DISSERTAÇÃO
PARA A OBTENÇÃO DE GRAU DE MESTRE

A exploração sexual de crianças no Ciberespaço - aquisição e valoração de prova forense de natureza digital

Manuel Eduardo Aires Magriço

Setembro de 2012

DISSERTAÇÃO
PARA A OBTENÇÃO DE GRAU DE MESTRE

A exploração sexual de crianças no Ciberespaço - aquisição e valoração de prova forense de natureza digital

Orientador: Prof. Doutor Luís Miguel de Castro Larcher Castela dos Santos Cruz

Co-Orientador: Major-General José António Henriques Dinis

Co-Orientador: Major-General José Coelho de Albuquerque

Mestrando: Manuel Eduardo Aires Magriço

Setembro de 2012

Resumo

A exploração sexual de crianças no Ciberespaço constitui presentemente um problema mundial: o desenvolvimento de novas tecnologias que aumentam as formas de acesso ao mundo virtual tem contribuído para a crescente divulgação de material de abuso sexual. Existindo constrangimentos na identificação de vítimas, agressores e locais da prática da violência sexual contra as crianças no Ciberespaço, impõem-se novas metodologias por parte investigação criminal na repressão do fenómeno. O aprofundamento da Cooperação Judiciária Penal Internacional, o reporte de conteúdos por parte de empresas e instituições cuja atividade esteja relacionada com o Ciberespaço às Autoridades de IC, designadamente por parte dos Internet Service Provider, uma análise centralizada da informação, a difusão de boas práticas, a formação especializada dos diversos operadores judiciários sobre os procedimentos relativos à aquisição, valoração e manutenção da cadeia de custódia da prova digital, o apoio pericial técnico e especializado junto do Ministério Público de peritos informáticos forenses, a que se deve aliar o desenvolvimento de ações de prevenção criminal encobertas em linha e a consciencialização pública dos perigos, constituem fatores estruturantes na prevenção e repressão do fenómeno, tendentes a garantir maior segurança às crianças.

Palavras-chave: **crime, exploração sexual, crianças, ciberespaço.**

Abstract

Sexual exploitation of children in Cyberspace is currently a worldwide problem: the development of new technologies which broaden the access to the virtual world has contributed to the ever growing spread of material of sexual abuse content. With the existing constraints to the identification of victims, aggressors and location of the practice of sexual violence against children in Cyberspace, it is crucial that criminal investigation develops new methodologies for the repression of the phenomenon. The deepening of International Judicial Cooperation in criminal matters, the reporting of contents to the criminal investigation authorities by companies and institutions whose activity is related to the Cyberspace, namely by Internet Service Providers, a permanent and centralized information analysis and the dissemination of good practices, the specialized training of judiciary agents regarding the procedures relating to the acquisition, valuing and maintenance of the chain of custody of digital evidence, the specialized technical support to the Public Prosecutor by forensic IT experts, combined with the development of criminal prevention, namely *on-line* undercover operations, and the raising of public awareness of the dangers, constitute structuring factors in the prevention and repression of the phenomenon, tending to guarantee more safety to the children.

Key-words: **crime, sexual exploitation, children, cyberspace.**

Agradecimentos

Na elaboração do presente trabalho tenho de agradecer à minha família, aos meus pais, aos meus irmãos, aos meus tios e à minha sobrinha Mariana, que pacientemente suportaram as minhas ausências em benefício do tempo que tive de dedicar na realização desta tarefa.

Aos meus Orientadores, Senhor Prof. Doutor Luís Miguel de Castro Larcher Castela dos Santos Cruz, Senhor Major-General José António Henriques Dinis e Senhor Major-General José Coelho de Albuquerque agradeço o tempo que me dedicaram e a paciência com que foram lendo e aconselhando.

Ao Senhor Procurador da República, Dr. Edgar Manuel Taylor de Jesus, meu "*Formador"*, tenho de agradecer a celeridade com que sempre me facultou os elementos que solicitei e o benefício da sua amizade.

Ao Senhor Tenente-coronel Francisco Manuel dos Ramos Nunes pelo contínuo apoio que me tem dispensado e pelas conversas que fomos mantendo no esclarecimento dúvidas.

Aos meus camaradas da 2.ª Edição do Curso de Mestrado de Guerra da Informação da Academia Militar, pelo que me ensinaram e pelo espírito de entreajuda que construímos.

E a todos os que me ajudaram, um singelo registo e agradecimento.

Índices

Índice de títulos

Lista de Tabelas

Lista de Figuras

Siglas e Abreviaturas

Art. – Artigo

Acórdão – Ac.

CEDH – Convenção Europeia dos Direitos do Homem

CMC – Comunicações Mediadas por Computador

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

CTCE - Convenção do Conselho da Europa relativa à luta contra o Tráfico de Seres Humanos

DNS – Domain Name System

DOJ – United States Department of Justice

ECPAT – End Child Prostitution, Child Pornography and the Traficking of Children for Sexual Purposes

EUA - Estados Unidos da América

FBI – Federal Bureau of Investigation

FTP – File Transfer Protocol ou protocolo de transferência de ficheiros

HTML – HyperText Markup Language

IC – Investigação Criminal

INML – Instituto Nacional de Medicina Legal

IP – Internet Protocol

ISP – Internet Service Provider

IWF - Internet Watch Foundation

LCiber – Lei do Cibercrime (Lei n.º 10/2009, de 15 de Setembro)

MAC – Media Access Control

MD 5 - Message-Digest Algorithm 5

NSPCC - National Society for the Prevention of Cruelty to Children

OIT – Organização Internacional do Trabalho

ONGs – Organizações não governamentais

ONU – Organização das Nacões Unidas

OPC – Órgão de Polícia Criminal

P2P – Peer-to-Peer

PGDL – Procuradoria-Geral Distrital de Lisboa

PGR – Procuradoria-Geral da República

SI – Sistemas de Informação

STE – Série de Tratados do Conselho da Europa

TIC – Tecnologias de Informação e Comunicação

TRL – Tribunal da Relação de Lisboa

TRP – Tribunal da Relação do Porto

URL – Uniform Resource Locator

VGT – Virtual Global Taskforce

WWW – World Wide Web

Capítulo 1
Introdução

1.1. Considerações iniciais

O contínuo e rápido desenvolvimento das Tecnologias de Informação e Comunicação (TIC) fez com que os Sistemas de Informação (SI) sejam hoje parte integrante da vida das pessoas, das empresas, dos governos e das organizações internacionais. A *"sociedade do papel"* tem transitado de uma forma acelerada para uma *"sociedade digital",* afluindo na Era da Informação.

Em termos similares, no que concerne a práticas delituosas de natureza criminal, temos assistido a uma transferência das ações criminosas para o Ciberespaço com a utilização intensiva das TIC e dos SI.

O presente estudo incide sobre os procedimentos e as técnicas utilizadas pela investigação criminal, na aquisição e valoração da prova de natureza digital no que concerne à exploração sexual de crianças no Ciberespaço. O estudo aborda as inúmeras variáveis e transmutações que este locus encerra, com destaque para as decorrências da introdução em curtos intervalos de tempo de novas tecnologias e serviços e sem escamotear o tipo de crime e a especificidade da população alvo desse tipo de crime.

O sistema legal tem produzido inúmeros textos normativos, no âmbito da Investigação Criminal (IC) que manifestam preocupação com as atividades criminosas no Ciberespaço, designadamente no que concerne ao abuso sexual de crianças e a pornografia de menores e de que são exemplo, entre outros, o Código Penal (CP), a Lei do Cibercrime (LCiber), a Convenção do Conselho da Europa contra a Exploração e o Abuso Sexual de Crianças e a Diretiva do Parlamento Europeu relativa à luta contra o Abuso e a Exploração Sexual de Crianças e a Pornografia Infantil, esta última, de 13 de dezembro de 2011. Em tempos de acelerada mudança, como são os que vivemos, as preocupações têm como enfoque o conseguir conferir maior eficácia no combate a este tipo de criminalidade no Ciberespaço, no respeito pela Constituição da República Portuguesa (CRP) e no cumprimento da Lei.

Tendo presente que as crianças e os mais jovens sentem grande atratividade pelas novas tecnologias, a condução de um estudo que tem como sujeitos seres humanos nos

primórdios da sua formação emocional, salvaguarda do futuro da sociedade, impõe que a abordagem do tema seja realizada com enorme delicadeza e se lhe reconheça primordial importância.

Âmbito

O âmbito da investigação está circunscrito ao fenómeno da exploração sexual de crianças no Ciberespaço concretizada no abuso sexual de crianças e na partilha e disseminação de pornografia de menores.

Contexto

A exploração sexual de crianças é uma das mais graves formas de violência cometida contra elas. A pornografia é uma das suas manifestações com particular dimensão. A incriminação da pornografia infantil autonomamente da incriminação que tem por objeto o abuso sexual de crianças, a nível nacional e internacional, constitui um progresso civilizacional relevante. Contudo, não podemos deixar de abordar os dois fenómenos per si e de forma conexa, uma vez que a posse e a disseminação no Ciberespaço da pornografia de menores ou de material de abuso sexual, pressupõem, na grande maioria dos casos, o abuso sexual de crianças e adolescentes em sentido próprio e material.

A IC deste tipo de fenómenos está confrontada com enormes dificuldades e constrangimentos expressos, por exemplo, nas preocupações ao nível da União Europeia no âmbito da utilização das TIC por parte das crianças. Das dificuldades com que a IC deste fenómeno está confrontada, merecem destaque as que emergem da utilização a nível mundial da Internet. Esta realidade provoca dispersão de agentes e esta dispersão é agravada pelas dificuldades inerentes à aquisição da prova de natureza digital. Este tipo de prova caracteriza-se pela volatilidade, instabilidade, diversidade de tecnologias utilizadas e o anonimato oferecido pelas TIC aos agentes deste tipo de violência. A essa caracterização acresce a necessidade de análise de grandes quantidades de informação. De tudo isto decorre uma extrema dificuldade na identificação de vítimas e agressores.

A repressão deste fenómeno confronta-se ainda com a dificuldade decorrente da diversidade de ordenamentos jurídicos nacionais. Esta diversidade requer que a validação da prova digital forense utilize metodologias diferentes, de país para país, com possibilidade de perda da eficácia da validade da prova obtida num determinado país, quando esta é necessária para a prova de outro caso numa investigação de um país terceiro.

Objetivo

No contexto descrito, este estudo procurará responder ao problema de como melhorar a produção de prova nas investigações criminais deste tipo de fenómenos, visando-se, em

sede de conclusões, formular recomendações e linhas orientadoras (*guidelines*) que permitam uma resposta célere e sólida a este tipo de casos, tendo em vista, por exemplo, o reconhecimento mútuo da prova digital adquirida, independentemente do local geográfico onde se cometeram os atos concretos e a colaboração conjunta entre entidades de diferentes países dedicadas à IC.

O conhecimento sobre os mecanismos tecnológicos e procedimentos utilizados na perseguição penal deste tipo de infratores nunca poderá ser dado por completo o que justifica ação contínua de formação, investigação e estudo das tecnologias. Acresce que, no âmbito desta investigação e no domínio da IC em causa, a intensificação da transferência de práticas criminais para o Ciberespaço justificam a premência em identificar as melhores práticas como ponto de partida de futuras melhorias incrementais, sobretudo no que concerne à aquisição e valoração da prova forense de natureza digital, práticas que não prejudiquem a eficácia do exercício da ação penal e permitam ganhos de eficiência no combate ao abuso sexual de crianças e à posse e disseminação de material de abuso sexual de menores no Ciberespaço.

Questão Central, Questões Derivadas e Hipóteses

O estudo pretende dar resposta à seguinte Questão Central:

Tendo em consideração a transferência para o Ciberespaço de atividade delituosa relativa à exploração sexual de menores é possível implementar procedimentos de IC que, com eficácia, acautelem a aquisição de prova digital e potenciem a condenação dos que se dedicam a tais tipo de práticas criminosas?

O esclarecimento da Questão Central será obtido através da resposta às questões derivadas (QD) seguintes:

QD1 – Na dimensão do Ciberespaço existem restrições às investigações deste tipo de casos de exploração sexual de menores?

QD2 – A nível nacional são seguidos procedimentos e metodologias de investigação padrão alinhados com o que é adotado por organizações internacionais que fazem IC neste âmbito?

QD3 – Existe uma ou mais dimensões de atuação comuns ao que é reconhecido como acervo das melhores práticas para a investigação deste tipo de criminalidade?

Das questões acima enunciadas, resultaram as seguintes hipóteses (H) que, total ou parcialmente, iremos procurar validar ou refutar ao longo do trabalho:

H1 – O Ciberespaço, pela sua natureza global, sofisticação e instabilidade tecnológica, sem fronteiras nem "capitais estáticas"/"centros de operação estáticos", confronta a IC com

dificuldades novas que, em paralelo com outros fenómenos de natureza global, exigem resposta que, para ser eficaz, tem de ser global.

H2 – A complexidade deste fenómeno e a prática da IC neste âmbito confronta-se a nível nacional com a ausência de padrões de atuação e com as dificuldades decorrentes de uma incipiente cooperação internacional.

H3 – Uma articulação investigatória com autoridades internacionais e a atuação concertada, com realce para a monitorização dos conteúdos no Ciberespaço, entre os prestadores de serviço neste domínio e as autoridades com competências de IC, são dimensões estruturantes do acervo das melhores práticas de IC neste tipo de casos.

1.2. Metodologia

No curso desta investigação o Ciberespaço será caracterizado em várias das suas vertentes e abordar-se-á, sucintamente, a legislação referente ao fenómeno, designadamente as convenções e recomendações relacionadas com a violência sexual sobre crianças sobretudo ao nível dos instrumentos jurídicos internacionais das Nações Unidas (ONU), do Conselho da Europa e da União Europeia. Subsequentemente, será analisada a legislação nacional, designadamente CP e CPP e outra legislação relevante no âmbito do Cibercrime e indagar-se-á da existência de linhas orientadoras (*guidelines*) para investigação de casos de exploração sexual de crianças no Ciberespaço e das metodologias utilizadas para a deteção do fenómeno e para a aquisição e valoração da prova digital, designadamente ao nível da ONU, da União Europeia, do *United States DOJ – Department of Justice* e da ECPAT – *End Child Prostitution, Child Pornography and the Traficking of Children for Sexual Purposes*.

Em Portugal o tratamento e acesso a dados quantitativos são drasticamente dificultados, porque na Justiça Portuguesa os indicadores estatísticos existentes não individualizam o agregado de crimes de exploração sexual de crianças que utilizaram dispositivos eletrónicos ou as TIC. Em conformidade, no contexto da presente investigação e atento o objetivo definido, far-se-á a revisão de 10 casos concretos que correram termos nos Serviços do Ministério Público responsáveis pela direção de investigações criminais relacionadas com estes casos, e também nos Tribunais. Estes casos iniciam-se por denúncia dos ofendidos, por identificação de tráfego na Internet conexo com esta realidade, por parte de Autoridades Policiais Internacionais (eg.: Interpol ou Europol) ou no decurso de perícias informáticas forenses relacionadas com outros crimes, designadamente crimes violência doméstica ou ameaças. Mereceram destaque casos que recorreram a perícias

informáticas forenses cuja realização questionaremos atentos os termos do direito penal português.

Em termos de enquadramento geral deste estudo passar-se-ão em revisão os casos de referência a nível internacional. Estes casos são indiciadores da extensão do problema que enfrentamos em Portugal no âmbito da IC.

1.3. Casos de referência a nível internacional

Caso *Cathedral*

Um dos processos-crime que maior impacto teve na comunicação social ocorreu nos E.U.A. – Estados Unidos da América e é identificado como o caso *Cathedral* iniciado no Estado da Califórnia, em abril de 1996 (Leite, 2004, p. 15 e 16). As investigações tiverem origem num pequeno episódio que à partida parecia isolado, mas que acabou por envolver várias centenas de investigadores, de vários países, face a um número incalculável de vítimas. A história do processo judicial inicia-se com a visita de uma criança de 10 anos a casa de uma amiga da escola, para aí passar o fim de semana. Durante essa visita, o pai da amiga fechou a criança no seu quarto, onde se encontrava um computador ligado à Internet equipado com uma *webcam* – câmara de filmar que projeta as imagens em tempo real nos computadores que se encontrem ligados a um determinado sítio, na Internet. No seu quarto, o pai da amiga abusou sexualmente da criança em causa, tendo filmado os abusos e difundido os mesmos, em tempo real, para o Ciberespaço, através da referida câmara de filmar. Durante o abuso sexual, o agressor recebeu instruções das pessoas que estavam a assistir pela Internet, relativamente aos abusos sexuais que deveriam ser praticados com a criança. As imagens foram difundidas num *website*, denominado *Orchid Club*. O agressor gravou as imagens do ato que praticou e vendeu-as, a troco de quantias monetárias, através da Internet. A investigação descobriu o que sucedeu através do testemunho da criança em causa e o agressor foi condenado a 100 anos de prisão.

Caso *Wonderworld*

Após a análise efetuada ao computador do agressor do caso *Cathedral* foram descobertas ligações relativas a outros clubes, que se dedicavam à prática de atos da mesma natureza, entre eles o *Wonderland Club*. Esse clube era altamente organizado, constituído por um presidente, um secretário e um comité executivo, existindo regras estritas de admissão e expulsão de membros. O acesso ao clube era também muito limitado, existindo cinco graus de segurança e várias áreas com códigos e informação encriptadas. Muita desta informação ou áreas do clube nunca foram descodificadas com

sucesso pela investigação e por isso ficarão desconhecidas para sempre. Entre os dados que a investigação criminal conseguiu obter, encontravam-se 1.263 crianças diferentes, num total de 750 mil imagens e 1.800 horas de filme.

À semelhança do caso *Cathedral*, os membros do *Woderland Club* abusavam de crianças com difusão de imagens em tempo real, seguindo instruções dos outros membros em linha. O membro mais ativo desse clube, que mantinha várias crianças detidas em casa, foi condenado numa pena de 12 anos de prisão.

Na sequência deste caso, detetaram-se conexões a vários países Europeus, tendo sido efetuadas buscas, apreensões e detenções de pessoas, de forma simultânea, nos seguintes países: Austrália, Áustria, Bélgica, Finlândia, França, Alemanha, Itália, Noruega, Portugal, E.U.A., Inglaterra e Suécia.

Operação *Avalanche*

A Operação *Avalanche* teve início nos E.U.A. em 1999 depois de terem sido apresentadas cerca de 250 queixas por parte de utilizadores da Internet por todo o mundo. As queixas referiam-se à maior rede de exploração sexual de crianças ativa, à data, nos E.U.A., denominada *Landslile Productions*. Tratava-se de um Portal contendo imagens de pornografia de menores, com ligações a aproximadamente 300 páginas de Internet, os quais continham também material de pornografia de menores. O acesso a essas imagens e vídeos de crianças era concretizado mediante pagamentos efetuados através de cartões de crédito. Estimou-se que este sítio tivesse cerca de 250.000 subscritores. Um mês de subscrição tinha um custo de 30 dólares. Em apenas 1 mês, o *website* em referência gerou um lucro US$ 1.400.000,00. A associação criminosa encontrava-se sediada nos E.U.A., tinham 1 parceiro na Rússia e 4 na Indonésia (Ecpat, 2011, p. 154).

Cerca de 100 pessoas foram acusadas pela prática de crimes contra a infância nos E.U.A., designadamente por posse e disseminação de pornografia de menores. Os suspeitos foram localizados através dos dados dos pagamentos efetuados com os cartões de crédito. O líder da associação criminosa, que se encontrava a gerir o Portal foi condenado a 1.335 anos de prisão. A mulher, que tratava da contabilidade do Portal foi condenada a 14 anos de prisão.

