste trabalho, os crimes de divulgação e armazenamento de material de pornografia infantojuvenil, tipificados nos arts. 241-A e 241-B do ECA, Lei n.º 8.009/1990, atualmente com a redação dada pela Lei n.º 11.829/2008.

Tal destaque decorre da consolidação da jurisprudência do Supremo Tribunal Federal, em regime de repercussão geral, no Recurso Extraordinário n.º 628624[2], no sentido de que "compete

[2] STF, RE n.º 628624/MG**,** Tribunal Pleno, Rel. Min. Marco Aurélio, Rel. p/ o acórdão Min. Edson Fachin, julg. 29 out. 2015, acórdão eletrônico repercussão geral - mérito DJe-062, divulg. 5 abr. 2016, public. 6 abr. 2016. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28628624%2ENUME%2E+OU+628624%2EACMS%2E%29&base=baseAcordaos&url=http://tinyurl.com/glp6gt6>. Acesso em: 5 mar. 2017.

à Justiça Federal processar e julgar os crimes consistentes em disponibilizar ou adquirir material pornográfico envolvendo criança ou adolescente (arts. 241, 241-A e 241-B da Lei n.º 8.069/1990), quando praticados por meio da rede mundial de computadores", bem como do fato de que, em tais crimes, a busca e apreensão tem se revelado, via de regra, de emprego necessário.

3 A busca e apreensão e os direitos fundamentais

A constatação de um potencial conflito entre a necessidade de utilização, pelo Estado, da busca e apreensão, como instrumento de investigação e prova, e os direitos fundamentais ocorre desde o próprio surgimento dos direitos e garantias individuais de primeira geração.

O conflito mais evidente é com a garantia da inviolabilidade de domicílio, conhecida dos ingleses desde antes do século XVIII, com a frase "o lar de um inglês é seu castelo", e pelo sempre citado discurso de Lord Chatham na Câmara dos Comuns:

> O homem mais pobre pode, em sua casa, desafiar todas as forças da Coroa. Essa casa pode ser frágil – seu telhado pode mover-se –, o vento pode soprar em seu interior – a tempestade pode entrar, a chuva pode entrar –, mas o Rei da Inglaterra não pode entrar – seus exércitos não se atreverão a cruzar o umbral da arruinada morada (apud BESSA, 2002).

Mas é a Constituição dos Estados Unidos da América (EUA), na sua Declaração de Direitos (*Bill of Rights*), talvez o documento mais importante do constitucionalismo moderno, que marca expressamente a solução do conflito, afirmando na Quarta Emenda a proteção do domicílio contra buscas e apreensões desarrazoadas, e exigindo, para a expedição do mandado, uma justa causa, apoiada em indícios probatórios, bem como a descrição do local da busca e das pessoas ou coisas a serem apreendidas:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or

> affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Em nosso país, todas as Constituições republicanas afirmaram a inviolabilidade do domicílio, sendo que a atual Carta de 1988, em seu art. 5º, inciso XI, excepciona expressamente a hipótese de determinação judicial. Apenas na vigência do Estado de Sítio é afastada a reserva de jurisdição para a busca e apreensão (art. 139, inciso V).

Dessa forma, não é necessária qualquer interpretação mediante o método da ponderação – tão caro aos neoconstitucionalistas –, já que o próprio texto constitucional prevê a possibilidade de afastamento da garantia de inviolabilidade de domicílio por determinação judicial.

A Constituição brasileira, embora preveja que a inviolabilidade do domicílio possa ser excepcionada, desde que sujeita à *reserva de jurisdição*, não estabelece, contudo, como faz a dos EUA, os requisitos mínimos para que seja judicialmente determinada uma busca e apreensão.

É o Código de Processo Penal (CPP), em seu art. 240, *caput* e § 1º, que estabelece, para a busca e apreensão domiciliar, a exigência de justa causa e indícios probatórios – empregando a expressão "fundadas razões" –, especificando as possíveis finalidades da diligência.

No seu art. 243, o CPP indica os requisitos do mandado de busca e apreensão, dos quais nos interessa especialmente, neste trabalho, a necessidade de indicação, mais precisa possível, da casa em que será realizada, bem como os motivos e os fins da diligência.

Por outro lado, também se afigura patente um potencial conflito entre a necessidade de investigação e prova criminal, mediante busca e apreensão, e a inviolabilidade da intimidade e privacidade, garantida no art. 5º, inciso X, da Constituição.

De desenvolvimento histórico mais recente do que a garantia da inviolabilidade do domicílio, a garantia da intimidade e

da privacidade das pessoas assume importância significativa a partir da segunda metade do século XX, por ser a sua violação identificada com os Estados totalitários:

> A violação dessa intimidade implica seu oposto, a desolação, uma das características do "totalitarismo" apontada por Hannah Arendt, que "impede a vida privada e promove o desenraizamento" e nela "não se dá o estar só ensejador do diálogo socrático do eu consigo mesmo" (MISSAGIA, 2002).

Dessa forma, cabe à autoridade judiciária, ao analisar um requerimento de busca e apreensão, proceder a um exame rigoroso da presença dos requisitos para o seu deferimento (em especial razoabilidade, justa causa e suporte indiciário mínimo), uma vez que estará afastando – ainda que para isso autorizado, no caso concreto – a preciosa garantia da inviolabilidade do domicílio, da intimidade e da privacidade.

Por outro lado, considerando que o descumprimento das formalidades legalmente exigidas, tanto para o deferimento quanto para o cumprimento de um mandado de busca e apreensão, poderá eventualmente implicar o reconhecimento de nulidades que podem vir a comprometer todo um longo trabalho de investigação, deverá a autoridade judiciária cuidar para que tanto a concessão da ordem quanto a efetivação da diligência sejam feitas de forma válida, com observância das garantias constitucionais e legais.

Discutem-se, a seguir, algumas dificuldades práticas comuns no deferimento e cumprimento de ordens de busca e apreensão de equipamentos de informática e dispositivos de armazenamento, na investigação e prova de crimes cibernéticos.

4 A busca e apreensão de equipamentos de informática e o acesso ao conteúdo dos documentos digitais

A experiência prática do foro tem revelado que tanto o Delegado de Polícia Federal quanto o representante do Ministério Público Federal têm formulado, juntamente com o requerimento de expedição de mandado de busca e apreensão, também

requerimento de autorização de acesso ao conteúdo das mídias digitais apreendidas, ou até mesmo de quebra de sigilo para acesso a tais conteúdos.

É essa inclusive a recomendação constante do *Roteiro de atuação sobre crimes cibernéticos*, elaborado pela 2.ª Câmara de Coordenação e Revisão do Ministério Público Federal, "de modo que não seja alegada a nulidade em razão dessa verificação".

Com a devida vênia das opiniões em sentido contrário, entendo que a expedição do mandado de busca e apreensão, com especificação de que devem ser apreendidos equipamentos de informática e dispositivos de armazenamento digitais, com vistas à colheita de elementos de prova de determinado crime, implica evidentemente ordem para acesso ao conteúdo de tais dispositivos.

Aliás, esse é um exemplo significativo de como a novidade representada pelos documentos digitais provoca dificuldades no meio jurídico. Antes do advento dos documentos digitais, ninguém cogitaria, por exemplo, da necessidade de autorização de acesso ou quebra de sigilo bancário para simples leitura de extratos bancários encontrados no local da diligência, se do mandado de busca e apreensão constasse a finalidade de obtenção de documentos e outros elementos de prova do cometimento de crimes contra o Sistema Financeiro Nacional.

Entender que, de posse da ordem de busca e apreensão de equipamentos de informática, não possa a autoridade policial vasculhar o conteúdo armazenado em tais equipamentos seria o mesmo que entender, ao tempo dos documentos apenas em papel, que, ao se deparar a autoridade policial com um envelope fechado no cumprimento de um mandado de busca e apreensão, teria de requerer a autorização judicial para abertura e verificação de seu conteúdo.

Contudo, considerando que se trata de questão ainda polêmica, é ideal que o magistrado, se entender pela necessidade

dessa autorização, faça-a constar expressamente da decisão de deferimento e do mandado de busca e apreensão; ou, mesmo se entender pela sua desnecessidade, faça constar da decisão que o deferimento da ordem de busca e apreensão dos equipamentos de informática implica autorização para que o conteúdo seja vasculhado.

É esse o entendimento a que chegaram os magistrados federais participantes do curso mencionado na introdução deste trabalho, indicado na primeira parte do Enunciado 1, elaborado na ocasião:

> Enunciado 1 – Busca e apreensão: equipamentos de informática
>
> A ordem de busca e apreensão de equipamentos de informática implica a autorização para que seu conteúdo seja vasculhado com a finalidade de contatar a presença de elementos de convicção. [...]

5 Busca e peculiaridades dos documentos digitais

De acordo com o inciso II do art. 243 do CPP, o mandado de busca deve mencionar o motivo e os fins da diligência, ou seja, deve especificar, o tanto quanto possível, o objeto da investigação, indicando qual o delito investigado.

A diligência deve ser efetuada com a invasão minimamente possível da privacidade e intimidade das pessoas atingidas, ou seja, somente devem ser buscados documentos e outros elementos de convicção que tenham relação com o delito investigado.

Como não é objeto deste trabalho a discussão sobre eventual descoberta fortuita, interessa saber apenas que não devem ser apreendidos, na diligência, documentos ou outros objetos que não tenham qualquer relação com um ilícito penal.

O desenvolvimento tecnológico das últimas décadas implicou um aumento exponencial da capacidade de armazenamento dos dispositivos digitais. Essa capacidade, que há poucos anos me-

dia-se em kB (*quilobytes*, ou 2^{10} *bytes*), em computadores de grande porte, hoje mede-se em TB (*terabytes*, ou 2^{40} *bytes*), em dispositivos computacionais portáteis e de preço acessível a praticamente qualquer pessoa.

Tal fato cria, para a diligência de busca em dispositivos de armazenamento digital, um problema hoje comum e que, na época do papel, era raro: a grande dificuldade de buscar elementos de convicção num universo de milhões de documentos armazenados.

Para a solução desse problema, a experiência prática tem demonstrado a necessidade de que a diligência de busca e apreensão em mídias digitais, para cumprir a sua finalidade, seja acompanhada por um técnico especializado em sistemas informatizados, de maneira que, utilizando-se inclusive de programas desenvolvidos especificamente para isso, seja possível localizar, dentre eventuais milhares ou milhões de documentos armazenados no local da busca, apenas aqueles que interessam ao objeto de investigação.

Cumpre aqui ressaltar que a participação desse técnico no acompanhamento da diligência limita-se a auxiliar na busca propriamente dita, e as técnicas e procedimentos empregados não constituem o exame de corpo de delito previsto no art. 158 do CPP. Portanto, não há necessidade de que esse técnico seja um perito oficial, pode ser um agente policial para tanto qualificado.

A perícia nos equipamentos de informática e na mídia digital eventualmente apreendidos na diligência deverá ser feita posteriormente por peritos criminais oficiais, via de regra nos laboratórios de criminalística (e não no local da apreensão), onde será possível o emprego de técnicas de investigação mais sofisticadas e que demandam maior tempo para serem concluídas.

Também é esse o entendimento a que chegaram os magistrados federais participantes do curso mencionado na introdução deste trabalho, indicado na segunda parte do Enunciado 1 e no Enunciado 2, elaborados na ocasião.

> Enunciado 1 – Busca e apreensão: equipamentos de informática
>
> […] Se possível, esse procedimento deve ser realizado no próprio local, a fim de que a apreensão se restrinja apenas aos objetos pertinentes. O ato não constitui a perícia a que alude o art. 158 e seguintes do Código de Processo Penal, a ser feita posteriormente.
>
> Enunciado 2 – Busca e apreensão: exame de equipamentos por agente policial
>
> Na busca e apreensão de equipamentos de informática, o procedimento para que seu conteúdo seja vasculhado no próprio local, para constatar a presença de elementos de convicção, pode ser realizado por agente policial tecnicamente qualificado, sendo facultativa a presença de perito criminal.

6 Apreensão e peculiaridades dos documentos digitais

Outro exemplo significativo de como a novidade representada pelo advento dos documentos digitais provoca dificuldades no meio jurídico é a perda de sentido da velha distinção entre o documento original e a cópia desse mesmo documento, distinção que assumia relevância no mundo dos documentos em papel.

Sendo um documento digital basicamente um arquivo binário (um conjunto de dígitos de base 2 sequenciados de forma organizada, em geral com dígitos de controle), armazenado em um suporte físico (qualquer dispositivo de armazenamento digital, ainda que volátil), não há nenhuma distinção entre o documento originariamente produzido em um determinado momento e uma cópia feita em momento posterior.

A Lei n.º 11.419/2006, que dispôs sobre a informatização do processo judicial, já adotou em seu art. 11 esse entendimento, explicitando que "os documentos produzidos eletronicamente e juntados aos processos eletrônicos [...] serão considerados originais para todos os efeitos legais".

Se nos documentos digitais a diferença entre original e cópia não tem a relevância que tinha nos documentos em papel, a apreensão dos documentos digitais reflete essa mudança: como anotam COSTA e LEONARDI (2011), "a doutrina americana equipara a cópia eletrônica de dados a uma apreensão".

Dessa forma, pode haver casos em que a apreensão de documentos digitais deve ser feita não mediante a apreensão do dispositivo de informática (computador, etc.) nem da mídia digital (HD, etc.) em que o documento foi localizado, no momento da diligência de busca e apreensão, mas sim fazendo-se uma cópia do documento.

Com efeito, é possível imaginar os problemas que poderia ocasionar, por exemplo, a apreensão de um computador, ou de um dispositivo de armazenamento vital para o funcionamento do sistema de uma instituição financeira, porque neles foram encontrados evidências de crime de pornografia infantil cometido por um funcionário do setor de informática.

Interessante anotar que a Portaria n.º 1.287/2005[3] do Ministério da Justiça determinava, em seu art. 3º, que não se efetuasse a apreensão de computadores e outros suportes eletrônicos, se fosse possível, sem prejuízo para a investigação, a análise por cópia feita por perito criminal especializado (GOMES, 2016). A determinação, contudo, foi revogada posteriormente pela Portaria 759/2009[4] do mesmo órgão.

É recomendável, portanto, que do mandado de busca e apreensão conste de modo expresso a possibilidade de apreensão de documentos digitais mediante simples cópia, sem a apreensão do suporte físico, quando as circunstâncias indicarem que esta última

[3] GOMES, Rodrigo Carneiro. A execução da busca e apreensão, capacidade de representação do delegado de polícia, etiquetamento e o controle judicial: atualidades. *Revista dos Tribunais*, São Paulo, v. 964/2016, p. 297-312, fev. 2016.

[4] Disponível em: <https://www.legisweb.com.br/legislacao/?id=218765>. Acesso em: 6 mar. 2017.

implique prejuízo de difícil reparação para o sistema informatizado subjacente, e desde que, evidentemente, isso seja possível, sem prejuízo para a adequada investigação.

Por outro lado, a necessidade de acompanhamento de um técnico especializado na diligência de busca e apreensão de equipamentos de informática e documentos digitais também se revela pela necessidade de adequada preservação dos elementos de convicção colhidos. Nesse sentido:

> A correta *preservação* da prova digital também é requisito essencial para que a prova seja válida, pois garantirá a autenticidade e integridade da mesma. Veja-se que, face à característica da volatilidade das evidências digitais apontada acima, a adulteração ou perda de conteúdo da prova poderá ser fatal para o correto deslinde do processo.
>
> Nos termos do *Manual de crimes cibernéticos*, "preservar uma evidência digital significa sobretudo garantir que ela não sofreu alterações desde o momento em que foi coletada de uma fonte externa até a fase final de apresentação" (DOMINGOS, 2015).

Com efeito, além da necessidade de adequada preservação do material, já apontada, há risco inclusive de que o manuseio inadequado de equipamentos de informática e dispositivos de armazenamento digital provoque a perda dos dados.

Acresce-se ainda o fato de que diversos equipamentos de informática, dispositivos computacionais ou de armazenamento podem ser acessados remotamente e ter seus dados alterados. Assim, é necessário cautela para evitar prejuízos para as investigações.

Com relação particularmente aos *smartphones* e similares, os magistrados federais participantes do curso mencionado na introdução deste trabalho expressaram sua preocupação, o que resultou no Enunciado 3, elaborado na ocasião:

> Enunciado 3 – Busca e apreensão: celulares em modo avião
>
> Na busca e apreensão de telefones celulares (*smartphones*) ou dispositivos similares, recomenda-se que, se possível, eles sejam examinados após serem colocados em modo *off-*

line (modo avião), de forma a evitar alteração remota de dados e interromper eventuais comunicações.

7 A indicação do local da busca e documentos digitais remotamente armazenados

Com o desenvolvimento tecnológico dos computadores também ocorre o desenvolvimento dos dispositivos dedicados às comunicações entre os equipamentos computacionais. O desenvolvimento de infraestrutura de redes de computadores com grande capacidade de transmissão possibilitou o oferecimento de serviço de armazenamento e processamento de dados em ambiente remoto (*cloud computing)*.

Hoje, o acesso por qualquer pessoa física com um dispositivo computacional, até mesmo um *smartphone*, possibilita o armazenamento de arquivos de dados em ambiente remoto.

Isso significa ser possível que, no cumprimento de um mandado de busca e apreensão, que indica um local precisamente determinado, a autoridade policial depare-se com o fato de que os documentos digitais que interessam à investigação estejam armazenados não nesse local, mas remotamente.

Note-se que, por vezes, sequer será possível saber a localização exata do servidor (computador ou dispositivo computacional dedicado a uma tarefa específica de armazenamento e/ou processamento, por demanda de outros dispositivos) no qual se encontram armazenados tais dados.

Trata-se de mais um exemplo significativo de como a novidade tecnológica – armazenamento remoto de documentos digitais – provoca dificuldades no meio jurídico, diante da necessidade de indicação, da forma mais precisa possível, do local onde será realizada a diligência de busca e apreensão.

O local onde se encontram armazenados documentos digitais de determinado investigado, acessível através de seus equipamentos de informática, ou mediante uso de códigos de

acesso, deve ser considerado uma extensão de sua casa, estando tais documentos, portanto, sujeitos à apreensão mediante cópia.

Contudo, para que tal procedimento seja validamente efetuado, é necessário que conste do mandado de busca e apreensão a possibilidade de que a diligência seja efetuada em documentos digitais remotamente armazenados. Nesse sentido:

> Tratando-se de busca e apreensão, conforme analisado, os requisitos legais devem ser rigorosamente observados, já que configura hipótese de limitação ao exercício do direito fundamental à intimidade e privacidade. Nessa linha, cabe aos juízes, quando decidirem pela ordem de busca e apreensão, detalhar, de modo específico, o objeto da ordem, incluindo expressamente no mandado, se for o caso, a possibilidade de se obterem dados por meio de acesso remoto a servidor localizado fora do endereço de cumprimento do mandado, com as indicações devidas (COSTA; LEONARDI, 2011).
>
> Tendo em vista que a medida de busca e apreensão visa justamente apreender documentos e coisas que possam auxiliar a elucidar os delitos, a ordem de busca deve incluir todo equipamento que possa conter informações digitalizadas e/ou acesso à Internet, como *tablets, videogames*, celulares, bem como equipamentos de armazenamento de mídia, como CDs, DVDs, *pen drives,* cartões de memória, etc. [...]
>
> A dúvida surge quanto a arquivos armazenados "nas nuvens", isto é, em servidores remotos, instalados em local diverso de onde está o equipamento a ser apreendido.
>
> Normalmente, para acessar esses arquivos, é necessário fornecer uma senha e, caso esse acesso a arquivos remotos não esteja especificado na ordem de busca, mesmo que a senha seja do conhecimento dos agentes cumpridores da ordem, não é recomendado acessar os arquivos remotos, sob pena de estar havendo excesso no cumprimento da ordem de busca e apreensão (DOMINGOS, 2015).

Constando do mandado a possibilidade de busca em conteúdo armazenado remotamente, e se o acesso é protegido por senha, nada impede a diligência, se esta puder ser obtida mediante busca nos arquivos localmente armazenados, ou mesmo mediante quebra por meio de programas específicos.

Também é esse o entendimento a que chegaram os magistrados federais participantes do curso mencionado na introdução deste trabalho, indicado no Enunciado 4:

> Enunciado 4 – Busca e apreensão: conteúdo armazenado remotamente
>
> Recomenda-se que, no mandado de busca e apreensão de equipamentos de informática, conste expressa autorização para que seja vasculhado conteúdo remotamente armazenado, se localizados meios de acesso. [...]

8 Conclusão

A evolução tecnológica no campo da documentação digital e seu armazenamento criam às novas realidades inúmeras dificuldades no âmbito do Processo Penal, decorrentes da inadequação dos antigos conceitos, entre os quais os de domicílio e documento.

A busca e apreensão é cabível tanto nos crimes que tenham por objeto os sistemas informatizados, quanto naqueles em que tais sistemas são empregados apenas como meio de execução.

Cabe à autoridade judiciária, ao analisar um requerimento de busca e apreensão, proceder a um exame rigoroso da presença dos requisitos para o seu deferimento (em especial, razoabilidade, justa causa e suporte indiciário mínimo), uma vez que estará afastando – ainda que para isso autorizado, no caso concreto – a garantia da inviolabilidade do domicílio, da intimidade e da privacidade.

A expedição do mandado de busca e apreensão de equipamentos de informática e dispositivos de armazenamento digitais implica ordem para acesso ao conteúdo de tais dispositivos.

Para que a diligência de busca e apreensão em mídias digitais cumpra a sua finalidade, deve ser acompanhada por um técnico especializado em sistemas informatizados, cuja participação limita-se a auxílio na busca. As técnicas e procedimentos empregados não constituem o exame de corpo de delito previsto no art. 158 do CPP, que deverá ser feito posteriormente.

É recomendável que, no mandado de busca e apreensão, conste expressamente a possibilidade de apreensão de documentos digitais mediante simples cópia, sem a apreensão do suporte físico, quando as circunstâncias indicarem essa necessidade.

Para que a diligência de busca e apreensão seja validamente efetuada em documentos digitais remotamente armazenados, é necessário que no mandado conste expressamente tal possibilidade.

Referências bibliográficas

BESSA, Leonardo Roscoe. *Direito à autodeterminação informativa*. Florianópolis, 2002. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/anexos/24306-24308-1-PB.htm> e <http://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2002;1000640785>. Acesso em: 5 mar. 2017.

BRASIL. Ministério Público Federal. 2.ª Câmara de Coordenação e Revisão. *Roteiro de atuação sobre crimes cibernéticos*. Brasília, 2013. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf>. Acesso em: 6 mar. 2017.

COSTA, Helena Regina Lobo da; LEONARDI, Marcel. Busca e apreensão e acesso remoto a dados em servidores. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 88, p. 203-223, 2011.

DOMINGOS, Fernanda Teixeira Souza. As provas digitais nos delitos de pornografia infantil na Internet. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). *A prova no enfrentamento à macrocriminalidade*. Salvador: *Jus*Podivm, 2015. cap. 6.

ESTADOS UNIDOS DA AMÉRICA. *US Constitution. Amendment IV*. Disponível em: <https://www.law.cornell.edu/constitution/fourth_amendment>. Acesso em: 5 mar. 2017.

GOMES, Rodrigo Carneiro. A execução da busca e apreensão, capacidade de representação do Delegado de Polícia, etiquetamento e o controle judicial: atualidades. *Revista dos Tribunais*, São Paulo, v. 964, p. 297-312, fev. 2016.

MISSAGGIA, Clademir. Da busca e da apreensão no Processo Penal brasileiro. *Revista do Ministério Público*, Porto Alegre, n. 48, p. 200-246, jul.-set. 2002.

A quantidade de material armazenado como causa de diminuição de pena no crime do art. 241-B da Lei n.º 8.069/90

Barbara de Lima Iseppi*

RESUMO

Este artigo tem como escopo analisar decisões proferidas por magistrados federais e Tribunais Regionais Federais entre os anos de 2015 e 2016, para verificar quais critérios são utilizados na dosimetria da pena por condenações pelo crime previsto no art. 241-B do Estatuto da Criança e do Adolescente, tal seja, adquirir, possuir ou armazenar arquivos com cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Isso porque o § 1º do referido dispositivo legal prevê causa expressa de diminuição de pena nos casos de "pequena quantidade" de material armazenado, com diversas repercussões práticas decorrentes da diminuição, a exemplo da possibilidade de oferecimento da suspensão condicional do processo ao réu e da dificuldade enfrentada pela perícia para a contagem individual dos arquivos, fato que dificulta e retarda a elaboração dos laudos periciais.

Palavras-chave: Pornografia infantojuvenil. Armazenamento. Decisão judicial. Dosimetria.

ABSTRACT

This article intends to analyze decisions issued by Brazilian federal judges and Federal Courts in 2015 and 2016 verifying which criteria are used to sentence defendants convicted for the crime established in

* Especialista em Direito Público pela Università della Calabria, Itália. Juíza Federal Substituta da 4ª Vara Criminal da Justiça Federal de São Paulo/SP. *E-mail*: biseppi@jfsp.jus.br.

article 241-B of the Children and Adolescents' Statute, which is, to acquire, possess and store files with pedophilia contents, since the first paragraph of the law determines a reduction of the sentence when the amount of files found with the defendant is "small". The judge must verify what is considered as a small amount, since the sentence reduction implies some practical issues, such as benefits granted to the offender like probation. Besides, forensic experts may face difficulties to specify the number of files, which hinders and delays the forensic reports required by the Court.

***Keywords**: Child and juvenile pornography. Storage. Court decision. Sentence criteria.*

1 Introdução

A aquisição, posse e armazenamento de material com conteúdo pornográfico infantil passaram a ser criminalizados a partir da Lei n.º 11.829/08, diploma que visou combater de forma mais severa a produção, venda e distribuição de pornografia infantil.

Publicada no *Diário Oficial* de 26 de novembro de 2008, a Lei n.º 11.829 alterou a redação dos já existentes arts. 240 e 241 do Estatuto da Criança e do Adolescente, acrescentando tipos penais nos arts. 241-A, 241-B, 241-C e 241-D. O legislador estabeleceu, ainda, o conceito de pornografia e cena de sexo explícito no art. 241-E do ECA, eliminando interpretações acerca do tema até então existentes.

A partir da nova redação, os chamados crimes de pedofilia (dispostos nos arts. 240 e 241) do Estatuto da Criança e do Adolescente passaram a possuir penas significativamente maiores, enquanto os arts. 241- A, 241-B, 241-C e 241-D visaram coibir práticas de pornografia na rede mundial de computadores, a Internet, assim como a divulgação de conteúdos e o chamado comércio virtual sexual alimentado por tal prática.

A lei foi promulgada a partir de projeto proposto pela Comissão Parlamentar de Inquérito, denominada "CPI da Pedofilia", instaurada com base no Requerimento n.º 200, de 2008, do Senado Federal, efetivado após a deflagração da *Operação Carrossel* da Polícia Federal.

Referida operação, ocorrida no ano de 2005, consistiu na primeira ação de grande porte no país com objetivo de reprimir a prática da pedofilia na rede mundial de computadores, tendo abarcado 14 (catorze) estados da Federação e o Distrito Federal, tornando-se o objeto da Comissão, segundo seu Relatório Final, para melhorar as condições de investigação por parte dos órgãos estatais, além de sistematizar dados relativos a crimes cometidos

pela Internet, o que também facilitaria a prevenção e punição dos delitos.

A análise das discussões mantidas pelo Poder Legislativo durante a elaboração do projeto, o qual contou inclusive com participação da sociedade civil, pois foram realizadas audiências públicas internas no âmbito do Senado, audiências públicas externas, eventos internacionais, além da campanha popular "Todos contra a Pedofilia" (SENADO FEDERAL, 2010, p. 1 589-1 657), permite concluir que a alteração legislativa se baseou em dois pilares.

O primeiro pretendeu conferir efetividade à norma do art. 227 da Constituição da República, segundo a qual toda criança e adolescente devem viver em ambiente saudável, livre de qualquer exploração, assegurado pelo Estado o desenvolvimento educacional infantojuvenil. O segundo foi o de "acompanhar os passos da modernidade e da tecnologia, cada vez mais disseminada entre os jovens", aprimorando a legislação brasileira acerca dos crimes de informática, tida à época como "incipiente, imatura e amplamente não consensual" (SENADO FEDERAL, 2010, p. 83).

Nesse ponto, de acordo com estudo internacional elaborado em 2006, que contou com a participação de 46 (quarenta e seis) países e diversas instituições, como a Interpol, Embaixadas e Representações Diplomáticas, a repressão à pedofilia através da Internet dependeria de *5 (cinco) requisitos legislativos básicos*, sendo que, até 2008, o Brasil só atendia a dois desses:

1) possuir lei que criminaliza a distribuição da pornografia infantil; e

2) prever, em lei, o uso do computador para a distribuição desses conteúdos.

Os outros três requisitos seriam:

3) a criminalização da posse de pornografia infantil;

4) a existência de um conceito jurídico de pornografia infantil; e

5) a existência de lei que regulamente a atividade dos provedores de acesso e de serviços à Internet (SENADO FEDERAL, 2010, p. 126).

A criminalização da posse e armazenamento de material pornográfico seria relevante a fim de, primeiramente, punir o consumidor do material pornográfico infantojuvenil, o qual fomenta o comércio ilícito deste (DAMÁSIO apud BALTAZAR JUNIOR, 2016).

Conforme justificou a Comissão Parlamentar de Inquérito n.º 2/2005, a Lei n.º 11.829/08 visou punir todas as etapas da pedofilia como produto de consumo. Com o art. 241-B, criminalizou a compra, a posse e o armazenamento de material pedófilo, fechando o ciclo desde a produção, passando pela venda, divulgação, até a aquisição e posse.

Além disso, citou-se a dificuldade obtida pela Polícia Federal, até então, em realizar prisões em flagrante durante as operações, as quais consistiam em verdadeiras diligências de busca e apreensão, considerando que a constatação de divulgação e compartilhamento de conteúdo pornográfico depende de prova pericial. Assim:

> O ônus da prova para a efetivação de prisões recai sobre a polícia, o que teria se verificado nas Operações *Carrossel* (2005) e *Azahar* (2006). As mídias e computadores têm de ser periciados e caberá à perícia o ônus de provar que aquele conteúdo foi repassado, que aquele conteúdo foi distribuído, de alguma forma.

Referida dificuldade prática foi debatida, durante os trabalhos da Comissão Parlamentar de Inquérito, tanto pela própria Polícia Federal quanto por representantes da sociedade civil (SENADO FEDERAL, 2010, p. 126 e 146).

Assim, quando da elaboração do projeto que culminou na Lei n.º 11.829/08, considerou-se primordial punir a simples posse do material pedófilo.

Especificamente no que diz respeito à causa de diminuição estabelecida no § 1º do art. 241-B, o escopo legislativo foi o de "*evitar excessos punitivos*", frase repetida em diversos trechos do Relatório Final da CPI da Pedofilia (SENADO FEDERAL, 2010, p. 207, 372 e 389).

Logo, é nítido constatar que, apesar de desejar punir toda a "*cadeia de consumo*" relacionada à pornografia infantojuvenil, no tocante ao criminoso que não divulga, produz ou alicia, mas "*apenas consome"* o material (adquire, armazena e possui), o legislador desde logo atribuiu tratamento mais ameno, com pena menor, de 1 (um) a 3 (três) anos de reclusão e multa, passível de suspensão condicional do processo, nos termos do art. 89 da Lei n.º 9.099/95.

Além disso, no próprio contexto do criminoso consumidor, o legislador distinguiu aquele que pratica as condutas com pequena quantidade de material, conferindo a este causa de diminuição de pena.

A aplicação de tal causa possui, além do benefício processual acima citado, outras implicações práticas, como a ausência de critérios objetivos a serem aferidos pelo magistrado no momento da dosimetria da pena. Exatamente por tal razão, mostra-se relevante o estudo ora formulado.

Destarte, traçado o contexto que ensejou a alteração legislativa para a inserção do tipo, analisar-se-á o crime do art. 241-B da Lei n.º 8.069/90 em seus pormenores, passando-se posteriormente à pesquisa acerca dos critérios utilizados pelos magistrados nos casos concretos.

Frise-se que não se fará análise crítica sobre a constitucionalidade do dispositivo em comento, pois a própria tipificação do crime de posse é questionada pela doutrina penalista, a qual alega violações aos princípios da ofensividade e presunção de inocência.

Em brevíssima síntese, aponta-se que a estrutura típica do referido crime se assemelha muito à punição de maus pensamentos,

porque a mera posse de material pornográfico não representaria nenhuma comissão, inexistindo injusto penal sem a prática de ação humana (LOBATO, 2013). Assim, mesmo que o indivíduo não tenha qualquer intuito de divulgar, trocar, publicar, comercializar o material obtido, a mera conduta de curiosidade ou interesse pela sexualidade perversa gerará o poder de punir ao Estado (SYDOW, 2009, p. 57).

Ainda afirma-se que a punição da posse ocorreria sob pretexto de evitar um mal maior potencialmente gerado, tendo o legislador pressuposto que imagens de natureza sexual com crianças ou adolescentes sirvam de estímulo para a continuidade de consumo e criação de tais materiais, assim como para o encorajamento de um passo seguinte, que seria a prática sexual abusiva propriamente dita. Na linha de pensamento de SYDOW (2009, p.57),

> pessoas que convivem (quiçá até sem conhecer tal preferência do colega) com a pedofilia ou a perversão sexual, não necessariamente tornam-se perversas. Não acreditamos que o Direito Penal seja instrumento apto para controle de pensamentos ou preferências, bem como não cremos que o direito de obter informações possa ser restringido.

Critica-se, ainda, o fato de se tratar de crime de perigo abstrato, com tendência à migração para a responsabilização objetiva do Direito Penal (SYDOW, 2009, p. 57).

Apesar de se tratar de discussão sedutora, este estudo apenas a mencionou para fins de esclarecimento, mas não se debruçará sobre o tema, partindo da presunção de constitucionalidade do crime previsto pelo art. 241-B do ECA para analisar objetivamente a causa de diminuição prevista em seu § 1º.

2 O crime do art. 241-B do Estatuto da Criança e do Adolescente

A prática do crime de publicação de imagens com conteúdo pornográfico envolvendo crianças ou adolescentes, através da rede

mundial de computadores, é, em regra, de competência da Justiça Federal.

Isso porque, nos termos do art. 109, inciso V, da Constituição da República, trata-se de fato previsto como crime em Tratado Internacional, tal seja a Convenção sobre os Direitos da Criança da Assembleia Geral das Nações Unidas, ratificada pelo Brasil em 24 de setembro de 1990 e internalizada em nosso ordenamento jurídico pelo Decreto n.º 99.710, de 21 de novembro de 1990.

De acordo com o art. 34 da referida Convenção, os Estados-partes tomarão todas as medidas de caráter nacional, bilateral e multilateral a impedir:

a) o incentivo ou a coação para que uma criança se dedique a qualquer atividade sexual ilegal;

b) a exploração da criança na prostituição ou outras práticas sexuais ilegais; e

c) a exploração da criança em espetáculos ou material pornográfico.

Ademais, por meio do Decreto n.º 5.007/2004, de 8 de março de 2004, o Brasil também aderiu ao Protocolo Facultativo da citada Convenção, adotado em Nova York em 25 de maio de 2000, o qual dispõe especificamente sobre a venda de crianças, prostituição infantil e pornografia infantil.

Assim, sendo signatário de compromisso internacional de combate ao delito, havendo ainda relação de internacionalidade entre a conduta criminosa praticada e o resultado produzido (ou que deveria ter sido produzido), no caso da rede mundial de computadores, a divulgação, o compartilhamento e a publicação de material pornográfico infantojuvenil estão entre os crimes de maior interesse da Justiça Federal. Trata-se de crimes cibernéticos, competência esta firmada pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário n.º 628624, de 28 de outubro de 2015.

Já em relação à posse, aquisição e armazenamento, condutas previstas no art. 241-B da Lei n.º 8.069/90, a competência é também da Justiça Federal na grande maioria dos casos. Isso porque o usuário que adquire material pornográfico infantojuvenil normalmente o faz através da rede mundial de computadores, por meio de diversos aplicativos e programas que possibilitam a visualização, *download* e transmissão de arquivos. Além de adquirir, tal usuário costuma possuir e armazenar o material em dispositivos eletrônicos, tanto de *hardware*, como em espaços na própria rede de Internet.

Ora, se a aquisição/posse/armazenamento adveio da rede mundial de computadores, está presente a transnacionalidade necessária à fixação da competência da Justiça Federal. Exatamente por tal motivo, o crime do art. 241-B é *geralmente* conexo ao crime previsto no art. 241-A, relativo à divulgação, por qualquer meio, de material contendo cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, pois o compartilhamento pressupõe a existência do arquivo em poder do réu.

A questão de haver, ou não, concurso entre os dois crimes deve ser verificada pelo magistrado em cada caso concreto, com base na prova pericial obtida, pois muitas vezes o usuário apenas compartilha ou divulga o material pornográfico sem armazená-lo ou mantê-lo, assim como em inúmeros casos há comprovação de armazenamento sem provas concretas sobre o compartilhamento. Insta asseverar, nesse ponto, prevalecer na jurisprudência o entendimento acerca do concurso de crimes, não de absorção do armazenamento (art. 241-B) pelo compartilhamento (art. 241-A). Precedente: TRF3, Apelação Criminal n.º 00051290620-10.403.6114 (BALTAZAR JUNIOR, 2016, p. 792).

Ademais, se o material for adquirido de outro modo que não através da Internet, mas armazenado em local passível de acesso via *web*, também haverá competência da Justiça Federal, conforme bem se ressaltou no julgamento do Recurso em Sentido Estrito n.º

00293811020134013500, julgado pelo TRF da 1ª Região em 13 de fevereiro de 2015:

> PENAL E PROCESSUAL PENAL. PORNOGRAFIA INFANTIL. ART. 241-A, LEI 8.069/90. DIVULGAÇÃO DE IMAGEM PELA REDE MUNDIAL DE COMPUTADORES. COMPETÊNCIA DA JUSTIÇA FEDERAL. RECURSO PROVIDO. [...] 3. A mera possibilidade de acesso transnacional à imagem contendo material pornográfico infantil, disponibilizado no SKYDRIVE (serviço *on-line* de armazenamento de arquivos disponibilizado pela Microsoft aos assinantes do *hotmail*), na rede mundial de computadores, caracteriza a competência da Justiça Federal, conforme previsão do art. 109, inciso V, da Constituição Federal. (Precedente: RSE n.º 0004578-55.2011.4.01.0000/GO, Terceira Turma, Rel.ª Des.ª Fed. Assusete Magalhães, e-DJF1 8 abr. 2011, p. 186.) 4. Recurso em Sentido Estrito Provido (Terceira Turma, Rel. Des. Fed. Mário César Ribeiro, e-DJF1 13 fev. 2015, p. 1 862.)

Em relação ao crime propriamente dito, trata-se de crime comum, formal e de forma livre, ou seja, as condutas podem ser praticadas por qualquer meio, conforme dispõe o próprio tipo. Isso significa dizer que a aquisição pode se dar a título gratuito ou oneroso, a posse pode ser precária, clandestina ou violenta e o armazenamento pode ser em meio físico ou eletrônico. O crime é, ainda, permanente nas modalidades possuir e armazenar, sendo instantâneo, de efeitos permanentes, na modalidade adquirir (BALTAZAR JUNIOR, 2016).

O sujeito ativo pode ser qualquer pessoa e o sujeito passivo é a criança ou adolescente, sendo o elemento subjetivo o dolo. Não há tipo específico nem forma culposa (NUCCI, 2014, p. 103).

A pena prevista é de 1 (um) a 4 (quatro) anos de reclusão e multa, ou seja, é cabível a suspensão condicional do processo. O Ministério Público Federal ainda baseia-se na quantidade de material encontrado, para visualizar a possibilidade, ou não, de oferecimento da suspensão, pois reputa que a quantidade reflete as circunstâncias do crime, conduta social e personalidade do agente (MPF, 2016, p. 290).

3. Da causa de diminuição prevista pelo parágrafo único do art. 241-B da Lei n.º 8.069/90

Conforme já mencionado por diversas vezes neste artigo, o Estatuto da Criança e do Adolescente previu causa de diminuição de pena de 1 (um) a 2/3 (dois terços), se de pequena quantidade o material pornográfico infantojuvenil adquirido, possuído ou armazenado, inexistindo definição ou parâmetros legais para o conceito de "pequena quantidade".

Conforme bem observado por SYDOW (2009, p. 55), além da dúvida acerca da expressão "pequena", porquanto frente à Internet qualquer quantidade é pequena, o § 1º do art. 241-B traz problema em sua própria redação, ao mencionar redução de pena de 1 (um) até 2/3 (dois terços):

> Resta dúvida interpretativa quanto à expressão *retro*: quis o legislador dizer que a redução pode ser do intervalo entre 1 (um) inteiro – totalidade da pena – e 2/3 (dois terços), como se atém gramaticalmente, ou a redução seria de 1/3 (um terço) até 2/3 (dois terços) sob pena de gerar impunidade ao usuário? No caso da segunda linha interpretativa, por que não seguiu o legislador a tendência do Código Penal, escrevendo por extenso, como, por exemplo, nos casos do art. 157, § 2º? [Grifo nosso]

Com a devida vênia ao entendimento acima, não nos parece que o legislador visou isentar o réu de pena, prevendo a diminuição na fração de 1 (um inteiro), ou seja, permitindo a exclusão da pena em sua totalidade, tratando-se de verdadeira falha de redação.

Isso porque, observada a maioria dos dispositivos legais, as frações são sempre dispostas em intervalos crescentes, ou seja, da menor para a maior, como nos arts. 14, parágrafo único, 16 e 26, parágrafo único, todos do Código Penal. Logo, não haveria lógica em escrever a fração em ordem decrescente apenas no art. 241-B do ECA. Aliás, coincidentemente, ou não, nos três dispositivos do Código Penal ora citados, as frações estão escritas tal como na Lei

n.º 8.069/90, de 1 (um) a 2/3 (dois terços), inexistindo discussão doutrinária ou jurisprudencial sobre tratar-se de um inteiro.

Dessa forma, considerando a lógica de disposição das frações em ordem crescente, o intervalo de diminuição previsto deve ser lido como de 1/3 (um terço) a 2/3 (dois terços).

Sobre o conceito de pequena quantidade, a doutrina brasileira é escassa.

NUCCI (2014, p. 104) afirma que a medida da redução deva se dar no cenário da *qualidade* do material apreendido, reputando essencial à censura da conduta criminosa o conteúdo do material pornográfico. Assim afirma o autor:

> Pensamos que devam existir três faixas: a) ínfima quantidade (uma foto de conteúdo levemente obsceno, por exemplo), capaz de configurar o crime de bagatela, tornando o fato atípico; b) pequena quantidade (algumas fotos ou um vídeo, que é a composição sequencial de várias fotos), apta a gerar a diminuição de um a dois terços; c) grande quantidade (várias fotos ou inúmeros vídeos, ou mesmo um vídeo muito extenso), que fomenta a aplicação da pena nos parâmetros normais (de um a quatro anos de reclusão).

O conteúdo do material, segundo o doutrinador, deve ser ponderado pelo juiz no momento de fixar o *quantum* da diminuição: em "situações grotescas" a apreensão de algum material permite a diminuição da pena no mínimo possível, enquanto em casos de "situações obscenas indiretas, mais sutis, sugestivas de sexo sem explicitação", pode-se operar a diminuição em patamar máximo (2014, p. 104).

Finaliza NUCCI declarando que "*outros percentuais devem ser aplicados, conforme o prudente critério do magistrado no caso concreto*" (2014, p. 104). [Grifo nosso]

No mesmo sentido ROSSATO; LÉPORE; CUNHA (2015, p. 562) defendem a análise qualitativa do material armazenado.

Os autores afirmam que

> como critério para a diminuição *poderá o juiz utilizar tanto a efetiva quantidade* de imagens, vídeos ou registros *quanto o conteúdo por eles revelado*. Se, por exemplo, forem duas ou três imagens que apenas insinuam a prática de algum ato sexual, a diminuição pode se dar no máximo, o que não se revela possível se a exibição for de sexo explícito. A benesse parece incompatível com a aplicação do princípio da insignificância. [Grifos nossos]

Com a devida vênia ao exposto pelos ilustres juristas, considerar o caráter qualitativo do material possuído/adquirido/armazenado para fins de aplicação da causa de diminuição do art. 241-B, § 1º, do ECA não nos parece plausível.

Em primeiro lugar, porque a lei é expressa ao prever a diminuição da pena apenas em razão da pequena *quantidade* do material encontrado, sendo que o *caput* do artigo se refere a "cena de sexo explícito ou pornográfica envolvendo criança ou adolescente".

Exatamente com o fim de evitar discussões a respeito, a própria Lei n.º 11.829/08 trouxe o conceito de "cena de sexo explícito ou pornográfica envolvendo criança ou adolescente", descrito no artigo 241-E, *verbis*:

> Art. 241-E. Para efeito dos crimes previstos nesta lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

Nota-se, assim, ter a própria lei falado em *cenas explícitas e exibição de órgãos genitais.*

O dispositivo é, inclusive, criticado pela doutrina, pois não abarcou as atividades sexuais implícitas e poses sensuais, sem a expressa mostra dos órgãos genitais, que constituem situações igualmente inadequadas (NUCCI, 2009, p. 110).

Mesmo tendo havido possível falha do legislador, o fato de o texto do art. 241-B, § 1º, falar apenas em quantidade não nos

parece permitir margem de análise de conteúdo para verificar se a cena pornográfica é explícita ou insinuada, sob pena de violação ao princípio da taxatividade.

É claro que o conteúdo do material adquirido, armazenado ou possuído certamente influencia a reprovabilidade da conduta, podendo e devendo ser analisado pelo juiz, mas em outra fase da dosimetria da pena, durante a verificação das circunstâncias judiciais.

Ora, a culpabilidade ou até mesmo as circunstâncias do crime comportam tal valoração.

Conforme é cediço, a culpabilidade está ligada à intensidade do dolo ou grau de culpa do agente, tendo em vista a existência de um *plus* de censurabilidade e reprovação social da conduta praticada, que poderia ser evitada. A frieza do agente e a premeditação, por exemplo, são características a serem examinadas nessa oportunidade. Já as circunstâncias do crime são elementos ou dados tidos como acessórios, ou acidentais, que cercam a ação delituosa e, embora não integrem ou componham a definição legal do tipo, exercem influência sobre a gradação da pena, pois promovem mudança qualitativa e quantitativa na reprovabilidade da conduta. As circunstâncias referidas no art. 59 não se confundem com aquelas relacionadas no texto legal (arts. 61, 62, 65 e 66 do CP), mas defluem do próprio fato delituoso, podendo-se mencionar: "forma e natureza da ação delituosa, os tipos de meios utilizados, objeto, tempo, lugar, forma de execução e outras semelhantes" (BITENCOURT, 2003, p. 554).

Destarte, entendemos que a melhor interpretação, por não ferir o princípio da taxatividade e seguir estritamente o parâmetro estabelecido pela lei, deve considerar os aspectos qualitativos do material encontrado durante a análise das circunstâncias judiciais, na primeira fase da dosimetria da pena. Deve ainda levar em conta unicamente a quantidade dos arquivos armazenados para fins da causa de diminuição.

No Direito Comparado é possível encontrar poucas referências sobre o tema.

O inciso II do art. 600 *quater* do Código Penal Italiano possui redação quase idêntica ao art. 241-B do ECA, punindo com reclusão de 1 (um) a 3 (três) anos e multa não inferior a € 1 549 (um mil, quinhentos e quarenta e nove euros) aquele que detém material pedopornográfico (expressão utilizada pela doutrina italiana, a exemplo de CASELLA, 2015).

Referido dispositivo legal estabelece causa de aumento de pena, em porção não excedente a 2/3 (dois terços), se o material for de "*ingente quantità*" (art. 600 *quater*, *comma* II, do citado Código), expressão que poderia ser traduzida como "quantidade significativa".

A causa de aumento incide, ainda, em todos os crimes relacionados à divulgação, publicação, cessão e distribuição de pornografia envolvendo crianças e adolescentes, por qualquer meio, inclusive o telemático, conforme art. 600 *ter* do Código Penal Italiano.

A interpretação da expressão "quantidade significativa" para fins de aumento de pena é pouco discutida pela jurisprudência italiana.

A *Corte Suprema di Cassazione della Repubblica Italiana* julgou a questão pela primeira vez em maio de 2011, afirmando que, até então, "a jurisprudência não havia tido oportunidade de se ocupar da referida expressão de modo explícito" (ZAMA, 2011).

Na Sentenza 3 maggio 2011, n. 17311 (Sezione Terza Penale), a citada Corte confirmou a decisão do Tribunal de Apelação de Bolonha, que, por sua vez, havia em grau de recurso ratificado a incidência da causa de aumento no caso de um réu que armazenava 175 (cento e setenta e cinco) DVDs contendo imagens de arquivos de pornografia infantojuvenil.

Como fundamentação da decisão, a Corte primeiramente considerou correto o critério utilizado pelo Tribunal para fins de aferição da grande quantidade: *um número médio considerando-se a prática judiciária envolvendo episódios do mesmo gênero*[1] [tradução livre desta Autora, grifo nosso].

Além disso, afirmou que a grande quantidade está diretamente relacionada à potencialidade lesiva da conduta diante da lógica de mercado baseada na oferta-demanda, sendo nítida a intenção do legislador em diferenciar quem detém "*algumas*" imagens em detrimento daquele que disponha de um quantitativo definível como " '*muito grande, relevante, consistente', sinônimos literais do adjetivo ingente na língua italiana*"[2] [tradução livre desta Autora, grifos originais].

Assim, a Corte entendeu por bem estabelecer como parâmetros interpretativos, sem "pretensão de considerá-los gaiolas numericamente preeestabelecidas" [tradução livre desta Autora][3], o número de 10 (dez) imagens para a não incidência da causa de aumento, assim como o número de 100 (cem) imagens para o aumento da pena.

O entendimento da Corte Suprema Italiana foi mantido em ano posterior ao precedente inicial acima citado, na Sezione

[1] *Con riferimento al caso di specie: "*è *sicuramente molto corretto il percorso argomentativo dei Giudici del Riesame quando affermano che, in relazione alla specificità della fattispecie sub iudice, la nozione di ingente quantità implica 'la presenza di un quantitativo di immagini tali da discostarsi, in termini davvero significativi da una condizione di detenzione di un numero contenuto di immagini illecite quale si riscontra nella pratica giudiziaria relativa ad episodi illeciti di tal genere' ".*

[2] *Proseguendo la riflessione, deve, comunque, considerarsi (alla luce della struttura della norma di cui all'art. 600 quater c.p.) che evidentemente il legislatore, nel disciplinare l'ipotesi di chi si procura o detiene materiale pedo-pornografico ha inteso differenziare le pene per chi abbia solo "alcune" immagini rispetto a chi disponga di un quantitativo di esse tale da potersi definire "molto grande, rilevante, consistente" (casi come argomentabile dallo stesso significato letterale annesso, nel dizionario della lingua italiana, all'aggettivo "ingente").*

[3] *Parametri che - senza avere la pretesa di contenere numericamente entro "gabbie" precostituite i concetti da definire - ne delimitino, tuttavia i "confini".*

Terza Penale, Sentenza 19 luglio 2016 (dep. 28 febbraio 2017), n. 9684, a qual confirmou o aumento de pena por "quantidade significativa" a um réu que mantinha "diversas centenas de arquivos" armazenados em um dispositivo HD externo e em um *notebook*.

Não há, na legislação penal codificada argentina, capítulo específico dedicado aos crimes cometidos contra crianças e adolescentes. Em geral, praticados delitos contra menores de 18 anos, a idade da vítima é considerada como circunstância agravante ou causa de aumento da pena.

Os arts. 120, 128 e 129 do Código Penal Argentino criminalizam condutas de produzir, financiar, oferecer, comerciar, publicar, divulgar ou distribuir, por qualquer meio, toda representação de menor de 18 anos dedicado a atividades sexuais explícitas ou toda representação de suas partes genitais com fins predominantemente sexuais, assim como aquele que organizar espetáculo ao vivo de representações sexuais explícitas de que participem ditos menores.

No entanto, não se considera ilícito penal a simples posse – sem finalidade comercial ou de distribuição – de material pornográfico.

Na Inglaterra, a pornografia infantil é tratada no capítulo 37 do *Protection of Children Act 1978* (Lei de Proteção às Crianças de 1978), com as emendas feitas pelo *Criminal Justice and Public Order Act 1994* (Lei sobre a Justiça Criminal de 1994) e pelo *Sexual Offences Act 2003* (Lei das Ofensas Sexuais de 2003).

Após 2003, passou a ser considerada criança para os fins de proteção qualquer pessoa menor de 18 anos, sendo puníveis as condutas de agenciar, facilitar, constranger ou submeter criança à prostituição ou à pornografia, fotografá-las e divulgar material fotográfico.

Nos termos da Seção 160 do *Criminal Justice and Public Order Act*, armazenar material pornográfico infantojuvenil é crime,

mas não há disposições específicas acerca de causas agravantes ou atenuantes.

Nos Estados Unidos da América vigora desde 2003 o *Protect Act*, o qual traz proibições à pornografia infantil virtual em sua seção 502: "Da Prevenção à Pornografia Infantil e à Obscenidade Infantil (*Child Obscenity and Pornography Prevention*)".

Tal lei foi sancionada pelo Congresso americano após o *Child Pornography Prevention Act* (Lei de Prevenção à Pornografia Infantil) de 1996, que visou aumentar a repressão à pornografia proibindo amplamente a produção e distribuição de material pornográfico infantil – inclusive simulado ou criado artificialmente –, entre outras medidas, incluído o armazenamento de material pornográfico.

A lei foi abolida em 2002 em razão do caso Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002), que apontou a excessividade de rigor no dispositivo legal, o qual se utilizava de termos muito amplos, vastos e de interpretação difícil (SYDOW, 2009, p. 55).

A pornografia infantil é tratada na Seção 184b do Código Penal Alemão. Nessa seção, é criminalizada a aquisição, distribuição e posse de pornografia infantil, compreendendo, apenas, as que representem crianças com menos de 14 anos. Quando o material retrata adolescente entre 14 e 18 anos, incorre-se no tipo da Seção 184c (pornografia juvenil), com penas mais brandas.

A pena é agravada se há intuito comercial, ou se atua como integrante de organização voltada para o cometimento desse crime, e se o material reproduz relação sexual verdadeira ou realística – prisão de 6 (seis) meses a 10 (dez) anos.

A pena é de prisão de não mais que 2 (dois) anos, ou multa, se se trata de mera posse de material.

As leis penais japonesa e francesa não tratam do crime de armazenamento (SENADO FEDERAL, 2010, p. 290-300).

Nota-se inexistir referência objetiva na legislação comparada, exceto à italiana, sendo que mesmo assim os limites numéricos para quantidade de material pornográfico infantojuvenil foram trazidos pela Suprema Corte, como sugestivos de interpretação.

Diante do quadro acima, nota-se inexistirem muitos parâmetros a auxiliarem o magistrado brasileiro a aferir o conceito de "pequena quantidade de material pornográfico infantojuvenil", exata razão pela qual se objetivou analisar, na prática, o que efetivamente está sendo utilizado pelos juízes e desembargadores no momento da prolação de decisões.

4 Da jurisprudência

Em pesquisa empírica realizada foram analisadas 8 (oito) sentenças condenatórias pelo crime do art. 241-B do ECA, proferidas por magistrados federais em primeira instância na cidade de São Paulo, entre os anos de 2014 e 2016.

Cada magistrado forneceu voluntariamente o material, o qual é passível de consulta pública no sítio eletrônico da Justiça Federal de São Paulo, pelos números dos processos[4].

Das 8 (oito) sentenças condenatórias, apenas 2 (duas) aplicaram a causa de diminuição prevista pelo art. 241-B, § 1º do ECA, tais sejam:

a) Processo n.º 0006125-60.2011.403.6181, da 4ª Vara Federal de São Paulo, cuja sentença foi prolatada em 23 de outubro de 2015, que considerou pequena a quantidade de um vídeo e 154 (cento e cinquenta e quatro) imagens, reduzindo a pena na fração mínima de um terço. Utilizou-se como fundamentos da diminuição: "a imensidão de imagens disponíveis na Internet, a quantidade média de imagens encontradas para os réus neste contexto espacial e social, ou seja, na cidade de São Paulo, neste Juízo (milhares), e a quantidade no caso concreto de 1 vídeo e 154 fotos".

[4] Disponível em: <https://www.jfsp.jus.br>. Acesso em: 4 mar. 2017.

b) Processo n.º 0005850-14.2011.403.6181, da 10ª Vara Federal de São Paulo, cuja sentença foi prolatada em 12 de março de 2014, a qual considerou pequena a quantidade de 2 (dois) vídeos e reduziu a pena na fração máxima de dois terços. Não foram explicitados os fundamentos adotados para a aplicação da referida fração.

A título de esclarecimento, cito os números de material armazenado analisados pelas sentenças que não aplicaram a causa de diminuição:

a) Processo n.º 0005499-41.2011.403.6181, da 4ª Vara Federal de São Paulo, sentença prolatada em 19 de janeiro de 2015: 510 (quinhentos e dez) arquivos de vídeos e 18 326 (dezoito mil, trezentos e vinte e seis) arquivos de imagens. A sentença valorou a quantidade negativamente na circunstância judicial da culpabilidade para aumentar a pena imposta.

b) Processo n.º 0004098-07.2011.403.6181, da 4ª Vara Federal de São Paulo, sentença prolatada em 29 de janeiro de 2015: 218 (duzentos e dezoito) arquivos de vídeos e 2 277 (dois mil, duzentos e setenta e sete) arquivos de imagens. A sentença valorou a quantidade negativamente na circunstância judicial da culpabilidade para aumentar a pena imposta.

c) Processo n.º 0003379-54.2013.403.6181, da 4ª Vara Federal de São Paulo, sentença prolatada em 3 de fevereiro de 2015: 309 000 (trezentos e nove mil) arquivos de imagens e 3 160 (três mil, cento e sessenta) arquivos de vídeos. A sentença valorou a quantidade negativamente na circunstância judicial da culpabilidade para aumentar a pena imposta.

d) Processo n.º 0003657-26.2011.403.6181, da 4ª Vara Federal de São Paulo, sentença prolatada em 22 de junho de 2015: 26 (vinte e seis) arquivos de vídeo ativos, que totalizavam cerca de 10 (dez) GB de dados. A sentença não valorou a quantidade para aumentar a pena imposta.

e) Processo n.º 0008150-12.2012.403.6181, da 4ª Vara Federal de São Paulo, sentença prolatada em 25 de abril de 2016: 1 251 (um mil, duzentos e cinquenta e um) arquivos ou 88 GB de espaço armazenados nas mídias, além de 115 (cento e quinze) arquivos ou 15,25 GB de espaço armazenados no disco rígido. A sentença valorou a quantidade negativamente na circunstância judicial da culpabilidade para aumentar a pena imposta.

f) Processo n.º 0006013-57.2012.403.6181, da 4ª Vara Federal de São Paulo, sentença prolatada em 28 de outubro de 2016: 6 238 (seis mil, duzentos e trinta e oito) arquivos de imagens e 769 (setecentos e sessenta e nove) arquivos de vídeos. A sentença valorou a quantidade negativamente na circunstância judicial da culpabilidade para aumentar a pena imposta.

Observa-se que os números médios encontrados nos casos julgados pela 4ª Vara Criminal de São Paulo, entre 2015 e 2016, são de 799 (setecentos e noventa e nove) arquivos de vídeos e de 67 418 (sessenta e sete mil, quatrocentos e dezoito) arquivos de imagens.

Considerando tal dado, há coerência no julgamento proferido nos Autos n.º 0006125-60.2011.403.6181, o único que aplicou a causa de diminuição do art. 241-B, § 1º, por considerar "pequena" a quantidade de 1 (um) vídeo e 154 (cento e cinquenta e quatro) imagens.

Foram analisadas, também, todas as decisões proferidas pelos Tribunais Regionais Federais disponíveis na Internet, entre os anos de 2014 e 2016, a respeito do crime do art. 241-B e a causa de diminuição do § 1º, tendo sido encontrados 7 (sete) acórdãos[5].

No julgamento da Apelação Criminal n.º 0006125-60.2011.403.6181/SP, proferido pela 11ª Turma (e-DJF3 Judicial 1 2 ago. 2016), o Tribunal Regional Federal da 3.ª Região reformou a sentença proferida em primeiro grau para afastar completamente a causa de diminuição anteriormente aplicada pela 4.ª Vara Criminal

[5] Pesquisa unificada de jurisprudência disponível no sítio eletrônico do Conselho da Justiça Federal: <http://www.cjf.jus.br>. Acesso em: 4 mar. 2017.

Federal no caso anteriormente citado neste artigo (Processo n.º 0006125-60.2011.403.6181), que havia considerado pequena a quantidade de *1 (um) vídeo e 154 (cento e cinquenta e quatro) imagens* armazenadas, contendo cenas de sexo explícito ou pornografia envolvendo crianças e adolescentes.

Em sua fundamentação, o acórdão assim consignou:

> Na terceira fase da dosimetria, o magistrado sentenciante aplicou a causa de diminuição prevista no § 1º, do art. 241-B da Lei n.º 8.069/90, porque considerou pequena a quantidade de material apreendido. Irresignado, o Ministério Público Federal pede seja afastada referida causa de diminuição, com razão. Tenho que 1 (um) vídeo e mais de uma centena de imagens armazenadas (mais especificamente 154), contendo cenas de sexo explícito ou pornografia envolvendo crianças e adolescentes, não pode ser considerado de pequena monta, para fins de aplicação da referida causa de diminuição. Por tais razões, afasto a aplicação da referida causa de diminuição, fixando a pena definitiva em 1 (um) ano de reclusão e 10 (dez) dias-multa, no valor de 1/30 (um trigésimo) do salário mínimo vigente na data dos fatos.

Já no julgamento da Apelação Criminal n.º 0005359-96.2011.403.6119, proferido pela 11ª Turma (e-DJF3 Judicial 1 1 set. 2016), o Tribunal Regional Federal da 3.ª Região também reformou a sentença proferida em primeiro grau para afastar completamente a causa de diminuição anteriormente aplicada, a qual havia se baseado no dado constante da perícia sobre haver nas mídias do réu *7 (sete) arquivos ativos de vídeo* com conteúdo pornográfico infantil.