O *FBI – Federal Bureau of Investigation* forneceu às Autoridades Inglesas informação sobre 7.272 suspeitos residentes noutros países. No total, a Polícia Inglesa concretizou 3.744 detenções durante a investigação da "Operação *Avalanche*" que em território

Britânico foi denominada "Operação *Ore*". Foram acusados 1.848 suspeitos dos quais foram condenados 1.451.

Aspectos relevantes

Os parágrafos seguintes constituem registo dos aspetos mais relevantes que emergem da revisão dos casos referenciados, e permitem distinguir papéis entre diferentes intervenientes, no âmbito da exploração sexual de crianças:

- Atores – os que aparecem nas imagens como abusadores;
- Produtores e realizadores – os que contribuem para a captação de imagem e produção do material pornográfico, diretamente ou fornecendo meios técnicos ou financeiros;
- Distribuidores – os que entram em contacto apenas com o produto final e o promovem e fornecem aos destinatários; e por fim,
- Consumidores.

A distinção supra releva de diferentes tipos de atividade com um denominador comum, toda ela de índole criminal e com utilização do Ciberespaço e das TI. Os locais de ocorrência dessas atividades são de difícil determinação e contabilização.

É difícil estimar o número de websites a nível mundial que retratam imagens de abuso infantil. A Internet Watch Foundation (IWF) identificou e tomou medidas contra 16.700 casos de conteúdos de pornografia de menores em páginas da web, em todo o mundo em 2010, em comparação com a identificação de cerca de 10.656 em 2006 (IWF, 2007-2010, p. 8). No entanto, a IWF reconhece a dificuldade de comparar dados anuais. As rápidas mudanças no armazenamento e manipulação de imagens de abuso infantil tornam o número de dados de imagens e páginas web incompatíveis, o que dificulta a comparação de dados.

O aumento de casos, observado entre 2006 e 2010, pode ser atribuído a uma mudança nos padrões do armazenamento das imagens – em vez de se colocar coleções de imagens numa pasta, ou numa única página da web, o conteúdo pode estar a ser disponibilizado em vários websites. Contudo, é de realçar que as imagens de abuso sexual de crianças são cada vez mais comuns entre as redes de indivíduos ligados através das redes peer-to-peer (P2P)[1] de distribuição e esse *modus operandi* não necessita de armazenamento das imagens em sistemas propriedade de terceiros (i.e. fornecedores de serviços Internet (ISP). Há milhões

[1] Peer-to-peer (P2P) - software que permite transmissão de dados diretamente de um computador para outro através da Internet, sem a necessidade de envolver um servidor de terceiros.

de imagens de abuso de menores na Internet, com dezenas de milhares de crianças retratadas em imagens individuais, relacionadas com o abuso sexual de crianças (Carr et al., 2009, p. 29). Uma vez na Internet, as imagens podem ser facilmente transmitidas para outros websites, carregadas para telemóveis ou distribuídos a um número desconhecido de destinatários via e-mail de um modo semelhante à difusão de um vírus informático, sem o conhecimento ou consentimento da pessoa retratada. Potenciais agressores são capazes de comunicar e partilhar imagens e outros materiais em todo o mundo. Conexões de alta velocidade à Internet, maior largura de banda, aumento do uso de redes P2P, mecanismos de compressão de dados, tecnologia mais sofisticada, técnicas de criptografia para facilitar a distribuição anónima, e novos meios de acesso à Internet através de Wi-Fi em telemóveis e com cartões pré-pagos, tudo isto reduz a rastreabilidade de quem utiliza esses meios e contribui para o aumento da atividade de exploração abusiva e on-line de crianças. A criança não tem controlo sobre as imagens e estas podem permanecer para sempre no ciberespaço. Algumas imagens atualmente em circulação podem ter sido produzidas há mais de 20 ou 30 anos e desde então foram digitalizadas e depois publicadas na Internet. No entanto, a grande maioria das imagens no ciberespaço foi produzida mais recentemente e estão ligadas à disponibilização de novas tecnologias de alta qualidade, designadamente câmaras digitais, e à circunstância de Internet ser hoje um produto de consumo em massa. Estas imagens mais recentes podem ter origem no ambiente familiar da criança, no seu círculo social, ou ter sido adquiridas através da prostituição infantil de menores.

A colocação de imagens de abuso infantil em linha pode ter consequências duradouras para as crianças. Essas imagens, uma vez publicadas no ciberespaço, são quase impossíveis de eliminar. As crianças dessas fotos podem perceber que para o resto de suas vidas alguém pode estar a visualizar as suas fotografias na Internet. Por outro lado, a ameaça da publicação das imagens pode, só por si só, constituir uma forma de coação utilizada por abusadores sexuais de crianças, permitindo-lhes continuar o abuso sexual a longo prazo.

Os agressores também podem *"vender"* as crianças para fins de abuso sexual, em linha em tempo real. Para o efeito, os utilizadores publicitam na sua *peer* (rede privada) *on-line* a sua intenção de abusar de uma criança numa data/hora (Tink et al., p. 10-14). Aqueles que desejam assistir ao vivo ao abuso organizam-se com o agressor para estar em linha naquele momento. O pagamento para assistir a este ato criminoso pode ser efetuado em dinheiro ou através da contraprestação de imagens ou produtos estupefacientes. As crianças podem ser atraídas para a casa do ator, e a vítima do abuso sexual, pode ou não estar ciente de que a transmissão ao vivo está a ocorrer.

Sucede que a aquisição, valoração e a preservação da prova de natureza digital devido às características inerentes a este tipo de prova, diversidade de tecnologias utilizadas e o anonimato oferecido pelas TIC aos agentes deste tipo de violência, demanda especiais exigências aos vários intervenientes num processo de IC, designadamente:

- Investigadores que intervêm na cena do crime;
- Peritos informáticos forenses, isto é que são nomeados pelas autoridades judiciárias, para proceder ao exame e análise dos dispositivos digitais apreendidos na sequência de mandado de busca domiciliária ou não domiciliária; e
- Magistrados judiciais e do Ministério público, que devem assegurar a validade da prova obtida, de acordo com as melhores técnicas da ciência computacional forense e as regras legais aplicáveis.

O objetivo deste estudo é, assim, analisar de que forma se procede à articulação entre os textos normativos que incidem sobre a exploração sexual de crianças no Ciberespaço e a pornografia de menores em Portugal, com as normas técnicas de computação forense, que assegurem a aquisição, integridade e validade técnica e jurídica na aquisição da prova digital, no âmbito deste tipo de atividade delituosa, de forma a detetar oportunidades na repressão deste fenómeno.

Para respondermos à questão central começaremos por abordar, no capítulo que se segue, o *locus* Ciberespaço, as normas jurídicas internacionais e internas aplicáveis ao fenómeno e analisaremos 10 casos que correram termos no Sistema de Justiça Penal.

Capítulo 2

O Ciberespaço, o direito e casos de exploração sexual de crianças

2.1. Enquadramento

No sentido de compreendermos as características inerentes à exploração sexual de crianças e a complexidade inerente à IC deste fenómeno no Ciberespaço identificar-se-ão as características e particularidades que este "espaço" encerra.

Com previsão notável, William Gibson, em 1984, no romance *"Neuromancer"* (Gibson, 1984, p. 12) previu que a crescente dependência da sociedade dos computadores e tecnologias de informação criaria um universo virtual eletrónico, a que denominou Ciberespaço. Pouco anos mais tarde, o Ciberespaço tornou-se muito mais do que uma premissa, uma ficção ou romance. A Internet, rapidamente e com surpresa, tornou-se comum na vida diária e cada vez mais vital para a aquisição de conhecimento e comunicação entre pessoas de todo o mundo. Não surpreendentemente, os jovens constituem um dos segmentos das populações que mais crescem na utilização da Internet, com especiais competências para interagir com as novas tecnologias, que as gerações dos seus pais não possuem.

A partir destas considerações, o termo "Ciberespaço" pode ser definido como *locus* virtual criado pela conjunção das diferentes tecnologias de telecomunicação e telemática, em especial, mas não exclusivamente, as mediadas por computador. É importante sublinhar que essa definição não circunscreve o Ciberespaço às redes de computadores, mas abarca as diferentes formas de comunicação da Informação, desde teleconferências analógicas, passando por redes de computadores, "*pagers*", comunicação entre radioamadores e por serviços do tipo *"tele-amigos"* ou redes sociais.

Um aspeto sinistro da premissa de Gibson tem implicações alarmantes para os pais, educadores e investigadores criminais. Gibson refere, que o conceito de Ciberespaço contém cantos escuros e becos escondidos onde a atividade criminosa floresce e que ações eletrónicas podem ter repercussões físicas. Na Internet de hoje, as ações eletrónicas dos incautos e vulneráveis podem levar à perseguição e roubo no mundo físico e à prática de ações que constituem outros ilícitos criminais. Com efeito, as crianças e adolescentes

podem tornar-se vítimas de abuso sexual fornecendo informações pessoais e desenvolver relacionamentos com os infratores que os atraem, a suas casas ou a espaços fechados, para fins de natureza sexual (Medaris et al., 2002).

A Internet, apesar de ser a mais presente, não é a única instância de CMC, e por extensão, de suporte ao Ciberespaço. Atualmente percebe-se uma tendência de unificação da esfera global de telecomunicações a partir de plataformas digitais, seja a partir da rede Internet *"pública"* ou de outro tipo redes e dispositivos. A Internet é a rede das redes, na medida em que constitui verdadeiramente uma rede global e integrante. É um sistema global de redes de computadores interconectadas, que usam o conjunto standard do Transmission *Internet Protocol* (TCP/IP). Esta rede é constituída por milhões de redes de computadores privados, públicos, de empresas, de governos, faculdades, entre outras instituições, que estão ligadas entre si através de tecnologias de rede diversas. A Internet disponibiliza uma série de serviços e protocolos como são os casos da *World Wide Web* (WWW) http, https, ftp e ftps, ou da infraestrutura de suporte ao correio eletrónico com recurso a SMTP, POP e IMAP, a título exemplificativo.

Um computador para estar ligado à Internet tem de ter uma identificação – endereço IP. Para que outros computadores que com ele queiram comunicar e lhe consigam endereçar as suas mensagens, têm que o identificar e localizar na rede, função que o endereço IP realiza. É possível estabelecer uma analogia entre números de telefone e endereços IP. Quando se telefona para alguém, antes de mais é necessário saber o seu número de telefone. Quando um computador ligado à Internet precisa de enviar dados para outro, precisa conhecer o endereço IP do destinatário. Se desconhecemos o número de telefone para onde queremos telefonar, recorre-se à lista telefónica para obter o número. De forma semelhante os computadores recorrem a um serviço de diretório, denominado DNS (*Domain Name System*) para traduzir os nomes para endereços IP. Por exemplo, o nome www.pgr.pt, da PGR, traduz-se atualmente para o endereço IP 194.76.65.202. Deste modo, para visualizar a página da PGR digita-se no nosso *browser* o endereço: http://www.pgr.pt., onde http é o método pelo qual a informação deve ser obtida e www.pgr.pt é o nome do servidor onde a página que desejamos está armazenada. Pelo nome do computador, normalmente, pode-se inferir o tipo de informação a encontrar e a sua localização geográfica (eg: .pt pertence a Portugal, .es a Espanha).

2.2. O correio eletrónico e aplicações afins

O correio eletrónico permite compor, enviar e receber mensagens através de sistemas eletrónicos de comunicação. O termo e-mail é aplicado tanto aos sistemas que utilizam a Internet e são baseados no protocolo SMTP – *Simple Mail Transfer Protocol*, como aqueles sistemas assentes em redes internas, que permitem a troca de mensagens dentro de uma empresa ou organização e são, normalmente, baseados em protocolos proprietários. O envio e a receção de uma mensagem eletrónica efetuam-se através de um sistema de correio eletrónico. Um sistema de correio eletrónico é composto por programas de computador que suportam a funcionalidade de cliente de e-mail e de um ou mais servidores de e-mail que, através de um endereço de correio eletrónico, conseguem transferir uma mensagem de um utilizador para outros endereços de e-mail.

Estes sistemas utilizam protocolos de Internet que permitem o tráfego de mensagens de um remetente para um ou mais destinatários que possuem computadores conectados à Internet – este serviço é disponibilizado em toda a Web, a nível mundial, designadamente pelos ISP e por outras empresas com atividade no Ciberespaço (eg.: Google, Microsoft, Yahoo), de forma gratuita, sendo possível criar contas de correio eletrónico em qualquer parte do mundo, indicando, com facilidade, uma identidade associada, não correspondente com a realidade objetiva. As aplicações de correio eletrónico normalmente oferecem ao utilizador uma série de funcionalidades. A maior parte delas fornece um editor de texto embutido e a possibilidade do envio de arquivos anexados à correspondência. As imagens digitais, música, filmes, ficheiros de texto e outros tipos de dados constituem exemplos típicos do tipo de arquivos anexados a uma mensagem de correio eletrónico. Assim, distribuidores de pornografia de menores podem utilizar o correio eletrónico para transmitir material de abuso sexual, mas não podem usá-lo para enviar ficheiros de grandes dimensões, uma vez que os sistemas de correio eletrónico não suportam o envio e a receção de grandes quantidades de informação. Na maioria das vezes, se as imagens são anexadas a uma mensagem de correio eletrónico, o remetente partilha, com o envio dessas imagens, os seus interesses particulares com outro coletor ou distribuidor de material de abuso de menores, sendo irrelevante o local físico onde o distribuidor e o consumidor se encontrem (eg.: a distribuição de pornografia infantil através de correio eletrónico para diversos destinatários de todo o mundo pode ser instantânea). O envio deste tipo de ficheiros pode ter como fim o aliciamento de uma vítima através da visualização de

imagens ou vídeos de abuso de menores (Ac. TRP, 2010-11-17)[2] – o envio deste tipo de imagens permite que o potencial abusador dê a conhecer à vítima o contexto sexual sobre o que poderia estar a acontecer com uma pessoa da sua idade, contribuindo para a dessensibilização da vítima-menor quanto à ilicitude de tais comportamentos, ou ainda fazer saber o que gostaria de praticar com a vítima.

Quando uma mensagem de correio eletrónico é enviada, dá-se um processo de divisão em "pacotes" contendo peças da mensagem. Cada pacote é rotulado com informação, como um conjunto de instruções para todos os servidores em que passará, com informação sobre o destinatário, a identificação de quem enviou, de onde enviou, e em que data-hora. Podemos considerar que seria complexo que alguém conseguisse reunir todos os pacotes para recuperar uma mensagem de correio eletrónico. Contudo, ferramentas como o *Ethereal* ou o *Wireshark*, disponíveis na Internet, conseguem tornar esse processo trivial, desde que sejam operadas por um utilizador com conhecimentos e capacidades técnicas avançadas, ou seja, é possível do ponto de vista técnico, cumpridas as formalidades legais e através, por exemplo de ações encobertas e ou no âmbito de um processo-crime, que as Autoridades de IC intercetem mensagens com ficheiros de material de abuso sexual de menores enviadas por predadores para potenciais vítimas (ver Apêndice 3 sobre ações encobertas).

2.3. *Websites* e conversação em linha

A Web tornou-se possível em 1989 com implementação do *HyperText Markup Language* (HTML). A criação de computadores e da linguagem HTML possibilitaram o acesso à Internet e a comunicação entre indivíduos e a possibilidade de "ver" e partilhar a mesma informação, apesar da utilização de diferentes tipos de sistemas operacionais. Desde 1989, a Web tem proliferado, permitindo a partilha sem precedentes de informação à escala global. A Web também permitiu o desenvolvimento do comércio eletrónico e de muitos outros serviços o que conduziu, indubitavelmente, ao aumento contínuo da utilização da Internet.

Um *site* é um serviço web a que corresponde um ficheiro principal (normalmente index.html) que tem ligações para outros ficheiros, denominados "páginas Web",

[2] Caso de difusão de material de exploração sexual de menores através do Ciberespaço, com conexão com Portugal e intervenção de indivíduos de diversas nacionalidades (ingleses, franceses, alemães, suíços e espanhóis), que se encontravam registados num *website* de pornografia infantil alemão e que utilizavam correio eletrónico para acordar no envio de suportes digitais de pornografia infantil.

acessíveis através dos *browsers* de navegação na Internet. Esses arquivos contêm texto, som, imagens, vídeo, e quaisquer combinações dos tipos de ficheiros precedentes. Cada *site* tem um endereço – um *Uniform Resource Locator* (URL). Cada página Web é, assim, composta pelas denominadas componentes HTML *tags* ou conjuntos de instruções, que dizem ao navegador como exibir a página da web, os quais podem conter material de abuso sexual de menores ou ainda salas de conversação *on-line*.

O termo conversação *on-line* ou *chat* consiste na comunicação em tempo real entre dois ou mais utilizadores. Sucede que a conversa entre um predador de crianças e a potencial vítima de abuso sexual inicia-se muitas vezes numa "sala virtual". Numa sala virtual, em princípio, todos os participantes são indexados, com identificação dos nomes de utilizadores ou de nomes inventados por estes – *nicknames* –, identificação do acesso à Internet, dados que podem ser vistos pelos outros utilizadores, embora seja possível esconder o ponto de origem físico da comunicação, através do estabelecimento de uma ligação "indireta" através de uma linha privada adquirida noutro país do mundo, dificultando a identificação concreta de eventual agressor sexual de crianças. As salas de conversação virtual têm muitas vezes um tema relativamente ao qual se pressupõe que as pessoas troquem ideias sobre esse assunto. Algumas salas são monitorizadas por um moderador, mas a maioria não o são. A conversa virtual apela para crianças mais velhas devido à necessidade de se ter aptidão para comunicar com muitas pessoas em tempo real. As conversações neste ambiente são mais abrangentes do que uma simples conversação telefónica, uma vez que se permite que os participantes conversem simultaneamente com um grupo, comuniquem com outro utilizador em salas privadas, naveguem na Internet e desenvolvam simultaneamente outras tarefas como a troca, partilha e envio de ficheiros. Muitas pessoas usam as salas de conversação para conhecer outras pessoas na Internet. Como exemplo, referimos o depoimento da vítima X, que descreve a sua primeira experiência em linha, quando tinha treze anos de idade*: "Foi inacreditável. O número de temas disponível era inimaginável. Nunca tinha suposto que muitos dos temas poderiam existir, incluindo um chamado overdrive sexual, o que quer que seja que isso significasse. Muitas das salas estavam preocupadas com sexo, mas também existiam de conversas de adolescentes. As salas de adolescentes não foram divididas em áreas de interesse. Em vez disso foram chamadas simplesmente TEEN1, TEEN 2, etc. – eu pensei que acolheriam pessoas da minha idade e que poderia conversar com eles, através de mensagens instantâneas e em privado"*(Ferraro et al., 2005, p. 135). A comunicação através de mensagens instantâneas acontece em tempo real e consiste no envio de mensagens escritas

de forma bidirecional. O recurso que distingue o serviço de mensagens instantâneas das salas de conversação é que aquele permite a transferência de arquivos, ao contrário do que sucede nas salas de conversação.

2.4. Outras formas de comunicação em linha

Muitos computadores pessoais dispõem de uma câmara que permite enviar imagens para outro destinatário. Uma câmara *web* ou *webcam* é um equipamento digital de recolha de imagem e som, de fácil instalação, cuja utilização é reconhecida pela maioria dos softwares de comunicação (eg.: *Skype*). Um dos casos referidos na utilização de uma *webcam* no âmbito da exploração sexual de crianças no Ciberespaço é o de um rapaz de 13 anos do Estado da Califórnia, nos EUA que, a troco de dinheiro e de presentes de adultos, sem o conhecimento dos seus pais, se passou a exibir perante terceiros, vendendo imagens do seu corpo através da Internet, estimando-se que a audiência tenha alcançado as 1500 pessoas, no ano de 2000 (Eichenwald, 2005) – o exemplo precedente oferece apenas um vislumbre sobre a dimensão deste fenómeno.