O acórdão afirma que

> apesar de grande parte dos arquivos terem sido apagados pelo réu, "foram encontrados 7 (sete) arquivos diretamente acessíveis (arquivos ativos) contendo vídeos apresentando conteúdo desta natureza" (pornografia infantil) no material apreendido em poder do recorrente, de modo que, ainda que fosse o caso de se entender que o apagamento dos arquivos ensejaria o arrependimento eficaz, não seria essa a hipótese dos autos, ante a manutenção desses 7 (sete) arquivos […]. No particular, destaco que não se aplica, *in casu*, o art. 241-B, § 1º, do ECA, eis que a quantidade de arquivos apreendidos em poder do réu não é de ser reputada pequena, tendo em conta que, além dos 7

> (sete) arquivos encontrados em atividade, milhares foram recuperados, conforme exposto no tópico precedente […].

Segundo o acórdão, com referência ao Laudo Pericial, o número de arquivos recuperados (que haviam sido apagados pelo réu) era de 3 194 (três mil, cento e noventa e quatro) arquivos de imagens, além de 31 (trinta e um) vídeos.

O Tribunal Regional Federal da 3.ª Região igualmente afastou a causa de diminuição prevista no § 1º do art. 241-B do ECA, no julgamento da Apelação Criminal n.º 0004496-22.2009.403.6181, afirmando que, "embora tenha sido localizado e apreendido apenas um CD, a quantidade de material, 1 708 imagens, não pode ser considerada pequena e insignificante" (Primeira Turma, e-DJF3 Judicial 1 11 jul. 2013).

Note-se não haver parâmetro objetivo para a aferição da "pequena quantidade" de material armazenado, pois os três acórdãos trabalharam com os seguintes números, considerando-os grande quantidade:

a) 1 (um) vídeo e 154 (cento e cinquenta e quatro) imagens, todos ativos;

b) 7 (sete) vídeos ativos (disponíveis), mais 3 194 (três mil, cento e noventa e quatro) imagens e 31 (trinta e um) vídeos apagados pelo réu, recuperados pela perícia; e

c) 1 708 (um mil, setecentas e oito) imagens ativas.

No mesmo sentido foi proferido acórdão pelo Tribunal Regional Federal da 1.ª Região, o qual afastou a causa de diminuição por não considerar pequena a quantidade de *1 (um) vídeo e 141 (cento e quarenta e uma) fotos* (Apelação Criminal n.º 0001922-11.2010.401.3800, Terceira Turma, e-DJF1 6 jul. 2015).

Por sua vez, o Tribunal Regional Federal da 4ª Região, no julgamento da Apelação Criminal n.º 5068954-21.2011.4.04.7100/RS (fonte: <http://www.trf4.jus.br>, 9 ago. 2016), considerou inviável falar em redução da pena em razão

da previsão do § 1º do art. 241-B da Lei n.º 8.069/90, porquanto, "no caso dos autos, o réu armazenava pornografia infantojuvenil no HD de seu *computador, conforme demonstrou o Laudo Pericial n.º 146/2011– SETEC/SR/DPF/RS, havendo dezenas de fotografias e vídeos ilícitos no interior do disco rígido apreendido*".

O Tribunal Regional Federal da 5ª Região, no julgamento da Apelação Criminal n.º 12389/CE, Processo n.º 0011815-11.2013.405.8100, Quarta Turma, julg. 30 jun. 2015, DJe TRF5 2 jul. 2015, p. 166, considerou grande para afastar a causa de diminuição do art. 241-B, § 1º do ECA, a quantidade de *8 (oito) vídeos, 116 (cento e dezesseis) bancos de dados, 60 (sessenta) fotos, 22 (vinte e dois) metadados e 106 (cento e seis) imagens.*

Da mesma forma, o TRF5 considerou inviável a redução de *mais de 1 300 (um mil e trezentos) arquivos de imagens* encontrados no julgamento da Apelação Criminal n.º 10093/AL, Processo n.º 200980010001861, Terceira Turma, julg. 10 abr. 2014, DJe TRF5 15 abr. 2014, p. 269.

Não foram encontrados acórdãos proferidos pelos Tribunais Regionais Federais da 1ª e 2ª Região em consulta realizada no sítio eletrônico do Conselho da Justiça Federal.

Somados os números encontrados, tem-se que a quantidade média considerada expressiva pelos Tribunais, de modo a afastar a causa de diminuição, é de 578 (quinhentos e setenta e oito) arquivos de imagens, assim como 2 (dois) arquivos de vídeos[6].

[6] Não foram considerados para o cálculo médio os números citados pelos acórdãos n.º 5068954-21.2011.4.04.7100/RS do TRF da 4ª Região, o qual mencionava apenas a palavra "dezenas", sem especificar se se tratavam de vídeos ou imagens, assim como os números de 116 (cento e dezesseis) bancos de dados e 22 (vinte e dois) metadados mencionados pelo acórdão n.º 0011815-11.2013.405.8100 do TRF da 5ª Região, o qual igualmente não especificava os tipos de arquivos.

5 Conclusão

Após a pesquisa efetuada, conclui-se inexistir, seja na doutrina, seja na jurisprudência brasileira, conceitos ou parâmetros para a interpretação da expressão "pequena quantidade de material contendo cena de sexo explícito ou pornográfica envolvendo criança ou adolescente", prevista como causa de diminuição de pena pelo art. 241-B, § 1º, do Estatuto da Criança e do Adolescente.

A análise de 8 (oito) decisões proferidas em primeira instância e 7 (sete) julgamentos prolatados em segunda instância constatou que, na maioria das vezes, utiliza-se o parâmetro genericamente citado por NUCCI (2014, p. 104) do "*prudente critério do magistrado no caso concreto*" [grifo nosso] para apenas se afirmar "*não se tratar de quantidade pequena*".

Tal critério, no entanto, causa certa discrepância e ausência de uniformidade na jurisprudência, pois, ao mesmo tempo que os números médios encontrados nos casos julgados em primeira instância na cidade de São Paulo, entre os anos de 2015 e 2016, foram de 799 (setecentos e noventa e nove) arquivos de vídeos e de 67 418 (sessenta e sete mil, quatrocentos e dezoito) arquivos de imagens, os Tribunais Regionais Federais de todo o país, no mesmo período, afastaram a causa de diminuição em casos com quantidade expressivamente menores, cuja média foi de 578 (quinhentos e setenta e oito) arquivos de imagens e de 2 (dois) arquivos de vídeos.

Considerando que o crime ora tratado depende muito das circunstâncias sociais e culturais de cada local de consumação, sendo variável principalmente conforme a possibilidade e disponibilidade de acesso à Internet, assim como das características pessoais dos usuários (como o grau de instrução), é de extrema relevância a análise da jurisprudência local por parte dos magistrados, a fim de *conferir maior objetividade à interpretação do dispositivo legal*, cujo parâmetro interpretativo não deve ser unicamente o prudente arbítrio do juiz.

A referida causa de diminuição pode implicar diversos efeitos práticos para o réu, desde o oferecimento da suspensão condicional do processo pelo Ministério Público Federal até benefícios decorrentes da condenação, como o regime inicial fixado e a substituição da pena por restritiva de direitos, não podendo ser ignorada.

Ademais, deve-se ressaltar a indispensabilidade da *quantificação dos arquivos nos laudos periciais*, pois se trata de crime com vestígios, cuja prova do corpo de delito é imprescindível, nos termos do art. 158 do Código de Processo Penal. Ainda que atualmente a Perícia Federal tenha dificuldade em efetuar a contagem individualizada de cada arquivo armazenado/possuído/adquirido pelos investigados, em razão do número cada vez maior encontrado, deve ser fornecido ao Juízo algum parâmetro quantitativo, para fins de melhor individualização da pena nos casos concretos e, por consequência, maior efetivação da justiça, sempre considerando que o Direito Penal trata de um dos bens mais preciosos do ser humano: a liberdade.

Referências bibliográficas

BALTAZAR JUNIOR, José Paulo. *Crimes federais*. 10. ed. São Paulo: Saraiva, 2016.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal:* parte geral. 8. ed. São Paulo: Saraiva, 2003.

BRASIL. Ministério Público Federal. *Roteiro de atuação sobre crimes cibernéticos*. 3. ed. rev. e ampl. Brasília, 2016.

___. Senado Federal. *Relatório Final da Comissão Parlamentar de Inquérito n.º 200/08*. BRASÍLIA, 2010. Disponível em: <http://www.senado.gov.br/noticias/agencia/pdfs/RELATORIOFinalCPIPEDOFILIA.pdf>. Acesso em: 25 fev. 2017.

CASELLA, Marco. *Il reato di detenzione di materiale (pedo) pornografico alla luce delle moderne tecnologie*, 3 mar. 2015. Disponível em: <http://www.dirittiweb.it/2015/03/il-reato-di-detenzione-di-materiale-pedopornografico-alla-luce-delle-moderne-tecnologie/>. Acesso em: 1 mar. 2017.

LOBATO, José Danilo Tavares. Panorama dos crimes de posse. IBCCRIM – Instituto Brasileiro de Ciências Criminais. *Revista Liberdades*, São Paulo, n. 12, jan.-abr. 2013. Disponível em: <https://www.ibccrim.org.br/revista_liberdades_artigo/155-ARTIGO>. Acesso em: 1 mar. 2017.

NUCCI, Guilherme de Souza. *Leis Penais e Processuais Penais comentadas.* 8. ed. rev., ampl. e atual. São Paulo: Revista dos Tribunais, 2014. v. II.

ROSSATO, Luciano; LÉPORE, Paulo Eduardo; CUNHA, Rogério Sanches. *Estatuto da Criança e do Adolescente*: Lei n. 8069/90. Comentado artigo por artigo. 7. ed. São Paulo: Saraiva, 2015. p. 560-562.

SYDOW, Spencer Toth. Pedofilia virtual e considerações críticas sobre a Lei 11.829/08. IBCCRIM – Instituto Brasileiro de Ciências Criminais. *Revista Liberdades*, São Paulo, n. 1, maio-ago. 2009, p. 46-65.

ZAMA, Antônio. *Cassazione Penale: detenzione di materiale pedopornografico aggravata per ingente quantità*. Bologna, 24 maggio 2011. Disponível em: <http://www.filodiritto.com/articoli/2011/05/cassazione-penale-detenzione-di-materiale-pedopornografico-aggravata-per-ingente-quantita?page=1>. Acesso em: 1 mar 2017.

A Internet das Coisas e o fim do mundo

Sílvio Luís Martins de Oliveira*

RESUMO

Este artigo aborda alguns dos requisitos e desafios tecnológicos associados ao conceito de Internet das Coisas, bem como externa a preocupação de que a maior amplitude da conectividade acabe por transformar máquinas e dispositivos em ciberarmas.

Palavras-chave: Internet das Coisas. Invasão de sistemas. Armas digitais.

ABSTRACT

This article covers some requirements and technological challenges associated to the concept of Internet of Things, as well as express concerns that the greater amplitude of connectivity converts machines and devices into cyberweapons.

***Keywords**: Internet of Things. Systems invasion. Digital weapons.*

* Engenheiro mecânico pela Escola Politécnica da USP. Mestre em Direito Penal pela Faculdade de Direito da USP. Procurador da República. *E-mail*: silviooliveira@mpf.mp.br.

1 Introdução

Em 1983, quando a Internet ainda não havia expandido para além dos restritos meios acadêmico e militar, o ator Matthew Broderick interpretou um adolescente extremamente hábil com computadores e jogos eletrônicos que se divertia invadindo o servidor da escola para alterar suas notas.

Decidido a experimentar um jogo de guerra ainda não lançado por uma empresa do ramo, ele inadvertidamente invade o computador do *North American Aerospace Defense Command* (NORAD) e, acreditando estar participando de um jogo, quase inicia uma guerra nuclear.

Esse é o enredo do filme *WarGames*. Não coincidentemente, um ano depois, em 1984, o Congresso americano aprovou o *Computer Fraud and Abuse Act* (CFAA), conhecido como a lei *anti-hacking* americana. O CFAA consiste em uma legislação que inicialmente se destinava a regular e punir fraudes bancárias cometidas através da rede de computadores. Porém, ameaças terroristas reais ou imaginárias levaram-no a sofrer, ao longo dos anos, reiteradas e seguidas modificações, tornando-se um diploma. Sua abrangência e falta de clareza são criticadas pelos juristas americanos por darem margem ao cometimento de arbitrariedades por parte de investigadores, acusadores e juízes.

O CFAA bem poderia chamar-se "Matthew Broderick Act".

No Brasil, quase trinta anos depois, um episódio, dessa feita real, deu origem à Lei n.º 12.737/12, que ficou conhecida como Lei Carolina Dieckmann, sancionada após a caixa de *e-mails* da atriz ter sido invadida e dela subtraídas dezenas de fotos eróticas, que foram utilizadas para extorqui-la. Como a atriz não cedeu às ameaças, as fotos vieram a público na Internet.

Embora a exposição desautorizada das fotos de Carolina Dieckmann não possa ser comparada à hecatombe nuclear do

filme *Jogos de Guerra*, ambos os episódios ilustram o que já é há muito tempo sabido: a política legislativa é reativa e não proativa. Legisladores em qualquer parte do planeta são em geral desprovidos de visão que lhes permita regulamentar eventos futuros, agindo na maioria das vezes por interesse, provocação ou temor, e de maneira irracional, o que leva à produção de textos imprecisos e lacônicos e, consequentemente, injustos.

O que salva os legisladores americanos é que sua iniciativa ocorreu 28 anos antes da ação dos legisladores brasileiros, quando a Internet ainda era incipiente e começava a ser disponibilizada para a população paralelamente ao surgimento dos primeiros *personal computers* (PCs).

A Lei n.º 12.737/12 incluiu no capítulo "Dos crimes contra a inviolabilidade dos segredos", do Código Penal, o art. 154-A, que definiu o que o legislador denominou "delitos informáticos", tipificando a invasão de dispositivos informáticos para obter, adulterar ou destruir dados ou informações, ou instalar vulnerabilidades visando obter vantagem ilícita, como delito punível com detenção de 3 (três) meses a 1 (um) ano e multa. Uma causa de aumento estabelece que a pena será acrescida de 1/6 (um sexto) a 1/3 (um terço), se da invasão resultar prejuízo econômico.

Desconsiderada a causa de aumento, trata-se de delito de menor potencial ofensivo nos termos da Lei n.º 9.099/95 e, portanto, sujeito à transação penal.

Certamente, se tivessem tomado conhecimento dessa rigorosíssima sanção penal, os criadores do *Stuxnet* cairiam da cadeira à frente de seus computadores, de tanto rir.

Mas, o que é *Stuxnet*? A história é um pouco longa.

2 Stuxnet, uma ciberarma

Em junho de 2010, Sergey Ulasen, gerente da divisão antivírus da *VirusBlokAda*, uma pequena firma de segurança de

computadores sediada em Minsk, capital de Belarus, recebeu um telefonema de um de seus clientes. Ele representava uma empresa iraniana, cujo computador desligava e religava repetidamente, sem que os operadores pudessem controlá-lo, fazendo crer que a máquina fora infectada por um vírus.

A equipe de pesquisas da *VirusBlokAda* confirmou essa hipótese e, ao isolarem o vírus, perceberam que ele estava se valendo de um mecanismo conhecido como *zero-day*. Esse mecanismo explora *softwares* em busca de vulnerabilidades desconhecidas pelos seus criadores ou vendedores de programas antivírus. São sistemas raros por requererem habilidade e persistência nesse processo de pesquisa por pontos fracos. Assim, de milhares de *malwares* que os pesquisadores descobrem a cada ano, menos de uma dúzia usa um explorador *zero-day*.

Especificamente, o vírus descoberto encaixava-se na categoria denominada *worm* (verme), pois não requeria uma ação do usuário do computador, como a inadvertida abertura de um arquivo enviado por *e-mail* para infectar a máquina; podia, portanto, disseminar-se rápida e silenciosamente entre diferentes computadores.

No caso, o mecanismo *zero-day* permitia que o vírus se espalhasse entre computadores através de *drivers USB* (*Universal Standard Bus*), nossos conhecidos *pen drives*. A vulnerabilidade estava no arquivo LNK do Windows Explorer, componente do Microsoft Windows. Ao escanear automaticamente o conteúdo de um *driver USB* infectado, inserido no computador, o *worm* era descarregado sem o conhecimento do usuário no *hard disk* da máquina.

A *VirusBlokAda* comunicou sua descoberta à Microsoft, que batizou o *malware* de *Stuxnet* devido a uma combinação de nomes de arquivos (.**stu**b e Mr**xNet**.sys) encontrados no código do vírus.

A indústria de segurança de computadores começou seus trabalhos de descriptografia e desconstrução do *Stuxnet*, e os pesquisadores concluíram que ele havia sido lançado um ano antes, em junho de 2009, e desde então tinha sido aprimorado e atualizado pelo seu criador, sendo lançadas três diferentes versões. Para enganar os computadores hospedeiros, fazendo-se passar por um programa certificado e confiável, *Stuxnet* valia-se de arquivos de *drivers* com certificados de segurança válidos, furtados de dois fabricantes: *RealTek Semiconductor* e *JMicron Technology*, o que demonstrava que seus criadores dispunham de consideráveis recursos econômicos e tecnológicos.

Os pesquisadores também descobriram que o vírus havia sido desenhado para atacar o *software Simatic WinCC Step 7*, um sistema de controle desenvolvido pela empresa alemã Siemens para computadores industriais de controle de motores elétricos, válvulas e sensores, os denominados Controladores Lógico Programáveis (CLPs), visando a aplicações que variavam de indústrias automobilísticas a unidades de tratamento de esgotos.

Essa também era uma novidade trazida pelo *Stuxnet*, uma vez que esse tipo de equipamento industrial não era um alvo comum de *hackers*, pois não haveria nenhum ganho econômico aparente associado a uma invasão desse tipo.

A maioria dos pesquisadores presumiu que, a princípio, o *Stuxnet* estaria furtando dados industriais de configuração e desenho dos CLPs e classificaram-no como mais um caso de espionagem industrial. As companhias de antivírus incluíram as assinaturas das várias versões de *Stuxnet* encontradas em seus programas de detecção, e o caso poderia ter se encerrado nesse ponto não fosse a curiosidade e persistência de pesquisadores da Symantec.

O *Stuxnet* era enorme, cerca de 500 *kbytes*, ao contrário dos usuais 10 a 15 *kbytes* observados nesse tipo de *malware*. Além disso, era composto de várias camadas de códigos, dados e comandos, tendo sido necessária a criação de uma equipe para investigá-lo.

Essa equipe percebeu que toda vez que o *Stuxnet* infectava um computador, ele reportava as informações do sistema infectado a um de dois domínios hospedados em servidores na Dinamarca e na Malásia. Ou seja, ele "telefonava para casa" para informar os resultados de sua atividade e receber atualizações.

Alertados pela descoberta do *Stuxnet*, seus criadores àquela época já haviam abandonado a utilização dos *sites*. A Symantec, no entanto, convenceu os provedores a redirecionarem o tráfego de dados das máquinas infectadas para um computador que eles controlavam. Descobriram que, de 38 (trinta e oito) mil infecções reportadas, 22 (vinte e duas) mil eram de máquinas localizadas no Irã, contrariando todos os padrões de infecção do passado e fazendo a Symantec acreditar que *Stuxnet* se tratava, na verdade, de uma ciberarma posta em ação pelos governos americano ou israelense, ou por ambos, embora não soubessem ainda qual o propósito da ação.

A Symantec percebeu que o vírus procurava por um valor específico nos endereços dos Controladores Lógico Programáveis – 2CCB0001 – antes de decidir infectar a máquina. Descobriram, então, que este endereço correspondia à placa de rede de comunicação do equipamento e que os dois endereços seguintes (9500h e 7050h) referiam-se a identificações de conversores de frequência de determinados fabricantes e modelos.

Os conversores de frequência são equipamentos eletrônicos destinados a alterar a rotação de motores elétricos. Finalmente, ficou claro que o *Stuxnet* destinava-se a localizar instalações com, no mínimo, 33 (trinta e três) conversores de frequência de determinados tipos e a alterar a velocidade dos motores a eles conectados para os valores máximo e mínimo, de forma abrupta, por determinados períodos.

Ou seja, o objetivo do *worm* era encontrar, identificar e destruir os motores de algum tipo de equipamento conectado aos

Controladores Lógico Programáveis da Siemens, em instalações de determinado porte e com conversores de frequência específicos.

Logo ficou claro que essa descoberta estava relacionada ao relato de inspetores da Agência Internacional de Energia Atômica (AIEA), que, em visita às instalações da usina de Natanz, no Irã, em janeiro de 2010, perceberam o enorme número de centrífugas – equipamentos destinados ao enriquecimento de urânio empregado em usinas e bombas nucleares – danificadas.

Cerca de uma semana após a Symantec ter divulgado as conclusões de sua pesquisa, em novembro de 2010, Ali Akbar Salehi, diretor da Organização de Energia Atômica do Irã (OIEA), em entrevista a jornalistas iranianos, afirmou que há um ano e vários meses, ocidentais teriam enviado um vírus às instalações nucleares do país, mas depreciou seus efeitos, acrescentando que os funcionários das usinas conseguiram evitar que os equipamentos fossem danificados.

Seis dias depois, os criadores do *Stuxnet* substituíram as armas digitais pelas convencionais. Majid Shahriari e Fereydoon Abbasi, cientistas do programa nuclear iraniano, foram vitimados por dois atentados a bomba cometidos por homens em motocicletas. Shahriari, gerente sênior do programa, morreu e Abbasi ficou seriamente ferido.

Nunca houve demonstração segura de que o programa nuclear iraniano tivesse sido afetado pelo uso do *Stuxnet* ou pelos dois atentados que se seguiram.

O *Stuxnet* demonstra como um vírus, que sequer contou com o auxílio da Internet para se propagar, é capaz de afetar o funcionamento ou, como foi o caso, destruir máquinas controladas por computadores.

Não se trata, pois, das deploráveis e usuais violações de segredos pessoais ou profissionais, da privacidade ou intimidade de cidadãos ou de obtenção de vantagens econômicas ilícitas por

meio de extorsão ou venda de dados industriais ou comerciais a concorrentes. Trata-se da utilização, por *hackers*, de máquinas como instrumentos capazes de causar sérios danos não apenas ao patrimônio, mas à incolumidade física de seus usuários e, eventualmente, levar à morte.

Essa preocupação ganha relevo na medida em que se aprofundam estudos e pesquisas no sentido de se conectarem cada vez mais dispositivos à rede mundial de computadores, levando ao que se costuma denominar *Internet das Coisas* (IoT, sigla em inglês, que passaremos a usar a partir de agora).

A *IoT European Research Cluster* (IERC) define IoT como uma infraestrutura de rede de informação global e dinâmica, com capacidades de autoconfiguração baseada em protocolos de comunicação, padronizados e interoperativos, onde são integradas "coisas" físicas e virtuais com identidades próprias.

Para o grupo de trabalho da *International Telecommunication Union* (ITU), a IoT é

> uma infraestrutura para a sociedade da informação, que possibilita serviços avançados através da interconexão de coisas (físicas e virtuais) baseadas em tecnologia de informação e telecomunicação interoperáveis, existentes e em desenvolvimento.

A definição é acompanhada de algumas notas, entre elas a de número 1, segundo a qual

> através da exploração de identificação, captura de dados e capacidades de processamento e comunicação, a IoT faz completa utilização das coisas para oferecer serviços de várias aplicações enquanto garante que os requisitos de segurança e privacidade sejam mantidos.

Portanto, a IoT considera um ambiente onde estão presentes várias coisas ou objetos conectados, seja fisicamente, com fios e cabos, ou de forma *wireless*, e que, através de sistemas envolvendo *hardware* e *software* específicos, são capazes de interagir, trocando informações que possibilitam a realização de uma ou diversas tarefas.

Nesse contexto, a palavra de ordem é *smart*: *smart homes*, *smart cars*, *smart factories*, *smart cities*.

Essa "esperteza" ou inteligência a ser conferida aos dispositivos e sistemas conectados à Internet consiste, num primeiro momento, em dotá-los de conectividade para integrá-los aos outros dispositivos ligados à rede, bem como de certo grau de autonomia de funcionamento, uma vez que tais dispositivos deverão operar com a mínima supervisão humana.

A conectividade e integração pressupõem, por seu turno, a padronização de interfaces, protocolos e linguagens. Ademais, a aceitação dos cidadãos estará condicionada à existência de interfaces amigáveis ao usuário e do tráfego confiável e seguro de informações.

Pelos requisitos contidos nos parágrafos anteriores, é possível observar a complexidade dos desafios tecnológicos e operacionais envolvidos na IoT, que incluem investimentos elevados no desenvolvimento de sensores cada vez mais sofisticados e confiáveis, na disseminação maciça e segura da computação em nuvem (*cloud computing*) e no armazenamento e análise do enorme volume de informações que os sistemas deverão processar (*Big Data*).

Como sempre, o objetivo é econômico, visando ao aumento dos lucros como consequência da maior eficiência na condução dos negócios atuais, além do desenvolvimento de novos ramos de prestação de serviços. Assim, há o funcionamento de vários sistemas, ou ecossistemas, como são denominados pelos especialistas da área, quais sejam nossa casa, nosso automóvel, uma fábrica, as usinas de produção e distribuição de energia, de fornecimento de água e tratamento de esgotos, os sistemas de transporte, logística e saúde. Esses sistemas, integrados e interconectados, fariam parte de um todo, com vistas a otimizar a aplicação de recursos e minimizar desperdícios.

Uma consequência inafastável é o fato de que a utilização de *hardware* e *software*, para tornar as coisas inteligentes, e sua conexão à Internet sujeitam essas mesmas coisas ao risco de seus sistemas de controle terem sua integridade corrompida por *malwares*.

O conceito de *smart homes*, por exemplo, implica a integração de sistemas domésticos de segurança, monitoramento, utilização de eletrodomésticos, iluminação, entretenimento e racionamento de energia.

Parece uma solução perfeita até imaginarmos que as câmeras que monitoram a eventual invasão do domicílio por intrusos, transmitindo a informação em tempo real para o *iPhone* do morador, podem capturar as imagens de sua família e transmiti-las justamente para furtadores ou sequestradores. O inventário de bens a serem furtados ou de hábitos dos alvos a serem sequestrados poderia ser realizado remotamente. Ou seja, os equipamentos que deveriam proteger o cidadão seriam utilizados para ameaçá-los, numa completa inversão do propósito da tecnologia.

Imagine um forno de micro-ondas, que tem seu programa de controle ludibriado para permitir que seja acionado com a porta aberta, enquanto você retira dele o alimento. Ou uma cerca elétrica que é religada durante um serviço de manutenção.

Deixando nossa *smart home,* em nosso *smart car*, podemos imaginar um sistema de frenagem que é desabilitado por um programa clandestinamente inserido no computador de bordo, quando o veículo alcança determinada velocidade. Ou sistemas de trânsito rodoviário ou ferroviário, que mudam de estado sem qualquer obediência à lógica de controle do sistema operacional original. E sistemas de gerenciamento de energia elétrica que causam *blackouts* longos e aleatórios. Ou, finalmente, silos de mísseis que se abrem sem controle como em *War Games*, prontos a desferir o golpe fatal no inimigo.

Na maioria dos exemplos triviais que podemos imaginar, as soluções jurídicas parecem apontar para as invasões de sistemas como crimes meio absorvidos pelos delitos mais graves, quais sejam homicídios, roubos, furtos e extorsões a que se destinam.

Obviamente, trilhamos sempre uma linha tênue entre o encantamento com a tecnologia e o pavor de que ela nos substitua ou nos mate. O complexo de Frankenstein habita sempre nossos corações.

3 Conclusão

A inviolabilidade dos sistemas, portanto, é um dos principais requisitos não apenas para o funcionamento eficaz e econômico da IoT, conforme as especificações de projeto, mas para garantir a aceitação da tecnologia pelos usuários.

O elevado nível de automatismo dos dispositivos exige múltiplos e, portanto, redundantes mecanismos de proteção cada vez mais sofisticados e que garantam padrões de segurança operacional, que, embora nunca sejam absolutos, possam levar ao cidadão a tranquilidade necessária à utilização dos sistemas conectados à rede.

No entanto, num mundo que caminha de forma cada vez mais acelerada em direção à automação total de tarefas e serviços, é conveniente repensarmos até que ponto devemos deixar sob o comando de máquinas muitos dos aspectos de nossa vida.

As decisões essenciais, capazes de causar dano amplo e difuso, deveriam ser deixadas, em último nível, sempre sob a supervisão humana e de forma a garantir a redundância desejada nos sistemas de controle, preferencialmente submetidas à avaliação de mais de um homem, já que este, assim como os *softwares*, também é falível e corrompível.

Para nossa própria segurança, a Internet das Coisas não deve nunca se transformar na Internet de Todas as Coisas.

Referências bibliográficas

THE INTERNET of things: an overview. Understanding the issues and challenges of a more connected world. Internet Society, out. 2015. Disponível em: <https://www.internetsociety.org/doc/iot-overview>. Acesso em: 5 mar. 2017.

VERMESAN, Ovidiu; FRIESS, Peter (Ed). *Internet of Things – From research and innovation to market deployment*. River Publishers, 2014.

ZETTER, Kim. *How digital detectives deciphered Stuxnet, the most menacing malware in History*, 7 nov. 2011. Disponível em: <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>. Acesso em: 5 mar. 2017.

Crimes cometidos contra a vulnerabilidade sexual de crianças e adolescentes no ECA e no Código Penal: a Internet como forma de cometimento e aproximação do sujeito ativo e vítima

Renata Andrade Lotufo*

RESUMO

Neste estudo, partimos de considerações sobre a Internet (como começou, sua dimensão e profundidade) para em seguida definirmos termos técnicos específicos e apresentarmos noções básicas para o entendimento, na prática, dos crimes cibernéticos, em especial os que envolvam pornografia infantil. A partir da incorporação dessas noções básicas, passamos a estudar a evolução histórica da legislação que trata das violações sexuais envolvendo crianças e adolescentes: dispositivos legais do Estatuto da Criança e do Adolescente e do Código Penal. Passamos pelo bem jurídico protegido pela tutela penal nos crimes cibernéticos envolvendo pornografia infantil e ressaltamos o conceito de vulnerabilidade sexual da criança e do adolescente. A partir daí, focamos nos crimes que colocam em xeque a vulnerabilidade sexual das crianças e adolescentes para depois estudarmos a proporcionalidade entre os preceitos primário e secundário dos tipos penais e a evolução das penas, de acordo com a maior ou menor aproximação com a vítima.

Palavras-chave: Pedofilia. Internet. Vulnerabilidade sexual. Crianças. Adolescentes.

* Mestre e especialista pela Pontifícia Universidade Católica de São Paulo. Possui pós-graduação em Direitos Fundamentais pelo IBCCrim e Ius Gentium Conimbrigae da Faculdade de Direito da Universidade de Coimbra. Juíza Federal desde 1996. Titular da 4ª Vara Criminal Federal em São Paulo. *E-mail*: rlotufo@trf3.jus.br.

ABSTRACT

In this study, we start with considerations about the Internet (how it began, its size and depth), then define specific technical terms and present basic notions for the understanding, in a practical way, of cybercrimes, especially those involving child pornography. Based on the incorporation of these basic notions, we began to study the historical evolution of legislation that deals with sexual violations involving children and adolescents: legal provisions of the Statute of Children and Adolescents and the Penal Code. We analyze the legal asset secured by the criminal protection in cybercrimes involving child pornography and we highlight the concept of sexual vulnerability of children and adolescents. From this point on, we focus on the crimes that challenge the sexual vulnerability of children and adolescents, and then study the proportionality between the primary and secondary precepts of the penal types and the evolution of sentences according to the greater or lesser proximity to the victim.

***Keywords**: Pedophilia. Internet. Sexual vulnerability. Children. Adolescents.*

1 Introdução

Quando se pensa na fusão de crime sexual envolvendo a vulnerabilidade infantil com Internet, nós, que atuamos nas varas criminais federais, recordamos claramente da Internet como forma de propagação de vídeos e imagens, conforme previsto nos arts. 241-A e 241-B do Estatuto da Criança e do Adolescente.

Mas este estudo serve para, em primeiro lugar, termos panorama macro da Internet em si; e, em segundo lugar, para percebermos que ela pode estar muito mais entremeada na tessitura desses crimes em análise do que antes pensara o legislador. Isso porque a Internet cada vez mais ganha o papel de *serviço básico* para a população, junto com a água, o gás e a energia elétrica.

Com a criminalidade não é diferente. A Internet é o meio para arregimentação de organização criminosa, preparação de crime doloso, e, em muitos casos, como, por exemplo, nos arts. 241-A e 241-B do ECA, pode vir a ser o instrumento e o local de *consumação* dos delitos.

Visto isso, ao refletirmos sobre as potenciais vítimas de todos os crimes envolvendo vulnerabilidade sexual infantil e seus respectivos sujeitos ativos, podemos ter também a Internet como fator de aproximação e aliciamento.

Com base nestas ponderações, passaremos a esmiuçar a relação da pena prevista para todos os crimes.

O motivo não é outro senão o nosso eterno atraso em relação aos avanços tecnológicos. O Estado corre atrás do tempo perdido, tal qual o coelho branco de Alice: hoje a Internet está no ar, todos estão conectados, e ela está em todos os lares. Nos tempos atuais, quem quiser entrar na casa – ou vida – alheia sem bater na porta, basta fazer o *login*.

2 A Internet e seus meandros

2.1 Internet: evolução – breve histórico

O primeiro passo para o surgimento da Internet foi dado em 1969 com um projeto do Departamento de Defesa dos Estados Unidos da América: a rede Arpanet, cujo objetivo era a interligação de computadores usados nos centros de investigação para fins militares. Por mais de uma década, o uso da Arpanet ficou restrito a essa finalidade. Com a criação, em 1983, de uma rede estritamente militar (Milnet), a Arpanet foi fundida à recém-criada CSNet (*Computer Science Network*), dando corpo ao embrião da nossa atual Internet, que passou a obedecer a um conceito-chave: *open network* – rede de arquitetura aberta. A opção de tecnologia passa a ser ditada pelo provedor que possibilita a conexão entre as redes[1].

Por ter financiado a criação da Arpanet, já na década de 1980 os Estados Unidos mantinham um contrato de gerenciamento com a Iana (*Internet Assigned Numbers Authority*), responsável pela gestão dos nomes dos domínios e dos endereços de IPs[2].

IP é a sigla de *Internet Protocol* ou Protocolo de Internet. Trata-se de um número inteiro de 32 *bits*, separado em quatro fragmentos de 8 *bits*[3].

O sistema dos nomes dos domínios, DNS (*Domain Name System*), estava ainda sob controle do Departamento de Comércio dos Estados Unidos, e, como era de se esperar, com o decorrer dos anos, o controle técnico e administrativo da Internet pelos Estados Unidos passou a causar tensão internacional.

[1] Disponível em: <http://www.tipografos.net/internet/internet-evolucao.html>. Acesso em: 15 fev. 2017.

[2] Disponível em: <http://www2.uol.com.br/historiaviva/reportagens/o_nascimento_da_internet.html>. Acesso em: 15 fev. 2017.

[3] "*Bit* é uma simplificação para o termo 'dígito binário' (*BInary digiT* em inglês). Um *bit* é a menor unidade de informação que pode ser armazenada ou transmitida." (MPF. *Roteiro de atuação sobre crimes cibernéticos.* Brasília, 2016, v. 5, p. 22-23.)

Dessa forma, em 2003, a ONU reclamou uma gestão "multilateral, transparente e democrática, com a plena participação dos Estados, do setor privado, da sociedade civil e das organizações internacionais"[4].

Isso explica o fato de que, mesmo depois de quinze anos, os Estados Unidos ainda têm um pouco de resistência em colaborar com o fornecimento de dados e IPs em várias investigações e processos criminais[5].

A Internet revolucionou toda a sociedade e também o Direito Penal. Trouxe novas formas de praticar crimes já antigos, como o estelionato, por exemplo; como também exigiu e ainda exige do legislador criar novos tipos penais outrora impensáveis[6].

De 2003 a 2008, a Internet e novas tecnologias se desenvolveram muito mais rápido do que os métodos de investigação. De 2001 a 2005, foi lançada a Wikipedia, ocorreu a ascensão do Fotolog, foram criados o Skype, o Orkut, e nasceu o YouTube[7]. O uso de *webcams* começou a popularizar-se em 2004, assim como novos meios de acesso à pornografia infantil surgiram com espantosa rapidez. No final de 2005, pelo menos um bilhão de pessoas no mundo tinha acesso à Internet, sendo que cerca de 25% (vinte e cinco por cento) já utilizava a Banda Larga ou conexões de alta velocidade. Em 2006, o número de usuários da Internet aumentou com o aparecimento dos *smartphones*[8], mesma época em que o

[4] Disponível em: <http://www2.uol.com.br/historiaviva/reportagens/o_nascimento_da_internet.html>. Acesso em: 15 fev. 2017.

[5] Disponível em: <https://internet-legal.jusbrasil.com.br/noticias/237428595/mpf-aponta-entraves-tecnicos-para-investigacao-de-crimes-ciberneticos>. Acesso em: 15 fev. 2017.

[6] Citamos, como meros exemplos, os arts. 313-A e 313-B do Código Penal, acrescidos pela Lei n.º 9.983/2000, ou os mais recentes arts. 154-A e 154-B, inseridos pela Lei n.º 12.737/2012 (Lei Carolina Dieckmann), regulados a partir de um caso concreto.

[7] Disponível em: <http://clickonedigital.com.br/blog/wp-content/uploads/2016/01/Linha-do-Tempo.png>. Acesso em: 13 fev. 2017.

[8] Disponível em: <http://www.ufpa.br/dicas/net1/int-h200.htm>. Acesso em: 10 fev. 2017.

Facebook saía do meio universitário e ganhava o mundo. A partir daí, foram só mais dois anos para os aplicativos caírem de vez no gosto e na vida das pessoas: Waze, WhatsApp, Instagram, Tinder, Uber, etc.[9]

A Internet cresceu e hoje em dia faz parte da vida de todos nós. Mas o que conhecemos é apenas a "ponta do *iceberg*". A Internet que acessamos é conhecida como Surface Web, que representa no máximo[10] 10% do conteúdo da *web.* Os outros 90% são a parte submersa do *iceberg*. Essa, aliás, é a expressão frequentemente utilizada para explicar a chamada Deep Web. *Na Surface Web todos os movimentos do usuário são rastreáveis*[11].

2.2 Deep Web (DW)

Deep Web, também conhecida como Undernet ou Darknet, é uma expressão inglesa que significa "Internet profunda" (dando a ideia realmente do *iceberg*). O acesso ao seu interior não é fácil para a maioria dos internautas, daí por que os produtores do material que circula nessas profundezas optam por manter seu anonimato utilizando *softwares* que dificultem sua identificação[12]. A Deep Web foi criada por Michael K. Bergman, CEO e cofundador da Structured Dynamics LLC. Trata-se de todo conteúdo que não pode ser indexado pelos *sites* de busca.

Alguns definem a Deep Web como tudo o que está abaixo da Surface Web, e a Dark Web ("Internet Escura") como a parte mais profunda do *iceberg.* Dentro da Dark Web existem páginas acessíveis apenas por *softwares* específicos, tais como o TOR (*The*

[9] Disponível em: <http://clickonedigital.com.br/blog/wp-content/uploads/2016/01/Linha-do-Tempo.png>. Acesso em: 13 fev. 2017.

[10] Há notícia de que a Surface Web representa 4% da Internet, enquanto a Deep Web ficaria com 96% do conteúdo. Disponível em: <http://www.saibanaweb.com/2013/02/acessandoadeepweb.html>. Acesso em: 14 fev. 2017.

[11] Disponível em: <http://olhardigital.uol.com.br/fique_seguro/video/voce-sabe-o-que-e-a-deep-web/32156>. Acesso em: 14 fev. 2017.

[12] Disponível em: <https://www.significados.com.br/deep-web/>. Acesso em: 13 fev. 2017.

Onion Router), que faz a intermediação entre o computador do usuário e os *sites* escondidos[13].

Figura 1: Diferença entre Web, Deep Web e Dark Web.
Fonte: Imagem disponível em: <https://suprimatec.com/2016/11/18/o-que-realmente-e-a-dark-web/>. Acesso em: 15 fev. 2017.

TOR Browser é como se fosse um provedor independente, ou seja, um programa que possibilita ao usuário navegar de forma anônima, tirando-o da mira de *plug-ins* como *Flash, Real Player* e *Quick Time*, que geralmente identificam e revelam o endereço de IP do usuário[14]. Como o próprio nome sugere, *The Onion Router* (TOR) significa o roteamento cebola: o usuário que está enviando a mensagem seleciona um caminho de roteadores da rede e "encripta" a mensagem diversas vezes via *encriptação assimétrica*; e, a cada servidor, o pacote recebido (a cebola) é "desencriptada" como se retirasse uma camada da cebola, abrindo um novo caminho randômico. Isso possibilita que apenas o remetente, o último servidor

[13] Disponível em: <https://www.tecmundo.com.br/internet/43025-muito-alem-da-deep-web-o-que-e-a-mariana-s-web-.htm>. Acesso em: 13 fev. 2017.

[14] Disponível em: <http://www.techtudo.com.br/tudo-sobre/tor.html>. Acesso em: 17 fev. 2017.

e o receptor vejam a mensagem original[15]. Em outras palavras, como a navegação do TOR se dá em várias camadas e cada uma delas com um roteador diferente, a ideia é que, ao final, o conteúdo chegue "supercriptografado" para o destinatário[16]. Segundo o Grupo de Trabalho da Disciplina de Rede de Computadores I – 2011-1 da Escola Politécnica da Universidade Federal do Rio de Janeiro, a imagem poderia ser representada da seguinte forma:

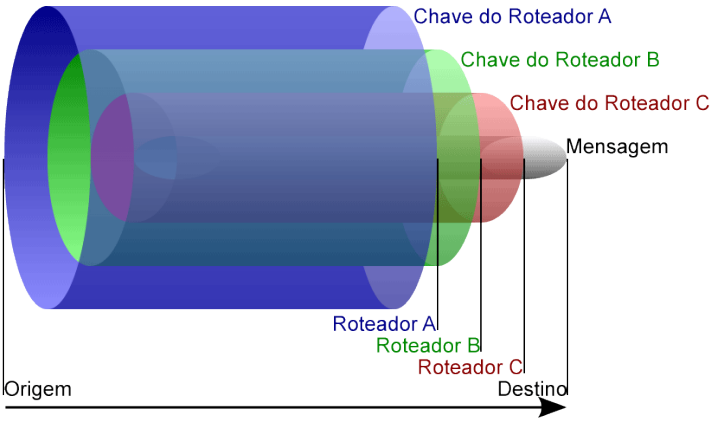

Figura 2: Diagrama do Onion Routing.
Fonte: Disponível em: <http://www.gta.ufrj.br/grad/11_1/tor/index.php?file=kop8.php>. Acesso em: 14 fev. 2017.

Por ser uma Internet profunda, onde o anonimato é a regra, a Deep Web pode servir para quaisquer fins, inclusive para o ser humano extravasar o que tem de pior dentro de si. Apenas para citar algumas situações: tortura por encomenda, fóruns de canibalismo, pornografia grotesca, pedofilia, grupos extremistas, *hitmans* (contratação de assassinos), venda livre de drogas e vídeos *snuffs* (termo utilizado para filmagens de homicídios premeditados,

[15] Disponível em: <www.gta.ufrj.br/grad/11_1/tor/index.php?file=kop8.php>. Acesso em: 17 fev. 2017.

[16] Disponível em: <https://www.tecmundo.com.br/internet/43025-muito-alem-da-deep-web-o-que-e-a-mariana-s-web-.htm>. Acesso em: 17 fev. 2017.

geralmente feito pelo próprio assassino com cenas de extrema brutalidade e violência)[17].

Diante dessa liberdade e anonimato, a Deep Web é o grande repositório de conteúdo pedófilo. Em 2014, uma investigação da rede de jornalismo BBC descobriu que dezenas de milhares de pessoas usavam a DW para essa finalidade. Uma das páginas com conteúdo de pornografia infantil recebia 500 visitas por segundo[18]. Segundo a revista *Exame*, um relatório da Trend Micro, intitulado *Abaixo da superfície: exploração da Deep Web*, revelou que mais de 25% das buscas na Deep Web e na Surface Web referem-se à exploração infantil e pedofilia[19].

A Deep Web (em especial a Dark Web) é realmente lotada de perversões, lixo e pessoas mal-intencionadas. Mas, ao analisarmos a evolução tecnológica, não há como concebê-la numa visão maniqueísta, como a representação pura do mal. Através da Deep Web muitos correspondentes estrangeiros conseguem burlar a censura e se comunicar com as suas redações[20], pessoas que moram em países com a Internet controlada (como Irã, Coreia do Norte e China), usam a DW para fugir à repressão e evitar o controle estatal, disseminar a cultura com artigos científicos, *e-books* e obras raras (*sites:* InfoMine e CompletePlanet), bem como o surgimento do movimento da *Primavera Árabe* (onda de protestos contra governos muçulmanos que eclodiu em 2010-2011)[21].

[17] Disponível em: <http://ahduvido.com.br/os-8-piores-casos-da-deepweb-que-foram-descobertos-por-internautas-da-surface>. Acesso em: 13 fev. 2017.

[18] Disponível em: <http://www.bbc.com/portuguese/geral-36920676>. Acesso em: 14 fev. 2017.

[19] Disponível em: <http://exame.abril.com.br/tecnologia/deep-web-o-que-se-esconde-no-submundo-da-internet/>. Acesso em: 14 fev. 2017.

[20] Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI331438-17770,00-NEM+TUDO+SAO+TREVAS+O+LADO+BOM+DA+DEEP+WEB.html>. Acesso em: 14 fev. 2017.

[21] Disponível em: <http://www.magicwebdesign.com.br/blog/internet/lado-bom-deep-web/; <https://canalcienciascriminais.com.br/ainda-sobre-a-deep-web-o-lado-positivo-da-rede/>. Acesso em: 14 fev. 2017.

Julian Assange registrou o domínio wikileaks.org em 4 de outubro de 2006 e, em 6 de dezembro, publicou o primeiro documento: *Inside Somalia and the Union of Islamic Courts*. O WikiLeaks é um dos instrumentos dos chamados *cyberpunks* na Deep Web. Os *cyberpunks* defendem a utilização da criptografia e de métodos similares como instrumento de provocação de mudanças sociais e políticas, utilizando-se do mote: "Privacidade para os fracos, transparência para os poderosos". Segundo VIANA (apud ASSANGE, 2013, p. 12), é o resumo do princípio fundamental da filosofia *hacker*: "a informação tem que ser livre".

Ao fundar a *WikiLeaks*, Assange agregou a *expertise* de desenvolvedor de códigos digitais aos fundamentos mais básicos do jornalismo, para trazer histórias de interesse público. O domínio ficou famoso mundialmente em 2010 quando publicou milhares de documentos secretos dos Estados Unidos vazados supostamente pelo soldado Bradley Manning, que servia no Iraque. A rede trouxe um vídeo chocante de dezessete minutos em que, dentro de um helicóptero, soldados norte-americanos atacavam doze civis desarmados (entre eles, dois jornalistas da agência de notícias Reuters). Mas foi com o projeto "Cablegate", com 251 287 comunicados de 274 embaixadas dos Estados Unidos no mundo, que a WikiLeaks relatou como funcionavam as relações internacionais e como seus líderes se comportavam na intimidade: reuniões discretas, comentários maliciosos e negócios escusos, tais como os pedidos da Secretária de Estado Hillary Clinton a 33 embaixadas e consulados para que diplomatas espionassem representantes de vários países da ONU, reunindo números de cartões de créditos, senhas e dados de DNA.

Assim, a Deep Web e o aprimoramento da criptografia pelos *cyberpunks* não serviu necessariamente para possibilitar a criação de universo *web* de perversidades e crimes hediondos.

Veja a seguir o que diz a respeito o próprio ASSANGE (2013, p. 25).

> A Internet, nossa maior ferramenta de emancipação, está sendo transformada no mais perigoso facilitador do totalitarismo que já vimos. A Internet é uma ameaça à civilização humana.
>
> Essas transformações vêm ocorrendo em silêncio, porque aqueles que sabem o que está acontecendo trabalham na indústria da vigilância global e não têm nenhum incentivo para falar abertamente. Se nada for feito, em poucos anos a civilização global se transformará em uma distopia da vigilância pós-moderna, da qual só os mais habilidosos conseguirão escapar. Na verdade pode ser isso que já esteja acontecendo.

A Surface Web, com todos os seus instrumentos de controle e identificação de IPs, faz com que o conceito de privacidade seja bastante relativo. De fato, cada vez mais se concretiza a profecia agoureira, "O Grande Irmão está de olho em você", da obra *1984*, de George ORWELL (2014, p.12). Daí por que Julian Assange relatou em seu livro que a ideia da Deep Web e dos *cyberpunks* é fazer o contraponto do controle de informação dos Estados como meio de submissão e vigilância da sociedade:

> Os *cyberpunks* originais, meus camaradas, foram em grande parte libertários. Buscamos proteger a liberdade individual da tirania do Estado, e a criptografia foi a nossa arma secreta. Isso era subversivo porque a criptografia era de propriedade exclusiva dos Estados, usada como arma em suas variadas guerras. Criando nosso próprio software contra o Estado e disseminando-o amplamente, liberamos e democratizamos a criptografia, em uma luta verdadeiramente revolucionária, travada nas fronteiras da nova Internet. A reação foi rápida e onerosa, e ainda está em curso, mas o gênio saiu da lâmpada (ASSANGE, 2013, p. 22).

A divisão da Internet em camadas não é estanque e pode gerar confusão entre os termos Dark Web, Deep Web, Mariana´s Web (um dos níveis mais profundos, cujo nome foi inspirado nas *Fossas Marianas*, o lugar mais profundo dos oceanos do planeta Terra)[22].

[22] Disponível em: <https://www.tecmundo.com.br/internet/43025-muito-alem-da-deep-web-o-que-e-a-mariana-s-web-.htm>. Acesso em: 15 fev. 2017.

Segundo o blog Deepweb2012, para termos uma noção, as camadas seriam assim divididas:

a) **Camada zero** (na superfície): *sites* comuns, tais como Facebook, Google, etc.

b) **Camada 1 – Superfície da Web** (na superfície): *sites* isolados, como Reddit, Digg, entre outros.

c) **Camada 2** ou **Bergie Web** (na superfície): *sites* ocultos que não aparecem nos resultados do Google, como *4chan, FreeHive* e muito conteúdo de pornografia infantil.

d) **Camada 3** (início da **Deep Web**): pornografia infantil, vírus, pirataria e fofocas não divulgadas pela mídia.

e) **Camada 4** ou **Charter Web**: tráfico de animais, pornografia infantil com inclusão de bebês, filmes e vídeos banidos e venda de drogas.

f) **Camada 5**: tráfico de pessoas, assassinos de aluguel, sociedades secretas, seitas satânicas, *snuff filmes* (já explicado), vendas de armas e outros.

g) **Camada 6** ou **Muro da Morte** (a partir daí é necessária a "computação quântica"): campo de batalha dos *hackers* com muitas informações "encriptadas", só decifráveis por computadores quânticos.

h) **Camada 7** ou "**A Névoa**": essa camada é chamada "neblina", pois é formada por várias pessoas poderosas, que lutam para chegar até a camada 8 e não querem concorrência; por isso o local é repleto de vírus e códigos maliciosos, para evitar que qualquer pessoa chegue à camada 7 para evitar a concorrência.

i) **Camada 8** ou **Mariana´s Web**: 80% do conteúdo da Internet[23], grupos terroristas, seitas e muitas lendas[24].

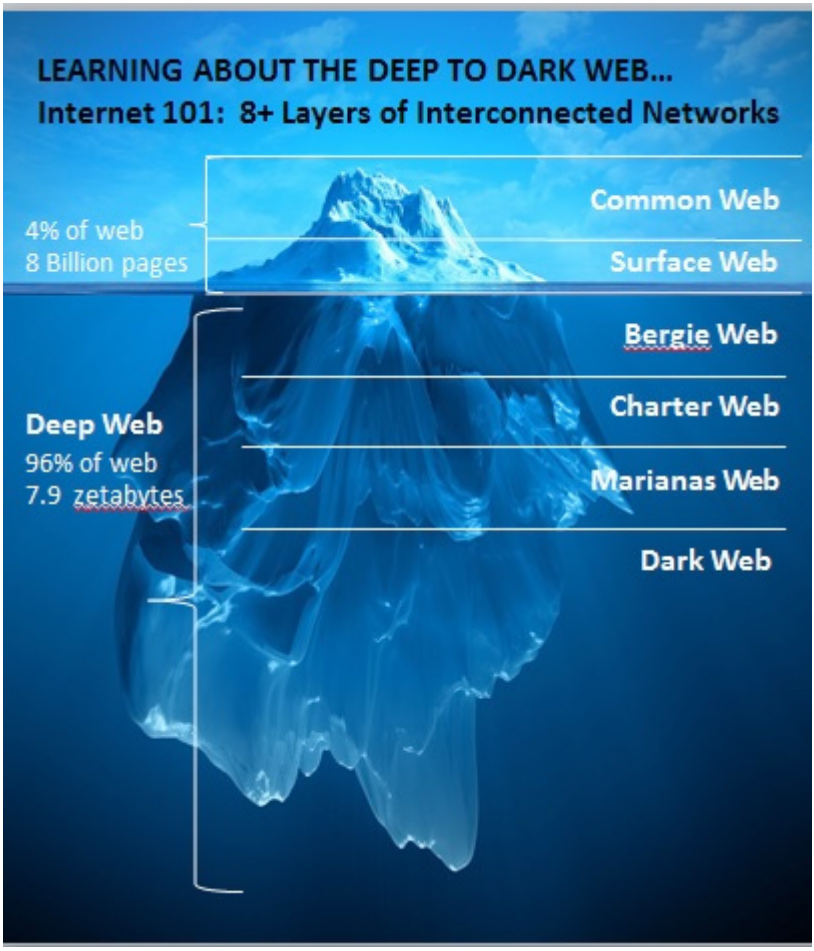

Figura 3: Diagrama da Web e suas diferentes camadas.
Fonte: Imagem disponível em: <http://www.chargertimes.com/2521/features/does-the-dark-web-exist/>. Acesso em: 15 fev. 2017.

[23] Disponível em: <http://deepweb2012.blogspot.com.br/2012/08/8-camadas-da-internet.html>. Acesso em: 15 fev. 2017.

[24] Disponível em: <https://www.youtube.com/watch?v=2-CcUVr1xiA>. Acesso em: 15 fev. 2017.

Apesar de a Dark Web não servir apenas para ações ilegais, a prática criminosa é facilmente localizada, como por exemplo: *site* de Crowd Funding para "auxílio" de produtores de pornografia infantil, manual do pedófilo, comércio de base governamental, curso para iniciantes em fraudes bancárias, entre outros (SHIMABUKURO; SILVA, 2017, p. 260-261).

2.3 Polícia, sociedade e *hackers* contra vídeos e fotos com conteúdo de exploração e pornografia infantil

Ainda que a Internet tenha facilitado e aproximado o contato e o compartilhamento de vídeos dos apreciadores de pornografia infantil, a sociedade, por outro lado, é praticamente coesa ao repudiar tais condutas.

Com o intuito de desenvolver pesquisas e projetos sociais voltados ao combate à pornografia infantil na Internet brasileira[25], nasceu em 2005 a SaferNet, associação civil de direito privado, sem fins lucrativos, fundada por um grupo de cientistas da computação, professores e bacharéis em Direito.

Os próprios *hackers*, ou *cyberpunks* (na denominação de Assange), que se utilizam da Deep Web como movimento libertário contra a censura, repudiam o uso da DW para divulgação e compartilhamento de imagens de cunho pedófilo. No começo de 2016, o grupo de *hackers* chamado *Anonymous* organizou-se para limpar a DW dos vídeos e imagens de pornografia infantil, lançando a *Operation Death Eaters* (*Operação Comensais da Morte*). Fazendo uma alusão aos Comensais da Morte da série de livros *Harry Potter*, os *hackers* pretendem "montar uma base de dados global sobre usuários pedófilos"[26].

[25] SAFERNET: quem somos. Disponível em: <http://www.safernet.org.br/site/institucional>. Acesso em: 14 fev. 2017.

[26] O GLOBO. *Grupo de hackers Anonymous mira expor redes internacionais de pedofilia.* Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/grupo-de-hackers-anonymous-mira-expor-redes-internacionais-de-pedofilia-15128693>. Acesso em: 14 fev. 2017.

Em maio de 2016, outro *hacker* lançou no Brasil a *Operação Hacker do Bem*, que identificou e enviou à Polícia 9 (nove) endereços de IPs suspeitos. Dentre as pessoas detidas, foi preso um diretor de ensino aposentado, de 74 anos, que usava um aplicativo que permitia o compartilhamento das imagens com outros usuários[27].

Basta fazer uma busca no Google, portanto em nível bem alto da superfície do *iceberg*, que vários *sites* e blogs fazem tutoriais ensinando evitar conteúdo pedófilo, inclusive advertindo a possibilidade de o usuário estar cometendo crime[28].

Em novembro de 2005, a UOL, o iG e a Abranet (Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet) celebraram um termo de compromisso de integração operacional com a Procuradoria da República do Estado de São Paulo, em que os provedores de Internet comprometeram-se a divulgar e incitar a população em campanhas contra a pornografia infantil; orientar o público contra a prática criminosa de tais condutas em salas de bate-papo e afins; inserir, nos contratos de adesão ao serviço de acesso, cláusula que preveja a rescisão da relação jurídica, caso o usuário se valha do provedor para veicular imagens de pornografia infantil; e, a informação de usuários que, de alguma forma, descumpram a cláusula. Três anos depois, o Ministério Público Federal em São Paulo conseguiu celebrar com o Google um Termo de Ajustamento de Conduta, assegurando várias medidas para evitar, investigar e punir usuários que usam o provedor, *e-mail* ou *site* de busca de conteúdo de pornografia infantil[29].

---

[27] Disponível em: <https://blog.deepwebbrasil.com/hacker-descobre-rede-de-pedofilia-e-entrega-a-policia/>. Acesso em: 14 fev. 2017.

[28] Disponível em: <http://www.desfavor.com/blog/2012/11/desfavor-explica-deep-web/>; <http://acrediteounao.com/os-10-sites-e-servicos-mais-infames-da-deep-web/> e <https://www.epochtimes.com.br/darknet-combate-crime-virtual-e-terrorismo-chega-lado-obscuro-internet/#.WKTJWtLyvbg>. Acesso em: 15 fev. 2017.

[29] MPF. *Roteiro de atuação sobre crimes cibernéticos*. Brasília, 2016, v. 5, apêndice.

Assim, a Deep Web também passou a ser frequentada pelos órgãos de repressão de pornografia infantil, sendo algumas das operações mais conhecidas: Torpedo (FBI, 2012), Dirtynet (Brasil, 2012), Onymous (FBI, 2012), Darknet (Brasil, dez. 2014), Playpen (FBI, mar. 2016)[30] e Darknet II (Brasil, nov. 2016)[31].

2.4 Programas para baixar arquivos de fotos e vídeos

Boa parte dos processos em que se acusa alguém da prática de crimes previstos nos arts. 241-A e 241-B do Estatuto da Criança e do Adolescente são casos em que, após a perícia, constata-se que a pessoa acusada instalou programas específicos para baixar arquivos na Internet.

A maioria das alegações das defesas baseia-se no fato de que a pessoa desconhecia que, ao baixar o arquivo considerado pedófilo, ela automaticamente compartilhava com outras pessoas.

Vamos entender como se operam esses programas.

O programa eMule, por exemplo, trabalha com a chamada transferência *peer-to-peer* (P2P), ou seja, com uma rede ponto a ponto, conforme explica o *site* TechTudo[32]:

> P2P vem de *peer-to-peer*, o que significa que uma transferência ocorre entre duas máquinas que têm um determinado arquivo instalado. O gerenciador P2P busca por outro computador com o mesmo programa instalado – no caso, o eMule – e que tenha o arquivo desejado pelo usuário já salvo na memória. Se não tiver o item completo, o que pode ocorrer quando o *download* não foi finalizado pelo par, o eMule então passa para outro PC, e assim por diante, até o arquivo ser baixado completamente.

[30] 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: Liv. do Advogado, 2017. p. 269.

[31] Disponível em: <http://g1.globo.com/rs/rio-grande-do-sul/noticia/2016/11/pf-deflagra-operacao-contra-pornografia-infantil-no-rs-e-15-estados.html> e <http://www.pf.gov.br/agencia/noticias/2016/11/pf-divulga-balanco-da-operacao-darknet-ii>. Acesso em: 22 fev. 2017.

[32] Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2015/11/como-funciona-o-emule.html>. Acesso em: 17 fev. 2017.

Como o eMule trabalha com esse sistema *peer-to-peer*, seu nível de segurança é baixo, motivo pelo qual muitos usuários migraram para o BitTorrent.

O BitTorrent trabalha com um modo mais coletivo de obtenção de arquivos, ou seja, baixa o arquivo desejado buscando retalhos em computadores diversos. Por tal motivo, para baixar, é necessário compartilhar, conforme explanação do *website* InfoWester[33]:

> Criado pelo programador norte-americano Bram Cohen em 2001, o BitTorrent é uma tecnologia que permite o compartilhamento de praticamente qualquer arquivo pela Internet, sendo especialmente utilizado para a distribuição de vídeos, músicas e *softwares*.
>
> O BitTorrent é bastante popular porque é um sistema fácil de se utilizar e, ao mesmo tempo, é muito eficiente. Isso se deve, basicamente, a dois motivos:
>
> – quando um arquivo está sendo baixado para um computador, "pedacinhos" dele são obtidos de várias outras máquinas simultaneamente, não apenas de uma;
>
> – ao mesmo tempo que um computador obtém um arquivo, os dados que já foram baixados também são compartilhados, ou seja, para receber é preciso também fornecer.
>
> O BitTorrent em si, na verdade, é um protocolo de compartilhamento de dados e não um sistema centralizado. Não há um servidor provendo os dados, mas sim um padrão de comunicação entre vários computadores, que permite que arquivos sejam localizados, distribuídos e obtidos por todos.