A facilidade de uso da tecnologia que suporta as *webcams*, aliada ao seu baixo custo e portabilidade, garantem por si que este tipo de equipamentos e tecnologias serão utilizados durante o processo de exploração sexual de crianças. Antevê-se que o alargamento do acesso a esta tecnologia e à Internet, a que se alia a constante inovação tecnológica (eg.: telemóveis com videochamadas) terá como correlação um número constante e crescente de vítimas de exploração sexual de crianças através do Ciberespaço.

Por outro lado, existem ferramentas tecnológicas que permitem a troca de grandes quantidades de material de abuso sexual de menores, sem as limitações do correio eletrónico: o *File Transfer Protocol* (FTP) ou protocolo de transferência de ficheiros é uma forma rápida e eficaz de transferir arquivos de grande dimensão através da Internet, como é o caso das imagens de abuso sexual de menores. O FTP permite o seguinte: a partilha de ficheiros entre máquinas distantes; uma independência dos sistemas de ficheiros das máquinas clientes e servidor e a possibilidade de transferir grandes quantidades de dados de forma eficaz. Através da utilização do protocolo FTP muitos criminosos partilham, consomem ou trocam centenas de milhares de imagens de pornografia de menores, com amplas dificuldades de deteção por parte das Autoridades de IC.

Refere-se ainda, a título de exemplo, as aplicações Peer-to-Peer (P2P). Estas aplicações foram desenvolvidas para colocar a capacidade de vários computadores a trabalhar para o mesmo objetivo: a partilha de ficheiros entre várias pessoas. As aplicações P2P embora

sejam utilizadas legitimamente para partilhar música, vídeos e outros tipos de arquivos e *softwares*, são também conhecidas e utilizadas para a partilha de material de abuso sexual de menores, conforme casos que veremos adiante. O *Napster*, por exemplo, é uma aplicação P2P disponível na Web para partilha de música. Este tipo de serviço permite aos utilizadores trocar arquivos e procurar por arquivos entre todos os materiais de utilizadores registados. Algumas aplicações actualmente mais conhecidas de tecnologia P2P são as seguintes: *Kazaa*, *BitTorrent*, *Morpheus*, *Gnutella*, *Frenet*, *WinMX* e *iMesh*. O *iMesh*, por exemplo, permite aos utilizadores pesquisar e gravar ficheiros de áudio, vídeo, imagem e arquivos de texto. O *iMesh* organiza-se em aglomerados de utilizadores *"próximos"* para pesquisar e partilhar ficheiros de forma mais eficiente. Se um arquivo não se encontrar numa máquina próxima, o *iMesh* estende a pesquisa através da rede, procurando o ficheiro pretendido pelo utilizador. Ou seja, este tipo de programas permite que os possuidores de ficheiros, com material de abuso sexual de menores, os distribuam com grande facilidade através da gravação de pequenos excertos ou pedaços do ficheiro original, que se juntam num determinado utilizador ou utilizadores, procedentes de várias localizações diferentes. Este tipo de configuração dificulta o trabalho de investigação da exploração sexual de crianças no Ciberespaço, uma vez que os recursos de *hardware* podem estar dispersos por várias partes do globo, existe anonimato dos utilizadores deste tipo de aplicações e os ficheiros só se encontram completos nas máquinas que gravam o ficheiro completo e, muitas vezes, as partes dos ficheiros não são percetíveis nas outras máquinas da rede privada.

2.5. Redes Sociais

Uma rede social é uma estrutura composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns. Uma das características fundamentais na definição das redes é a sua abertura e porosidade, possibilitando relacionamentos horizontais e não hierárquicos entre os participantes.

Muito embora um dos princípios da rede social seja a sua abertura e porosidade, por ser uma ligação social, a conexão fundamental entre as pessoas dá-se através da identidade. As redes sociais *on-line* podem operar em diferentes níveis, como, por exemplo, redes de relacionamentos (*Facebook*, *Orkut*, *MySpace*, *Twitter*), redes profissionais (*LinkedIn*), redes comunitárias (redes sociais em bairros ou cidades), redes políticas, entre outras: permitem analisar a forma como as organizações desenvolvem a sua atividade, como os

indivíduos alcançam os seus objetivos ou medir o capital na rede – o valor que os indivíduos obtêm da rede social.

Tem-se constatado que as redes sociais têm adquirido importância na sociedade moderna, existindo, por exemplo, casos recentes de mobilização de massas para manifestações, em todas as partes do mundo, designadamente no Médio-Oriente, no âmbito da denominada Primavera Árabe e mais recentemente na Europa e mesmo em Portugal, face às situações de crise económico-financeira. As redes sociais são caracterizadas primariamente pela autogeração do seu desenho, pela sua horizontalidade e descentralização. Um ponto em comum entre os diversos tipos de rede social é a partilha de informação, conhecimento, interesses e esforços em busca de objetivos comuns. A intensificação da formação das redes sociais, nesse sentido, reflete um processo de fortalecimento da Sociedade Civil, um contexto de maior participação democrática e mobilização social, que pode, contudo, potenciar o abuso sexual de menores, uma vez que, muitas vezes, a identidade virtual ou social não corresponde à identidade real.

Sobre a utilização de redes sociais na exploração sexual de crianças veja-se caso relatado no *site* da Procuradoria-Geral Distrital de Lisboa (PGDL) sobre a utilização de uma rede social para deteção e aliciamento de menor no âmbito da exploração sexual de crianças, que transcrevemos: Crimes sexuais sobre menor. *"Foi ontem concluído o julgamento (em 4 sessões), em Sesimbra, de indivíduo de 22 anos que, pelo Facebook, logrou captar a atenção de menor de 14 anos, com quem, por 5 vezes, teve relações sexuais completas, coito vaginal e oral, sempre numa viatura, a quem filmou, numa primeira vez com violência instrumental, nas outras usando a sua maior experiência e liderança afetiva, situação que se estendeu por Agosto e Setembro de 2011. Foram determinantes para a convicção judicial o depoimento da vítima, em memória futura e em audiência, e a apreensão de telemóvel que continha as imagens captadas durante os atos sexuais pelo próprio arguido* (PGDL, Atualidades, 2012).

Deste modo, o exponencial crescimento das redes sociais nos últimos anos e a partilha de informação pessoal aí disponibilizada, sobretudo pelos adolescentes (gostos, locais que frequentam, escola, família, morada, números de telefone, endereço de correio eletrónico) suportam a antevisão de que os que desejam explorar sexualmente as crianças recolham grandes quantidades de informação disponível e selecionem os seus alvos para realização de crimes, utilizando para o efeito identidades fictícias e escondendo-se através do anonimato e do *"amigo do amigo"* que as redes socias podem oferecer. De notar, que todos os exemplos de redes sociais indicados são geridos por empresas sedeadas fora de

Portugal, pelo que qualquer IC relacionada com factos conexos com a exploração sexual em Portugal naquelas redes sociais, pressupõe, neste âmbito, articulação e ativação dos mecanismos de cooperação judiciária internacional com as Autoridades de IC do país onde estas estão sediadas, designadamente os EUA.

2.6. Enquadramento Jurídico Internacional da exploração sexual de crianças

Para se investigar e detetar factos suscetíveis de configurar exploração sexual de crianças em sentido amplo é necessário apreendermos, do ponto de vista técnico-jurídico as condutas que estão em causa quando nos referimos a este fenómeno, efetuando uma análise dos textos internacionais, de natureza geral e enquadradora, e do direito interno português, mais específico no que concerne à descrição de condutas concretas.

Como primeira abordagem podemos referir que o abuso sexual de menores consiste no envolvimento de crianças e adolescentes dependentes e imaturos, com idade inferior à maioridade legal (18 anos, em Portugal), em atividades sexuais que não compreendem verdadeiramente, e para as quais são incapazes de dar consentimento informado. Já a pornografia de menores consiste em qualquer tipo de 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.

A nível internacional foram aprovados recomendações, relatórios e textos normativos no sentido de proteger as crianças contra o abuso sexual e a pornografia de menores no âmbito da ONU, do Conselho da Europa e da União Europeia, que vinculam o Estado Português enquanto membro dessas organizações internacionais, nos termos do Art. 8.º, n.º 2 da CRP. Para tanto é necessário que tais textos, constantes de convenções internacionais tenham sido regularmente ratificados e aprovados por Portugal, entrando em vigor na ordem jurídica interna após a sua publicação oficial.

No que concerne ao termo *"pornografia infantil"* importa referir o seguinte: apesar de o termo *"pornografia infantil"* poder ser utilizado com frequência na legislação e convenções internacionais, entende-se que o mesmo não descreve adequadamente o sentido material da conduta em causa que consiste no abuso e exploração de forma gravosa de crianças que estão envolvidas em representações visuais ou audiovisuais. A verdadeira natureza do problema é, em essência, imagens sexualmente explícitas ou representações de crianças, como definido, por exemplo, nas convenções internacionais. O termo *"pornografia"*, no entanto, é geralmente entendido como estando associado a descrições de atividade sexual entre indivíduos maiores e conscientes. Por esta razão, entende-se que o uso do termo

"pornografia infantil" descaracteriza a gravidade das representações sexuais, onde as crianças estão envolvidas e o uso contínuo deste termo é suscetível de gerar confusão de conceitos, impedindo que se percecione o dano real que é vivido por jovens vítimas e a gravidade das atividades dos indivíduos que exploram sexualmente crianças dessa forma. Este equívoco pode comprometer a eficácia dos esforços existentes para proteger as crianças a partir desta forma de exploração sexual, pelo que quando utilizamos o termo *"pornografia infantil"* deverá ter-se sempre presente que se trata de *"material de abuso sexual de menores"* (G8, 2007).

2.6.1. As Nações Unidas

No âmbito da ONU é de referir a Convenção das Nações Unidas sobre os Direitos da Criança, em particular o seu Art. 34.º que estabelece que os Estados Partes se comprometem a proteger a criança contra todas as formas de exploração e de violência sexuais. Como concretização do referido Art. 34.º foi aprovado o Protocolo Facultativo relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil no âmbito do qual os Estados ficam obrigados a proibir a venda de crianças, a prostituição infantil e a pornografia infantil.

De referir, ainda, no âmbito da Organização Internacional do Trabalho (OIT), os termos do disposto no Art. 3.º (b) da Convenção n.º 182 (1999) *"Relativa à Interdição das Piores Formas de Trabalho das Crianças e à ação Imediata Com Vista à Sua Eliminação"* que enquadra nas *"piores formas de trabalho de crianças*", a utilização, recrutamento ou oferta de crianças para fins de prostituição, de produção de material pornográfico ou de espetáculos pornográficos.

2.6.2. O Conselho da Europa

No âmbito do Conselho da Europa é de relevar, entre outros textos normativos, a Convenção sobre a Cibercriminalidade (STE – Série de Tratados do Conselho da Europa, n.º 185), em particular o seu Art. 9.º que dispõe que se deve punir no âmbito do direito interno as condutas praticadas de forma intencional e ilegítima que consubstanciem:

- A produção de pornografia infantil com o propósito de a divulgar através um sistema informático;
- A oferta ou disponibilização de pornografia infantil através de um sistema informático;

- A difusão ou transmissão de pornografia infantil através de um sistema informático;
- A obtenção para si ou para outra pessoa de pornografia infantil através de um sistema informático; e
- A posse de pornografia infantil num sistema informático ou num dispositivo de armazenamento de dados informáticos.

Esclarece-se no âmbito da referida Convenção que a expressão "pornografia infantil" deverá abranger todo o material pornográfico que represente visualmente:

- Um menor envolvido em comportamentos sexualmente explícitos;
- Uma pessoa com aspeto de menor envolvida em comportamentos sexualmente explícitos; e
- Imagens realistas de um menor envolvido em comportamentos sexualmente explícitos.

Inerente à violência contra as crianças tem igualmente relevância a Convenção do Conselho da Europa relativa à luta contra o Tráfico de Seres Humanos (CTCE) (n.º 197), em que se prevê um tratamento específico no que concerne às crianças vítimas de exploração sexual nas seguintes vertentes:

- A proteção da vida privada das vítimas e, se for caso disso, da sua identidade;
- A segurança das vítimas e a sua proteção contra ações de intimidação, segundo as condições previstas no seu direito interno; e, tratando -se de crianças-vítimas,
- A necessidade de assegurar o seu direito a medidas de proteção específicas.

No que respeita a tratados estruturantes gerais sobre a proteção das crianças foram aprovadas no âmbito do Conselho da Europa a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (1950, STE n.º 5), que refere no seu Art. 5.º que toda a pessoa tem direito à liberdade e à segurança, a Carta Social Europeia revista (1996, STE n.º 163), que refere no ponto 7 (Parte I) que *"as crianças e os adolescentes têm direito a uma proteção especial contra os perigos físicos e morais a que se encontrem expostos"* referindo-se ainda no Art. 17.º, n.º 1, alínea b) o direito das crianças e adolescentes a uma proteção social, jurídica e económica, com previsão da serem tomadas medidas para *"proteger as crianças e adolescentes contra a negligência, a violência ou a exploração"*.

De atender igualmente, à Convenção Europeia sobre o Exercício dos Direitos da Criança (STE n.º 160) e a Convenção de Lanzarote (2007, STE n.º 201), referindo esta

última no seu Art. 30.º, n.º 5 que deve ser permitido que as unidades ou serviços de investigação identifiquem vítimas das infrações penais em causa (leia-se pornografia de menores e abuso sexual de crianças), em particular *"através da análise de material relacionado com pornografia infantil tal como fotografias e registos audiovisuais transmitidos ou disponibilizados através de tecnologias de informação ou comunicação"*.

2.6.3. A União Europeia

No quadro da União Europeia tem relevância, entre outros textos normativos, a Diretiva do Parlamento Europeu e do Conselho relativa à luta contra o abuso e a exploração sexual de crianças e a pornografia infantil (2011/92/EU), de 13 de dezembro de 2011, que refere em termos sintéticos o seguinte:

A investigação dos crimes e a dedução da acusação em processo penal deverão ser facilitadas, tendo em conta não só as dificuldades que as crianças vítimas destes crimes enfrentam para denunciar os abusos sexuais, mas também o anonimato dos autores dos crimes no ciberespaço;

Os responsáveis pela investigação e pela ação penal relativas aos crimes referidos deverão dispor de instrumentos de investigação eficazes. Estes instrumentos podem incluir a interceção de comunicações, a vigilância discreta, inclusive por meios eletrónicos, a monitorização de contas bancárias ou outras medidas;

Deverão ser tomadas as medidas necessárias para garantir o bloqueio de acesso e a supressão imediata das páginas eletrónicas que contenham ou difundam pornografia infantil sediadas em território nacional, e bem assim, para procurar obter o bloqueio de acesso do mesmo tipo páginas sediadas fora de território nacional.

2.7. Breve incursão sobre o Direito Português

As condutas subsumíveis ao abuso sexual de crianças encontram-se previstas no Art. 171.º – menores com idade inferior a 14 anos, no Art. 172.º – menores dependentes entre os 14 e os 18 anos, no Art. 173.º – menores dependentes entre os 14 e os 18 anos e no Art. 176.º – pornografia de menores, todos do CP. De relevar a circunstância de *"nos crimes contra a liberdade e autodeterminação sexual de menores, o procedimento criminal não se extinguir, por efeito da prescrição, antes de o ofendido perfazer a idade de 23 anos"*, conforme o disposto no Art. 188.º, n.º 5 do CP. Subjacente a esta norma está a possibilidade da vítima, após atingir a maioridade, poder promover, com a liberdade que lhe confere a idade adulta, o início de procedimento relativamente a condutas de que tenha

sido vítima na idade menor. Acresce que, nos termos do disposto no Art. 179.º do CP quem for condenado por este tipo de crimes pode, atenta a concreta gravidade dos factos e a função que exerce em relação ao menor, ser inibido do exercício do poder paternal, da tutela ou da curatela e, bem assim, ser proibido do exercício de profissão, função ou atividade que implique ter menores sob a sua responsabilidade, educação, tratamento ou vigilância (ver Apêndice 4 sobre a criminalização da exploração sexual de crianças em Portugal).

Atento o quadro legal descrito perspetiva-se que o crime de pornografia de menores será aquele que com maior frequência será objeto da IC em Portugal uma vez que prevalece a ausência de indícios sobre o autor ou autores dos atos retratados no material (abuso sexual em sentido próprio) que circula no Ciberespaço e a dificuldade de identificação das vítimas.

Cotejados os textos internacionais com os tipos de ilícito criminal da legislação nacional conclui-se que, em termos de atos tipificados como crime, existe alinhamento entre a legislação nacional e os instrumentos internacionais. Neste alinhamento analisar-se-á se o mesmo se verifica em termos de regras para a aquisição de prova.

2.8. Regras legais relativas à aquisição de prova eletrónica

No que concerne a instrumentos legislativos relevantes no âmbito da investigação da exploração sexual de crianças no Ciberespaço e da aquisição da prova, refere-se a Lei n.º 32/2008, de 17 de julho que regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes. Dispõe o Art. 2.º, alínea g) deste texto normativo que este regime se aplica, apenas, aos crimes graves, a saber: o crime de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima e que corresponde à redação atual prevista no Art. 187.º, n.º 2 do CPP. Nos termos do disposto no Art. 1.º, alínea j) do CPP considera-se criminalidade violenta as condutas que dolosamente se dirigirem contra a vida, a integridade física ou a liberdade das pessoas e forem puníveis com pena de prisão de máximo igual ou superior a 5 anos.

Constatamos, deste modo, que fica fora do alcance da Lei n.º 32/2008, e assim inviabilizada a recolha de prova digital no Ciberespaço (eg.: interceções telefónicas e em linha, pedidos de identificação de IP associado a determinada comunicação com pornografia de menores, entre outra diligências de obtenção de prova), dos seguintes crimes, por serem punidos com pena inferior a 5 anos de prisão:

- Importunação sexual de crianças, previsto e punido nos termos conjugados do disposto nos Art.s 171.º, n.º 3 e 170.º do CP;
- Importunação sexual de dependentes, com e sem intenção lucrativa, previsto e punido nos termos conjugados do disposto nos Art.s 172.º, n.º 2 e n.º 3 do Art. 171.º do CP;
- Abuso sexual de crianças com idade entre os 14 e os 16 anos, previsto e punido nos termos do disposto no Art. 173.º do CP;
- Pornografia de menores previsto e punido nos termos do disposto nos Art.s 176.º, n.º 3 e n.º 1, alíneas c) e d) do CP;
- Pornografia de menores, previsto e punido nos termos do disposto no Art. 176.º, ns.º 4 e n.º 1, alínea b) do CP.

Para a criminalidade descrita, a IC está impedida de aceder aos dados relacionados com atividade conexa com o Ciberespaço suscetível de configurar a prática daqueles ilícitos e que se encontra na posse dos ISP ou das operadoras de telecomunicações dado que a pena prevista para este tipo de ilícitos não ultrapassa os 5 anos de prisão. As consequências que este tipo de condutas provoca nas vítimas (crianças), sendo certo que tais condutas, embora menos graves, antecedem, na maioria dos casos, condutas mais graves de violência sexual contra as crianças, justifica uma avaliação crítica não só pela desproporcionalidade entre os efeitos nefastos que tais condutas poderão acarretar para as vitimas e a sociedade, os recursos para a ação preventiva ou punitiva a que a sociedade pode recorrer, como pelo facto da IC estar impossibilitada de utilizar informação acessível a baixo custo (Pinho, 2012, p. 91).[3]

Nos termos do disposto no Art. 4.º da Lei n.º 32/2008, de 17 de Julho os prestadores dos serviços de comunicações conservam os dados para, no âmbito da IC se: a) encontrar e identificar a fonte de uma comunicação; b) encontrar e identificar o destino de uma

[3] Veja-se igualmente os termos do disposto nos Art.ºs 189.º, 187.º e 188.º do Código de Processo Penal e os termos do disposto na Lei n.º 109/2009, de 15 de setembro, em que se permite o recurso às ações encobertas para investigação deste tipo de criminalidade, o que indicia incoerência quando raciocinamos em termos de unidade de sistema jurídico, na medida em que as ações encobertas se constituem como um dos métodos mais intrusivos de obtenção de prova.

comunicação; c) identificar a data, a hora e a duração de uma comunicação; d) identificar o tipo de comunicação; e) identificar os equipamentos de telecomunicação dos utilizadores, ou o que se considera ser o seu equipamento e f) identificar a localização do equipamento de comunicação móvel. O período de conservação deste tipo de dados é o de (1) um ano a contar da data da conclusão da comunicação – Art. 6.º da Lei n.º 32/2008, de 17 de Julho – e a transmissão dos dados opera-se mediante despacho fundamentado do Juiz de Instrução Criminal, no âmbito da investigação, deteção e repressão de crimes graves. Por seu lado, a Lciber tem aplicação relativamente aos a) crimes previstos na Lei do Cibercrime, b) os cometidos por meio de um sistema informático ou c) aqueles que exijam recolha de prova em suporte eletrónico, desde que, nestes casos, se não contrarie o regime previsto na Lei n.º 32/2008, de 17 de julho (cfr. Art. 11.º da LCIber). No que concerne à apreensão de dados informáticos, através de cópia dos dados, prevê o referido regime que a cópia é efetuada em duplicado, sendo uma das cópias selada e confiada ao Secretário Judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital – Art. 16.º, n.º 8 da LCIber.

Verifica-se que a legislação interna relativa à repressão deste fenómeno se encontra dispersa por 4 instrumentos normativos principais (CP, CPP, Lei n.º 32/2008, de 17 de julho e Lciber) e que não permite cabalmente a investigação de algumas práticas, já identificadas. Acresce, que o Estado Português se encontra em dívida com instrumentos internacionais que ratificou sendo urgente e necessário implementar medidas legislativas que garantam:

- A supressão imediata das páginas eletrónicas que contenham ou difundam material de abuso de menores, localizadas em território nacional;
- O bloqueio imediato do acesso a páginas eletrónicas que contenham ou difundam material de abuso sexual de menores sediadas fora do território nacional;
- A comunicação por parte das entidades bancárias dos pagamentos efetuados com cartões de débito e de crédito associados a sites com material de abuso de menores.

As medidas legislativas cuja necessidade foi identificada têm de ser complementadas com iniciativas que possibilitem a execução de múltiplas actividades conducentes a alcançar as garantias enunciadas, nomeadamente:

- Articulação com os ISP e outras entidades de monitorização de conteúdos no Ciberespaço;
- Articulação com as instituições bancárias;
- Vigilância preventiva de conteúdos no Ciberespaço tendente a identificar material de abuso sexual de menores, mediante autorização prévia do Ministério Público e acordo do Juiz de Instrução Criminal;
- Constituição de uma base de dados, tutelada pelas Autoridades de IC, com material relacionado com o abuso sexual de menores,
- Troca de informações com entidades de IC estrangeiras, designadamente o Eurojust, a Europol e a Interpol.

2.9. Casos nacionais

Em Portugal inexistem dados estatísticos quanto ao abuso sexual de menores cometidos através de recursos disponíveis no Ciberespaço. No entanto dados da Polícia Judiciária, constantes do Relatório de Segurança Interna de 2011, referem a seguinte estatística no que concerne a casos de crimes sexuais (Sistema de Segurança Interna, 2011, p. 97-100):

Tabela 1 - Participações crimes sexuais

Ano	N.º participações crimes sexuais/total
2010	2202
2011	2177

Tabela 2 - Participações lenocínio e pornografia de menores

Ano	Lenocínio e pornografia de menores
2010	65
2011	89

Tabela 3 - - Participações abuso sexual de crianças

Ano	Abuso Sexual de crianças, adolescentes e menores dependentes o
2010	777
2011	783

Contudo, estes números não identificam o número de vítimas por caso, verificando-se que em alguns casos de pornografia de menores consultados no âmbito do presente estudo,

foram detetadas milhares de fotografias de menores retratando situações de abuso sexual, o que indicia um número correspondente de vítimas.

No quadro estatístico supra, analisar-se-ão 10 casos que foram investigados no Sistema de Justiça Penal, em Portugal, com a finalidade de identificar especificidades e balizar juridicamente as metodologias de investigação e se estas estão alinhadas com Jurisprudência dos Tribunais Superiores. Os casos agora descritos foram objeto de adaptação, pelo que os factos relatados não são coincidentes com a realidade objetiva, visando-se fundamentalmente identificar e analisar os procedimentos de investigação.

2.9.1. Caso 1 – Contacto de menor através da rede *HI5.com*

Este processo teve início em agosto de 2009, através de queixa efetuada às autoridades policiais, por parte da mãe de um menor, do sexo masculino, com 13 anos de idade. O agressor tinha à data dos factos 21 anos de idade. O menor conheceu o agressor através da rede social Hi5, tendo depois trocado correspondência eletrónica, quer através do MSN – *Messenger* quer através de contas de correio eletrónico. Mediante os contactos estabelecidos através quer da rede social Hi5 quer através do MSN, e também através de mensagens de correio eletrónico, o agressor convenceu o menor a encontrar-se consigo numa estação de comboios, de onde se deslocaram os dois para casa do agressor. Aí chegados o menor foi sujeito a contactos de natureza sexual por parte do agressor. Poucos dias depois o agressor enviou ao menor mensagens e desenhos com conteúdo sexual, no sentido de o tentar convencer a novos encontros.

No decurso da investigação foi apreendido o computador do agressor onde se encontravam as mensagens de correio eletrónico, as imagens e os desenhos de cariz sexual enviados para o menor, apreensão ordenada e validada pelo Juiz de Instrução Criminal, após pedido do Ministério Público, uma vez que este tipo de dados respeita à reserva da intimidade da vida privada das pessoas, beneficiando de proteção constitucional, face ao ordenamento jurídico Português (cfr. Art. 16.º, n.º 3 da LCiber).

Interessa-nos, neste caso, averiguar dos procedimentos legais tendentes à validação e a apreensão das mensagens de correio eletrónico. No que concerne à apreensão de correspondência eletrónica, a LCiber determina no seu Art. 17º que quando no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático forem encontrados armazenados nesse sistema informático ou noutro que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão

daqueles que se afigurem de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime de apreensão de correspondência previsto no CPP. O regime de apreensão de correspondência previsto no CPP encontra-se disciplinado no Art. 179º, o qual estabelece desde logo no nº 1 que tais apreensões são determinadas por despacho judicial, sob pena de nulidade e que o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Este preceito aplica-se ao correio eletrónico já convertido em ficheiro legível por perito informático designado, o que significa que constitui ato da competência exclusiva do Juiz de Instrução Criminal, nos termos do Art. 268º nº 1 alínea d) do CPP. A falta de exame da correspondência pelo juiz constitui uma nulidade prevista no Art. 120º n.º 2 alínea d) do CPP, porque se trata de um ato processual legalmente obrigatório, querendo significar que, caso estes procedimentos não sejam observados, a prova recolhida não pode ser utilizada no processo-crime (Ac. TRL, 2011-01-11). Deste modo, no caso de correspondência eletrónica, entendemos que esta difere da correspondência física em termos lógicos e factuais, pelo que estando armazenada ou "fechada" num computador, mesmo que tenha já sido lida pelo seu destinatário, aplicar-se-á sempre o regime de apreensão de correspondência previsto no Art. 179.º do CPP e no 17.º da LCiber, exigindo-se a autorização, visualização e conhecimento em primeiro lugar e seleção do conteúdo das mensagens de correio eletrónico relevantes para a investigação por parte do Juiz de Instrução Criminal, na sequência de promoção do MP, enquanto titular da ação penal. O Juiz de Instrução Criminal, na realização desta diligência, deve ser sempre assessorado por um perito informático forense, atenta a tecnicidade em causa e a necessidade de assegurar a manutenção da cadeia de custódia da prova.

2.9.2. Caso 2 – Atração de menor através do computador

Este caso teve início com a apresentação de queixa por parte da mãe de uma menor, de 14 anos de idade, às autoridades policiais, no ano de 2007. O agressor, com 38 anos de idade, era vizinho da vítima, e deixou que esta consultasse a Internet, através do computador que tinha em sua casa, dado que em casa da menor não existia Internet nem computador. O agressor a partir desse acontecimento passou a conviver com a menor e com o seu grupo de amigos, apesar da diferença de idades. Pouco tempo depois, o agressor passou a noite em casa da menor, aproveitando a ausência da mãe, que se encontrava a trabalhar, e abusou sexualmente da mesma. O agressor praticou várias vezes atos da mesma natureza com a menor.

No mesmo período de espaço temporal o agressor praticou igualmente atos da mesma natureza com outra menor, de 7 anos de idade, aquando de visitas efetuadas por esta a uma familiar que residia perto do arguido, atraindo-a também para sua casa para esta utilizar o seu computador. Para diminuir a sensibilidade da menor aos atos que pretendia praticar exibiu-lhe fotografias de menores com conteúdo pornográfico e efetuou fotografias à referida menor com conteúdo pornográfico. Foi efetuado exame pericial ao conteúdo do computador do agressor, onde se encontraram imagens de conteúdo pornográfico.

Foi efetuada busca, mediante consentimento prévio do agressor à sua residência tendo sido apreendidos, entre outros objetos, CDs com filmes pornográficos.

Interessa-nos neste caso procurar concretizar o conceito de domicílio, na expressão da lei *"buscas em casa habitada ou sua dependência"*, no sentido de identificar os casos em que é necessária autorização do Juiz de Instrução Criminal para a realização da referida diligência, conforme os termos do disposto no Art. 177.º do CPP. Constituirá habitação o local onde o visado tem a sua casa, onde vive e tem os seus bens domésticos e onde desenvolve a sua vida íntima e familiar, como por exemplo o local de morada habitual de uma pessoa, a sua casa de férias, a tenda de um cigano, um quarto de hotel, um quarto de um militar num quartel (o qual difere de uma camarata), uma casa de função de um funcionário público ou um quarto de um navio de cruzeiro. Já a *"dependência"* tem de ser fisicamente contínua à zona de habitação e manter- se no espaço de reserva da vida íntima do visado para merecer a proteção do Art. 177.º do CPP. Uma garagem coletiva de um condomínio que se encontra fechada, mas que todos os condóminos usufruem igualmente não é uma dependência do domicílio do visado. A garagem fechada arrendada conjuntamente com o apartamento pelo arguido já é dependência do domicílio (Albuquerque, 2008, p. 482).

2.9.3. Caso 3 – Filmagens – devassa da vida privada

Este caso iniciou-se com queixa da mãe de uma menor, de 14 anos de idade, às autoridades policiais, no ano de 2006. O agressor, com 17 anos de idade, na sequência de contactos mantidos entre ambos, convenceu a menor a entrar em sua casa, onde tiveram relações de caráter sexual, que o agressor filmou, utilizando para o efeito uma máquina fotográfica digital. Posteriormente, exibiu as referidas imagens a terceiros, os quais reconheceram quer o agressor quer a vítima. Foi realizada busca domiciliária à casa do agressor tendo-se encontrado e apreendido um disco rígido e um cartão de memória de uma máquina de fotografia digital, pertencentes ao agressor.

Não se provou que o agressor tivesse transferido as imagens para o seu computador, nem que a vítima desconhecesse a circunstância de estarem a ser recolhidas filmagens.

Interessa-nos procurar concretizar a metodologia a observar na realização de uma perícia informática forense ao equipamento digital apreendido destacando que no presente caso não está disponível orientação emitida por Tribunal Superior sobre como fazer.

Neste tipo de apreensão, as boas regras indicam que deve ser nomeado um perito informático forense que deverá proceder à elaboração de uma imagem certificada dos dados constante do disco rígido e do cartão de memória, que se manterão intactos. A partir dessa imagem, deverá proceder-se à extração de dados para pesquisa para outro suporte, destinado a análise de informação, trata-se da denominada *"cópia de trabalho"*. A partir da *"cópia de trabalho"* procede-se à extração das imagens relevantes para o processo, que serão incluídas no relatório pericial. Deste modo, o processo deverá manter os dispositivos digitais apreendidos (originais), a imagem certificada dos dados em suporte próprio, a "cópia de trabalho" também em suporte próprio e o relatório pericial.

2.9.4. Caso 4 – CyberCafe

Este caso iniciou-se com queixa apresentada pela mãe de uma menor de 13 anos de idade no ano de 2010, relatando que o agressor encetou conversa com a menor, num CyberCafe, onde ambos se encontravam, após a menor sair das aulas. No decorrer da conversa a menor disse-lhe o seu nome, a sua idade e forneceu-lhe o seu contacto de telemóvel. Durante cerca de um mês o agressor enviou mensagens escritas (SMS) para o telemóvel da menor e dialogou com esta através do Messenger (MSN), no início sobre assuntos banais, até ao momento em que disse estar apaixonado pela menor. Na sequência desta convivência o agressor conseguiu convencer a menor a ir a sua casa e aí abusou sexualmente da mesma. Após conhecer o agressor a menor começou a faltar à escola regularmente, perdeu o ano escolar, fechava-se no seu quarto às escuras, passando a maior parte do tempo na cama. Isolou-se e deixou de brincar com as suas amigas e de ser uma criança extrovertida.

Foi efetuado exame ao telemóvel da menor e extraída cópia das mensagens enviadas pelo agressor.

Interessa-nos procurar concretizar o regime legal de acesso às mensagens constantes do telemóvel da vítima. No caso, tendo existido autorização da vítima e da sua mãe torna-se desnecessária a intervenção da autoridade judiciária para ratificar o acesso ao conteúdo das referidas mensagens, não se aplicando, assim, o regime previsto no Art. 179.º do CPP para

a apreensão de correspondência, uma vez que as mensagens enviadas para o telemóvel encontram-se na disponibilidade da vítima e esta deu o seu consentimento ao seu acesso, para investigação de um crime de que foi vítima (Ac. TRL, 2012-03-29).

2.9.5. Caso 5 – Filmagens – telemóvel – devassa da vida privada

Este caso iniciou-se com denúncia da avó paterna de uma menor de 16 anos de idade às autoridades policiais, no ano de 2007 dando conta da existência de um dispositivo de armazenamento de dados – *"pen drive"* – que continha imagens da menor a trocar de roupa no seu quarto, parcialmente despida.

Foi efetuada perícia informática forense ao referido dispositivo de armazenamento de dados, com extração de imagens da menor parcialmente despida.

Neste caso, interessa-nos averiguar de que modo o relatório pericial, com imagens íntimas da ofendida, deve ser junto ao processo e, bem assim, qual o regime de acesso à informação nele contido. Atenta a sensibilidade dos dados a tratar no relatório pericial, a imagem certificada dos dados, a "cópia de trabalho" e o relatório pericial devem constar de "apenso próprio" ao processo, com a menção de "Reservado" (ACPO, 2007, p. 22), no sentido de assegurar que apenas acedem àquela informação as pessoas que têm necessidade de a conhecer, na sequência de autorização por parte da autoridade judiciária, assim se preservando a dignidade da vítima (Conselho Consultivo do Ministério Público, 2009)[4] em conformidade com os termos do disposto nos Art.s 18.º, n.º 2 e 26.º, n.º 1 da CRP.

2.9.6. Caso 6 – Deteção de ficheiros com pornografia de menores

Este caso iniciou-se com extração de certidão, na sequência de perícia informática forense realizada no âmbito de uma investigação relacionada com criminalidade económico-financeira, que correu termos no ano de 2011. Na perícia informática forense realizada foram detetados ficheiros contendo imagens e vídeos com pornografia de menores, na sequência de apreensão de dispositivos de armazenamento de dados digitais.

O Instituto Nacional de Medicina Legal (INML) emitiu parecer médico-legal concluindo que algumas das imagens retratavam menores com idade entre os 13 anos e os 16 anos.

Na investigação realizada não foi possível proceder à concreta identificação das crianças retratadas nas imagens.

[4] Manutenção do regime do segredo no processo - crime, independentemente da existência ou não de segredo de justiça.

No caso, importa indagar, se o parecer médico-legal do INML constitui elemento probatório suficiente para a prova de que as vítimas tinham idade inferior à legal, justificando-se a punição do detentor das imagens em causa. No que concerne à prova da idade das vítimas que são objeto de filmagem e de fotografia é de referir que em direito penal, na impossibilidade de se juntar certificado de assento de nascimento, ou porque este não existe ou porque o nascimento não tenha sido registado ou porque não é possível recolher dados que tornem o registo localizável, pode tal prova ser feita com recurso a perícias, já que o Tribunal tem poderes de investigação na audiência de julgamento para tal – Art. 340.º do CPP.

Assim, a prova da idade das vítimas, nos casos de pornografia de crianças, deve basear-se no relatório de perícia médico-legal elaborado pelo INML, reportado à escala dos estadios de Tanner[5], para avaliação dos carateres sexuais secundários, reforçado e em conjugação com as regras da experiência de vida, da normalidade e da apreciação do homem médio ao caso concreto. As escalas de Tanner são um instrumento de trabalho com credibilidade científica na área médica para o estudo do desenvolvimento das crianças e jovens, sendo o melhor método de trabalho existente na atualidade no que se refere à determinação da idade das crianças nos casos de exploração sexual de crianças no Ciberespaço (Ac. TRP, 2010-11-17).

2.9.7. Caso 7 – Interpol – Autoridades Alemãs – pornografia de menores

Este caso iniciou-se com a participação das Autoridades Alemãs às Autoridades Portuguesas, no ano de 2005, dando conta que se encontravam a investigar um indivíduo Russo, de identidade não completamente apurada, por colocar em circulação num subdomínio de sua propriedade imagens de pornografia infantil.

As entradas e as ligações colocadas davam acesso a fotografias e vídeos com material de abuso sexual de menores. O *website* em causa era também utilizado para troca por correio eletrónico de fotografias e vídeos de pornografia infantil, tendo sido identificadas mais de 800 entradas em menos de 1 mês. Através desse subdomínio eram disponibilizados serviços de troca de ficheiros de grandes dimensões, com as respetivas ligações para *download* e ainda para preparação de encontros com menores, com o objetivo de os abusarem sexualmente e, bem assim, para disponibilização de vídeos de pessoas a abusarem sexualmente dos seus próprios filhos.

[5] Os estadios de Tanner, ou estádios de desenvolvimento pubertário, para avaliação dos carateres sexuais secundários incidem sobre o desenvolvimento das mamas, volume e distribuição dos pelos púbicos e configuração dos genitais externos.

Cerca de 1 mês depois da deteção do primeiro *website*, as Autoridades Alemãs detetaram um novo web site, com *nicknames* e endereços de correio eletrónico que já eram conhecidos do anterior, existindo suspeitas de que este novo domínio era o sucessor daquele. As Autoridades Alemãs informaram ainda que o sítio web ainda continuava ativo e que à data já tinha cerca de 3400 entradas. Referiram ainda que foram iniciadas diligências para bloquear o acesso ao referido sítio web a partir do servidor de São Petersburgo, na Federação Russa. As Autoridades Alemãs pediram às Autoridades Portuguesas para iniciarem a investigação quanto ao acesso por parte de computadores localizados fisicamente em território nacional (endereço IP de Portugal) que acederam um ficheiro de vídeo exibindo o seguinte:

Uma criança do sexo feminino nua, de pele escura, deitada numa cama;

Um homem branco, que não está visível, a manipular os órgãos genitais da criança, primeiro com os dedos e depois com o pénis ereto e, finalmente, introduz um dedo na vagina da criança;

Durante algum tempo, a criança é agarrada por uma mulher de pele escura.