Existem vários *sites* que oferecem o serviço Torrent[34], sendo um dos mais famosos o *Pirate Bay* e o KAT (*Kickass Torrents*), que ficou fora do ar por metade do ano de 2016, em virtude da

[33] Disponível em: <https://www.infowester.com/bittorrent.php>. Acesso em: 17 fev. 2017.

[34] Disponível em: <https://olhardigital.uol.com.br/noticia/estes-sao-os-10-sites-de-torrent-mais-populares-do-momento/65182>. Acesso em: 14 fev. 2017.

prisão do administrador da plataforma por suspeita de pirataria e lavagem de dinheiro[35].

Os programas do tipo Torrent não deixam de constituir um nível mais aprofundado da Internet, não acessado pela maioria dos usuários. Conforme a figura 4, estaria no nível 3 da Deep Web.

Seja, porém, nos programas para baixar vídeos ou na própria Dark Web, o conteúdo pedófilo precisa ser buscado pelo usuário. Alguns tutoriais alertam para o fato de que possuir tais vídeos já é considerado crime e ensinam até a evitar termos de buscas em fóruns ou repositórios na DW: *hard candy* (conteúdo com fotos e vídeos com participantes menores de 10 anos de idade); *jail bait* (fotos e vídeos com participantes adolescentes)[36], CP (*child porn*), *pedo* (*pedophilia*)[37], "12yo", "10yo", "7yo" (12, 10 ou 7 anos de idade)[38], entre outros.

Um pouco mais cientes dos meandros da Internet, passaremos a examinar toda a legislação correlata à pornografia infantil.

[35] Disponível em: <https://olhardigital.uol.com.br/noticia/maior-site-de-pirataria-do-mundo-e-derrubado-em-operacao-policial/60468>. Acesso em: 14 fev. 2017.

[36] Disponível em: <http://peloamordedeus.com/conheca-deep-web-sem-medo-de-ser-feliz/>. Acesso em: 14 fev. 2017. Notícia de um *hacker* que derrubou 10 mil *sites* de conteúdo pedófilo na DW. Disponível em: <https://www.tecstudio.com.br/seguranca/hacker-derruba-sites-pornografia-infantil-deep-web/>. Acesso em: 14 fev. 2017.

[37] Disponível em: <https://www.genbeta.com/a-fondo/kit-de-supervivencia-en-la-deep-web>. Acesso em: 14 fev. 2017.

[38] Disponível em: http://www.prsp.mpf.gov.br/sala-de-imprensa/sala-de-imprensa/noticias_prsp/14-05-09-mpf-jales-denuncia-policial-civil-por-divulgacao-de-pornografia-infantil/. Acesso em: 22 fev. 2017.

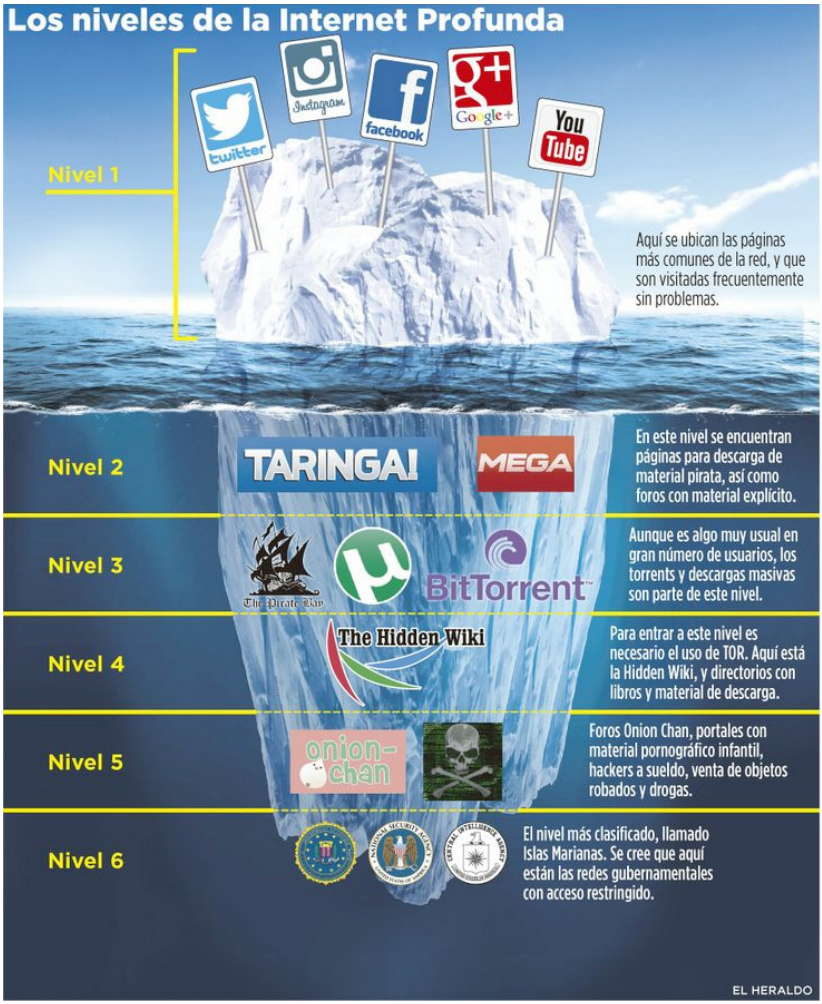

Figura 4: Modelo de classificação em seis níveis.

Fonte: Imagem disponível em: <https://gustavoaugustobardo.wordpress.com/2016/03/20/introducao-a-navegacao-online-niveis-e-geografia-da-internet/>. Acesso em: 14 fev. 2017.

3 Legislação dos crimes envolvendo a vulnerabilidade sexual de crianças e adolescentes

3.1 Final dos anos 1980 e anos 1990

A Constituição anterior não dispunha expressamente sobre a proteção à criança. O art. 175, § 4º da Constituição de 1967 (EC n.º 1/69), prescrevia apenas que lei especial disporia sobre a assistência à maternidade, infância, adolescência e sobre a "educação de excepcionais".

Já a Constituição de 1988, ao preceituar a necessidade de lei especial para a proteção da criança, foi mais categórica prevendo a necessidade de proteção infantil face à violência e exploração sexual, como dispõe o art. 227 a seguir:

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.
>
> [...]
>
> § 4º *A lei punirá severamente o abuso, a violência e a exploração sexual da criança e do adolescente*[39] [grifo nosso].

Segundo o UNICEF (Fundo das Nações Unidas para a Infância), a Convenção sobre os Direitos da Criança, de 20 de novembro de 1989, é a "carta magna" para as crianças de todo o mundo, por ter sido o instrumento de direitos humanos mais aceito na história universal, já ratificado por 196 países[40].

[39] Constituição da República Federativa do Brasil, promulgada em 5 de outubro de 1988. Redação original. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-publicacaooriginal-1-pl.html>. Acesso em: 10 fev. 2017.

[40] UNICEF. *Convenção sobre os Direitos da Criança*. Disponível em: <https://www.unicef.org/brazil/pt/resources_10120.htm>. Acesso em: 10 fev. 2017.

No Brasil, a Convenção foi aprovada pelo Congresso Nacional através do Decreto Legislativo n.º 28, de 14 de setembro de 1990, e promulgado pelo Presidente da República através do Decreto n.º 99.710, de 21 de novembro de 1990.

O art. 19 da Convenção sobre os Direitos da Criança dispôs que o âmbito de sua proteção contra violências físicas, mentais, abuso e exploração envolveriam medidas legislativas, administrativas, sociais e educacionais apropriadas. Além do mais, a alínea 2 do art. 19 previu:

> Essas medidas de proteção deveriam incluir, conforme apropriado, procedimentos eficazes para a elaboração de programas sociais capazes de proporcionar uma assistência adequada à criança e às pessoas encarregadas de seu cuidado, bem como para *outras formas de prevenção*, para a *identificação*, *notificação*, *transferência a uma instituição*, *investigação*, *tratamento e acompanhamento posterior dos casos acima mencionados de maus-tratos à criança e, conforme o caso, para a intervenção judiciária*[41] [grifos nossos].

Assim, de acordo com a Convenção, a proteção à criança vítima de abuso real ou em potencial é de responsabilidade de toda a sociedade, inclusive com instrumentos preventivos, pesquisas e acompanhamento posterior dos casos de abuso.

O *boom* da Internet e do "WorldWideWeb" (www) ocorreu nos primeiros anos da década de 1990[42], motivo pelo qual o legislador do Estatuto da Criança e do Adolescente (ECA) não poderia supor que a rede seria o instrumento para a troca de vídeos e fotos de crianças em situação de abuso sexual. Assim, inicialmente, o art. 241 do ECA proibia singelamente *fotografar* ou *publicar* cena de sexo explícito ou pornográfica envolvendo criança ou adolescente com a pena de reclusão de 1 (um) a 4 (quatro) anos.

[41] Decreto Executivo n.º 99.710, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D99710.htm>. Acesso em: 10 fev. 2017.

[42] TECHTUDO. *Internet completa 44 anos; relembre a história da web.* Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html>. Acesso em: 10 fev. 2017.

Com o avanço da tecnologia no decorrer da década de 1990, a Europa sentiu a necessidade de criminalizar a veiculação de imagens obtidas pela Internet. Assim, em 1999, ocorreu em Viena a Conferência Internacional de Combate à Pornografia Infantil na Internet, de onde se conclui que a pornografia infantil na rede mundial de computadores era um problema crescente e, quanto mais o mundo se conectava *on-line*, mais o problema cresceria sem o conhecimento ou o respeito das fronteiras[43].

Em maio de 2000, a Assembleia Geral das Nações Unidas adotou o Protocolo Facultativo para a Convenção sobre os Direitos da Criança, tratando da venda de crianças, prostituição e pornografia infantis. Em seu preâmbulo, o Protocolo citou expressamente as conclusões da Conferência Internacional de Viena do ano anterior:

> Preocupados com a *crescente disponibilidade de pornografia infantil na Internet e em outras tecnologias modernas*, e relembrando a Conferência Internacional sobre o Combate à Pornografia Infantil na Internet (VIENA, 1999), em particular, sua conclusão, que *demanda a criminalização em todo o mundo da produção, distribuição, exportação, transmissão, importação, posse intencional e propaganda de pornografia infantil*, e enfatizando a importância de cooperação e parceria mais estreita entre governos e a indústria da Internet […] [grifos nossos].

A Internet desenvolveu-se de modo muito mais célere do que as figuras de repressão e meios de investigação. Fez-se necessário um adendo à Convenção sobre os Direitos da Criança para protegê-la adequadamente.

3.2 Século XXI

O novo século começou com a comunidade internacional debruçando-se sobre o abuso sexual das crianças. Segundo o UNICEF, as dez primeiras ratificações tornaram o Protocolo

[43] EUROPOL. Child Sexual Exploitation. *Fact Sheet 2011*, p. 3. Disponível em: <https://www.europol.europa.eu/.../child-sexual-exploitation-fact-sheet.pdf>. Acesso em: 17 mar. 2017. Redação original: "*Child Pornography on the Internet is a growing problem, and as more of the world comes online, it will continue to grow in the future since it does not know or respect borders*".

Facultativo válido desde 18 de janeiro de 2002. Atualmente, 117 Estados assinaram-no e 132 Estados ratificaram-no.

O Brasil depositou o instrumento de ratificação na Secretaria-Geral da Organização das Nações Unidas (ONU) em janeiro de 2004, o qual começou a vigorar no país a partir de 27 de fevereiro do mesmo ano[44]. No mês seguinte, o Decreto n.º 5.007, de 8 de março de 2004, aprovou o Protocolo Facultativo[45], indo ao encontro da Lei n.º 10.764/2003[46], que quatro meses antes arrefecera alguns crimes previstos no ECA, dentre eles o crime previsto no art. 241. A pena base de 1 (um) a 4 (quatro) anos de reclusão foi aumentada para 2 (dois) a 6 (seis) anos nas seguintes condutas:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.
>
> § 1º Incorre na mesma pena quem:
>
> I – agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;
>
> II – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo;
>
> III – assegura, por qualquer meio, o acesso, na rede mundial de computadores ou Internet, das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo.

[44] UNICEF. *Protocolo Facultativo para a Convenção sobre os Direitos da Criança sobre a venda de crianças, prostituição e pornografia infantis*. Disponível em: <https://www.unicef.org/brazil/pt/resources_10123.htm>. Acesso em: 10 fev. 2017.

[45] Decreto n.º 5.007, de 8 de março de 2004. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5007.htm>. Acesso em: 10 fev. 2017.

[46] Lei n.º 10.764, de 12 de novembro de 2003. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/2003/L10.764.htm>. Acesso em: 10 fev. 2017.

Além disso, a Lei n.º 10.764/2003 trouxe a figura qualificada no § 2º, aumentando a pena base de 2 (dois) para 3 (três) anos de reclusão no caso do agente que cometesse o crime prevalecendo-se do exercício de cargo ou função; ou ainda, se o agente cometesse o crime com o fim de obter vantagem patrimonial para si ou para outrem.

O Protocolo Facultativo à Convenção sobre os Direitos da Criança sobre a venda de crianças, prostituição e pornografia infantis, em seu art. 2º, dispôs que a pornografia infantil é *qualquer representação, por qualquer meio, de uma criança envolvida em atividades sexuais explícitas, reais ou simuladas, ou qualquer representação dos órgãos sexuais de uma criança para fins primordialmente sexuais.* O Protocolo enfatizou a mútua colaboração dos signatários na investigação e extradição dos casos envolvendo tais violências, e total atenção na reparação das crianças vitimadas.

3.3 Crimes de pedofilia na Internet – art. 241 do Estatuto da Criança e do Adolescente na atualidade

Muito embora a expressão "pedofilia na Internet" tenha sido incorporada informalmente entre os profissionais do Direito, do ponto de vista médico, o termo não é o mais adequado. Isso porque *pedofilia* é considerada uma doença pelo Manual Diagnóstico e Estatístico de Transtornos Mentais, DMS da Associação Psiquiátrica Americana, assim como previsto no CID 10 (Classificação Estatística Internacional de Doenças e Problemas Relacionados à Saúde) – F65.4[47].

De acordo com estudos médicos, o pedófilo é considerado doente, portanto inimputável sob a ótica do Direito Penal, a teor do art. 26 do Código Penal.

Diz-se que os verdadeiros *pedófilos* têm atração exclusiva por crianças, não mostrando nenhum interesse erótico/sexual

[47] MEDICINA NET. Disponível em: <http://www.medicinanet.com.br/cid10/1555/f65_transtornos_da_preferencia_sexual.htm>. Acesso em: 23 fev. 2017.

por adultos. Os abusadores infantis podem ou não ser pedófilos, já que existe a possibilidade de terem atração sexual apenas por crianças, ou pelos mais variados tipos humanos[48]. Daí por que, para não restar dúvidas, pode ser usado o termo *pedopedofilia*, como o fez o Vaticano em 2010[49], ou simplesmente *pornografia infantil*, como consta no manual sobre violência sexual do UNICEF (FIGUEIREDO; BOCHI, 2006, p. 58-59):

> A definição para esse termo é difícil porque os conceitos de criança e pornografia diferem de país para país e referenciam convicções morais, culturais, sexuais, sociais e religiosas que nem sempre se traduzem nas respectivas legislações. No entanto, atualmente a pornografia infantil é considerada pelos especialistas como "todo material audiovisual utilizando crianças num contexto sexual" ou, segundo a INTERPOL, é "a representação visual da exploração sexual de uma criança, concentrada na atividade sexual e nas partes genitais dessa criança". Para os especialistas participantes do Encontro sobre Pornografia Infantil na Internet, realizado em maio de 1999, em Lyon, na França, significa "uma exposição sexual de imagens de crianças, incluindo fotografias de sexo explícito, negativos, projeções, revistas, filmes, vídeos e discos de computadores". A produção pornográfica utilizando crianças e adolescentes constitui, portanto, exploração sexual, sendo que são considerados exploradores os produtores (fotógrafos e *videomakers*), os intermediários (aliciadores e pessoas de apoio), os difusores (anunciantes, comerciantes, publicitários) e os colecionadores ou consumidores do produto final. Os envolvidos, em sua grande maioria, são pedófilos. Mas entre os consumidores encontram-se também aqueles que, por já terem acesso a toda a gama de pornografia adulta, buscam material na produção que utiliza meninos e meninas.

Diante das discussões sociais sobre o tema, cinco anos depois da última alteração legislativa no ECA, em 25 de novembro de 2008, a Lei n.º 11.829 cindiu o art. 241 do Estatuto da Criança

[48] Disponível em: <http://www.abc.med.br/p/psicologia..47.psiquiatria/807419/principais+diferencas+entre+pedofilia+doenca+e+pedofilia+criminosa.htm>. Acesso em: 23 fev. 2017.

[49] Disponível em: <http://www.ilgiornale.it/news/vaticano-introdotto-reato-pedopornografia.html>. Acesso em: 23 fev. 2017.

e do Adolescente em *cinco tipos penais*, consoante evolução histórica prevista no quadro a seguir:

LEI e DATA	TIPO PENAL	PENA
Lei n.º 8.069, de 13 de julho de 1990	Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.	Reclusão de 1 a 4 anos
Lei n.º 10.764, de 12 de novembro de 2003	Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente. § 1º Incorre na mesma pena quem: I – agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo; II – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo; III – assegura, por qualquer meio, o acesso, na rede mundial de computadores ou Internet, às fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo.	Reclusão, de 2 a 6 anos, e multa
Lei n.º 10.764, de 12 de novembro de 2003	Acréscimo do § 2º – figura qualificada: I – se o agente comete o crime prevalecendo-se do exercício de cargo ou função; II – se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.	Reclusão, de 3 a 8 anos, e multa

Lei n.º 11.829, de 25 de novembro de 2008. Cindiu o art. 214 do ECA em 241, 241-A, 241-B, C, D e E	Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.	Reclusão, de 4 a 8 anos, e multa
	Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. § 1º Nas mesmas penas incorre quem: I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o *caput* deste artigo; II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o *caput* deste artigo.	Reclusão, de 3 a 6 anos, e multa
	Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.	Reclusão, de 1 a 4 anos, e multa

	Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual. Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga, por qualquer meio, adquire, possui ou armazena o material produzido na forma do *caput* deste artigo.	Reclusão, de 1 a 3 anos, e multa
	Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: Parágrafo único. Nas mesmas penas incorre quem: I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso; II – pratica as condutas descritas no *caput* deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.	Reclusão, de 1 a 3 anos, e multa
	Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.	

Vê-se, assim, que o comércio de fotos ou vídeos de pornografia infantil teve suas penas mínima e máxima aumentadas em dois anos, passando de 2 (dois) a 6 (seis) anos de reclusão para 4 (quatro) a 8 anos (oito). A pena mínima foi aumentada em um ano, passando-se de 2 (dois) anos de reclusão para 3 (três) anos, em caso de oferecimento, troca, disponibilização, transmissão, distribuição, publicação ou divulgação de conteúdos de pornografia infantil. O art. 241-B do ECA passou a criminalizar o "mero" arquivamento, posse e armazenamento de fotos ou vídeos de pornografia infantil. Por fim, o art. 241-C trouxe as figuras de montagem de vídeos e o derradeiro art. 241-D delimitou a figura do agente aliciador.

Parte da doutrina critica o art. 241-B. Segundo esse entendimento, o dispositivo legal estabeleceu uma "violação à liberdade de informação", criando um conceito exagerado de sociedade de risco e direito penal do inimigo através de uma presunção de periculosidade punível, pois a posse do material de pornografia infantil já é considerada como um crime de perigo abstrato (SYDOW, 2009, p. 54). O contraponto a essa percepção, a nosso ver, reside no bem jurídico penal tutelado, como veremos mais adiante.

Já o art. 241-C traz o chamado *cyberbullying* e também os casos em que o material pornográfico não é produzido com a participação de uma criança ou adolescente *diretamente*, mas sim por outros meios. Como exemplo, podemos citar filmes que se utilizam de adultos com aparência de criança, ou ainda, com o avanço da tecnologia, montagens de filmes e/ou fotos com crianças, cujo resultado final gere um material de pornografia infantil, estimulando-se a prática ilegal.

Por seu turno, o art. 241-D, a nosso ver, trouxe uma figura penal com uma pena de pouca relevância diante da gravidade dos fatos. O aliciador de menores neste caso é o grande pesadelo dos

pais: pessoas que se aproveitam do anonimato e das facilidades da Internet para invadir os lares alheios e assediar crianças[50].

Trata-se, como veremos a seguir, do tipo penal que mais se aproxima *fisicamente* das figuras penais do estupro de vulnerável. Analisando o *iter criminis*, percebe-se que a saúde mental da criança já está sendo afetada efetivamente e a incolumidade física da criança já pode estar em perigo iminente.

Assim, resta examinarmos qual é o bem jurídico a ser tutelado nos tipos penais previstos no art. 241, *caput*, e nos arts. 241-A, B, C e D do Estatuto da Criança e do Adolescente. SILVA (2017, p. 92-93) traz a opinião da doutrina sobre o assunto, separando-se um bem jurídico para os arts. 241 a 241-C, e outro para o art. 241-D para alguns autores e ele próprio. Assim, os arts. 241-A a 241-C tutelariam apenas a integridade[51] ou proteção à formação moral[52] de crianças e adolescentes, enquanto o art. 241-D se refere à proteção dos mesmos valores apenas em relação à criança. Outros autores citam o compromisso com a preservação dos direitos humanos[53], o respeito à imagem, à liberdade sexual e ao domínio

[50] Com a devida vênia, pensamos que não é o caso de considerarmos aqui a concorrência de culpas entre o ofensor e o genitor que não cumpriu com os deveres de cuidados com o seu filho, já que cabe aos pais restringir o uso da informática pelos filhos. SYDOW (2009, p. 56) afirma textualmente: "O art. 241-D também nos parece desvirtuar as funções do Direito Penal. Partindo-se da concepção de que a rede mundial de computadores é um ambiente de risco, assim como o mundo real, mas potencializado, cabe aos pais buscarem restringir o uso da informática quanto a seus filhos. Há notoriedade acerca do fato de que conteúdos pornográficos de todos os estilos permeiam a rede. Assim, a criança ou o adolescente que ingressa em ambientes de sexualidade exacerbada, como salas de bate-papo e comunidades virtuais, será, como qualquer outro usuário, assediado e instigado". Discordamos do referido autor porque, em primeiro lugar, o universo da Internet é imenso e inesgotável, o que torna bem difícil aos pais vigiar e proibir todos os passos da criança e do adolescente junto aos equipamentos de informática; em segundo lugar, o crime em exame, como veremos, é o que mais se aproxima do estupro de vulnerável.

[51] Entendimento de Válter Kenji Ishida, op. cit.

[52] Entendimento de Guilherme de Souza Nucci, op. cit.

[53] Entendimento de Ricardo Breier, op.cit.

do corpo da criança e do adolescente[54], e o livre desenvolvimento da personalidade[55].

Os crimes em comento são similares à relação entre roubo e furto e o crime de receptação. Pune-se principalmente, nas figuras do art. 241 a 241-B, a figura do *cliente* do material de abuso infantil.

Ainda que muitos filmes e fotos encontrados nos computadores apreendidos nos processos que versam sobre tais crimes sejam repetidos – alguns até já conhecidos previamente pela perícia técnica –, é fato inegável que *em algum momento e em algum lugar do mundo alguma criança foi abusada* para possibilitar a produção do material de conteúdo de pornografia infantil.

Voltando ao conceito amplo de vulnerabilidade da criança, deve-se relevar que, além da vulnerabilidade como indivíduo em formação, para servir de material de filmes e fotos envolvendo pornografia infantil, muitas crianças também sofrem de seríssimas vulnerabilidades familiares e sociais.

Cremos, assim, que o bem jurídico protegido é de fato a vulnerabilidade individual, integridade física, psíquica e moral da criança e do adolescente e a formação de sua personalidade.

Segundo JESUS e MILAGRE (2016, p. 49), os crimes previstos no ECA são os chamados crimes *informáticos*, pois preveem fato típico e antijurídico cometido por meio da tecnologia da informação, cujo bem ofendido já é protegido pelo Direito Penal.

O que os crimes informáticos têm em comum no que concerne ao bem jurídico protegido e às crianças que foram efetivamente violadas para a produção do material pornográfico é que elas jamais terão direito ao esquecimento. Essa é uma consequência muito triste e muito séria em relação a tais crimes.

[54] Entendimento de José Paulo Baltazar Junior, op. cit.

[55] Entendimento de Jorge de Figueiredo Dias, em comentário ao art. 172º do Código Penal Português, similar ao dispositivo do ECA em comento, op. cit.

Melhor dizendo, uma criança vítima de estupro de vulnerável poderá sofrer danos físicos, psíquicos e morais gravíssimos, mas, com o passar do tempo, ela pode optar por não contar a ninguém e não ter provas fotográficas ou em audiovisual do ato criminoso. Ao contrário, uma criança que foi vítima dos crimes previstos de todas as figuras típicas do art. 241 do ECA, e destas condutas resultou material de cunho pornográfico, terá esse material compartilhado na DeepWeb para todo o sempre, mesmo depois de adulta. É impossível fazer a gestão de propagação da Deep e da Dark Web. Diferentemente de ações judiciais contra a empresa Google, que pretendem o reconhecimento do direito ao esquecimento, um material colocado nas camadas mais profundas do *iceberg* da Internet *nunca mais poderá ser apagado*.

Assim, neste caso, deve ser acrescido ao bem jurídico protegido o direito à imagem do ser humano violado, já que, mesmo depois de adulto, ele poderá se deparar no futuro com as imagens de seu abuso.

3.4 Estupro de vulnerável

Vejamos, da mesma forma que analisamos o crime previsto no art. 241 do Estatuto da Criança e do Adolescente, a evolução do chamado "estupro de vulnerável":

LEI e DATA	TIPO PENAL	PENA
Redação original do CP	NÃO HAVIA.	
ECA, de 13 de julho de 1990, incluiu parágrafo único aos arts. 213 e 214	Se a ofendida é menor de 14 anos (estupro). Se o ofendido é menor de 14 anos (atentado violento ao pudor).	Reclusão de 4 a 10 anos Reclusão de 3 a 9 anos

Lei n.º 8.072, de 25 de julho de 1990	Tornou os crimes acima hediondos (art. 1º). Art. 6º. Aumentou a pena-base e igualou o estupro e o atentado violento ao pudor cometidos contra menores de 14 anos.	Reclusão de 6 a 10 anos
Lei n.º 12.015, de 7 de agosto de 2009. Diferenciou o estupro de criança e adolescentes	Acrescentou o § 1º ao art. 213: Se a vítima é menor de 18 ou maior de 14 anos. Criou o art. 217-A – Estupro de vulnerável (meninas e meninos): Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 anos. Estupro de vulnerável qualificado por lesão corporal grave (§ 3º). Estupro de vulnerável qualificado por morte (§ 3º).	Reclusão de 8 a 12 anos Reclusão de 8 a 15 anos Reclusão de 10 a 20 anos Reclusão de 12 a 30 anos

Percebe-se que, com o passar do tempo, o conceito de *vulnerabilidade* passou a integrar o tipo penal, repassando-se ao Judiciário a responsabilidade de analisá-la no caso concreto em alguns casos. Porém, verificamos que a vulnerabilidade infantojuvenil não pode ser vista isoladamente.

Em outras palavras, a vulnerabilidade da criança como indivíduo singular, e de acordo com a sua maturidade, é presunção absoluta da lei, já que, por ser criança, ela pode não ter condição de distinguir ou conseguir se defender de ataques sexuais.

Aprofundando, verifica-se que infelizmente é muito comum crianças estarem envolvidas também em situação de vulnerabilidade do grupo familiar (PETTENGIL, 2003)[56].

[56] Várias pesquisas citam que é muito comum a proximidade do agressor com a vítima, inclusive dentro do seio familiar. Nesse sentido, ROMERO (2007, p. 16 e 33) afirmou: "MEICHENBAUM (1994) revela em seu estudo que nos Estados Unidos o padrasto é o maior agressor das meninas, sendo que,

Por fim, têm-se também, somando-se às vulnerabilidades individuais e familiares da criança e do adolescente, muitos casos de vulnerabilidade social (TELLES, SUGUIHIRO e BARROS, 2011), ou seja, crianças em situação de desamparo total do Estado: sem escola, morando na rua e muitas vezes fazendo uso de drogas e outras substâncias nocivas (RIZZINI et al., 2010).

3.5 Contexto conjunto dos crimes envolvendo a *vulnerabilidade sexual* de crianças e adolescentes

Vimos, assim, separadamente os crimes previstos no Estatuto da Criança e do Adolescente e os crimes previstos no Código Penal, mas todos se referindo à vulnerabilidade sexual de crianças e adolescentes.

O bem jurídico a ser protegido, em última análise, é o bem-estar dos menores e sua incolumidade física e mental. O que varia entre tais crimes é, então, a *proximidade* do agente em relação à vítima, e, por aí, vê-se em escala crescente uma pena maior para aqueles que chegaram mais perto das vítimas: quanto maior a aproximação e violação, maior a pena. A situação poderia ser resumida da forma *crescente*, como exposta no quadro a seguir.

---

no Brasil, SAFFIOTI (1997) identifica o pai biológico como o principal agressor". A Autora trouxe ainda o triste aspecto do *complô do silêncio*, muito comum dentro da estrutura familiar nos casos de abuso sexual infantil: "Outro aspecto que contribui para a manutenção do abuso sexual no seio da família é o dito 'complô do silêncio', que pode ser entendido como o silêncio mantido tanto pelos agentes das agressões quanto pelos vitimizados, assim como pelos demais membros da família. O complô do silêncio pode perpetrar o abuso por várias gerações até que seja interrompido. De acordo com SCODELARIO (2002), as razões para a manutenção desse complô estão relacionadas a várias possibilidades. No caso do silêncio do cônjuge não agressor, encontramos algumas situações: medo do perpetrador, desejo de manutenção da unidade familiar, não aceitação da provável perda do companheiro, cumplicidade inconsciente que ocorre através da identificação com o agressor e da fragilidade no que tange ao papel de protetor. Já no caso do silêncio da criança vítima, encontramos sentimentos de desproteção, temor de perder o afeto do agressor, receio de ser desacreditada e julgada culpada, medo de sofrer agressões ou ser retirada da família. Quanto maior a proximidade com o agressor (o pai biológico, por exemplo), mais a criança se cala".