As análises efetuadas revelaram que o ficheiro em causa foi aberto 2682 vezes em menos de 14 horas.

Concluem as Autoridades Alemãs que pessoas localizadas geograficamente em Portugal tentaram aceder a esse material porque os endereços IP detetados no acesso a esses conteúdos pertenciam a operadores de serviços de Internet portugueses. Na sequência da informação das Autoridades Alemãs solicitou-se informação à operadora de serviços de Internet em causa sobre o nome do utilizador do IP nacional identificado pelas Autoridades Alemãs. A operadora forneceu o nome e a morada do utilizador em causa, tendo sido ordenada busca domiciliária pelo Juiz de Instrução Criminal, para apreensão de documentação e objetos relacionados com a prática do crime de abuso sexual de criança, nos termos do Art. 34.º da CRP e ao abrigo do disposto nos Art.s 269.º, alínea a), 174.º, n.º 2 e 3, 176.º e 177.º do CPP.

Na residência do suspeito foram encontrados e apreendidos um computador de secretária e vários DVDs, que continham conteúdos relativos a abusos sexuais cometidos contra menores, entre os 3 e os 14 anos de idade, sobre o qual incidiu perícia e análise informática forense – foram detetadas na posse do agressor, entre outros conteúdos, dezenas de milhar de imagens de conteúdos relativos a abusos sexuais de menores, consistindo estas em fotografias de menores de ambos os sexos, com idades que variam

entre os 5 e os 14 anos de idade, em diversas poses enquanto se despem e tocam nos órgãos genitais e outras partes do corpo.

Neste caso interessa-nos averiguar como é que do ponto de vista de procedimento legal podemos, neste momento, obter a identificação dos dados do utilizador ou de registo de determinado IP. Conforme Jurisprudência do TRL propugna-se que *"a identificação completa, morada e endereço de correio eletrónico do titular de determinado blog, bem como o IP de criação desse blog e o IP onde foi efetuado determinado "post", constituem dados de base, que embora cobertos pelo sistema de confidencialidade, podem ser comunicados a pedido de uma autoridade judiciária, aplicando-se o regime do Art. 135º, do CPP, quando tenha sido deduzida escusa*" (Ac. TRL, 2011-01-18). Atenta a natureza do crime, esta Jurisprudência não deveria obstar a que os dados pudessem ser diretamente solicitados por quem dirige a IC, ponderando entre o dever de sigilo das comunicações e o da célere administração da justiça.

2.9.8. Caso 8 – Interpol – Autoridades Suíças – pornografia de menores

Este caso iniciou-se em 2006 com comunicação das Autoridades Suíças às Autoridades Portuguesas dando conta da disponibilização de serviços no Ciberespaço com origem naquele país que disponibilizavam vídeos e imagens, cujo conteúdo configurava pornografia infantil. As Autoridades Suíças referem que efetuaram pesquisas aos referidos serviços (*monitoring*) e com base nessa diligência identificaram 466 utilizadores de 48 países diferentes, que na data do controlo estavam na posse de pelo menos 3 ficheiros de carácter totalmente pedo-pornográfico.

Os países que tinham clientes desses serviços residentes na Suíça eram os seguintes: Alemanha, Arábia Saudita, Argentina, Austrália, Áustria, Bélgica, Brasil, Canadá, Chile, China, Chipre, Coreia, Dinamarca, Espanha, Estónia, Finlândia, França, Grã-Bretanha, Grécia, Hong Kong, Hungria, Israel, Itália, Japão. Kuweit, Lituânia, Malásia, Marrocos, México, Noruega, Holanda Perú, Polónia, Portugal, Quatar, República Checa, Rússia, Sérvia Montenegro, Eslovénia, Suécia, Suíça, Taiwan, Tailândia, Trinidad e Botago, Turquia, Ucrânia, EUA, Uruguai e Venezuela.

Consta-se que no caso foi efetuada uma vigilância aos referidos serviços, mediante a qual foram detetados os endereços IP dos utilizadores de vários países.

Neste caso, importa saber se era possível efetuar em Portugal uma ação semelhante de *monitorização de conteúdos relacionados com a exploração sexual de crianças no Ciberespaço*, perante uma denúncia que relatasse a disponibilização de serviços do mesmo

teor em Portugal, designadamente através de uma rede privada, na eventualidade de inexistirem indícios sobre o local onde está fisicamente instalado esse serviço. A resposta é positiva: para este efeito era necessário que o Juiz de Instrução Criminal autorizasse a *infiltração em linha em sistemas informáticos*, com vista à obtenção de informação dos visados, através dos registos, configurando-se materialmente como uma "busca em linha" para apreensão de dados. Nesse sentido, era necessário obter autorização para realização de uma acção encoberta que permite, nos termos do disposto no n.º 2 do Art. 19.º da LCiber o *"recurso a meios e dispositivos informáticos"* observando-se, naquilo que for aplicável, *"as regras previstas para a interceção de comunicações"*, estando possibilitada a realização desta diligência quanto a crimes relacionados com a exploração sexual de crianças no Ciberespaço – n.º 2, alínea b) do Art.ª 19.º da LCiber.

O regime das interceções de comunicações encontra-se previsto no Art. 18.º da LCiber e pressupõe a existência de um juízo de indispensabilidade da diligência para a descoberta da verdade e ainda que a prova seja impossível ou de muito difícil obtenção sem a realização da referia diligência - a acção encoberta, pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha de dados de tráfego, devendo o despacho do Juiz de Instrução Criminal, na sequência de promoção do Ministério Público, especificar o respetivo âmbito, de acordo com as necessidades concretas da investigação - Art. 18.º, n.º 3 da LCiber (veja Apêndice 3 sobre ações encobertas *on-line*).

2.9.9. Caso 9 – Interpol – Autoridades Alemãs – pornografia de menores – *website*

Este caso iniciou-se em 2007 com comunicação das Autoridades Alemãs às Autoridades Portuguesas dando conta da divulgação através do programa *eMule* na Internet, de um filme contendo imagens de abusos sexuais de crianças. De entre todas as ligações identificadas como procedendo à referida divulgação, encontram-se 10 oriundas de Portugal, conforme se verificou através da identificação dos endereços IP. Verificou-se ainda que esse vídeo foi divulgado em *website*s de diferentes países, verificando-se que um deles se situava em Portugal.

Em relação ao *website* em causa procedeu-se à identificação do ISP onde o mesmo se encontrava alojado e ordenou-se o seu bloqueio, através de determinação do Juiz de Instrução Criminal, na sequência de promoção do Ministério Público, nos termos do disposto no Art. 7.º do Decreto-Lei n.º 7/2004, de 7 de janeiro, 269.º, alínea f) do CPP e Art.s 35.º, n.º 6, 37.º, n.ºs 1,2 e 3 e Art.s 18.º e 19.º da Constituição, verificando-se assim, ser possível, bloquear *website*s nacionais com material de abuso sexual de menores.

2.9.10. Caso 10 - Interpol – Autoridades Alemãs – pornografia de menores – P2P

Este caso iniciou-se em 2009 com comunicação das Autoridades Alemãs às Autoridades Portuguesas dando conta da divulgação através do programe *EMule* de um filme contendo imagens de abusos sexuais de crianças. De entre todas as ligações identificadas como procedendo à referida divulgação, encontravam-se 3 oriundas de Portugal, conforme se verificou através da identificação dos endereços IP. O caso diz respeito à divulgação através da Internet de um vídeo contendo imagens de abuso explícito (coito anal) de uma criança do sexo feminino de 3 anos de idade, na Internet, através do programa de partilha de ficheiros P2P *EMule*.

Constata-se que neste caso, foi efetuada na Alemanha uma "pesquisa aleatória" na Internet, com base em informação retirada de casos similares - no caso solicitou-se aos ISP que fossem facultados os dados elencados no Art. 4.º da Lei n.º 32/2008, de 24 de julho, relativos às comunicações identificadas, bem como os *MAC adress* do modem e placa de rede do computador[6] utilizado em cada comunicação, no sentido de se verificar a identificação das pessoas que acederam ao conteúdo integral do vídeo.

Importa saber se era possível efetuar em Portugal uma ação semelhante. Trata-se de efetuar uma "*ação de monitorização e de prevenção na Internet, contra alvos aleatórios, relativamente a conteúdos materialmente configuradores da exploração sexual de crianças"*, com base em informação de casos similares. A resposta a esta questão é negativa: ou seja, não é possível efetuar em Portugal uma acção de prevenção criminal no Ciberespaço, semelhante à possibilidade que existe, por exemplo, no mundo físico, no âmbito das ações especiais de prevenção da lei das armas – cfr. Art.s 109.º a 111.º da Lei n.º 5/2006, de 23 de fevereiro. Em conformidade deve promover-se a construção de legislação habilitante que permita efetuar este tipo de ações, sendo necessária colaboração dos ISP, designadamente no que concerne à deteção de conteúdos relacionados com a exploração sexual de crianças, mediante autorização e validação das Autoridades Judiciárias.

Caracterizado o *locus* e o enquadramento jurídico da IC aplicável a este tipo de crimes analisaremos no próximo capítulo da adequação ao combate, neste *locus*, dos procedimentos e metodologias de IC. O enfoque será colocado na aquisição e valoração de prova digital.

[6] O *MAC adress* (Media Access Control Adress) é um identificador único de um determinado equipamento físico de comunicação.

Capítulo 3

Aquisição e valoração de prova digital no Ciberespaço

3.1. Pesquisa em fontes abertas

A informação para uso no processo penal durante a IC - fase do inquérito - no abuso sexual de crianças e da difusão de material de abuso de menores no Ciberespaço pode ser obtida nas redes que versam esta temática de forma especializada ou dispersa, em regra, de utilização livre. Esta fonte de informação de livre acesso liberta o Estado do financiamento de operações de aquisição de informação mais onerosas.

Efetivamente, alguns motores de busca, designadamente o *Google*, permitem o recurso a opções avançadas para circunscrever os numerosos resultados obtidos ao tipo de informação pretendida, seja de modo passivo[7], seja de modo ativo[8]. Independentemente da qualidade desses resultados existem atualmente dois motores de busca que em regra permitem a utilização de comandos – (Blachman – 2012b) – destinados a otimizar (Google Inside Search, 2012) as consultas e procura de informação: o Google e o Bing. A indicação destes dois motores de busca e a preferência pelo *Google* decorre do facto de serem os que, atualmente, melhores resultados têm proporcionado no âmbito das investigações criminais com conexões ao Ciberespaço. Os referidos motores de busca também permitem apontar uma busca diretamente para a Web, imagens, tradutor automático (no caso do *Bing*) e também a vídeos, mapas, notícias, livros, calendários, fotografias, documentos, sites e grupos – (Blachman – 2012b) .

Nas tabelas seguintes identificam-se comandos que podem ser utilizados no Google para pesquisar informação sobre a exploração sexual de crianças no Ciberespaço.

[7] O modo passivo, refere-se à possibilidade do Google emitir alertas, ou seja, de permitir a atualização de informação com frequência base diária, automática, de registos contendo determinadas expressões pretendidas e explicitadas pelo interessado, enviando os resultados para um endereço de correio eletrónico indicado pelo utilizador. Veja a informação do Google Alert FAQS, 2012.
[8] O modo ativo refere-se à busca de informação diretamente efetuada pelo utilizador no motor de busca.

Tabela 4 - Comandos de Pesquisa na Internet

Descrição do Operador	**Exemplo de formato**	**Descrição**	**Resultado**
Filetype:	"procuradoria-geral da república" filetype: pdf	Restringe os resultados da pesquisa pela extensão do tipo de ficheiro	Devolve todos os documentos "pdf" indexados pelo GOOGLE que incluam, no título ou no conteúdo, a expressão "procuradoria-geral da república"
site:	"procuradoria-geral da república" site: dn.pt	Pesquisa numa página ou num domínio	Devolve todos os conteúdos existentes no "dn.pt" e indexados pelo GOOGLE cujo título ou conteúdo inclua a expressão "procuradoria-geral da república"
inrul:	inurl:"procuradoria-geral da república"	Pesquisa por mútiplas palavras no URL	Devolve todos os conteúdos indexados no GOOGLE que contenham a expressão "procuradoria-geral da república no URL
allinrul: procuradoria geral da república dciap	allinrul: procuradoria-geral da república dciap	Pesquisa por múltiplas palavras no URL	Devolve todos os conteúdos indexados no GOOGLE que contenham as palavras PROCURADORIA, GERAL, DA REPÚBLICA e DCIAP , no URL
intext:	intext:pgr	Pesquisa por uma palavra no corpo do texto das páginas indexadas	Devolve todas as páginas indexadas no GOOGLE que contenham no corpo do texto a palavra PGR
allintext:	allintext:pgr dciap	Pesquisa por múltiplas palavras no corpo do texto das páginas indexadas	Devolve todas as páginas indexadas no GOOGLE que contenham no corpo do texto as palavras pgr e dciap

Tabela 5 – Comandos de Pesquisa na Internet

intitle:	intitle:“procuradoria geral da república”	Pesquisa por uma palavra ou frase no título das páginas indexadas	Devolve todas páginas indexadas pelo GOOGLE que contenham a expressão “procuradoria geral da república” no título.
allintitle:	allintitle: pgr diap	Pesquisa por múltiplas palavras no título das páginas indexadas	Devolve todas páginas indexadas pelo GOOGLE que contenham no título as palavras pgr diap
inanchor:	inanchor:“pgr”	Pesquisa por uma palavra ou frase no texto de ancoragem das páginas indexadas	Devolve todas páginas indexadas pelo GOOGLE que contenham a expressão “pgr” no texto de ancoragem.
allinanchor:	allinanchor: pgr circulares	Pesquisa múltipla - palavras no texto de ancoragem - páginas indexadas	Devolve todas páginas indexadas pelo GOOGLE que contenham no texto de ancoragem as palavras PGR e CIRCULARES
[#]..[#]	2009..2010 “Academia Militar”	Mostra conteúdos produzidos num intervalo de datas	Mostra todos os conteúdos indexados que tenham sido produzidos entre 2009 e 2010 e que contenham a expressão “Academia Militar”
related:	related: http://www.pgr.pt	Mostra páginas de conteúdo semelhante	Exibe páginas cujo conteúdo é semelhante ao de www.pgr.pt
info:	info:www.academiamilitar.pt	Exibe informação sobre uma página	Exibe a informação disponível na página www.academiamilitar.pt. Note-se que pode não existir informação disponível.

Tabela 6 – Comandos de Pesquisa na Internet

link:	ink:www.academia militar.pt	Exibe páginas que contenham ligações para a página Especificada	Exibe todas as páginas que têm ligações para www.academiamilitar.pt
cache:	cache:www.pgr.pt	Exibe a versão em memória cache no GOOGLE da página especificada	Exibe a versão existente na memória CACHE do GOOGLE da página www.pgr.pt
phonebook:	phonebook: pgr, rua da escola politécnica, 140,	Mostra uma lista telefónica	Mostra os registos telefónicos associados

Tabela 7 – Comandos de Pesquisa de Serviços na Internet

Serviços a pesquisar	**Operadores de pesquisa a utilizar**
Pesquisa de páginas	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, site:
Pesquisa de imagens	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Grupos	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directório	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
Notícias	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
Pesquisa de produtos	allintext:, allintitle:

Estes exemplos de pesquisa do *Google* são aplicáveis a outros motores de busca. O *Google* é um indexador de páginas Internet. É muito provável que não indexe todas as páginas, pelo que será aconselhável utilizar outros motores de busca de que são exemplo os seguintes: *Yahoo* (www.yahoo.com); *Altavista* (www.altavista.com); www.excite.com, Sapo – (www.sapo.pt) e *Metacrawler* (www.metacrawler.com) - acciona outros motores de busca para proporcionar os resultados.

3.2. Recuperação de Páginas Internet

Suponhamos agora que o investigador soube da existência de uma página a qual, em 2008, continha determinados conteúdos e fotografias relacionadas com o abuso sexual de crianças. O investigador procura a página na Internet, acede ao seu conteúdo, mas verifica que os referidos elementos se encontram indisponíveis para visualização. Uma solução, para ultrapassar este obstáculo consiste na utilização do motor *wayback*, serviço disponível através da ligação www.archive.org, e digitar, em local próprio, a página a procurar. Por exemplo, conforme pesquisa efetuada, a página da PGR está disponível em www.archive.org e, em 26 de junho de 2008 tinha a seguinte apresentação:

Figura 1 – Apresentação da página da PGR (26-06-2008)

3.3. Domínios de Internet e Endereços IP

Como referimos anteriormente, qualquer dispositivo que comunique através da Internet tem que ter associado um endereço IP. É o endereço IP que permite a localização do computador que a ele está associado: quando escrevemos no navegador www.google.com, ou www.pgr.pt, o nosso computador vai mostrar, respetivamente, a página inicial do motor de busca *Google* ou da PGR, e para isso, a máquina tem que conhecer o endereço IP de cada computador (ou grupo de computadores) que aloja o *Google* ou a página da PGR.

Este mesmo raciocínio é válido para chamadas VOIP (voz sobre IP), ou para a transferência simples de ficheiros. Como se fosse um sistema telefónico, em que o telefone

chamador e de destino têm que estar ligados à rede telefónica e ter um número atribuído, na Internet, os computadores para comunicarem entre si necessitam de um endereço IP.

Existindo informação disponível na investigação criminal sobre um endereço IP, ou de um endereço de uma página Internet ou de outro tipo de recurso, poder-se-á recorrer a serviços disponíveis em linha, gratuitos, especificamente desenhados para fornecer a informação disponível sobre os titulares de endereços IP e de páginas Internet, indicando-se, a título de exemplo, os seguintes:

Central Ops - www.centralops.net;

DNSStuff - www.dnsstuff.com;

Domain Tools - www.domaintools.com; www.ip-address.org/;

IP Adress - www.ip-adress.org/.

Estes serviços são pesquisadores que procuram nas bases de dados dos denominados RIR's -*Regional Internet Registry*, os recursos numéricos da Internet numa determinada região do globo. No caso da página ou endereço IP pesquisado estar associado à exploração sexual de crianças, a informação, por exemplo, do titular do equipamento que aloja determinada página com conteúdos relativos a pornografia infantil pode ser facultada à investigação por essa empresa. De realçar, no entanto que, mesmo assim, não existe a garantia de identificar logo o titular da página, ou do endereço, porque o titular da rede pode identificar-nos uma entidade que, por sua vez, tenha subalugado a outra entidade, o domínio ou o endereço IP, e assim sucessivamente por vários níveis, podendo existir cinco ou mais intermediários. [9] Se, por exemplo, pretendermos saber quais é que são os dados identificativos da página da PGR, pesquisando por exemplo na ferramenta disponível *on-lineDomain Tools* – www.domaintools.com - obtemos o seguinte resultado:

[9] Tanto o "Central Ops" como "DNSStuff" dispõem de uma funcionalidade que se designa por "Traceroute". Esta ferramenta permite determinar o número de nós/saltos que os pacotes que compõem uma comunicação de dados através da Internet atravessa até chegar ao seu destino. Esta ferramenta permite, desta modo, conhecer os sítios (routers/servidores) por onde os pacotes da comunicação viajam até ao seu destino e traçar assim o caminho do emissor da comunicação até ao seu destinatário.

Nome de domínio / Domain Name: pgr.pt
Data de registo / Creation Date (dd/mm/yyyy): 14/06/1996
Data de expiração / Expiration Date (dd/mm/yyyy): 27/06/2016
Estado / Status: ACTIVE
Titular / Registrant
Procuradoria-Geral da Republica
Rua do Arsenal, letra G
1100-038 Lisboa
Email:
zeluis@gddc.pt ; correio@lisboa.mptr.mj.pt ; tecnologiasdeinformacaodogddc@gddc.pt ;
mp.lisboa.tr@tribunais.org.pt ; mailpgr@pgr.pt
Entidade Gestora / Billing Contact
Procuradoria-Geral da Republica
Email:
zeluis@gddc.pt ; correio@lisboa.mptr.mj.pt ; tecnologiasdeinformacaodogddc@gddc.pt ;
mp.lisboa.tr@tribunais.org.pt ; mailpgr@pgr.pt

Responsável Técnico / Tech Contact
Jose Luis Cristovao
Email: zeluis@pgr.pt

Figura 2 – Registo da página da PGR

Existem também ferramentas que permitem localizar geograficamente uma página. Se por exemplo, pretendêssemos localizar a página da PGR obteríamos o seguinte resultado:

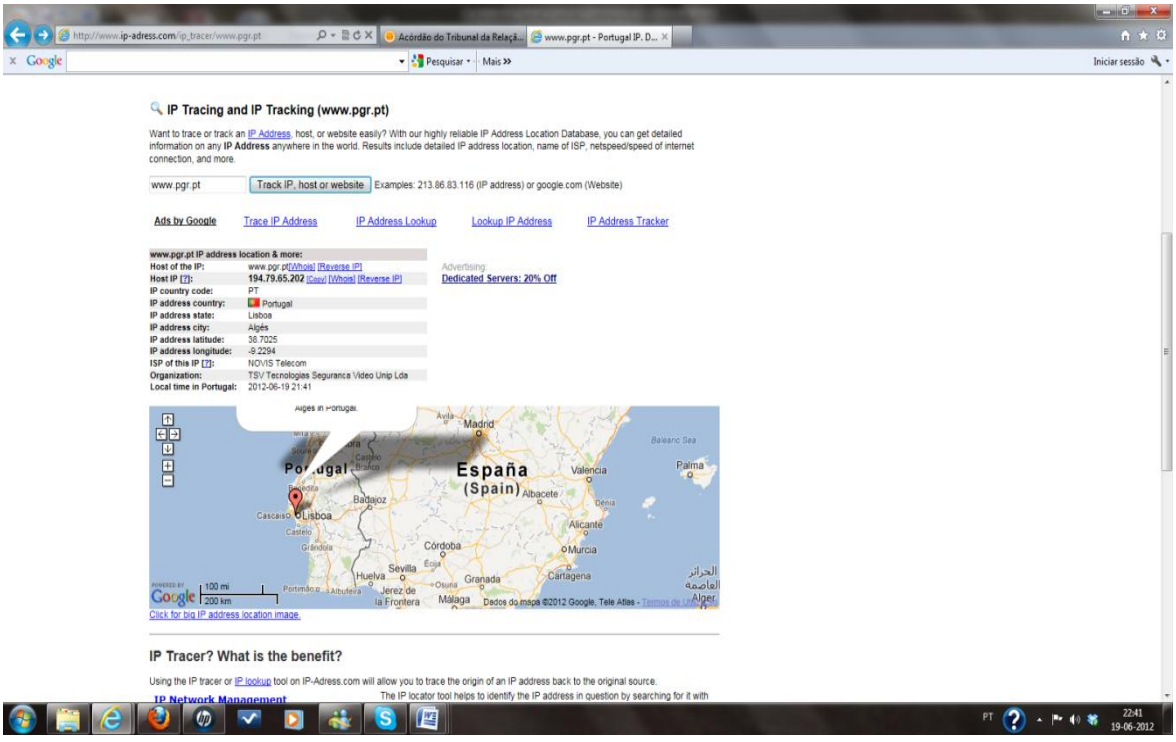

Figura 3 – Localização da página da PGR

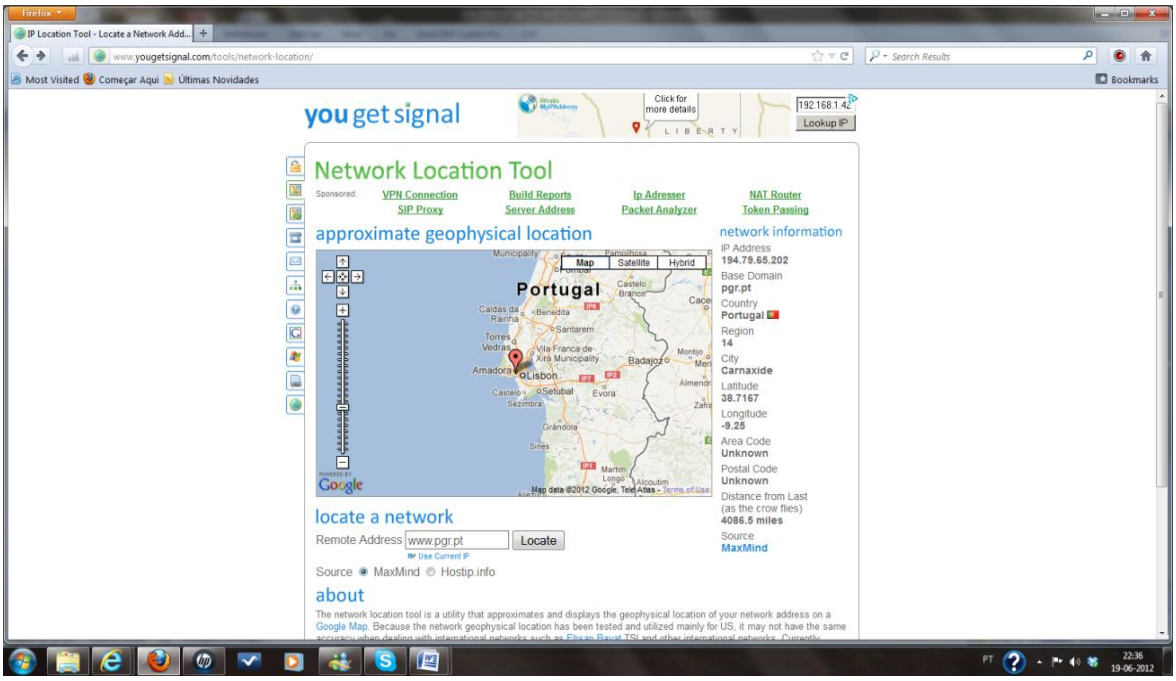

Figura 4 – Localização da página da PGR

De notar que existem endereços IP que não irão ter qualquer resposta útil para a investigação nos serviços acima descritos, com prejuízo para a IC. Tratam-se dos endereços de IP privados, que existem apenas em redes locais e não têm qualquer exposição pública. Estes endereços são utilizados em redes empresariais ou residenciais e correspondem aos computadores utilizados internamente numa rede privada. Essas redes terão um ponto de comunicação com o exterior, que se denomina *Gateway*, habitualmente componente integrante de um *Router* ou de um *Switch* e esse ponto de comunicação com o exterior já disporá de um endereço IP público.

3.4. Cabeçalhos técnicos de mensagens de correio eletrónico

Distribuidores de material pornográfico podem usar o correio eletrónico para transmitir pornografia infantil, desde que não seja de grandes dimensões. Os cabeçalhos técnicos das mensagens de correio eletrónico contêm informação da *"viagem"* de uma mensagem de correio eletrónico, detalhando o caminho que uma mensagem fez ao cruzar os servidores de e-mail, sendo possível identificar o IP associado ao envio de uma mensagem suspeita. Uma vez na posse do IP é possível solicitar às empresas prestadoras de serviços de Internet quem é o titular da conta de correio eletrónico. O modo de aceder aos cabeçalhos técnicos de mensagens de correio eletrónico difere de aplicação para aplicação. Vejamos:[10]

[10] Google mail – página inicial de ajuda – cabeçalhos de mensagem.

Tabela 8 – Aceder aos cabeçalhos técnicos do Gmail

1. Faça login no Gmail 2. Abra a mensagem cujos cabeçalhos pretende visualizar. 3. Clique na seta para baixo ao lado de **Responder**, no canto superior do painel da mensagem. 4. Selecione **Mostrar original** – os cabeçalhos completos são exibidos numa nova janela.

Tabela 9 – Aceder aos cabeçalhos técnicos do Hotmail

1. Faça login na sua conta do Hotmail. 2. Selecione **Caixa de Entrada** no menu à esquerda. 3. Clique com o botão direito do mouse na mensagem cujos cabeçalhos pretende visualizar e selecione **Exibir código - fonte da mensagem** – os cabeçalhos completos são exibidos numa nova janela.

Tabela 10 - Aceder aos cabeçalhos técnicos do Yahoo!

1. Faça login na sua conta de e-mail do Yahoo! 2. Selecione a mensagem cujos cabeçalhos pretende visualizar. 3. Clique no menu suspenso **Ações** e selecione **Exibir cabeçalho completo** – os cabeçalhos completos são exibidos numa nova janela.

Tabela 11 – Aceder aos cabeçalhos técnicos do Apple Mail

1. Abra o Apple Mail. 2. Clique na mensagem cujos cabeçalhos pretende visualizar. 3. Vá para o menu **Visualizar**. 4. Selecione **Mensagem** e, em seguida, **Cabeçalhos longos** – os cabeçalhos completos aparecerão na janela abaixo da sua caixa de entrada.

Tabela 12 – Aceder aos cabeçalhos técnicos do Mozilla

1. Abra o Mozilla. 2. Clique na mensagem cujos cabeçalhos pretende visualizar. 3. Clique no menu **Visualizar** e selecione **Origem da mensagem** – os cabeçalhos completos são exibidos em uma nova janela.

Tabela 13 – Aceder aos cabeçalhos técnicos do Opera

1. Abra o Opera. 2. Clique na mensagem cujos cabeçalhos pretende visualizar para que sejam exibidos na janela abaixo de sua caixa de entrada. 3. Clique em **Exibir todos os cabeçalhos** em frente ao campo **Para** – os cabeçalhos completos serão exibidos na janela abaixo.

Tabela 14 – Aceder aos cabeçalhos técnicos do Outlook

1. Abra o Outlook. 2. Abra uma mensagem. 3. Na guia **Mensagem**, no grupo **Opções**, clique na imagem de ícone **Iniciador da caixa de diálogo**. 4. Na caixa de diálogo **Opções de mensagem** – os cabeçalhos são exibidos na caixa **Cabeçalhos de internet**

Tabela 15 – Aceder aos cabeçalhos técnicos do Outlook Express

1. A partir de sua caixa de entrada, localize a mensagem cujos cabeçalhos pretende visualizar. 2. Clique com o botão direito na mensagem e selecione **Propriedades**. 3. Abra a guia **Detalhes**, na caixa de diálogo – os cabeçalhos completos são exibidos na caixa de diálogo.

Os cabeçalhos de mensagens de correio eletrónico podem ser lidos e descodificados com facilidade, desde que se utilizem ferramentas disponíveis em linha, como por exemplo a disponível no seguinte endereço web: http://www.ip-address.org/tracker/trace-email.php. Em alternativa pode-se ler um cabeçalho de mensagem, seguindo o caminho de uma

mensagem de forma cronológica, isto é lendo a partir da parte inferior do cabeçalho, e analisando os cabeçalhos técnicos de baixo para cima. Vejamos, um exemplo de um cabeçalho de mensagem de um mail, enviado do endereço de correio eletrónico: MrJones@emailprovider.com para o endereço: MrSmith@gmail.com.

Tabela 16 – Exemplo de cabeçalho técnico de mensagem de correio eletrónico

Delivered-To: MrSmith@gmail.com Received: by 10.36.81.3 with SMTP1 id e3cs239nzb; Tue, 29 Mar 2005 15:11:47 -0800 (PST) Return-Path: **Received:** from mail.emailprovider.com (mail.emailprovider.com [**111.111.11.111**]) by mx.gmail.com with SMTP id h19si826631rnb.2005.03.29.15.11.46; Tue, 29 Mar 2005 15:11:47 -0800 (PST) Message-ID: <20050329231145.62086.mail@mail.emailprovider.com> Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue, 29 Mar 2005 15:11:45 PST Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST) From: Mr Jones Subject: Hello To: Mr Smith

Depois de analisados os elementos do cabeçalho, no sentido de identificarmos o IP do remetente podemos copiar integralmente o seu conteúdo para uma ferramenta automática de análise de cabeçalhos técnicos, neste caso a ferramenta disponível em http://www.ip-address.org/tracker/trace-email.php. O resultado obtido é o seguinte:

Email Header Analysis

Delivered-To: MrSmith@gmail.com
Received: by 10.36.81.3 with SMTP1 id e3cs239nzb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
Return-Path:
Received: from mail.emailprovider.com (mail.emailprovider.com [111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb.2005.03.29.15.11.46; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
Message-Id: <20050329231145.62086.mail@mail.emailprovider.com>
Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue, 29 Mar 2005 15:11:45 PST
Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)
From: Mr Jones
Subject: Hello
To: Mr Smith

Figura 5 – Exemplo de análise automática de cabeçalho técnico

Da análise efetuada verificamos que o IP da mensagem suspeita é o seguinte: IP 11.11.111.111, pelo que teremos de descobrir a que empresa prestadora de serviços de Internet pertence o referido IP, socorrendo-nos para o efeito da ferramenta disponível em http://whois.domaintools.com/. O resultado é o seguinte:

IP Location: United States Columbus Dod Network Information Center
IP Address: 11.11.111.111 **OrgName:** DoD Network Information Center OrgId: DNIC **Address**: 3990 E. Broad Street City: Columbus StateProv: OH PostalCode: 43218 Country: US OrgAbusePhone: +1-800-365-3642 OrgAbuseEmail: registra@nic.mil OrgAbuseRef: http://whois.arin.net/rest/poc/REGIS10-ARIN

Figura 6 – Identificação da entidade/empresa associada ao IP de mensagem

Uma vez identificada a empresa e a entidade titular do referido IP é necessário solicitar informação sobre a pessoa titular da referida conta de correio eletrónico com indicação da respetiva morada ou seja, a pessoa que na data e hora indicada no cabeçalho técnico se encontrava a utilizar aquele IP – quando se pede a informação é necessário indicar a data e hora local tendo em conta o fuso horário, ou seja indicar a hora dos EUA, uma vez que a mensagem de correio eletrónico que serve de exemplo foi enviada desse país (no caso de nos pedidos se não identificar a data e hora local a resposta da empresa não corresponderá ao IP detetado). Estes pedidos podem ser efetuados através de Carta Rogatória - pedido de cooperação judiciária internacional entre autoridades judiciárias – mas, em alguns casos, as empresas consultadas têm respondido a pedidos efetuados através de fax ou de correio electrónico, desde que solicitados por autoridade judiciária, em prol da celeridade. Obtidos esses elementos, efetuadas ulteriores diligências para confirmação da morada do suspeito de enviar pornografia de menores por correio eletrónico, é necessário ponderar a realização de uma busca para apreensão de prova digital.

Contudo, existem alguns países, que simplesmente não respondem a estes pedidos de identificação de titulares de IP, ou a resposta a estes pedidos demora muito tempo a ser prestada à IC (vários anos), o que provoca, naturalmente, prejuízos graves quanto à eficácia das investigações deste fenómeno.[11]

[11] São do conhecimento público as referências à demora na resposta por parte de autoridades de IC estrangeiras a pedidos de cooperação judiciária internacional em matéria penal.

3.5. Buscas e Apreensões de dados digitais

As buscas e as apreensões, são instrumentos (meios de obtenção de prova) de que se servem as autoridades judiciárias para recolher meios de prova. Os meios de obtenção de prova distinguem-se dos meios de prova numa dupla perspetiva: lógica e técnico-operativa. Na perspetiva lógica os meios de prova caracterizam-se pela sua aptidão para serem por si mesmos fonte de convencimento, ao contrário dos meios de obtenção de prova que apenas possibilitam a aquisição daqueles meios. Na perspetiva técnico-operativa os meios de obtenção de prova caracterizam-se pelo modo e também pelo momento da sua aquisição no processo, em regra nas fases preliminares[12]., sobretudo no inquérito-crime (Silva, 1999, p. 189).O Art. 174.º n.ºs 1 e 2 do CPP dispõe que quando houver indícios de que existam objetos, em local reservado ou não livremente acessível ao público, relacionados com o crime ou que possam servir de prova, é ordenada busca. A competência para ordenar busca pertence à autoridade judiciária, leia-se magistrado do Ministério Público ou magistrado judicial, nos termos do disposto no Art. 174.º, n.º 3 do CPP, com exceção dos casos previsto no Art. 174.º, n.º 5 do CPP, que regula os casos em que os órgãos de polícia criminal podem efetuar buscas, por iniciativa própria, ou seja, nos seguintes casos:

- Terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática de crime que ponha em grave risco a vida ou integridade física de qualquer pessoa;
- Quando os visados consintam, desde que o consentimento prestado fique, por qualquer forma documentado;
- Aquando da detenção em flagrante delito a que corresponda pena de prisão.

No caso de ser necessária a realização de busca domiciliária ou numa sua dependência fechada, a competência para ordenar a busca pertence ao juiz e só pode ser realizada entre as 07.00 horas e as 21.00 horas, sob pena de nulidade, nos termos do disposto no Art. 177.º, n.º 1 do CPP. Tratando-se de busca em escritório de advogado ou em consultório médico esta é, sob pena de nulidade, presidida pessoalmente pelo juiz, o qual avisa previamente o presidente do Conselho local da Ordem dos Advogados ou da Ordem dos Médicos, para que o mesmo, ou um seu delegado, possa estar presente – Art. 177.º, n.º 5 do CPP. Após a apreensão de prova eletrónica efetuada por órgão de polícia criminal, esta é validada ou não validada pela autoridade judiciária competente, consoante esta seja útil ou não para a investigação ou esteja relacionada com a prática de crime, nos termos do

[12] Assim, por exemplo, enquanto a escuta telefónica é um meio de obtenção de prova, as gravações e as transcrições das conversações efetuadas são já um meio de prova.

disposto no Art. 178.º, n.º 5 do CPP. A omissão da validação pela autoridade judiciária de apreensão efetuada pelo órgão de polícia criminal constitui uma nulidade sanável, nos termos do disposto no Art. 120.°, n.° 2, al .d) do CPP.

Para a IC do âmbito deste trabalho, a realização de buscas carecerá, na maioria dos casos, de decisão do Ministério Público ou do Magistrado Judicial, ou seja estão para além das competências dos órgãos de polícia criminal, sobretudo no que concerne à apreensão de material de abuso sexual de menores. Esta situação merecerá ponderação do ponto de vista de encontrar mecanismos legais e organizativos por parte da IC, que possibilitem eficácia de resposta em situações que justifiquem celeridade de ação, sem prejuízo do princípio da inviolabilidade do domicílio e da reserva da intimidade da vida privada.

3.6. Cadeia de custódia da prova

A *"cadeia de custódia da prova"* também identificada como *"cadeia probatória*" refere-se à capacidade de garantir a identidade e integridade de um espécime ou amostra no decurso da sua obtenção (por exemplo numa busca), durante a sua análise e até ao final do processo. Consiste em salvaguardar e proteger a informação digital apreendida, de forma documentada, de modo a que não possa alegar-se que foi modificada ou alterada durante a IC. Com os objetos físicos que constituem prova, a prática é armazená-los em sacos ou envelopes selados, com um formulário que especifica o número do processo, os dados de identificação do objeto, a pessoa que procedeu à sua apreensão, a quem foi apreendido (normalmente um suspeito ou a um arguido), em que local e em que data e, bem assim, cada pessoa que a tenha utilizado ou acedido, de modo a que inexistam dúvidas sobre quem teve acesso à prova, em que termos e porque motivo.