TIPO PENAL	SUJEITO ATIVO	PENA
Art. 241-B do ECA	O *voyeur*, pessoa que solitariamente guarda, observa as fotos e assiste aos vídeos.	Reclusão de 1 a 4 anos
Art. 241-A do ECA	Apreciador de pornografia infantil que age anonimamente ou não interage com outros de gosto semelhante.	Reclusão de 3 a 6 anos
Art. 241-C do ECA	Aquele que simula, monta, modifica e adultera imagens; *cyberbullying*.	Reclusão de 1 a 3 anos
Art. 241-D do ECA	Aquele que alicia, assedia, instiga e constrange crianças e adolescentes à prática de sexo virtual, ou se exibe de forma pornográfica ou sexualmente explícita; e/ou facilita ou induz o acesso à criança de material pornográfico ou contendo sexo explícito.	Reclusão de 1 a 3 anos
Art. 217-A, *caput*, do CP	Aquele que chega às vias de fato: pratica conjunção carnal ou outro ato libidinoso com menor de 14 anos.	Reclusão de 8 a 15 anos
	Aquele que, além de estuprar (ou em decorrência do estupro), causa lesão corporal grave na vítima.	Reclusão de 10 a 20 anos
	Aquele que, além de estuprar (ou em decorrência do estupro), mata a vítima.	Reclusão de 12 a 30 anos

Prezando pela proporcionalidade, a quantidade da pena imposta deve obviamente ser maior quanto mais perto o sujeito ativo se aproximar da lesão ao bem jurídico protegido pela lei penal. Porém, verificamos que, no caso do art. 241-D, ou seja, do aliciador de menores na Internet, a pena ainda é muito branda, considerando a proporção crescente entre proximidade do bem jurídico tutelado e quantidade de pena prevista para o crime, conforme mostra o gráfico a seguir.

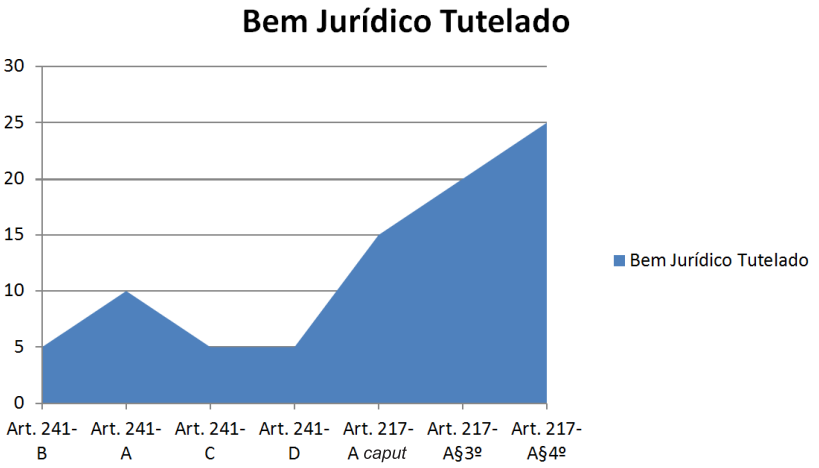

Gráfico 1: Evolução da quantidade da pena de acordo com a aproximação do sujeito ativo com a vítima.
Fonte: Gráfico elaborado pela Autora.

Observando o gráfico, fica mais fácil perceber que, passando pelo *voyeur* (art. 241-B do ECA) e seguindo para o "compartilhador" (art. 241-B do ECA), a pena prevista aumenta. Depois, a pena de reclusão prevista diminui para aquele que altera e modifica imagens (*cyberbullying*, manipulador digital – art. 241-C do ECA) e para o aliciador de sexo virtual, de *striptease* ou que, de alguma forma, insere virtualmente pornografia infantil para a vítima. O gráfico de proporção entre bem jurídico tutelado e pena *in abstrato* volta a subir quando o sujeito ativo realmente chega às vias de fato através das figuras típicas do art. 217-A, *caput,* §§ 3º e 4º do Código Penal.

Percebe-se aqui que houve um lapso do legislador, subestimando a atividade do aliciador digital de crianças e adolescentes. A criança atrás do computador continua sendo uma criança com vulnerabilidades: de indivíduo em processo de maturação e talvez vulnerabilidade familiar. Mesmo colocando

inúmeros filtros ou fiscalizando, a evolução da Internet – com vários patamares de profundidade e aperfeiçoamento – permite que o aliciador digital consiga sem grandes dificuldades aliciar e instigar crianças e adolescentes. O crime demanda maior atenção da sociedade como um todo.

A informática é o grande meio de aliciamento e comunicação entre o crime organizado de exploração sexual infantil, conforme dados do UNICEF (FIGUEIREDO e BOCHI, 2006, p. 62):

> Ainda conforme a PESTRAF [Pesquisa sobre Tráfico de Mulheres, Crianças e Adolescentes para Fins de Exploração Sexual Comercial no Brasil], de um universo de 161 aliciadores detectados, 109 eram brasileiros e 52 estrangeiros (provenientes da Espanha, Holanda, Venezuela, Paraguai, Alemanha, França, Itália, Portugal, China, Israel, Bélgica, Rússia, Polônia, Estados Unidos e Suíça). A maior parte dos aliciadores é formada por homens (59%), sendo 41% mulheres. A pesquisa mostrou ainda que a exploração e o tráfico para fins sexuais estão organizados em sofisticadas redes. Essas redes funcionam com a participação de diversos atores que desempenham diferentes funções (aliciadores, proprietários, empregados e outros tipos de intermediário), com o objetivo de explorar para obter algum bem material ou lucro. De modo geral, elas se escondem sob as fachadas de empresas comerciais (legais e ilegais), voltadas para o ramo do turismo, do entretenimento, do transporte, da moda, da indústria cultural e pornográfica, das agências de serviços (massagens, acompanhantes, etc.), dentre outros mercados que facilitam a prática do tráfico para fins de exploração sexual comercial. *As redes de tráfico também estão respaldadas pelo uso da tecnologia, o que facilita o sistema de informação entre elas, o aliciamento, o transporte, o alojamento, a vigilância e o controle de suas ações. Portanto, elas podem estruturar-se e desmobilizar-se com tremenda agilidade*. Cabe ressaltar ainda que as redes estão organizadas dentro e fora do Brasil, mantendo relações com o mercado do crime organizado internacional. [Grifo nosso]

4 Crimes envolvendo a vulnerabilidade sexual de crianças e adolescentes e perfil do sujeito ativo

Neste estudo, chamamos a atenção para quatro fatores em especial:

a) precisamos entender melhor o extenso mundo e linguagem da Internet;

b) necessitamos examinar mais conjuntamente os crimes que envolvem a vulnerabilidade sexual da criança e do adolescente previstos separadamente no Estatuto da Criança e do Adolescente e no Código Penal;

c) os perfis dos sujeitos ativos não são estanques e previsíveis, devendo-se preservar também a integridade física e psíquica da vítima e sua imagem; e

d) o legislador precisaria atentar mais para o crime previsto no art. 241-D do ECA e a proporcionalidade de seu preceito secundário em relação aos demais crimes que envolvam a vulnerabilidade sexual da criança e do adolescente.

É importante, assim, atentarmos para o fato de que a doutrina agora começa a se debruçar sobre a criminologia do sujeito ativo dos crimes em estudo.

Em relação aos crimes praticados pela Internet, pode-se pensar apenas nos chamados *voyeurs*, como também em pessoas que usam a rede mundial de computadores como ato preparatório para futuras violações físicas.

Conforme já explanou SANTOS ALMEIDA (2014, p. 92-93):

> De um modo geral, os consumidores de pornografia infantil também compram tais imagens para facilitar o contato *on-line* e *off-line* com as crianças. Às vezes, eles mesmos produzem o material, tanto de forma virtual (*v.g.* capturando a imagem da criança que se exibe pela *webcam*), quanto durante um contato real e *off-line*. Mas, até onde se sabe, entre as pessoas que usam a Internet para

> fins sexuais, há mais quem compre do que quem produza essas imagens pornográficas. Com base nisso, seria possível distinguir ao menos dois tipos de pornógrafos com interesse em crianças: aqueles que fazem o *download* de imagens quando não têm a possibilidade de abusar efetivamente de uma criança (ou quando não têm esta intenção); e aqueles que usam a Internet para expressar as suas fantasias inibidas pelas regras sociais (produzindo este material, por exemplo). Entretanto, é claro que uma distinção dicotômica e reducionista como esta não seria suficiente, já que o envolvimento com a pornografia infantil pode se dar de outras formas, concomitantemente, inclusive.

O *Federal Bureau of Prisons, Sex Offender Certification Review Branch,* em Washington, D.C., estudou dados do Sistema de Justiça Criminal para comparar dois grupos de agressores sexuais. Nesta pesquisa, o critério divisor foi justamente a proximidade e o contato físico com a vítima. Delimitou-se, assim, o *child pornography offender* (agressor virtual), que nunca teve contato com as vítimas, e o *child contact sex offender* (agressor físico), aquele que consome pornografia virtual e buscou contato com as vítimas (DIAS, apud SILVA, 2017, p. 198).

Precisamos pensar melhor no estudo holístico de todos os crimes envolvendo a vulnerabilidade sexual infantil, sem procurar encaixar o sujeito ativo em um perfil criminológico estanque. Ao invés, devemos buscar a proporcionalidade dos crimes em relação à menor e à maior aproximação, e danos, com as vítimas.

5 Conclusão

Vimos que a Internet é um universo muito maior e mais complexo do que concebemos na nossa vida diária em aplicativos, redes sociais e buscas no Google. A partir daí, a Internet em suas camadas mais profundas (Deep Web) **é o meio ideal tanto para a prática** quanto para a perpetuação de delitos e suas consequências.

Cabe, assim, aos profissionais do Direito se afeiçoarem com os novos termos técnicos e os meandros da Internet para entender o novo Direito Penal cibernético e seus resultados.

Os crimes que envolvem pornografia infantil e abuso sexual infantil devem ser vistos sob o mesmo enfoque: a proteção da vulnerabilidade sexual infantil presumida como absoluta, já que se trata de indivíduo em processo de amadurecimento. Mesmo assim, algumas crianças têm vulnerabilidades maiores, envolvendo a questão da vulnerabilidade familiar e social.

Os crimes que preveem violação à vulnerabilidade sexual infantil estão divididos de acordo com a maior ou menor aproximação da vítima, separando-se os crimes cibernéticos envolvendo pornografia infantil no Estatuto da Criança e do Adolescente e os crimes envolvendo abuso sexual infantil físico no Código Penal. Percebe-se que, mesmo que o sujeito ativo nunca tenha se aproximado fisicamente de uma criança com o fim de cometer abuso sexual, ao consumir o material virtual de pornografia infantil, já contribui para que a indústria da pornografia e abuso infantil aumente e se propague. E, diante da característica perpetuadora *ad infinitum* e do conteúdo "supercriptografado" da Deep Web, as imagens da violação sexual infantil não estão sujeitas ao esquecimento.

Não só isso, a Internet mostra-se cada vez mais um componente aproximador da vítima com o sujeito ativo dos delitos, motivo pelo qual este critério foi eleito como norteador do estudo da proporcionalidade das penas de todos os delitos.

O parâmetro da proximidade entre vítima e sujeito ativo foi escolhido também pelo fato de que a criminologia está começando a se debruçar sobre o perfil dos sujeitos ativos dos delitos, separando-os a princípio em uma visão reducionista entre agressores virtuais e agressores físicos. Mas esta é uma visão simplista; é a ponta de outro *iceberg*. A pedofilia é vista como uma doença, do ponto de vista médico, quando o ser humano tem atração sexual tão somente por crianças, mas os agressores não se resumem a esse modo de agir. O perfil dos agressores deve ser mais bem estudado e aprofundado

para servir de parâmetro de repressão criminal, tanto em relação ao combate aos crimes, como a tratamentos corretos.

A Internet cada vez mais facilita a reunião de apreciadores de pornografia infantil, perpetua e redistribui infinitamente imagens e vídeos de pornografia infantil, arregimenta organizações criminosas, e, também, é o espaço ideal de aproximação de agressores e vítimas em potencial.

Neste passo, comparamos os preceitos secundários de todos os tipos penais do Estatuto da Criança e do Adolescente e do Código Penal e concluímos que há uma discrepância na pena prevista para o delito do art. 241-D do ECA: a figura do aliciador virtual que ardilosamente usa a Internet para se aproximar da vítima.

O legislador subestimou o sujeito ativo que rompe eventual rede de proteção familiar e busca crianças externas a seu mundo social. Ele introduz a criança precocemente à sexualidade, dentro de fantasias e realidade incompatíveis com sua maturação física e psíquica. As consequências podem ser nefastas para a criança e a família aliciada, sem prejuízo de crimes mais graves que possam resultar desta aproximação. Daí por que concluímos que a pena prevista para este delito deveria ser majorada, tornando a aproximação vítima/sujeito ativo um gráfico crescente para a reprimenda penal.

Referências bibliográficas

ALMEIDA, Jéssica Pascoal Santos. *Pedofilia*: aspectos clínicos, éticos e forenses. Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de São Paulo. São Paulo, 2014, p. 92-93. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2136/tde-03082015-115519/pt-br.php>. Acesso em: 23 fev. 2017.

ASSANGE, Julian. *Cypherpunks*: liberdade e o futuro da Internet. São Paulo: Boitempo, 2013.

BRASIL. Constituição da República Federativa do Brasil, promulgada em 5 de outubro de 1988. Disponível em: <http://www2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-publicacaooriginal-1-pl.html>. Acesso em: 10 fev. 2017.

___. Decreto n.º 5.007, de 8 de março de 2004. *Diário Oficial da União,* p. 4, 9 mar. 2004. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5007.htm>. Acesso em: 10 fev. 2017.

___. Decreto n.º 99.710, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança. *Diário Oficial da União,* p. 2, 22 nov. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D99710.htm>. Acesso em: 10 fev. 2017.

___. Lei n.º 10.764, de 12 de novembro de 2003. *Diário Oficial da União,* p. 1, 13 nov. 2003. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/2003/L10.764.htm>. Acesso em: 10 fev. 2017.

___. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. *Roteiro de atuação sobre crimes cibernéticos.* 3. ed. rev. e ampl. Brasília/DF, 2016. v. 5. (Série Roteiros de Atuação.)

EUROPOL. Child Sexual Exploitation. *Fact Sheet 2011*, p. 3. Disponível em: <https://www.europol.europa.eu/.../child-sexual-exploitation-fact-sheet.pdf>. Acesso em: 17 mar. 2017.

FIGUEIREDO, K.; BOCHI, S. *Violência sexual*: um fenômeno complexo. UNICEF, p. 58-59. Disponível em: <https://www.unicef.org/brazil/pt/Cap_03.pdf>. Acesso em: 23 fev. 2017.

JESUS, Damásio de; MILAGRE, José Antonio. *Manual de crimes informáticos.* São Paulo: Saraiva, 2016.

MEDICINA NET. Disponível em: <http://www.medicinanet.com.br/cid10/1555/f65_transtornos_da_preferencia_sexual.htm>. Acesso em: 23 fev. 2017.

O GLOBO. *Grupo de hackers Anonymous mira expor redes internacionais de pedofilia.* Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/grupo-de-hackers-anonymous-mira-expor-redes-internacionais-de-pedofilia-15128693>. Acesso em: 14 fev. 2017.

ORWELL, George. *1984.* São Paulo: Schwarcz, 2014.

PETTENGILL, Myriam Aparecida Mandetta. *Vulnerabilidade da família: desenvolvimento do conceito.* Tese apresentada à Escola de Enfermagem da Universidade de São Paulo. São Paulo, 2003. Disponível em: <www.teses.usp.br/teses/disponiveis/7/7136/tde-16092009.../Myriam_Pettengill.pdf>. Acesso em: 22 fev. 2017.

RIZZINI, Irene et al. *Crianças e adolescentes com direitos violados*: situação de rua e indicadores de vulnerabilidade no Brasil urbano. Rio de Janeiro, CIESPI – Centro Internacional de Estudos e Pesquisas sobre a Infância/PUC-Rio, 2010. Disponível em: <http://sistemas.tjam.jus.br/coij/wp-content/uploads/2014/06/CriancasAdolescentesDireitosViolados.pdf>. Acesso em: 22 fev. 2017.

ROMERO, Karen Richter Pereira dos Santos. *Crianças vítimas de abuso sexual: aspectos psicológicos da dinâmica familiar.* Curitiba: Ministério Público do Estado do Paraná, Centro de Apoio Operacional das Promotorias da Criança e do Adolescente, 2007. p. 16 e 33. Disponível em: <http://www.crianca.mppr.mp.br/arquivos/File/publi/caopca/vitimas_de_abuso.pdf>. Acesso em: 6 mar. 2017.

SAFERNET: quem somos. Disponível em: <http://www.safernet.org.br/site/institucional>. Acesso em: 14 fev. 2017.

SILVA, Ângelo Roberto Ilha da (Org). *Crimes cibernéticos.* Porto Alegre: Liv. do Advogado, 2017. p. 260-261.

SYDOW, Spencer Toth. “Pedofilia virtual” e as considerações críticas sobre a Lei 11.829/08. *Revista Liberdades*, São Paulo, n.1, p. 54 , maio-ago. 2009.

TECHTUDO. *Internet completa 44 anos; relembre a história da web.* Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html>. Acesso em: 10 fev. 2017.

TELLES, Tiago Santos; SUGUIHIRO, Vera Lucia Tieko; BARROS, Mari Nilza Ferrari de. Os direitos de crianças e adolescentes na perspectiva orçamentária. Revista *Serviço Social & Sociedade*, São Paulo, n. 105, p. 50-66, jan.-mar. 2011. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-66282011000100004>. Acesso em: 22 fev. 2017.

UNICEF. *Convenção sobre os Direitos da Criança*. Disponível em: <https://www.unicef.org/brazil/pt/resources_10120.htm>. Acesso em: 10 fev. 2017.

___. *Protocolo Facultativo para a Convenção sobre os Direitos da Criança sobre a venda de crianças, prostituição e pornografia infantis*. Disponível em: <https://www.unicef.org/brazil/pt/resources_10123.htm>. Acesso em: 10 fev. 2017.

O perigo por trás dos compartilhadores e detentores de arquivos de pornografia infantil

Guilherme Barby Simão*

RESUMO

Este artigo tem por finalidade alertar sobre o alto grau de periculosidade que indivíduos acusados de posse, ou compartilhamento de arquivos de pornografia infantil, podem apresentar para crianças e adolescentes à sua volta. Será demonstrado um caso real, acompanhado por este signatário no trabalho de inteligência da Polícia Federal, no ambiente virtual denominado Deep Web ou "Internet Profunda". Será exposto também o paradoxo comportamental apresentado por esses acusados, antes e depois de suas transgressões tornarem-se públicas, o que vem auxiliando na formação da errônea convicção de que tais indivíduos não ostentam relevante grau de periculosidade.

Palavras-chave: Pornografia infantil. Deep Web. Polícia Federal.

ABSTRACT

The proposal of this article is to alert about the dangerousness that individuals accused of possessing or sharing child pornography files may present to children and adolescents around them. The article describes a real case in the virtual environment "Deep Web" followed by this signatory as part of the intelligence work of the Federal Police. It also discusses the behavioral paradox displayed by the accused before and after their transgressions become public, which has been contributing to create the erroneous conviction that they do not represent a relevant degree of dangerousness.

***Keywords**: Child pornography. Deep Web. Federal Police.*

* Graduado em Processamento de Dados pela FATEC/SP. Escrivão de Polícia Federal. Analista do Núcleo de Inteligência do Grupo de Repressão a Crimes Cibernéticos de São Paulo (GRCC-SP). *E-mail*: guilherme.gbs@dpf.gov.br.

1 Introdução

Nos dias de hoje, com o advento da Internet, das facilidades de comunicação que ela proporciona e, mais especificamente, do ambiente virtual denominado Deep Web, é crescente a disseminação de conteúdos pornográficos infantis. Por consequência, cresce também o número de indivíduos compartilhadores e detentores de arquivos desse teor.

Como é de conhecimento amplo entre os estudiosos da área jurídica, são distintos, e de penas variadas, os crimes de compartilhamento e posse de arquivos de pornografia infantil (arts. 241-A e 241-B, Lei n.º 8.069/90), e o de estupro de vulnerável em si (art. 217-A, Código Penal). Os primeiros, além de possuírem menor reprovabilidade e penas mais baixas, são crimes com maior facilidade de elucidação, em comparação ao último citado. Ou seja, é mais fácil identificar um indivíduo que compartilha ou possui arquivos de pornografia infantil do que um abusador de menores.

Conforme orientam PFEIFFER e SALVAGNI (2005), os casos de abuso sexual na infância e na adolescência são de difícil suspeita e complicada confirmação. São praticados, na sua maioria, por pessoas ligadas diretamente às vítimas e sobre as quais exercem alguma forma de poder ou dependência. As referidas autoras também alertam que o abuso nem sempre vem acompanhado de violência física aparente, podendo se apresentar de várias formas e níveis de gravidade. Isso dificulta enormemente a possibilidade de denúncia pela vítima e a confirmação diagnóstica pelos meios hoje oferecidos pelas medidas legais de averiguação do crime.

Ademais, pela prática policial vivenciada por este signatário, foi possível constatar que os acusados dos crimes de posse ou compartilhamento de arquivos de pornografia infantil apresentam um evidente paradoxo comportamental. Mostram-se extremamente inofensivos na oitiva policial e no interrogatório judicial, o que diverge sobremaneira do apresentado em seus

relacionamentos com crianças, adolescentes, ou outros criminosos, antes de suas transgressões tornarem-se conhecidas.

Tudo isso faz com que seja criada erroneamente a ideia de que estamos lidando com dois grupos de indivíduos diversos:

1) aqueles que apenas compartilham ou armazenam arquivos de pornografia infantil, não representando risco real a crianças em seu convívio;

2) aqueles que abusam de menores e sentem-se atraídos por crianças à sua volta.

Assim, tem-se como objetivo principal deste artigo desmistificar a ideia de que são diversos os dois grupos de criminosos acima apresentados. Será demonstrado através de estudos e, principalmente, da prática policial vivenciada no combate a crimes cibernéticos e de pornografia infantil, que os indivíduos que compartilham ou armazenam arquivos de reportado teor são os mesmos que abusam e se sentem atraídos por crianças à sua volta. Será exibido também um caso real, acompanhado por este signatário no trabalho de inteligência da Polícia Federal, no ambiente virtual denominado Deep Web, bem como uma maior explanação do paradoxo comportamental supracitado.

2 A Deep Web

A Deep Web, ou "Internet Profunda", compreende grande parte do mundo cibernético em que são hospedados anonimamente *sites* que não podem ser detectados pelos tradicionais mecanismos de busca, como o Google. Tais *sites* necessitam de aplicativos específicos para o seu acesso, como o *Tor Browser*[1].

O objetivo primordial desse ambiente é o anonimato, tanto para quem hospeda determinado conteúdo como para o usuário que o acessa. Isso faz com que a Deep Web se torne

[1] *Tor Browser* é um aplicativo que se utiliza de técnicas computacionais para "mascarar" o real IP do usuário e, consequentemente, a sua identificação.

extremamente atrativa para diversos tipos de criminosos de todas as partes do mundo.

Podemos imaginar o mundo virtual como um grande *iceberg*, no qual a Internet tradicional que conhecemos, denominada Surface Web, é representada pela parte visível e superior desse *iceberg*, e a Deep Web, pela parte oculta.

Segundo HARADA (2015):

> Quanto ao seu tamanho, estudos estimam que a Deep Web seja 500 vezes maior que a Surface Web. Especula-se também que a parte da Internet que exploramos todos os dias compreende apenas 4% do todo – o restante pertence à porção submersa do *iceberg*.

Em razão da grande diversidade disponibilizada, não há como explanar todo tipo de conteúdo que pode ser encontrado na Deep Web. Comércio ilegal de drogas, armas, órgãos e pessoas, contratação de matadores de aluguel, transmissão ao vivo de tortura e estupro, técnicas *hackers*, bem como pornografia infantil, são alguns dos exemplos.

2.1 Caso real na Deep Web

Ao longo dos últimos anos, com a vivência do trabalho de inteligência policial na Deep Web e em outros ambientes cibernéticos, pude acompanhar a ação de diversos criminosos amantes da pornografia infantil. Aqui se incluem os compartilhadores de arquivos, bem como os que apenas frequentam grupos e fóruns dedicados a esse tipo de conteúdo.

Um fato inusitado, e digno de atenção, é que a maior parte desses infratores relatou algum tipo de abuso a crianças ou adolescentes, ou demonstrou, visivelmente, o seu desejo por tal prática. Os abusos declarados variavam desde um simples toque, despercebido, no corpo da criança, até mesmo a própria conjunção carnal ou coito anal.

Um dos casos que aqui merecem destaque foi encontrado em um famoso fórum brasileiro de pornografia infantil da Deep Web denominado "Anjos Proibidos". Lá foi possível acompanhar a ação de um dos condenados na *Operação Darknet* da Polícia Federal, deflagrada no ano de 2014, com o intuito de combater crimes relacionados à pornografia infantil.

Primeiramente, ressalto que o fórum "Anjos Proibidos" é acessado exclusivamente por amantes da pornografia infantil e dedicado à troca de arquivos e informações relacionadas a esse tipo de conteúdo ilícito. O ambiente atrai criminosos com interesse na filosofia "*BL – Boy Lover*", ou seja, pessoas com interesses sexuais em crianças do sexo masculino.

No referido fórum, em janeiro de 2016, foi aberto um tópico exclusivo para divulgação de informações relacionadas à *Operação Darknet*, chamado de "Operação Darknet 2014, lembram ?", cujo propósito era o compartilhamento de conhecimentos entre os criminosos, com o fim de alertar todos sobre as formas de prevenção contra novas investigações de combate à pornografia infantil da Polícia Federal, conforme ilustra a Figura 1 a seguir:

Figura 1: Mensagem de abertura do tópico "Operação Darknet 2014, lembram ?".
Fonte: Disponível em: <http://anjosp2t7yv47qvc.onion>. Acesso em: 14 abr. 2016.

Em fevereiro do mesmo ano, em uma das respostas à discussão aberta, houve manifestação de um dos presos da *Operação Darknet*, de codinome "henrique", conforme demonstra a Figura 2:

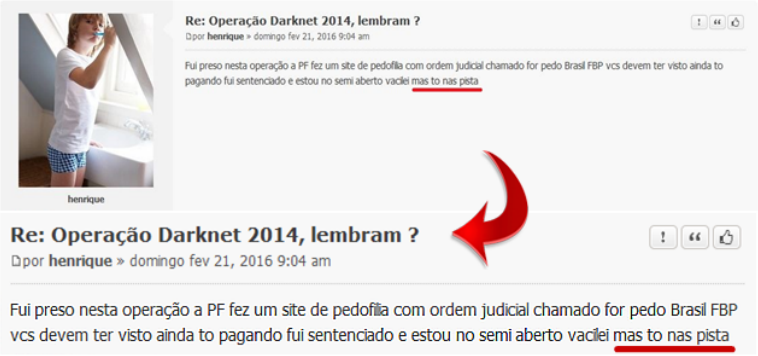

Figura 2: Resposta de um dos presos na "Operação Darknet" da Polícia Federal.
Fonte: Disponível em: <http://anjosp2t7yv47qvc.onion>. Acesso em: 14 abr. 2016.

Como pôde ser observado, "henrique" assevera claramente que possuía conhecimento da aludida operação e explica aos demais usuários a forma de investigação utilizada pela Polícia Federal no caso. Além disso, tal usuário deixa claro que, mesmo após sua condenação, "continua na pista", gerando a ideia de que continua cometendo ilícitos penais.

Por meio de técnicas investigativas e após certo período de colheita de informações do criminoso, foi possível constatar que "henrique" foi condenado pelos crimes dos arts. 241-A e/ou 241-B do Estatuto da Criança e do Adolescente.

Então, no exemplo em tela, temos um criminoso que muitas vezes é visto como um indivíduo de baixo grau de periculosidade, ou seja, condenado apenas pelos crimes de posse e/ou compartilhamento de arquivos contendo imagens eróticas e de sexo explícito envolvendo crianças e adolescentes.

Contrapondo a ideia dessa baixa periculosidade, é possível visualizar na sequência um tópico aberto em março de 2016 por

este mesmo usuário de codinome "henrique", intitulado "como vocês agem quando estão com um lekinho", conforme ilustra a Figura 3:

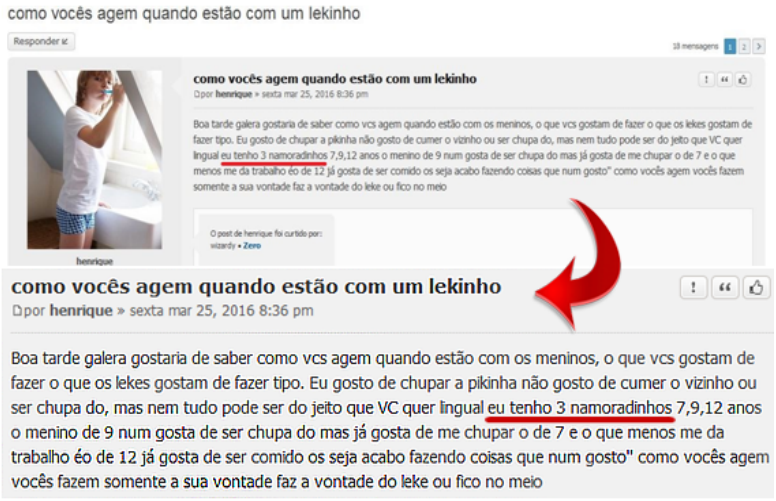

Figura 3: Declaração do usuário "henrique" contendo informações de abusos reais. Fonte: Disponível em: <http://anjosp2t7yv47qvc.onion>. Acesso em: 14 abr. 2016.

O aludido tópico foi aberto por "henrique" com o propósito de trocar experiências e informações sobre a prática de atos de abuso sexual infantil. O criminoso é enfático ao declarar que abusa constantemente de três crianças [!], inclusive expondo os detalhes dos atos sexuais que pratica com cada uma delas.

Em diálogos posteriores, o criminoso confirma que nunca houve quem desconfiasse dos abusos por ele praticados, e que as crianças violentadas são de sua "total confiança", filhos de pessoas próximas a ele.

Cumpre destacar que, pela experiência adquirida na prática policial, bem como em cursos ministrados por polícias de outros países que atuam no combate à pornografia infantil, pude constatar que grande parte dos criminosos que possuem ou compartilham

esse tipo de arquivo, de certa forma, já abusaram de alguma criança ou adolescente, ou estão apenas aguardando a "oportunidade ideal" para que isso aconteça. Essa oportunidade ideal pode ser entendida como o desenvolvimento de um relacionamento de confiança e proximidade com as crianças, ou mesmo com os responsáveis diretos por elas, se estes não forem os próprios abusadores.

O abuso sexual de crianças ainda pode ser observado como um tópico complexo e difícil, tanto na investigação como na sua compreensão, para profissionais e pesquisadores (MALGARIM; BENETTI, 2010). Como o crime de estupro de vulnerável é mais difícil de ser elucidado, muitos acusados por posse ou compartilhamento de pornografia infantil são tratados erroneamente como inofensivos.

Uma prática muito comum e perigosa, que vem sendo observada, é a soltura quase imediata desses criminosos, nos casos de prisão em flagrante pelo crime do art. 241-B da Lei n.º 8.069/90. Em muitos desses casos, as fianças são reduzidas, ou mesmo retiradas, voltando o indivíduo a ser uma ameaça para crianças e adolescentes à sua volta.

3 O paradoxo comportamental

Um dos fatores que mais contribuem para a errônea convicção de que os acusados de compartilhamento ou posse de arquivos de pornografia infantil são de baixa periculosidade é o comportamento apresentado por eles após suas transgressões tornarem-se públicas. Este comportamento mostra-se muito divergente do constatado na fase de investigação.