A prova eletrónica caracteriza-se pela volatilidade, instabilidade e diversidade das tecnologias utilizadas, pelo que a manutenção da cadeia probatória exige especiais cautelas por parte da IC. A volatilidade da prova eletrónica refere-se à existência de possibilidade de perda irremediável de dados digitais, que impossibilita a apreensão, acesso e exibição desses dados com a segurança exigida pelas regras de produção de prova e do método científico – configuram-se como exemplos da volatilidade da prova digital os ficheiros temporários, os registos de acesso à Internet ou o registo de acesso remoto a outros sistemas, que podem facilmente desaparecer durante uma operação de busca, com um simples desligar do computador ou mediante ação do suspeito. A instabilidade refere-se à circunstância de qualquer interação com os dados digitais originais provocar a sua alteração e a consequente impossibilidade de repetição no âmbito do processo-crime por

comprometimento da integridade da informação, sendo que as regras do método científico e de manutenção da cadeia de custódia da prova impõem a possibilidade de repetição. A diversidade de tecnologias utilizadas refere-se à circunstância de existirem inúmeras aplicações, por vezes desenvolvidas à medida, ficando impedida a observação dos dados apreendidos quando não se possui a ferramenta aplicacional que os permita interpretar (Casey, 2011, p. 289).

Uma das metodologias para assegurar a integridade da prova eletrónica (imagens de discos e memória, arquivos de dados e ficheiros executáveis, etc.) consiste em obter *hashes* (vulgo assinaturas digitais) da informação no momento da sua recolha, de modo que possa comprovar-se em qualquer momento que essa prova não foi modificada ou alterada durante o decorrer do processo-crime. Assim, na apreensão de dados digitais e na realização de perícias informáticas forenses, as boas regras indicam que o perito informático forense deverá proceder à elaboração de uma imagem certificada dos dados constantes dos suportes digitais apreendidos, que se manterão intactos, isto é sem iniciar o respetivo processo de *startup* dos instrumentos de acesso e visualização. A partir dessa imagem, deverá proceder-se à extração de dados para pesquisa para outro suporte, destinado a análise de informação - trata-se da denominada "cópia de trabalho". Deste modo, na perspetiva de manutenção da cadeia de custódia da prova é necessário manter à ordem do processo os originais de hardware e dados apreendidos, uma imagem certificada dos dados e uma terceira cópia, também certificada, com "extração dos dados" para se proceder à pericia informática forense e análise de dados, de acordo com os quesitos formulados.

3.7. Planeamento e execução de busca para apreensão de dados digitais

A prova eletrónica digital é um tipo de prova valioso para as investigações criminais relacionadas com exploração sexual de crianças no Ciberespaço e, em consequência, deve ser tratada com exigência e cuidado, no sentido de manter a integridade dos dados. Nesse sentido, no âmbito de buscas e apreensões de dados digitais é necessário observar as seguintes regras gerais:

- As ações desencadeadas pelas forças policiais ou seus agentes não devem alterar os dados guardados num computador ou num dispositivo de armazenamento que possa ser apresentado em tribunal como prova;
- Em circunstâncias excecionais, caso se considere necessário aceder aos dados originais mantidos num computador ou num dispositivo de armazenamento de

dados, essa pessoa deve ter competência legal e técnica para o fazer e poder apresentar provas, explicando a relevância e as implicações das suas ações;

- Deve ser criada e preservada uma linha de auditoria ou outro registo de todos os processos aplicados a elementos de prova eletrónicos informáticos. Um terceiro independente deve poder examinar esses processos e obter o mesmo resultado.
- A pessoa responsável pelo processo (responsável do processo: magistrado do Ministério Público e ou magistrado judicial) deve assumir a responsabilidade global pela observância da lei e dos presentes princípios.[13]

No caso de ser previsível a apreensão de prova digital, no âmbito de uma diligência de investigação deve ser garantida atempadamente a presença de um perito informático forense, devidamente designado no processo por parte da autoridade judiciária competente para a diligência, nos termos do disposto nos Art.s 151.º, 152.º, 153.º e 154.º do CPP que com as ferramentas de hardware e software adequadas garantirá a integridade dos dados no decorrer da apreensão. Deste modo, caso se trate de busca domiciliária ou em que estejam em causa direitos liberdades e garantias deverá ser o Juiz de Instrução Criminal a nomear o perito, caso contrário deve ser o magistrado do Ministério Público a proceder à sua nomeação, prevendo-se que, inexistindo esse despacho de nomeação, advenha perigo para a garantia da prova e para a posterior perícia, que poder ser considerada irregular (Ac. TRL, 2011-09-15). Acresce que todos os intervenientes em processos crimes relacionados com a criminalidade informática devem ter formação adequada sobre as metodologias de investigação e as especificidades inerentes à prova digital.

Em concertação com o perito nomeado e em função da informação previamente recolhidas, deverá em primeiro lugar ser decidido que tipo de busca se vai realizar, no sentido de o perito ou os peritos estarem preparados para o que vão encontrar no local. A título de exemplo, sempre que possível, deverá ser recolhida informação preliminar sobre o seguinte (Ferraro et al., 2005, p. 152-154).

- Computadores, Sistemas Operativos, Programas e dispositivos de armazenamento;
- Redes de comunicações e informáticas (ISP, telefones, faxes, modems, redes, equipamento de rede, etc.);
- Identificação do responsável pelos sistemas ou rede (se tem um administrador local ou é administrada por uma empresa externa);
- Identificação da quantidade de equipamento que é expectável apreender;

[13] OLAF – Office Européene de Lutte Anti - Fraud - Informações sobre os procedimentos de informática forense do OLAF.

- Identificação da quantidade de dados que se prevê copiar;
- Informação sobre a existência de um sistema de *backup* (relevante para o tipo de busca a empreender).

Chegados ao local da busca é necessário desenvolver ações que permitam que a diligência se desenvolva em ambiente de segurança e serenidade, sendo aconselhável que se efetue um reconhecimento prévio do local a buscar, sobretudo nos casos que envolvam a exploração sexual de crianças no Ciberespaço. Indicam-se brevemente alguns passos a seguir no âmbito de uma operação de busca:

- Afastar todas as pessoas dos equipamentos informáticos, incluído das ligações elétricas e quadros elétricos;
- Proteger todos os dispositivos com dados voláteis, física e eletronicamente;

Identificar, proteger, documentar e fotografar todos os dispositivos que contenham dados a apreender;

- Elaborar reportagem fotográfica do local onde se encontram os dispositivos a apreender, bem como de outros locais que se entenda poderem vir a ser relevantes para a prova;
- Durante a diligência, controlar constantemente todas as pessoas presentes no local, para evitar que estas possam interferir com os elementos de prova;
- Manter sempre os dispositivos a apreender debaixo da vigilância atenta de pelo menos um dos elementos da equipa de busca;
- Identificar e documentar todas as redes a que os dispositivos estavam ligados (dados, voz, *wireless*, etc...);
- Verificar se será relevante a recolha de outros tipos de vestígios, tais como biológicos, lofoscópicos, produto estupefaciente, e, se necessário, chamar ao local outros elementos técnicos e em caso afirmativo: recolher impressões digitais de teclados, ratos, disquetes, discos ópticos ou outros componentes, depois de salvaguardada a prova digital;
- Procurar outros objetos não eletrónicos, mas com eles relacionados, indicando-se a título de exemplo: palavras-chave escritas em post-it, papéis, cadernos ou diários, blocos de apontamentos com marcas manuscritas latentes, calendários e manuais de software, fotografias, folhas impressas, informações de interesses pessoais (matriculas, filhos, números de telefone, hobbies, nomes dos animais de estimação, etc...), que poderão ajudar na elaboração de dicionários para quebra de *passwords*;

- Efetuar entrevistas preliminares - separar e identificar as pessoas, descrevendo os locais onde se encontravam quando se entrou na cena da busca, no sentido de tentar obter informação sobre a finalidade de um dispositivo em concreto, o proprietário e utilizadores do dispositivo, os *usernames* e ISP que utiliza, todas as passwords necessárias para aceder ao sistema, programas e dados BIOS, disco, sistema operativo, rede, ISP, bases de dados, sistemas de encriptação, correio electrónico, etc, quais os sistemas/dispositivos de segurança e destruição utilizados, locais externos de armazenamento de dados, e documentação explicativa de hardware e software instalados (Ferraro et al., 2005, p. 172-176).

Como consequência, na execução de uma busca para apreensão de prova eletrónica, configuram-se os seguintes procedimentos operacionais:

- **Presença múltipla no quadro de busca e apreensão de prova digital**

Uma busca para apreensão de elementos de prova digital deve ser efetuada por duas ou mais pessoas, ou seja pelo menos duas pessoas devem estar envolvidas na interação de cada um dos objetos a apreender. Esta metodologia, por um lado, vai permitir uma maior proteção dos agentes e por outro permitirá uma maior eficácia da busca, seguindo aqui os princípios gerais das buscas, que determinam que a busca do mesmo local seja efetuada por pelo menos duas vezes, por mais do que uma pessoa e em sentido inverso um do outro.

- **Preservação da integridade dos dados desde a apreensão até ao julgamento**

Nenhuma ação das autoridades deverá alterar os dispositivos eletrónicos ou o seu conteúdo, garantindo a sua integridade probatória em sede do processo. Quando se manipulam os dispositivos eletrónicos e os dados, nada deve ser alterado, nem o hardware nem o software (quanto à preservação dos dados a longo termo ver Apêndice 5).

- **Registo da cadeia da prova**

No âmbito de uma busca é necessário registar todos os procedimentos executados, na interação com os dispositivos eletrónicos. Uma entidade externa ou designada pelo arguido deve poder chegar aos mesmos resultados executando os mesmos procedimentos. Este registo é impreterível, sob pena de poder comprometer a validade da prova. Todas as atividades relacionadas com a apreensão, acesso, armazenamento ou transferência da prova digital, devem ser documentadas e armazenadas para posterior análise. Caso seja possível, esta informação deve ser registada no respetivo auto de apreensão. Este registo auxiliará os intervenientes na busca e na apreensão e na descrição das atividades desenvolvidas

aquando da produção da prova em sede de julgamento, que normalmente tem lugar vários anos depois da apreensão dos objetos.

3.8. Tipos de Apreensão

Nos termos do disposto na LCiber existem quatro modalidades gerais de apreensão de prova digital:

- **Apreensão dos equipamentos e dos meios de armazenamento;**

Este tipo de apreensão pode ser adequado nas seguintes situações:

- Inexistência de grande quantidade de equipamento para apreender - por exemplo, um PC isolado ou uma pequena rede numa residência particular;
- Inexistência de previsibilidade de graves prejuízos financeiros ou outros, em virtude da apreensão dos equipamentos;
- Necessidade de interromper a atividade suportada pelos equipamentos, uma vez que a atividade é em si ilícita.

Conseguem-se configurar algumas vantagens deste tipo de apreensão, a saber:

- Possibilidade de ser executada com alguma facilidade por agentes de polícia sem especialização;
- Permite operações de busca mais rápidas, o que pode ser vantajoso em ambientes adversos;
- A prova digital fica integralmente na posse das autoridades;
- Permite uma análise pericial forense mais cuidada, em ambiente próprio e com as ferramentas adequadas.

- **Cópia por imagem de conteúdos de memória**

No que concerne a este tipo de apreensão é necessário utilizar equipamento e programas informáticos forenses especiais que criam uma cópia exata, bit a bit, do conteúdo alvo para um dispositivo externo de armazenamento. Estes dispositivos e programas informáticos permitem assegurar que os dados não são posteriormente alterados e que a integridade da informação possa ser verificada em sede de julgamento, caso seja levantada essa questão pelo arguido.

Este tipo de apreensão é adequado nas seguintes situações:

- Existe uma grande quantidade de equipamentos para apreender (normalmente em empresas médias ou grandes);
- Não é possível nem viável a apreensão dos equipamentos (ex: Sistemas informáticos de grandes empresas, tais como Bancos ou Seguradoras);

- A apreensão dos equipamentos causaria graves prejuízos financeiros a organização;
- Em função dos factos sob investigação não é necessário apreender o equipamento.

As vantagens desta modalidade de apreensão são as seguintes:

- Redução do risco de danificação dos equipamentos;
- Previne risco de prejuízos para terceiros que partilhem os equipamentos ou beneficiem de Serviços disponibilizados por estes;
- Permite que a organização continue a exercer a sua atividade normal, sem prejudicar a sua atividade económica;

As desvantagens que se configuram quanto a este tipo de apreensão são as seguintes:

- É necessário equipamento especial no cenário da busca;
- É necessária a presença de um perito informático forense devidamente nomeado pela autoridade judiciária para concretizar a operação de busca;
- Usualmente é necessária a colaboração do suspeito ou do administrador de sistemas, na identificação dos locais exactos dos elementos de prova;
- A apreensão é muito mais morosa, podendo demorar várias dezenas de horas, não sendo por vezes possível conclui-la num só dia de trabalho.

- **Apreensão dos dispositivos contendo as cópias de segurança existentes**

Este tipo de apreensão é adequada para as situações descritas na modalidade de apreensão através de elaboração de imagem integral dos conteúdos de memória acima referida, sobretudo se existe uma grande quantidade de equipamentos e dados a apreender (grandes redes ou ambientes de *Mainframe*).

As vantagens são semelhantes às da realização de imagem forense, a que acresce a circunstância de não ser necessário a utilização equipamento especial e a busca é mais célere. Configuram-se, no entanto, as seguintes desvantagens operacionais:

- É necessária a presença de um perito informático forense, devidamente designado por parte da autoridade judiciária competente;
- É necessária a colaboração do visado ou do seu administrador de sistemas;
- Possibilidade de os *backups* estarem danificados ou não conterem a informação integral, com o inerente prejuízo para a prova;
- É necessário replicar o ambiente do sistema informático do visado, para que o *restore* tenha sucesso, nomeadamente com motores da base de dados e outros o que se pode revelar demasiado dispendioso.

Pelos motivos acima apresentados é uma modalidade de busca a utilizar apenas em último recurso.

- **Cópia seletiva de dados**

Esta modalidade consiste em copiar para um suporte apenas aqueles dados que se selecionam no momento.

Este tipo de apreensão deve apenas ser utilizado em circunstâncias especiais e se nenhum dos métodos anteriores for viável, sendo aconselhável a presença da(s) autoridade(s) judiciária(s) a acompanhar a busca, as quais devem validar, no local a apreensão e o método utilizado.

As desvantagens que se apontam à realização desta modalidade de busca são as seguintes:

- É necessário garantir a presença de um perito, o que nem sempre é possível;
- É necessária a utilização de programas informáticos forenses para triagem, recolha e certificação dos dados;
- É necessário ter no local um suporte de armazenamento com dimensão suficiente para gravar todos os dados;
- É obrigatório preparar a busca previamente com a elaboração de palavras ou termos que facilitem a pesquisa e o uso do programa de triagem;
- Perde-se a possibilidade de pesquisar em ficheiros escondidos ou arquivados noutros locais ou em locais não autorizados (eg.: privilégios de utilizador em vez de privilégios de administrador), em partições não acessíveis, em ficheiros encriptados e em zonas dos discos não alocadas ou no *slack space* (espaço de alocação distribuído por vários sectores do disco, deixado "livre" por gravação ou eliminação de ficheiros);
- Deixa de ser possível estabelecer um histórico da atividade do sistema;
- Deixa de ser possível registar a existência ou não existência de antivírus/*firewall/Malware* no sistema e que poderá levantar a dúvida em sede de julgamento, sobre a consciência do titular do sistema da autoria dos factos em investigação.

De referir que na cópia por imagem e na cópia seletiva de dados os dispositivos de suporte da gravação dos dados devem estar previamente "limpos" de todos os dados (*wiped devices*), designadamente de dados de investigações anteriores, uma vez que, se assim se não proceder, não vai ser possível efetuar uma cópia/imagem certificada, por os

dados existentes no suporte de destino serem diferentes dos dados existentes no suporte original. Quando se apreende algum dispositivo com informação digital é necessário tratar este tipo de prova de modo semelhante às apreensões de outros objetos relacionados com outro tipo de criminalidade. Por exemplo, numa cena de crime relativo à prática de um crime de homicídio os investigadores não apreendem a arma do crime sem ter especiais cuidados: velam para que a arma não fique com impressões digitais de outras pessoas que não os visados pela investigação, utilizando luvas para o efeito, evitam carregar no gatilho e procedem ao acondicionamento em embalagem própria, com indicação do número do processo, da descrição da arma, da data e do local da apreensão e do(s) responsável(eis) pela apreensão. Do mesmo modo, num cenário de busca para apreensão de prova digital, salvo raras exceções (eg.: buscas a empresas com grande quantidade de informação, em que é necessária uma pesquisa de dados para se proceder à sua apreensão), deve evitar-se ligar um computador que esteja desligado, por perigo de contaminação da prova e quebra da sua integridade. Por vezes, pode suceder que investigadores com excesso de zelo, num cenário de busca comecem a aceder aos dados existentes no computador, corrompendo deste modo a prova digital. Sucede que uma perícia informática forense revela que a informação digital foi acedida ou alterada em determinada data, documentando esse facto no relatório pericial. Por esse motivo, caso seja necessário aceder ao conteúdo de um computador num cenário de busca é necessário documentar esse facto, de modo a evitar que a prova seja colocada em causa pelo suspeito com invocação de que foram terceiros ou os próprios investigadores que colocaram no computador, por exemplo, imagens de abuso sexual de menores. Concretizando, é prejudicial para a validade da prova digital que um investigador, sem a formação e as ferramentas informáticas adequadas, ao nível de hardware e de software, examine provas originais, contidas por exemplo num disco rígido de um suspeito.[14]

No que concerne a recomendações ou boas práticas gerais a seguir num cenário de busca para apreensão de prova eletrónica e dispositivos digitais encontram-se as seguintes (Ferraro et al., 2005, p. 178-179).

- Verificando-se que o computador ou outro tipo de dispositivo digital não se encontram em funcionamento, assim devem permanecer (tratando-se de computadores portáteis com bateria deve-se proceder à sua remoção);

[14] Um dos cuidados a ter na análise de dados é fazer correr um programa anti-vírus antes de aceder aos ficheiros.

- De seguida é necessário desligar a corrente elétrica, desligando primeiro os cabos da unidade principal do computador (em vez da tomada) e registando a hora;
- Depois é necessário etiquetar os cabos e as respetivas portas de ligação correspondentes, pois isso facilita o trabalho dos peritos quando analisam várias dezenas de dispositivos num processo;
- No caso do computador se encontrar ligado é necessário documentar esse facto, fotografar o aspeto do monitor e contactar um perito, no sentido de garantir a preservação da prova. Desligar da corrente um computador ligado, vai afetar todos os programas que estejam a ser executados. Desaparece o conteúdo da memória *RAM* e são interrompidas as ligações à Internet, a (ou) impressoras, a (ou a) *drives* remotas e ou a *drives* encriptadas.
- No caso de existir uma rede de computadores é necessário contacar um perito, pois podem existir serviços associados que se desligarão quando o investigador decida interagir com os equipamentos.

A prova digital, tal como os outros tipos de provas, deve ser manipulada de modo a preservar o seu valor probatório. Isto não tem apenas a ver com a sua integridade física, mas sobretudo com os dados que os dispositivos contêm. Os dispositivos digitais são frágeis e sensíveis à temperatura, à humidade, a choques, à eletricidade estática e a campos eletromagnéticos. Sob pena de danificação dos dados, devem ser tomadas medidas especiais quando se acondicionam, transportam e armazenam, designadamente através de acondicionamento em embalagens apropriadas. De igual modo e para que se mantenha a custódia da prova, em reforço do acima referido, é necessário registar e documentar todos os procedimentos que foram levados a cabo no manuseamento da prova digital.