Ao longo do trabalho de inteligência policial no combate a crimes cibernéticos e de pornografia infantil, pude constatar que esses infratores têm total consciência de que os atos por eles praticados são extremamente repudiados pela sociedade. Mas também possuem o discernimento de que os crimes de

compartilhamento e, principalmente, o de posse de arquivos de pornografia infantil apresentam menor reprovabilidade e penas mais baixas, se comparados ao de estupro de vulnerável.

Nesse sentido, foi realizado um estudo de comportamento que levou em conta uma amostra de criminosos investigados pela Polícia Federal e acusados pelos crimes dos arts. 241-A e/ou 241-B da Lei n.º 8.069/90, no ano de 2016.

Diferente do encontrado predominantemente em fases investigativas, o padrão observado nas declarações colhidas em entrevistas informais, oitivas policiais e interrogatórios judiciais foi o de que:

a) nunca abusaram de uma criança;

b) jamais abusariam de uma criança;

c) não se sentem atraídos por crianças à sua volta;

d) possuem arquivos apenas por curiosidade ou por engano;

e) sabem que é errado ter arquivos de pornografia infantil e por isso já haviam decidido parar com essa prática;

f) não se lembram de terem compartilhado arquivos deste teor.

Diante do exposto, é inequívoco que os acusados se mostram como pessoas inofensivas, que não representam risco real para crianças e adolescentes à sua volta, contrapondo o que foi verificado na fase investigativa.

Para SILVA (2008), pedófilos podem ser considerados como psicopatas. A referida autora ainda explica que, em geral, os psicopatas são indivíduos frios, calculistas, inescrupulosos, dissimulados, mentirosos [!], sedutores e que visam apenas ao próprio benefício.

Para que fique evidente a diferença de comportamento apresentada por esses indivíduos, as Figuras 4 e 5, a seguir, contêm declarações reais de um dos criminosos observados na análise,

colhidas em ambiente virtual, em datas diversas, anteriores à sua prisão em flagrante por posse de arquivos de pornografia infantil:

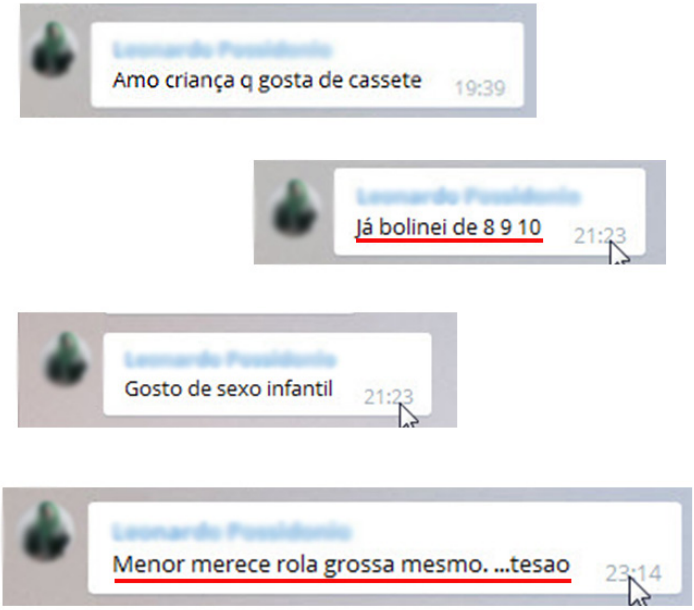

Figura 4: Declarações reais de criminoso em dias e horários diversos.
Fonte: Grupo de Mensageria Instantânea.

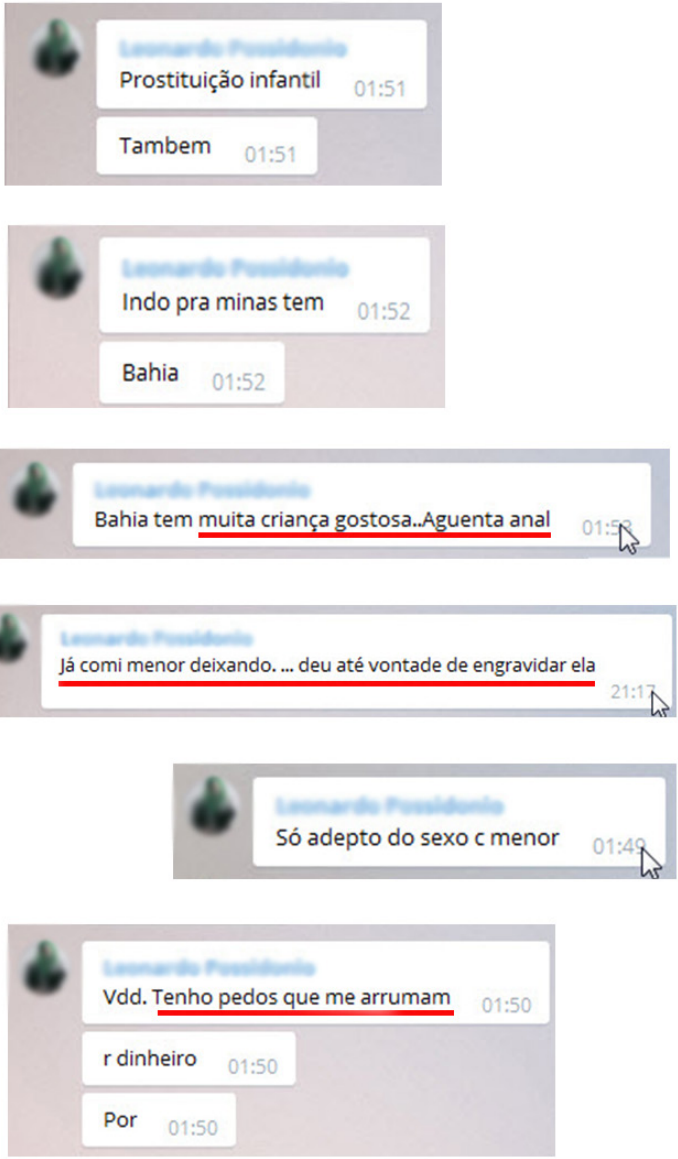

Figura 5: Demais declarações reais de preso pela Polícia Federal.
Fonte: Grupo de Mensageria Instantânea.

Conforme verificado, o comportamento apresentado pelo criminoso no seu cotidiano, durante certo período em que ele não detinha o conhecimento de que estava sendo monitorado, é de alta reprovabilidade e desperta atenção. Além de notoriamente afirmar que já abusou de diversas crianças, e que também as consegue por dinheiro, mostra o seu total desprezo em relação a elas.

O referido infrator foi preso em flagrante pela Polícia Federal infringindo o art. 241-B do Estatuto da Criança e do Adolescente e, apesar de todo o exposto, apresentou o mesmo padrão inofensivo, acima retratado, após sua prisão.

Por fim, e não menos relevante, em posse de dois dos indivíduos observados no estudo de comportamento, foi encontrado um manual de abuso sexual infantil, que instrui criminosos a iniciarem práticas sexuais com crianças. Nele era descrito um passo a passo de como introduzir, aos poucos, objetos na parte genital ou no ânus da criança, até se efetivar a prática sexual da penetração, bem como outros atos libidinosos. Importante salientar que os dois indivíduos ora citados possuem filhas menores de idade e, assim como os demais, também apresentaram, após sua captura, o padrão de comportamento inofensivo já descrito.

4 Conclusão

Os autores dos crimes de compartilhamento ou posse de arquivos de pornografia infantil não devem ser tratados como indivíduos inofensivos e de baixa periculosidade. Os abusadores de menores aparentam ser pessoas normais, que dificilmente levantam suspeitas. O silêncio da vítima e, muitas das vezes, da própria família torna ainda mais difícil a identificação desses criminosos.

O psicopata pedófilo usa, de forma maquiavélica, artimanhas para acercar-se de suas vítimas, sem despertar suspeitas (SILVA, 2008). Ademais, por se sentirem atraídos por crianças ou adolescentes, também compartilham e obtêm arquivos de cunho pornográfico infantil. Diante disso, o compartilhamento ou a posse

desses arquivos podem ser vistos como um indício do abuso ou de um iminente abuso de menores [!].

SILVA (2012) alerta que:

> O autor de determinados crimes com certo grau de perversidade tende a repetir. Um exemplo clássico é o pedófilo. Não existe pedófilo que não seja psicopata, ele fica maquinando de forma maquiavélica o ataque ao que há de mais puro e usa a criança como objeto de poder e diversão. E ele sempre volta a cometer o mesmo crime.

É necessário que sejam tomadas medidas mais severas e restritivas aos acusados e presos em flagrante pelos crimes dos arts. 241-A ou 241-B da Lei n.º 8.069/90, bem como é preciso maiores investigações e cuidados para com crianças e adolescentes que com eles interajam, ou já interagiram.

Pessoas abusadas sexualmente na infância apresentam mal-estar psicológico prolongado até a idade adulta, consubstanciado em sentimentos de nojo, culpa e, sobretudo, de isolamento, podendo apontar a morte como solução para os seus problemas (PEREIRA, 2014). Efeitos psicológicos do abuso sexual podem ser devastadores, e os problemas decorrentes do abuso persistem na vida adulta dessas crianças (BERLINER; CONTE, apud PFEIFFER; SALVAGNI, 2005).

O dever de garantir a proteção integral à criança e um futuro digno é responsabilidade de todos nós.

Referências bibliográficas

BRASIL. Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal. *Diário Oficial da União*, Rio de Janeiro, 31 dez. 1940.

___. Lei n.º 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Diário Oficial da União*, Brasília, 16 jul. 1990.

HARADA, Eduardo. *TecMundo Explica: o que é essa tal de "Deep Web"?*, 10 mar. 2015. Disponível em: <https://www.tecmundo.com.br/tecmundo-explica/74998-tecmundo-explica-tal-deep-web.htm>. Acesso em: 2 jan. 2017.

MALGARIM, Bibiana Godoi; BENETTI, Silvia Pereira da Cruz. *O abuso sexual no contexto psicanalítico: das fantasias edípicas do incesto ao traumatismo*. Canoas: Universidade Luterana do Brasil, dez. 2010. Disponível em: <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1413-03942010000300011>. Acesso em: 4 jan. 2017.

PEREIRA, Sónia Vilela Cardoso. *Abuso sexual: trajetórias de vida*. Dissertação de Mestrado em Psicologia da Justiça. Portugal: Instituto Universitário da Maia (ISMAI), out. 2014. Disponível em: <https://repositorio.ismai.pt/bitstream/10400.24/284/1/Tese%20Completa%20S%C3%B3nia%20Pereira.pdf>. Acesso em: 9 jan. 2017.

PFEIFFER, Luci; SALVAGNI, Edila Pizzato. Visão atual do abuso sexual na infância e adolescência. *Jornal de Pediatria*. Rio de Janeiro, 2005. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0021-75572005000700010>. Acesso em: 2 jan. 2017.

SILVA, Ana Beatriz Barbosa. *Mentes perigosas*: o psicopata mora ao lado. Rio de Janeiro: Fontanar, 2008.

___. *Psiquiatra autora de best-seller defende prisão perpétua para psicopatas*. Entrevista ao *site Correio Braziliense*, conduzida por Helena Mader. Brasília, 2012. Disponível em: <http://www.correiobraziliense.com.br/app/noticia/cidades/2012/06/04/interna_cidadesdf,305617/psiquiatra-autora-de-best-seller-defende-prisao-perpetua-para-psicopatas.shtml>. Acesso em: 9 jan. 2017.

Reflexões sobre o registro de identificação criminal de condenados pela prática de crimes e a liberdade sexual do menor em Portugal

Marilaine Almeida Santos*

RESUMO

Este artigo pretende investigar os aspectos jurídicos pertinentes ao registro de identificação criminal de condenados pela prática de crimes contra a autodeterminação sexual e a liberdade sexual de menores, instituído pela Lei n.º 103/2015, de 24 de agosto de 2015, da Assembleia da República de Portugal. O referido registro será analisado sob a perspectiva do Direito Internacional, do Direito Comunitário Europeu e do Direito Constitucional e Infraconstitucional Português, com enfoque na ponderação de aparente conflito entre o interesse superior da criança, por um lado, e, de outro, a dignidade da pessoa humana, o direito à privacidade e o direito ao esquecimento, conferidos ao condenado.

Palavras-chave: Registro. Identificação criminal. Autodeterminação sexual. Liberdade sexual. Menor. Portugal.

ABSTRACT

This article intends to investigate the legal aspects related to the criminal identity register of convicted people for the commission of crimes against sexual self-determination and sexual freedom of children, established by Law no. 103/2015, from August 24th, 2015, of the Assembly of the Republic of Portugal. The register will be analyzed from the perspective of the International Law, the European Community Law and the

* Doutoranda em Ciências Jurídicas pela Universidade Autônoma de Lisboa. Juíza Federal Titular da 2ª Vara Federal em Barueri/SP. *E-mail*: marisant@jfsp.jus.br.

Portuguese Constitutional and Infraconstitutional Law, focusing on the balance of an apparent conflict between the best interest of the child, on the one hand, and, on the other, the dignity of the human person, the right to the privacy and the right to forgetfulness of the convicted person.

***Keywords**: Register. Criminal identity. Sexual self-determination. Sexual freedom. Minor. Portugal.*

1 Introdução

Os crimes sexuais praticados contra crianças e adolescentes têm se proliferado, sobretudo na modalidade pedopornografia cibernética, com a massificação do acesso à telefonia móvel, à Internet e às demais tecnologias da informação. O abuso, a exploração e a violência sexual contra menores são caracterizados pela transversalidade, pois ocorrem em todas as faixas socioeconômicas, em cada um dos países do mundo.

A palavra "pedofilia" tem sua origem etimológica na língua grega: resulta da junção de *paidíon/paidós* (criança) com *filia* (amizade, afeição). Na mitologia grega, inclusive, há referência a uma relação pedófila entre o rei Laio e seu tutelado Crísipo (menor púbere), que teria se matado após o rompimento. Em outra versão, ocorreu sedução e estupro do menor. Textos da antiga literatura greco-romana também apresentam referências a casos passíveis de enquadramento como pedofilia.

Para as ciências médicas, a pedofilia (atração por crianças) consiste em um dos transtornos de preferência sexual, constante do Código Internacional de Doenças, item F65.4. Já à luz da psicanálise, a pedofilia é considerada como perversão sexual.

Segundo estatística da Organização das Nações Unidas[1] (ONU), em todo o mundo cerca de 50% (cinquenta por cento) dos crimes sexuais são cometidos contra meninas com idade inferior a 16 (dezesseis) anos, sendo que a primeira experiência sexual de cerca de 30% (trinta por cento) das mulheres no mundo foi forçada. O percentual é ainda mais elevado entre aquelas com menos de 15 (quinze) anos de idade ao tempo da sua iniciação sexual, chegando a 45% (quarenta e cinco por cento) de relatos de experiência forçada.

[1] Disponível em: <http://www.endvawnow.org/en/articles/299-fast-facts-statistics-onviolence-against-women-and-girls-.html>. Acesso em: 10 fev. 2017.

Estudo conduzido pelo UNICEF (United Nations Children's Fund), denominado *Break the Silence – End Child Sexual Abuse*[2], constatou que 47,6% (quarenta e sete vírgula seis por cento) das mulheres jovens e 31,9% (trinta e um vírgula nove por cento) dos homens jovens tiveram seu primeiro intercurso sexual forçado ou, de algum modo, coagido por membros da família ou outras pessoas conhecidas de sua família.

Como os crimes sexuais, em regra, acontecem na esfera privada ou íntima, com reduzidos relatos às autoridades para apuração e processamento criminal, a magnitude real de sua ocorrência é inacessível. No entanto, alguns órgãos e entidades desenvolvem pesquisas quanto à matéria. A *American Professional Society on the Abuse of Children*[3] refere que as meninas comunicam mais casos de abuso sexual que os meninos, 18% (dezoito por cento) para vítimas do sexo feminino e 7,6% (sete vírgula seis por cento) para vítimas do sexo masculino, e o remanescente das notificações vinculado às pessoas maiores, de diferenciadas faixas etárias. Tal estudo justifica essa disparidade, além da questão de gênero, com maior exposição do sexo feminino a esses delitos, ao fato de que os meninos são mais relutantes em confidenciar suas experiências abusivas, por várias razões, tais como: o sentimento de fraqueza ou de falha diante do padrão da sociedade tradicional de que o homem representa figura ativa, não assumindo a condição de vítima; a evitação de serem rotulados como instigadores da conduta abusiva; a não concepção da ideia de experiência sexual entre o menor e a mulher de faixa etária incompativelmente superior como abuso sexual, em razão de estereótipos sexuais restritivos, pelos quais é negada a ocorrência do abuso ou minimizados os seus efeitos negativos; ou, ainda, a não aceitação de serem interpretados como homossexuais. Esses fatores, aliados à distinção entre

[2] Disponível em: <https://www.unicef.org>lac>Break_the_Silence--Introduction_.pdf>. Acesso em: 10 fev. 2017.

[3] Disponível em: <http://russwilson.coffeecup.com/Stoltenborgh%202012%20-%20Global%20Perspective%20on%20Child%20Sexual%20Abuse.pdf>. Acesso em: 13 fev. 2017.

definições legais de abuso contra menores em cada país, geram a imprecisão dos dados estatísticos a respeito das condutas violadoras da autodeterminação e da liberdade sexual.

Os crimes de cunho sexual podem causar consequências negativas no desenvolvimento físico, psicológico, mental, social e moral das crianças e adolescentes, razão pela qual a comunidade internacional tem proposto a se empenhar na prevenção e repressão de tais condutas.

Como uma das medidas preventivas e repressivas de crimes sexuais contra crianças e adolescentes, alguns países, a exemplo do Chile (*Ley* n.º 20.594/2012), dos Estados Unidos (*Megan's Law*/1996) e de Portugal, têm adotado a instituição de um cadastro ou registro de identificação criminal de condenados pelos referidos crimes, comumente denominada "lista de pedófilos". No Brasil, tramita o Projeto de Lei Federal n.º 629/2015, que, inicialmente, previa a formação de um cadastro nacional de suspeitos e condenados por pedofilia, porém, após apreciação da Comissão de Segurança Pública, os suspeitos foram excluídos do texto do projeto. No âmbito estadual, a Lei n.º 10.315/2015, do estado de Mato Grosso, criou o cadastro de suspeitos, indiciados ou condenados, e, no estado de Santa Catarina, tramita o Projeto de Lei n.º 0134.3/2016, que prevê a inclusão cadastral após decisão condenatória por crime sexual contra menores.

Em Portugal, o registro de identificação criminal de condenados pela prática de crimes contra a autodeterminação sexual e a liberdade sexual de menores foi instituído pela Lei n.º 103/2015, de 24 de agosto de 2015, que, até 16 de novembro de 2016, implicou o cadastro de 5 739 (cinco mil, setecentos e trinta e nove) condenados, segundo informação do Ministério da Justiça de Portugal[4].

[4] Disponível em: <http://www.dn.pt/sociedade/interior/ha5-739-pessoas-na-listade-pedofilos-condenados-5500852.html>. Acesso em: 22 fev. 2017.

O registro em comento, tanto no curso do processo legislativo, quanto após a promulgação da respectiva lei, vem sendo objeto de acirrados debates no confronto entre o superior interesse da criança em coibir e reprimir o abuso e a exploração sexual e, sob a ótica do condenado, a dignidade da pessoa humana, o direito à privacidade e o direito ao esquecimento.

Neste artigo, pretende-se trazer à reflexão os principais aspectos do registro de identificação criminal de condenados por crimes sexuais contra menores; o contexto das normas que asseguram o superior interesse da criança e o combate ao abuso, à violência e à exploração sexual de menores; e os argumentos contrários à instituição do referido registro, nomeadamente, violação à dignidade da pessoa humana, ao direito à privacidade e ao direito ao esquecimento.

2 Principais aspectos do registro de identificação criminal instituído pela Lei n.º 103/2015 em Portugal

A Lei n.º 103/2015 foi promulgada em decorrência da transposição da Diretiva n.º 2011/93/UE, do Parlamento Europeu e do Conselho da União Europeia, para o ordenamento jurídico interno de Portugal. A diretiva em questão estabelece as condutas que devem ser internalizadas pelos países membros da União Europeia como crimes sexuais contra crianças.

Por força da previsão contida no art. 1º, da Lei n.º 103/2015, foi criado em Portugal o sistema de registro de identificação criminal de condenados pela prática de crimes contra a autodeterminação sexual e a liberdade sexual de menores, assim considerada toda pessoa com idade inferior a 18 (dezoito) anos.

Os arts. 1º e 2º, item 1, do Anexo da Lei n.º 103/2015, estabelecem que o registro de identificação consiste em base de recolhimento, tratamento e conservação de elementos de identificação de criminosos sexuais, nacionais e estrangeiros

residentes em Portugal, com antecedentes criminais relativos aos crimes sexuais contra crianças e adolescentes.

Como elementos de identificação dos condenados, o art. 9º do Anexo elenca nome completo, residência, domicílio profissional, data de nascimento, naturalidade, nacionalidade, número de identificação civil, número de passaporte (com informação do órgão e do país emissor), número de identificação fiscal, número de segurança social e número do registro criminal. Além da identificação do agente, o registro conterá o extrato da decisão judicial condenatória, outras decisões judiciais subsequentes, os crimes imputados e as disposições legais aplicadas. Na forma do art. 2º, item 2, do Anexo, devem integrar o sistema de registro:

a) decisões que apliquem penas e medidas de segurança, as que determinem o seu reexame, substituição, suspensão, prorrogação da suspensão, revogação e as que declarem a sua extinção;

b) acórdãos de revisão e de confirmação de decisões condenatórias estrangeiras;

c) decisões de inibição de exercício de responsabilidades parentais, tutela ou curatela;

d) decisões de proibição do exercício da profissão, função ou atividade que impliquem ter menores sob sua responsabilidade, educação, tratamento ou vigilância.

O Professor BRAZ (2016, p. 31) relaciona a acepção filosófica de identidade à individuação da pessoa e considera a identificação como processo de classificação ou categorização. Vejamos:

> O conceito de identidade é, num plano filosófico, sinônimo de unicidade, de identidade individual, ou seja, de individualidade. Assim, o conceito de identificação refere-se basicamente não a um resultado, mas sim a um processo metodológico de integração ou inclusão de um determinado objeto de análise e de pesquisa numa determinada categoria ou classe específica.

Sob essa ótica, a Lei n.º 103/2015 traz os elementos de identidade que serão utilizados no processo de identificação dos criminosos sexuais contra menores, sendo responsável pela base de dados o Diretor-Geral da Administração da Justiça de Portugal, na forma do art. 7º, item 1, do Anexo. A inscrição no registro é promovida pelos serviços de identificação criminal da Direção-Geral da Administração da Justiça, com fulcro no art. 8º, item 1, do Anexo. As decisões anteriores à criação do registro também devem ser inscritas no sistema pela Direção-Geral da Administração da Justiça, nos moldes do art. 8º, item 2. O agente deverá ser pessoalmente notificado da sua inscrição no registro, bem como dos seus direitos e deveres, consoante estabelece o art. 12 do Anexo, podendo requerer a retificação, atualização ou supressão de dados quando indevidamente registrados, segundo admitido pelo art. 15 do Anexo. Durante o período em que perdurar a inscrição no cadastro, deverá o condenado manter atualizado o seu local de residência, com base no art. 13.

A teor do art. 3º do Anexo, o sistema de registro de condenados por crimes sexuais contra menores tem como finalidade o acompanhamento da ressocialização do agente, o auxílio à investigação criminal e a promoção, em obediência ao princípio do interesse superior das crianças e jovens, da concretização do desenvolvimento pleno e harmonioso destes. Não se pode descartar, também, a função preventiva de reincidência. Ademais, conforme o art. 5º, da Lei n.º 103/2015, os dados do registro de identificação criminal de condenados por crimes sexuais deverão ser consultados para o fim de expedição de certificado negativo de condenações criminais, como medida preventiva na contratação de profissional para o exercício de funções que envolvam contato regular com menores. O recrutador, empregador ou responsável pelas atividades, está obrigado a solicitar tal certificado anualmente ao profissional e o descumprimento configura contraordenação equivalente à contravenção do Direito Penal brasileiro, com pena de multa.

Além disso, a contratação dolosa de pessoa condenada para o exercício de atividade que envolva contato regular com menores é crime, punido com pena de prisão de até 1 (um) ano e pena de multa de até 120 (cento e vinte) dias, sem prejuízo das penas de interdição do exercício de profissão ou atividade, privação do direito a subsídio ou benefício público, fechamento de estabelecimento cuja atividade dependa de autorização ou licença da autoridade administrativa, ou, ainda, suspensão de autorizações, licenças ou alvarás. O Tribunal de Execução das Penas pode determinar, mediante requerimento do titular, a não transcrição da condenação em certificado de registro criminal, quando já extinta a pena principal e a eventual pena acessória, havendo fundada verossimilhança de que o condenado não voltará a praticar condutas da mesma espécie e sendo sensivelmente diminuto o perigo para a segurança e bem-estar dos menores em contato durante o exercício da sua profissão, emprego, função ou atividade, consoante preconizado no art. 5º da Lei n.º 103/2015. No caso, deve ser realizada perícia psiquiátrica, com intervenção de 3 (três) especialistas, para checar a reabilitação da pessoa requerente.

O art. 4º do Anexo dispõe que o registro de identificação criminal em comento está sujeito aos princípios informativos do estrito respeito à legalidade, da autenticidade, da veracidade, da univocidade e da segurança dos elementos identificadores.

Conforme o art. 16 do Anexo, só podem ter acesso ao registro os magistrados, o Ministério Público, as entidades responsáveis pela condução de inquéritos ou instruções, os órgãos de cooperação internacional na prevenção e repressão à criminalidade, a Direção-Geral de Reinserção e Serviços Prisionais e as Comissões de Proteção de Crianças e Jovens, no âmbito de suas atribuições. Tais órgãos e entidades devem manter a reserva das informações, uma vez que o art. 19 do Anexo confere natureza confidencial a tais dados e impõe sigilo profissional. Excepcionalmente, acesso limitado pode ser franqueado, nos termos dos itens 2 a 6 do mesmo artigo, aos cidadãos que exerçam responsabilidades parentais sobre

menor de até 16 (dezesseis) anos de idade, quando alegarem uma situação concreta, justificada por fundado receio de que, na área de residência ou na área em que o menor frequenta atividades paraescolares, ou nas imediações do seu estabelecimento escolar, resida, trabalhe ou circule habitualmente pessoa que conste do registro. Esse requerimento, dirigido à autoridade policial, terá por objeto apenas a confirmação e a averiguação dos fatos, cujo sigilo deve ser preservado, não sendo permitido ao requerente acesso à identidade e ao endereço da pessoa inscrita no registro. Confirmados os fatos, as autoridades policiais competentes devem desenvolver ações de vigilância para garantir a segurança dos menores na área.

O art. 11 do Anexo, combinado com o seu art. 13, diz que o registro da condenação pode perdurar pelo período de 5 (cinco) a 20 (vinte) anos, computado a partir do cumprimento ou da extinção da pena, variável conforme o prazo da sanção de prisão fixada, sendo, após aquele decurso temporal, cancelado o registro, desde que não tenha ocorrido nova condenação por crime contra a autodeterminação sexual e a liberdade sexual de menor, ou quando verificada a morte do agente.

E, por fim, subsidiariamente, nos termos do art. 20, item 1, do Anexo, são aplicáveis, com as necessárias adaptações, as normas que regulam o funcionamento da identificação criminal, no caso, a Lei n.º 37/2015.

3 O contexto das normas relativas ao interesse superior da criança e à sua proteção, em face da exploração e do abuso sexual

No plano do Direito Internacional, as normas de *Hard Law* são aquelas dotadas de força cogente, que impõem o cumprimento pelos Estados-partes, independentemente de internalização. Ao contrário, normas de *Soft Law* consistem em princípios projetivos, de inspiração ao legislador de cada Estado-membro, sendo que, em caso de não atendimento, não incidem em sanções internacionais.

As normas atualmente vigentes no Direito Internacional, que preconizam o superior interesse da criança, são tidas como de natureza *Hard Law*, portanto, são regras impositivas, de cumprimento obrigatório.

No seu desenvolvimento histórico, concebe-se que, inicialmente, a proteção da criança e do adolescente estaria embutida nas garantias de liberdade e igualdade, que contemplam toda a humanidade, no art. 1º da Declaração dos Direitos do Homem e do Cidadão, de 1979, de inspiração iluminista, decorrente da Revolução Francesa.

A proteção específica dos direitos básicos das crianças e dos adolescentes teve como marco as ações de Eglantyne Jebb, fundadora do *Save the Children Found* (Londres, 1919), e da União Internacional (Genebra, 1920). Contudo, somente em 26 de setembro de 1924, na Declaração de Genebra sobre os Direitos da Criança, adotada no âmbito da Liga das Nações, foi expressamente estabelecido que "a criança deve ser colocada em uma posição que garanta a subsistência e deve ser protegida contra toda forma de exploração".

Na Declaração Universal dos Direitos Humanos, editada pela Organização das Nações Unidas (ONU), em 10 de abril de 1948, além da previsão geral do art. 1º de que "todos os seres humanos nascem livres e iguais em dignidade e em direitos", o item 2, do art. 25, confere à maternidade e à infância direito a ajuda e a assistência especiais.

Em 20 de novembro de 1959, com o advento da Declaração dos Direitos da Criança, como princípio 2º, foi contemplado o melhor interesse da criança; e, no princípio 9º, a proteção contra quaisquer formas de negligência, crueldade e exploração.

Na data de 16 de dezembro de 1966, o Pacto Internacional sobre Direitos Civis e Políticos trouxe previsões específicas sobre alguns direitos da criança, a exemplo dos seus arts. 14, item 1

(exceção no caso de interesse de menores ou tutela de crianças), e 24 (direitos à proteção não discriminatória, ao nome e à nacionalidade).

Nos diplomas antes referidos, embora estabelecendo uma condição jurídica mais favorável às crianças e adolescentes, o exercício dos direitos era atrelado ao do poder parental, figurando os menores como objetos de direito.

Com a superveniência da Convenção sobre os Direitos da Criança, em 20 de novembro de 1989, a criança foi alçada à condição de sujeito titular de direitos.

Do ponto de vista da Filosofia Política, o Professor FORST (2010, p. 340) discorre sobre o reconhecimento como pessoa de direito, nestes termos:

> Ser reconhecido como pessoa de direito significa ser respeitado em sua autonomia pessoal segundo os padrões do Direito para determinar sua própria vida. Os direitos subjetivos à liberdade de ação cabem a toda pessoa como pessoa de direito; são definidos de modo jurídico positivo e valem para todas as pessoas de forma igual. As pessoas de direito são, portanto, consideradas juridicamente como iguais e reconhecidas como indivíduos independentes.

O acima transcrito dá sustentação à ideia de que o ser humano é dotado de autodeterminação, sendo a todos conferida aptidão para figurar como pessoa de direito, sem sofrer indevida discriminação. O Estado viola a autonomia existencial quando desconsidera a identidade própria de cada ser, sem que exista justificativa pública razoável e de ordem superior. Portanto, considerar a criança como pessoa de direito representa o reconhecimento de sua própria identidade e personalidade.

A Convenção sobre os Direitos da Criança, em seu art. 1º, considera como criança "todo ser humano com menos de dezoito anos de idade, a não ser que, em conformidade com a lei aplicável à criança, a maioridade seja alcançada antes". No art. 2º contempla o interesse maior da criança como regra a ser observada

por instituições públicas ou privadas de bem-estar social, tribunais, autoridades administrativas ou órgãos legislativos. No art. 19, item 1, estabelece a adoção, pelos Estados-partes, de medidas legislativas, administrativas, sociais e educacionais para proteger a criança, dentre outros, de abuso sexual; e, no art. 34, proíbe expressamente a exploração e o abuso sexual.

Segundo informação da UNICEF[5], a Convenção sobre os Direitos da Criança foi ratificada por 196 (cento e noventa e seis) países, constituindo o instrumento de direitos humanos mais amplamente endossado no campo do Direito Internacional. Necessário ressaltar que a Convenção em questão consiste em instrumento de *Hard Law*, impondo-se o seu cumprimento pelos Estados-partes.

Para melhor realizar os objetivos da Convenção, em 25 de maio de 2000, o Protocolo Facultativo relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil, em seu art. 3º, estabeleceu a obrigação de os Estados-partes ampliarem a criminalização de condutas relacionadas à exploração sexual de crianças.

No âmbito do Conselho da Europa, em 25 de janeiro de 1996, foi adotada a Convenção Europeia sobre o Exercício dos Direitos das Crianças, que, no art. 1º, item 2, consagrou o superior interesse da criança, a fim de promover seus direitos, inclusive processuais, e facilitar o exercício desses direitos, por si mesma ou por meio de outras pessoas ou organismos, informados e autorizados a participar de processos que lhes digam respeito.

A Carta Social Europeia, do mesmo Conselho, no art. 7º, diz que "as crianças e os adolescentes têm direito a uma proteção especial contra os perigos físicos e morais a que se encontrem expostos". A respeito do tema, pelo Conselho da Europa foram editadas: a Recomendação n.º 1065/1987 (exploração infantil),

[5] Disponível em: <www.unicef.org/brazil/pt/resources_10120.htm>. Acesso em: 15 fev. 2017.

a Resolução n.º 1099/1996 (exploração sexual de crianças), a Resolução n.º 1307/2002 (exploração sexual de crianças: tolerância zero), a Recomendação n.º 1778/2007 (erradicação de todas as formas de violência, exploração e abuso) e a Declaração sobre a Proteção da Dignidade, da Segurança e da Privacidade das Crianças na Internet, de 6 de fevereiro de 2008.

A Convenção de Budapeste sobre o Cibercrime, de 23 de novembro de 2001, elenca diversas condutas com relação à pornografia infantil, a serem tratadas como infrações penais pelos países subscritores, quando cometidas de forma intencional e ilegítima. Embora celebrada junto ao Conselho da Europa, a Convenção foi aberta à assinatura de outros países àquele não vinculados. Tal ato ainda não foi ratificado pelo Brasil. Portugal transpôs os preceitos da Convenção e adaptou sua ordem jurídica interna através da Lei n.º 109/2009.

O Conselho da Europa também editou, em 25 de outubro de 2007, a Convenção para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais, conhecida como Convenção de Lanzarote.

Na esfera da União Europeia, a Carta dos Direitos Fundamentais, de 18 de dezembro de 2000, em seu art. 24, item 1, confere à criança o direito à proteção.

O Conselho da União Europeia adotou a Decisão-Quadro 2004/68/JAI, de 22 de dezembro de 2003, relativa à luta contra a exploração sexual de crianças e a pornografia infantil, impondo aos Estados-membros a criminalização de inúmeras condutas intencionais àquelas correlatas.

Por sua vez, a Diretiva nº 93/2011, do Conselho da União Europeia, define vinte crimes divididos em quatro categorias:

1) os abusos sexuais, tais como a prática de atos sexuais com uma criança que não tenha atingido a maioridade sexual ou forçá-la a se submeter a tais atos com outra pessoa;

2) a exploração sexual, como, por exemplo, coagir uma criança a participar em prostituição ou em espetáculos pornográficos;

3) a pornografia infantil: possuir, aceder, distribuir, fornecer e produzir pornografia infantil; e

4) o aliciamento de crianças por via eletrônica para fins sexuais: propor na Internet um encontro com uma criança com o intuito de cometer abusos sexuais, bem como instigá-la, pelo mesmo meio, a fornecer material pornográfico representando essa criança.

O art. 15, item 3, do mesmo diploma, permite aos Estados-membros, na investigação ou no processamento da ação penal relativa a tais crimes, o "acesso a instrumentos de investigação eficazes, tais como os utilizados no caso da criminalidade organizada e de outros crimes graves". Importante observar que, no Considerando n.º 43, a Diretiva possibilita aos Estados-membros o registro de pessoas condenadas pelos crimes sexuais nela previstos, de acesso limitado, em regra, às autoridades judiciais e/ou policiais, conforme os princípios constitucionais nacionais e as normas de proteção de dados. Vale dizer que, no Direito Comunitário Europeu, há base jurídica para a instituição do registro de identificação criminal de condenados por crimes sexuais perpetrados em face de crianças.

No plano do ordenamento jurídico interno português, a Constituição da República, no art. 69, item 1, diz que "as crianças têm direito à proteção da sociedade e do Estado".

A legislação infraconstitucional portuguesa é pródiga no tocante à proteção do menor em sua autodeterminação e liberdade sexual. A Lei n.º 147/1999, que dispõe sobre a proteção de crianças e jovens em perigo, em seu art. 3º, item 2, "b", considera em estado de perigo a criança ou jovem vítima de abusos sexuais. Por sua vez, a Lei n.º 113/2009 prevê medidas de proteção aos menores vítimas de exploração e abuso sexual. E a Lei n.º 103/2015, objeto deste estudo, cria o sistema de registro de identificação criminal

de condenados pela prática de crimes contra a autodeterminação sexual e a liberdade sexual de menores.

As normas anteriormente referidas prestigiam o interesse superior da criança, justificado pela sua vulnerabilidade e situação peculiar de pessoa em desenvolvimento.

Na doutrina, o Professor Doutor ALEXANDRINO (2008, p. 8-9) instrui que o interesse superior da criança consiste em:

> a) "princípio jurídico-formal, que atua como critério orientador";
>
> b) "*standard* hermenêutico, parâmetro auxiliar na concretização";
>
> c) "pauta para a conformação do ordenamento jurídico pelo legislador";
>
> d) "pauta obrigatória na resolução de casos concretos".

Seja na perspectiva de princípio orientador, de parâmetro para a execução das normas, de pauta informativa da ação do legislador ou de critério obrigatório na aplicação das regras aos casos concretos, o superior interesse da criança impõe a máxima eficácia do regime protetivo, de modo a coibir, prevenir e reprimir todo ato atentatório aos direitos das crianças e dos adolescentes, notadamente aqueles que violem a sua autodeterminação e liberdade sexual, dadas as sérias implicações em seu desenvolvimento.

Conforme visto, no contexto do Direito Internacional, do Direito Comunitário Europeu e do Direito Português, o superior interesse da criança tem autorizado o rígido tratamento de violações aos seus direitos e, inclusive, em caso de crimes sexuais, a implementação do registro de identificação criminal de condenados.

4 Os argumentos defensivos da dignidade da pessoa humana, do direito à privacidade e do direito ao esquecimento

Em oposição à instituição do registro de condenados por crimes sexuais contra menores em Portugal, os argumentos jurídicos que vêm sendo mais comumente levantados consistem nas possíveis violações à dignidade da pessoa humana, ao direito à privacidade e ao direito ao esquecimento.

A dignidade da pessoa humana, como já visto, está mencionada no art. I, da Declaração Universal dos Direitos Humanos da ONU, ao dizer que "todos os seres humanos nascem livres e iguais em dignidade e direitos [...]".

O Pacto Internacional sobre Direitos Civis e Políticos, no art. 10, item 1, prevê expressamente o tratamento com humanidade e respeito à dignidade inerente à pessoa humana, inclusive à pessoa privada de sua liberdade.

A Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais, de 4 de novembro de 1950, editada pelo Conselho da Europa, em seu art. 3º, diz que "ninguém pode ser submetido a torturas, nem a penas ou tratamentos desumanos ou degradantes".

No âmbito do Direito Comunitário, a Carta dos Direitos Fundamentais da União Europeia, em seu art. 1º, considera inviolável a dignidade do ser humano, devendo ser respeitada e protegida.

A Constituição da República de Portugal, no art. 13, item 1, diz que "todos os cidadãos têm a mesma dignidade social e são iguais perante a lei".

Na atual fase de humanitarismo do Direito Penal e Processual Penal, é defendida a ideia de que não há mais espaço para arbitrariedades ou práticas que violem os direitos fundamentais, dentre os quais se inserem o direito à presunção de inocência, ao tratamento igualitário, ao contraditório e à ampla defesa, de modo

que o Direito Penal objetivo e subjetivo se submetam ao escrutínio do princípio da dignidade da pessoa humana.

Para o doutrinador ALEXY (2011, p. 267-268), a dignidade da pessoa humana perfaz-se nas acepções de valor, princípio e regra do Estado Democrático de Direito. Enquanto valor, significa que a pessoa humana não poderá ser alijada de sua dignidade, pois tal atributo precede a própria organização do Estado, independentemente de positivação, ou seja, o valor humano tem prioridade em face do Estado. A dignidade da pessoa humana, considerada como princípio, segundo o mesmo autor, impõe-se como mandamento de otimização do ordenamento jurídico, a ser concretizado, na maior medida possível, dentro das possibilidades jurídicas e fáticas. Assim, constitui-se em elemento estruturante do Estado, devendo ser observada na produção do Direito, tendo conteúdo deontológico, voltado ao "dever" ou ao "dever ser". E, como regra, ou princípio-regra, sustenta ALEXY que a dignidade da pessoa humana prevalece diante de todos os demais princípios e regras, embora possa ser relativizada perante a igual dignidade de todos os seres humanos. É, porém, de cumprimento obrigatório pelo Estado (efeito vertical), pela comunidade e pelo particular (efeito horizontal), dotada de *status* constitucional formal e material, com plena eficácia. Consiste, assim, em prescrição imperativa de conduta.

A respeito do tema, o Professor NOVAES (2017, p. 107) ensina que a dignidade da pessoa humana se desenvolve nos seguintes planos:

> [...]
>
> (i) a proscrição de subjugação e de exclusão, com a garantia da essencial autonomia da pessoa;
>
> (ii) a inadmissibilidade correlativa de degradação da pessoa como objecto ou como coisa;
>
> (iii) a proibição de alienação identitária e de devassa humilhante, com a garantia do controlo do próprio sobre a sua identidade, o seu reino interior e a sua apresentação pública;

> (iv) a inaceitabilidade da incapacitação da pessoa, a quem devem ser garantidas as condições materiais e a educação que lhe permitam afirmar-se, ou desenvolver-se na medida de suas capacidades, como sujeito da própria vida.

Refere o mesmo autor (2017, p. 133), ainda, que a dignidade da pessoa humana, enquanto valor supremo e princípio constitucional de vinculação absoluta, tem conteúdo aberto e de aplicação relativizante. Para ele, na apreciação de eventual violação à dignidade da pessoa humana, devem ser valoradas as circunstâncias do caso concreto e o contexto.

As doutrinas acima referidas, na abordagem da dignidade da pessoa humana, concebida como valor, princípio ou regra, são uníssonas no sentido de que, havendo aparente conflito entre bens jurídicos daquela imanentes, deve ser procedida a sua ponderação e relativização, diante das especificidades da situação concreta apresentada.

Uma das posições contrárias ao registro de pedófilos em Portugal sustenta que a inclusão e a permanência em lista, sobretudo quanto aos condenados que já cumpriram sua pena, ou que a tiveram extinta, ou seja, àqueles que não mais estejam em dívida com a sociedade, viola a dignidade da pessoa humana, por impor uma medida que transcende a própria pena da esfera criminal, submetendo o indivíduo a uma situação de incapacitação e de inferioridade jurídica, dadas as limitações ao exercício de direitos durante o período de manutenção do nome no registro, ocorrendo múltipla punição pelo mesmo fato. Propõem a humanização da pessoa do pedófilo. Acrescentam, ainda, que a providência questionada, no caso, é extrema, pois, para atender à finalidade de repressão ao crime sexual, em atenção ao superior interesse da criança, há a cominação de sanções penais. Salientam, por fim, que melhor solução seria o agravamento da pena, e não a adoção de penas brandas com emprego de medidas jurídicas extrapenais, que perduram além do tempo da sanção individualizada imposta.

No tocante ao respeito pela vida privada, a Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais consagra tal direito no art. 8º, que, todavia, no item 2, permite a restrição desse direito pela autoridade pública, quando necessário à segurança nacional, à segurança pública, ao bem-estar econômico do país, à defesa da ordem, à prevenção de infrações penais, à proteção da saúde ou da moral, ou à proteção dos direitos e das liberdades de terceiros.

A Carta dos Direitos Fundamentais assegura o respeito à vida privada, no art. 7º, e a proteção de dados pessoais, no art. 8º, o qual, entretanto, no item 2, prevê que "esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei".

A Diretiva n.º 679/2016 regula a proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais. No art. 9º, *caput*, proíbe o tratamento de dados pessoais relativos à vida sexual ou orientação sexual de uma pessoa. Porém, o item 2, "g", excepciona a hipótese de necessidade de tratamento do dado por motivo de interesse público importante, fundado no direito da União ou de um Estado-membro. Nesse caso, devem ser observadas a proporcionalidade entre a medida e o objetivo visado, a essência do direito, a proteção dos dados pessoais e a adoção de providências adequadas e específicas, que salvaguardem os direitos fundamentais e os interesses do titular dos dados. No art. 10, permite o tratamento de dados pessoais relacionados com condenações penais e infrações, pela autoridade pública, quando houver autorização no direito da União ou de um Estado-membro, contanto que previstas as garantias adequadas para os direitos e liberdades dos titulares dos dados.

Os antagonistas alegam que o registro de pedófilos vulnera o direito à privacidade, vez que representa a inclusão, a manutenção e a utilização de dado a respeito de escolha estritamente

pessoal e preferência sexual do indivíduo, cujo tratamento lhe causa exposição e constrangimento. Aduzem que não cabe ao Estado regular a esfera íntima da pessoa, pois, no seu entender, a idade mínima para o início da atividade sexual tem atualmente decorrido mais de um discurso histórico, pautado numa escolha social, do que num elemento biopsicológico, exemplificando que, num passado não muito remoto, o intercurso sexual e as relações maritais tinham início em tenra idade, coincidindo com o início das funções reprodutivas na fase de puberdade. Para essa corrente, a maturidade sexual e psicológica não está atrelada a um dado etário.

Por fim, outro argumento jurídico que vai de encontro ao registro de condenados por crimes perpetrados contra menores consiste no denominado "direito ao esquecimento", expressamente regulado no art. 17 da Diretiva n.º 679/2016, cujo reconhecimento dá-se nestes termos:

> Art. 17
>
> 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:
>
> a) os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
>
> b) o titular retira o consentimento em que se baseia o tratamento dos dados nos termos do art. 6º, n.º 1, alínea "a", ou do art. 9º, n.º 2, alínea "a", e se não existir outro fundamento jurídico para o referido tratamento;
>
> c) o titular opõe-se ao tratamento nos termos do art. 21, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do art. 21, n.º 2;
>
> d) os dados pessoais foram tratados ilicitamente;
>
> e) os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-membro a que o responsável pelo tratamento esteja sujeito;

> f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no art. 8º, n.º 1.

Com fundamento no direito ao esquecimento, salientam que não pode o Estado manter o nome do autor do fato inscrito em registro com restrições jurídicas que podem se protrair por até 20 (vinte) anos, após o cumprimento ou a extinção da punição estabelecida. Aqui, defendem que o fato deve ser esquecido, não sendo mais utilizado para nenhum fim que possa denegrir a imagem do indivíduo, sob consequência de ofensa ao seu direito de personalidade.

Nada despiciendo destacar que, por outro lado, o item 3, do mesmo art. 17, elenca as situações em que não é aplicável o direito ao apagamento de dados, quais sejam:

> 3. Os números 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:
>
> a) ao exercício da liberdade de expressão e de informação;
>
> b) ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
>
> c) por motivos de interesse público no domínio da saúde pública, nos termos do art. 9º, n.º 2, alíneas "h" e "i", bem como do art. 9º, n.º 3;
>
> d) para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do art. 89, n.º 1, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou
>
> e) para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Impende observar que, como exceção ao direito ao esquecimento, a Diretiva n.º 679/2016, art. 17, item 3, alínea "d", permite a utilização do dado para fins de arquivo de interesse público.

Os opositores da instituição de um registro de identificação criminal de pedófilos sustentam, além dos fundamentos jurídicos acima esposados, argumentos sociais no sentido de que o cadastro determinado pela lei tem como consequências o etiquetamento, o vigilantismo e o isolamento. O etiquetamento traduz-se em rótulo que adere à identidade da pessoa condenada, estigmatizando-a em sua comunidade, o que comprometeria o seu aprimoramento moral e o autorreconhecimento de seu valor pessoal, frustrando o propósito de recuperação do infrator. O vigilantismo consiste no permanente estado de alerta das autoridades competentes e da sociedade sobre o condenado, o que poderia conduzir a situações de exposição a suspeitas injustas e a procedimentos apuratórios indevidos. Ainda, alegam os críticos que a "lista de pedófilos" provoca o isolamento do condenado, sobretudo daquele privado de exercer as responsabilidades parentais e atividades em contato com menores, prejudicando o objetivo de ressocialização do agente. Outro ponto de questionamento também tem sido a eficácia da instituição de tal registro como medida preventiva, especialmente considerando-se os significativos dados sobre a ocorrência de crimes sexuais no âmbito intrafamiliar – das relações familiares, privadas e/ou íntimas. Ou seja, a norma que instituiu o registro de pedófilos protegeria em caráter preventivo, tão somente, as possíveis vítimas do perigo extrafamiliar, não sendo hábil para proteger a criança ou o adolescente exposto ao agressor que lhe é próximo.

5 Conclusão

Apesar dos acirrados debates por ocasião do trâmite do seu processo legislativo, a Lei Portuguesa n.º 103/2015, até a data de finalização deste trabalho, não sofreu impugnação quanto à sua constitucionalidade formal ou material. Também não foi identificada decisão reconhecendo eventual inconstitucionalidade da Lei n.º 20.594/2012 (Chile) e da Lei de Megan/1996 (Estados Unidos da América). Igualmente, não foi ventilada inconstitucionalidade acerca da Lei n.º 10.315/2015, do estado de Mato Grosso.

A criação de cadastro ou registro de identificação de condenados pela prática de crimes sexuais contra crianças e adolescentes tem sido justificada pela crescente proliferação de casos, impulsionada, especialmente, na modalidade de crimes cibernéticos, com comprometimento de combate pela comunidade internacional e, de forma mais contundente, nos Estados Unidos da América e na União Europeia.

Na esfera do Direito Internacional, a Convenção dos Direitos da Criança, que tem força de *Hard Law*, e seu Protocolo Facultativo, ambos com o fito de assegurar o superior interesse da criança, concitam os Estados-partes a proteger os menores em face do abuso e da exploração sexual, inclusive no que se refere à venda de crianças, à prostituição e à pornografia infantis, com a ampliação da tipificação de condutas afins. Com semelhante propósito, foram editadas a Carta Social Europeia, a Resolução n.º 1307/2002, a Recomendação n.º 1778/2007, a Declaração sobre a Proteção da Dignidade, da Segurança e da Privacidade das Crianças na Internet/2008, a Convenção de Budapeste e a Convenção de Lanzarote.

No Direito Comunitário Europeu, a proteção da criança contra a exploração e o abuso sexual consta da Decisão-Quadro n.º 2004/68/JAI/2003 e da Diretiva n.º 93/2011. Esta última permite a utilização de instrumentos de investigação eficazes, tais quais os admitidos em face do crime organizado e de outras condutas de maior gravidade, autorizando também o registro de pessoas condenadas por crimes sexuais contra menores. Assim, no contexto da União Europeia, há sólida base jurídica para a criação do registro de identificação de pedófilos.

Para adequar seu ordenamento jurídico interno às proposições normativas do Conselho da União Europeia e do Parlamento Europeu, Portugal promulgou a Lei n.º 103/2015, que instituiu o registro de identificação criminal de pedófilos, com a finalidade de prevenir a reincidência, auxiliar na investigação e,

sobretudo, assegurar o melhor interesse da criança e do adolescente no tocante à sua autodeterminação e liberdade sexual. O cadastro é norteado pelos princípios do estrito respeito à legalidade, da autenticidade, da veracidade, da univocidade e da segurança dos elementos identificadores.

O registro de condenados por crimes sexuais contra menores, na forma estabelecida pela Lei n.º 103/2015, não implica violação à dignidade da pessoa humana, por se tratar de mero registro de interesse público, sujeito à confidencialidade, não se caracterizando como pena principal ou acessória. As restrições ao exercício de atividade em contato com menores e as limitações do poder parental são sanções acessórias, decorrentes da condenação pela prática do fato em si, e não da inclusão no registro. O argumento de que a cominação de pena mais severa atenderia de modo mais satisfatório ao propósito de prevenir e reprimir o crime não se confirma diante do elevado grau de reincidência em pedofilia, mesmo nos países onde há a imposição de penas mais graves, a exemplo do Brasil. Ademais, reprimenda penal severa não exclui a possibilidade da adoção de medidas extrapenais de controle e prevenção.

De igual modo, a denominada "lista de pedófilos" não vulnera o direito à privacidade, que, na forma da Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais, da Carta dos Direitos Fundamentais da União Europeia e da Diretiva n.º 679/2016, pode ser restringido para fins de prevenção de infrações penais, se houver fundamento legítimo estabelecido em lei ou por motivo de interesse público relevante, respectivamente, caso da prevenção e repressão aos crimes sexuais praticados contra crianças e adolescentes. Importante observar que a liberdade de exercício das escolhas pessoais, assim como os demais direitos, não tem caráter absoluto, encontrando limitações quando houver o risco de ameaça ou lesão ao direito de outrem. A opção do legislador por fixar idade mínima para considerar lícito o intercurso sexual tem o objetivo de estabelecer um parâmetro razoável do que se

entende ser o atingimento da maturidade sexual e psicológica, para a compreensão do ato, e a livre manifestação da vontade, de modo a assegurar a autodeterminação e a liberdade sexual da pessoa. Cabe frisar que a linha relativista acerca da pedofilia expõe as crianças e os adolescentes a condutas arbitrárias e manipuladoras por parte dos agressores.

Quanto ao alegado direito ao esquecimento, a inserção e a manutenção do nome do condenado no registro, pelo prazo admitido em lei, por não consistirem em penas, e por estarem abrangidas pela confidencialidade, isoladamente consideradas, não violam direito de personalidade, pois não há que falar em mácula à imagem ou à reputação do indivíduo. Outro aspecto é que a Diretiva n.º 676/2016 excepciona da incidência do direito ao apagamento da informação o fim de interesse público, caso da prevenção de práticas abusivas ou de exploração sexual infantil.

Os argumentos sociais de etiquetamento, vigilantismo e isolamento de condenados, em razão da adoção do sistema de registro de identificação criminal, também não justificam a vedação de tal medida, pois confundem-se com as consequências sociais da prática de atos delituosos e da respectiva condenação. Referidos fenômenos não ocorrem apenas com a existência do registro, mas são comumente observados quando da tentativa de reingresso do condenado à vida em sociedade, o que deve ser objeto de políticas públicas. Quanto à alegada impossibilidade de eficácia do registro, no que tange à prevenção dos crimes sexuais praticados no ambiente intrafamiliar, há de se observar que o registro somente será efetuado após a condenação do agente. Portanto, prevalece sua função de prevenção de reincidência, o que é possível mesmo se tratando de abuso ou exploração sexual intrafamiliar, caso em que pode ser imposta pena acessória de perda do poder parental. Por oportuno, insta salientar que, se o registro prevenir o abuso de uma única criança, já terá atingido sua finalidade normativa e social.

Em suma, após a ponderação desenvolvida neste trabalho, entendemos que o superior interesse da criança na prevenção e no combate às práticas abusivas e de exploração sexual suplanta os argumentos de violação à dignidade da pessoa humana, do direito à privacidade e do direito ao esquecimento, empregados na defesa dos autores de crimes sexuais contra menores, não havendo incompatibilidade normativa e constitucional na instituição de registro de identificação de condenados em Portugal, previsto na Lei n.º 103/2015.

Referências bibliográficas

ALEXANDRINO, José de Melo. Os direitos das crianças: linhas para uma construção unitária. *Revista da Ordem dos Advogados*. Lisboa, Portugal, v. 68, n. 1. Disponível em: <http://www.oa.pt/Conteudos/Artigos/detalhe_artigo.aspx?idc=30777&idsc=71981&ida=72376>. Acesso em: 8 fev. 2017.

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgílio Afonso da Silva. 2. ed.; 3. reimp. São Paulo: Malheiros, 2011. Título original: *Theorie der Grundrechte*. ISBN 978-85-392-0073-3.

BRAZ, José. *Investigação criminal*: a organização, o método e a prova; os desafios da nova criminalidade. 3. ed. Coimbra: Almedina, 2016. ISBN 978-972-40-5317-2.

FORST, Rainer. *Contextos da Justiça*: Filosofia Política para além de liberalismo e comunitarismo. Trad. Denílson Luís Werle. São Paulo: Boitempo, 2010. Título original: *Kontexte der Gerechtigkeit, Politishe Philosophie Jenseits Von Liberalismus und Kommunitarismus*. ISBN 978-85-7559-148-2.

NOVAES, Jorge Reis. *A dignidade da pessoa humana*. Coimbra: Almedina, 2017. v. II. ISBN 978-972-40-6346-1.

Enunciados

Enunciado 1 – Busca e apreensão: equipamentos de informática

A ordem de busca e apreensão de equipamentos de informática implica a autorização para que seu conteúdo seja vasculhado com a finalidade de constatar a presença de elementos de convicção. Se possível, esse procedimento deve ser realizado no próprio local, a fim de que a apreensão se restrinja apenas aos objetos pertinentes. O ato não constitui a perícia a que alude o art. 158, e seguintes, do Código de Processo Penal, a ser feita posteriormente.

O Enunciado 1 teve origem nas dificuldades práticas em relação ao cumprimento de mandados de busca e apreensão, em que os investigados e seus advogados exigem ordens judiciais específicas, para que o agente policial tenha acesso, durante a diligência (antes da perícia, *in loco*, durante a pesquisa de elementos que ensejam a apreensão dos equipamentos) a todo e qualquer equipamento de informática, *software* e arquivo de dados. Na prática, os magistrados procuram redigir mandados muito detalhados, na tentativa de prever toda e qualquer possibilidade fática de pesquisa em sistemas, o que não é possível, tendo em vista a rápida evolução tecnológica. Isso tampouco é útil, uma vez que a determinação para buscar elementos de convicção em panorama informático abarca todo e qualquer banco de dados e compartilhamento.

Enunciado 2 – Busca e apreensão: exame de equipamentos por agente policial

Na busca e apreensão de equipamentos de informática, o procedimento para que seu conteúdo seja vasculhado no próprio local, para constatar a presença de elementos de convicção, pode ser realizado por agente policial tecnicamente qualificado, sendo facultativa a presença de perito criminal.

Justamente por não se tratar da prova pericial prevista no art. 158, e seguintes, do Código de Processo Penal, mas de cumprimento de diligência para verificar a existência de elementos indiciários de convicção referentes a ilícitos cibernéticos, e também considerando o pequeno número de peritos criminais na área de informática, chegou-se à conclusão de que, neste primeiro momento de apreensão de material para posterior perícia técnica, basta a presença de agente policial qualificado a tal pesquisa.

Enunciado 3 – Busca e apreensão: celulares em modo avião

Na busca e apreensão de telefones celulares (smartphones) ou dispositivos similares, recomenda-se que, se possível, eles sejam examinados após serem colocados em modo off-line (modo avião), de forma a evitar alteração remota de dados e interromper eventuais comunicações.

Delimitar o tempo de validade da determinação judicial é imprescindível para a validade da prova, assim como garantir a documentação do que foi encontrado e apreendido, até mesmo buscando a prescindibilidade da produção de prova oral, posteriormente, em juízo.

Enunciado 4 – Busca e apreensão: conteúdo armazenado remotamente

Recomenda-se que, no mandado de busca e apreensão de equipamentos de informática, conste expressa autorização para que seja vasculhado conteúdo remotamente armazenado, se localizados meios de acesso.

Considerando, porém, que a busca e apreensão de material indiciário pode se dar fora dos equipamentos diligenciados, mas com base em meios de acesso neles encontrados (como o sistema de armazenamento na "nuvem"), em discussão sobre a extensão da ordem judicial, concluiu-se pela recomendação de expressa autorização em mandado.

Enunciado 5 – Busca e apreensão: fotografias do investigado

Recomenda-se que, no mandado de busca e apreensão, conste expressa autorização para apreensão de fotografias do investigado, inclusive em meio físico, quando úteis à elucidação da autoria do crime.

Levando em conta a dificuldade de se chegar à autoria delitiva, diante da impessoalidade que a tecnologia permite nos relacionamentos pela rede mundial de computadores, bem como de garantir que o investigado tenha seus bens apreendidos no exato limite da determinação judicial, concluiu-se pela necessidade de se fazer constar, no mandado de busca e apreensão, a autorização do magistrado para apreensão de fotografias.

Enunciado 6 – Crimes virtuais: ação controlada e infiltração

Em crimes cometidos em ambiente virtual, constituem meios eficazes para apuração de autoria a ação controlada e a infiltração de agentes, a serem feitas na forma do art. 1º, § 2º, inciso I, e dos arts. 8º a 14, todos da Lei n.º 12.850/2013.

Todos os institutos jurídicos, mesmo que preexistentes à realidade virtual, podem ser utilizados, de maneira motivada e de acordo com a regra legal pertinente, para a investigação e a produção de prova. Dessa forma, institutos modernos, como a ação controlada e a infiltração policial, são meios válidos de apuração de autoria.

Enunciado 7 – Crimes de pornografia infantojuvenil: prova produzida no estrangeiro

Nos crimes tipificados nos arts. 241-A e 241-B da Lei n.º 8.069/1990, por força da Convenção sobre os Direitos da Criança, promulgada pelo Decreto n.º 99.710/1990 e respectivo Protocolo, promulgado pelo

Decreto n.º 5.007/2004, são aproveitáveis como prova os relatórios de diligências feitos por autoridade policial estrangeira.

Na prática, há discussão sobre a consideração de trabalhos realizados por autoridades policiais estrangeiras. Com base em Convenção Internacional internalizada no país, concluiu-se que relatórios e diligências executados por autoridade policial estrangeira são meios de prova a serem valorados pelo Juízo, no contexto probatório dos autos.

Realização

EMAG

ESCOLA DE MAGISTRADOS
DA JUSTIÇA FEDERAL
DA 3ª REGIÃO

Apoio

AJUFESP

ASSOCIAÇÃO DOS JUÍZES FEDERAIS DE SÃO PAULO E MATO GROSSO DO SUL