3.9. Análise Forense e Prova Pericial Digital

Após a apreensão de dispositivos com dados informáticos é necessário realizar uma perícia informática forense, no sentido de, mantendo a cadeia de custódia da prova, extrair elementos probatórios dos suportes digitais, que permitam sustentar uma acusação criminal, a cargo do Ministério Público ou, na ausência de indícios probatórios, o arquivamento do processo. Nos termos do disposto no Art. 151.º do CPP *"a prova pericial tem lugar quando a perceção ou a apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos"*.

A prova pericial distingue-se do exame, uma vez que o exame visa a deteção de vestígios, enquanto a perícia visa a avaliação especializada desses vestígios. Com efeito, o

exame não subentende a existência de especiais conhecimentos técnicos, ao contrário da perícia, que pressupõe necessariamente a existência desses conhecimentos.[15] A prova pericial distingue-se igualmente do parecer da autoria de um técnico, uma vez que só o perito nomeado pela autoridade judiciária pode produzir uma perícia no âmbito do processo penal. Na determinação para a realização da perícia a autoridade judiciária e o perito nomeado devem ter em especial consideração a reserva da intimidade da vida privada, em consonância com previsto no Art. 26.º da CRP e no Art. 8.º da CEDH - Convenção Europeia dos Direitos do Homem[16], expurgando do relatório pericial e, se possível do processo, a informação privada desnecessária à investigação, aplicando-se nesta sede os termos do disposto no Art. 16.º, n.º 3 da LCiber.

Constitui boa prática na realização de perícias a preparação de um ambiente descontaminado e organizado de trabalho. Realizar, por exemplo, uma perícia informática recorrendo a suportes *"limpos"* de dados de investigações anteriores (*wiped devices*), à semelhança do que sucede em algumas modalidades de apreensão de prova digital, é fundamental para a manutenção da cadeia de custódia da prova, na medida em que se evita a corrupção da prova com dados não relacionados com a investigação. Acresce que a classificação individualizada dos suportes digitais no processo, com a atribuição de nomes exclusivos para os suportes de informação objeto de análise, constitui boa prática de controlo sobre o local onde os artefactos específicos estão localizados, evitando erros, como por exemplo, gravar ficheiros recuperados para um disco ótico não correspondente, em termos de identificação e registo. Deste modo, a cada suporte deve corresponder uma classificação específica, ligada a uma autorização de busca para apreensão, a um auto de apreensão, a um despacho de validação de apreensão por parte da autoridade judiciária competente, o Juiz de Instrução Criminal ou o Magistrado do Ministério Público, a um despacho de nomeação de perito com formulação de quesitos que delimitam o objeto da perícia e a um relatório pericial.

Quando se inicia o processamento da informação constante dos dispositivos digitais de armazenamento, é aconselhável compará-los com a documentação original da cena do crime, no sentido de verificar se os números de série de unidades, valores de MD5 e se quaisquer outras características de identificação se mantêm – esta operação inicial,

[15] A deteção de vestígios que exija especiais conhecimentos técnicos é ainda um exame, indicando-se, a título de exemplo, a pesquisa de substâncias químicas venenosas num cadáver, a identificação de um tipo de arma de fogo ou a recolha de impressões digitais.
[16] Deste modo, caso sejam encontrada correspondência íntima do visado pela investigação, esta informação deve ser retirada do processo, mediante despacho fundamentado do Juiz de Instrução Criminal.

devidamente documentada permite a rastreabilidade do manuseamento da prova. O Message - Digest Algorithm 5 (MD 5) gera uma mensagem com um código de identificação único e irrepetível, a que se denomina função "*hash*", sobre determinada prova digital, quer seja um ficheiro ou um conjunto de ficheiros (certificação digital de dados). Deste modo, calcular um valor "*hash*" sobre determinada informação digital apreendida, permite que um perito ou um examinador certifique que os elementos digitais subjacentes não foram alterados ao longo do tempo. Se a prova digital foi alterada de forma alguma, o algoritmo irá produzir um valor diferente do original, permitindo comparar a integridade dos dados em diferentes datas. O valor MD5 é, assim, o equivalente ao DNA digital, na medida em que é univocamente identificada uma determinada informação de carácter digital. Como tal, um valor MD5 pode também ser útil para pesquisar numa grande quantidade de dados, um determinado ficheiro em particular, indicando-se a título de exemplo uma imagem de pornografia infantil num *website*.

O objetivo da análise forense é estabelecer o que se passou (o quê?), quem o fez (quem?), quando ocorreu (o quando?), como aconteceu (como?). O procedimento específico dependerá do tipo de incidente ou caso que estivermos a investigar. Por exemplo, no caso de uma intrusão num sistema, a informação sobre ligações e a investigação sobre o processamento de dados e portas utilizadas, pode indiciar o tipo de acesso e *software* utilizado, confirmando-se depois mediante a análise do sistema de arquivos. Esta operação inclui a recuperação de ficheiros e estabelecimento da sequência temporal (o "quando").

Em qualquer caso, o estabelecer uma série de factos a partir da análise da prova, que confirme de forma total ou parcial a hipótese ou modelo, é o objetivo da investigação. No caso de abuso sexual de crianças no Ciberespaço, importa, entre outros, procurar obter os registos de acesso à Internet, as pesquisas realizadas na Internet, os *website*s acedidos, os ficheiros de vídeo e imagens guardadas no computador, os ficheiros enviados para outros destinatários, a identificação das vítimas, a existência de jogos ou de material de entretenimento de menores, os registos de pagamentos de acessos a sites contendo material de abuso sexual de menores e todos os dados que permitam confirmar ou infirmar a existência de indícios probatórios da prática de crime.

Na análise deste tipo de criminalidade é importante perspetivar que a Internet pode ser uma valiosa fonte de recolha de indícios probatórios, mesmo no caso de o visado não utilizar a Internet para trocar material de abuso sexual de menores ou comunicar com as vítimas. Um aspeto importante de qualquer exame de computação forense está em

identificar todos os locais remotos onde possam ser encontrados materiais de abuso sexual de menores. O suspeito pode, por exemplo, manter um *site* com material de abuso sexual de menores ou transferir dados que o incriminem para um servidor na Internet, localizado fisicamente noutro país. Efetivamente, neste tipo de casos, foram detetados colecionadores, produtores, comerciantes e consumidores de pornografia infantil que se introduziram ilegalmente em servidores de empresas ou de instituições públicas e os utilizaram para armazenar e comercializar materiais de abuso sexual de menores.

A etapa de análise forense envolve, assim, uma avaliação objetiva e crítica dos elementos probatórios disponíveis, com o objetivo de reconstruir o crime. De referir, a título de exemplo, que não é seguro assumir que imagens de abuso sexual de menores encontradas no sistema de um arguido, foram por ele produzidas, uma vez que pode ser um mero consumidor desse tipo de material.

Uma análise cuidadosa das características de classe geral e individual dos dados de uma determinada fotografia, pode levar os investigadores a obter outros elementos de prova, como a identificação da câmara digital que captou a imagem ou a identificação das vítimas ou de outros suspeitos. Este tipo de análise é particularmente importante durante as investigações que envolvem material de abuso sexual de menores, porque é desejável e urgente localizar as vítimas e protegê-las contra novos abusos. Podem identificar-se características numa imagem, que podem auxiliar nas investigações, a saber:

Característica de classe: é uma marca distintiva geral partilhada entre objetos semelhantes, indicando-se a título de exemplo as câmaras digitais Kodak, que incorporam os nomes marca e modelo nas fotografias que captam;

Característica individual: é uma marca distintiva única, específica e particular, correspondente a um determinado lugar, pessoa, objeto ou ação. Por exemplo, um arranhão na lente de uma câmara digital que aparece em fotografias, um monumento que aparece no fundo de uma fotografia, uma cicatriz ou tatuagem que aparece no corpo de um arguido ou de uma vítima, constituem-se como características individuais que podem ajudar os investigadores a associar a fotografia com a sua fonte, ou seja, câmara, local, objeto ou pessoa.

No que concerne à análise de imagens e de vídeos que constituem material de abuso sexual de menores é, assim, de analisar com prudência as propriedades data e hora, uma vez que este tipo de dados pode ter sido alterado ou ser impreciso. É de ter em conta as diferenças de fusos horários e os horários de verão e de inverno, uma vez que podem causar erros de interpretação da data e hora associada a uma determinada imagem. É

possível configurar, por exemplo, no âmbito de um caso de posse de material de abuso sexual de crianças, que um perito ou um consultor técnico nomeado para examinar o computador apreendido, possa concluir que este tinha sido usado para aceder à Internet, durante as primeiras horas após ter sido apreendido pela polícia, designadamente para aceder a um *website* de pornografia infantil ou ao correio eletrónico pessoal fornecido pelo ISP (eg: Sapo, Clix, Netcabo, etc.). A comprovar-se esta situação poder-se-ia verificar o comprometimento da integridade da prova digital apreendida e a quebra da cadeia da custódia da prova, com as inerentes consequências legais, que poderiam determinar a invalidade da prova. No caso de a polícia não ter utilizado o computador após a apreensão, esta conclusão pode derivar da circunstância de se não ter em conta a diferença de fusos horários na análise efetuada, raciocínio que se deve efetuar, por paralelismo de situações, quando se efetua qualquer tipo de perícia informática forense no sentido de determinar quando ocorreram os factos sob investigação.

Da multiplicidade de situações e procedimentos analisados importa sublinhar que a recolha, preservação e análise dos elementos de prova conexos com ocorrências de natureza criminal no *locus* em consideração exigem aos intervenientes na IC o domínio de tecnologias de desenvolvimento recente quando se considera o legado de aprendizagem da IC em termos latos. Esse legado sustenta padrões de atuação experimentados e validados por gerações mas que quando transpostos para este locus carece ainda de tempo e exercitação para se constituírem como doutrina, O caminho que se percorre é o de aprender fazendo.

As TIC quando indevidamente utilizadas podem mesmo determinar a destruição de elementos essenciais de prova ou produzir novas versões desses elementos que sustentarão ações de impugnação do processo por parte da defesa colocando em risco o sucesso da investigação e da acusação. Acresce que o esforço dos agentes de IC para responder aos desafios que a investigação de crimes ocorridos no ciberespaço lhes coloca é significativamente incrementado pelas dificuldades observadas na obtenção da cooperação internacional (o que não é especifico deste tipo de crimes mas que também aqui se verifica).

Capítulo 4

Cooperação Transnacional entre o Setor Público e o Setor Privado

4.1. Enquadramento

A Relatora Especial da ONU sobre a venda de crianças, prostituição infantil e pornografia infantil, Najat M´jid Maalla refere que a pornografia infantil na Internet constitui um problema mundial alavancado pelo desenvolvimento de tecnologias que aumentam em muito as formas de acesso, divulgação e venda deste material criminoso. Daqui decorre que a cooperação judiciária internacional concertada se constitui como premissa inevitável numa estratégia de repressão eficaz do fenómeno. Com efeito, as novas tecnologias aumentam consideravelmente as oportunidades disponíveis aos predadores, permitem-lhes recrutar, aliciar e explorar crianças em qualquer lugar do mundo. A Organização das Nações Unidas para a Infância (UNICEF) estima que existam mais de 4.000.000 de sites com vítimas menores jovens, incluindo mesmo crianças menores de 2 anos (!). Os predadores podem perseguir novas vítimas anonimamente em salas de chat e blogs (ONU, 2009, p. 6).

Em Julho de 2011, a *National Society for the Prevention of Cruelty to Children* (NSPCC), uma das principais instituições de proteção de crianças do Reino Unido, realizou um estudo no qual avaliava relatos de casos judiciais em Inglaterra e País de Gales, entre os meses de Abril e Setembro de 2010. A NSPCC descobriu que cerca de 3.000.000 de imagens foram distribuídos por 284 suspeitos objeto de condenação. De acordo com os padrões da NSPCC, cerca de 35.000 imagens pertenciam aos níveis mais elevados em termos de conteúdo abusivo (NPCSS, Press releases, 2011-07-27).

A cooperação e os esforços das autoridades judiciárias e de investigação criminal de vários países, permitiu identificar e desmantelar redes internacionais de predadores sexuais de crianças. Para além de outros casos já referidos, é de mencionar, a título de exemplo, a

"Operação Carrossel" ocorrida em 2007, no âmbito da qual se procedeu à detenção de 700 suspeitos dispersos por 35 países; à apreensão de 76.000 imagens de crianças e à identificação de 31 vítimas (ONU, 2009, p. 21).

A colaboração regular de vários países com o Grupo Oito (G-8), a Comissão para a Prevenção do Crime e da Justiça Penal da ONU, o Conselho da Europa, a Interpol e a Europol para ações no âmbito do combate aos crimes em questão constitui o reconhecimento de que a cooperação internacional é essencial para lidar com este fenómeno.

Como exemplo, na adoção de medidas contra o abuso sexual de crianças no Ciberespaço, os países do Grupo (G-8), adotaram em 2003 a sua estratégia de combate a este tipo de crimes. A estratégia adotada formaliza o compromisso de recolha e troca de informação, o desenvolvimento da cooperação com o setor privado e Organizações não-governamentais (ONGs), e a expansão dos seus esforços para países não-membros do G-8. Em 2007 estes Estados reconheceram que a pornografia infantil prejudica gravemente todas as crianças e todos os menores porque os retrata como uma classe de objetos para fins de exploração sexual (G-8, 2007).

A metodologia de identificação da vítima surgiu nos últimos anos propulsionada pela necessidade de atuar sobre o material de abuso de menores encontrado no Ciberespaço e apreendido pela polícia. No material de abuso sexual de menores é mais provável que estejam retratadas as vítimas de abuso e não os agressores o que determina o enfoque centrado na vítima por parte dos analistas de imagem.

No âmbito da cooperação policial internacional e da partilha de informação, a *"Interpol"* mantém uma base de dados com imagens de abuso sexual de menores, que ajuda a polícia a identificar e resgatar vítimas de exploração sexual no Ciberespaço. A identificação das vítimas de exploração sexual de crianças no Ciberespaço exige a análise de fotografias e filmes, com o objetivo de localizar a criança e ou o abusador visualizados. De acordo com a metodologia preconizada pela "Interpol", a identificação das vítimas de exploração sexual no Ciberespaço apenas tem sucesso se aliar a análise de imagem a métodos de investigação tradicionais. A análise de imagem consiste no exame do conteúdo digital, áudio e visual, das fotografias e filmes para fins de identificação. Os indícios para a identificação podem chegar ao conhecimento da investigação através de uma multiplicidade de fontes, designadamente através de informação policial, da comunicação social, dos suspeitos ou dos familiares das vítimas (Website Interpol – Victim Identification, 2012). Os resultados desta análise do mundo virtual são cruciais para a

investigação que pode ocorrer no mundo físico. Devido à natureza global da Internet e ao seu conteúdo específico, os especialistas em identificação de vítimas da "Interpol" trabalham em estreita colaboração com os seus homólogos de todo o mundo para garantir que os indícios que são típicos e únicos, ou facilmente reconhecíveis num país, não são negligenciados noutro.

Atenta a multiplicidade de Órgãos de Polícia Criminal (OPCs) que podem lidar com este tipo de casos a nível nacional, e atentas as necessidades de racionalizar e especializar recursos, simplificar e potenciar a eficácia da cooperação internacional existe um benefício acrescido no sucesso da identificação e localização das vítimas, se a atribuição de competências a nível nacional, for centralizada e aí fiquem sediadas todas as imagens apreendidas. A entidade que venha a deter competências neste domínio é quem deverá promover a análise e partilha de informação.

4.2. O problema da exploração sexual de crianças no Ciberespaço

O comércio de material com imagens de abuso sexual de menores constitui um problema global que continua a crescer a uma velocidade alarmante. A utilização de computadores e de tecnologia de diversa natureza para cometer crimes relacionados com a difusão de material de abuso sexual de menores sofreu um incremento significativo, seja através de correio eletrónico, *website*s comerciais, salas de conversação *on-line*, aplicações P2P, webcams, ou outros mecanismos tecnológicos. Uma vez que a Internet não conhece fronteiras, uma imagem produzida num país pode ser enviada para todo o mundo em segundos. No Ciberespaço não existem controlos nas fronteiras, pelo que as imagens circulam livremente dos fornecedores de material de abuso sexual de menores para os consumidores, sem ser necessário um encontro pessoal ou uma entrega física, por contraposição, por exemplo, ao tráfico de estupefacientes ou ao contrabando de tabaco.

Existem redes internacionais de produtores, comerciantes e colecionadores de imagens de crianças com conteúdo sexual. Acresce que aqueles que vendem essas imagens, estão muitas vezes ligados ao crime organizado (traficantes de produto estupefaciente, traficantes de armas, traficantes de pessoas, etc.) e ao branqueamento de capitais – este tipo de organizações criminosas tem assim, com facilidade, acesso a um mercado mundial, a partir de um simples terminal de acesso à Internet.

Em consequência, uma vez que os produtores, comerciantes e os colecionadores de material de abuso sexual de menores podem encontrar-se em qualquer país, todos os países devem desenvolver esforços conjuntos para reprimir com eficácia este tipo de

criminalidade – de notar que se, por exemplo, essas imagens não forem objeto de perseguição penal em qualquer lugar do mundo físico, esse tipo de material estará mais disponível e acessível em todos os lugares no Ciberespaço.

Deste modo, a coordenação entre as autoridades dos diversos países, a partilha de recursos humanos e técnicos e de informação sobre o fenómeno, e um compromisso coletivo a nível internacional, são indispensáveis para possibilitar investigações de sucesso e a repressão eficaz da exploração sexual de crianças.

4.3. A cooperação e a competência penal internacional

A comunidade internacional tem reafirmado repetidamente o compromisso de proteger as crianças contra a exploração e o abuso sexual. A Lciber, no âmbito da cooperação internacional, refere que deverá ser observado o regime geral da cooperação penal em vigor e que se encontra plasmado na Lei n.º 144/99, de 31 de agosto (Art. 28.º).[17] A LCiber prevê alguns institutos inovadores que pretendem adequar a cooperação internacional aos desafios que a cibercriminalidade encerra. Deste modo, no Art. 22.º prevê-se a preservação e revelação expedita de dados em cooperação internacional, o Art. 24.º prevê o acesso aos dados em processo de cooperação internacional e o Art. 26.º a possibilidade de interceção de dados a pedido de Autoridades de IC estrangeiras. Com relevância em termos operacionais estabeleceu-se no Art. 21.º a existência de um ponto permanente de contacto, a funcionar 24 horas por dia, 7 dias por semana, na Polícia Judiciária. Quanto à competência territorial, tendo em conta que este tipo de criminalidade não se rege pelo princípio da territorialidade e do lugar da prática dos factos, a LCiber veio prever a competência de Portugal para factos praticados por Portugueses, se a estes não for aplicável a lei de nenhum outro Estado; a factos cometidos em benefício de pessoas coletivas com sede em território português e ainda a qualquer tipo de factos praticados em Portugal, se visarem sistemas informáticos localizados no estrangeiro – Art. 27.º, n.º 1 da LCiber. A LCiber prescreve ainda que os dispositivos normativos nela previstos são aplicáveis a qualquer tipo de factos, independentemente do local onde tenham ocorrido – mesmo no estrangeiro – desde que visem sistemas informáticos localizados em território português (Verdelho, 2009, p. 748). Contudo a LCiber apenas se aplica, no plano da extensão da competência dos Tribunais Portugueses aos crimes previstos e punidos nos termos do referido texto normativo (criminalidade contra sistemas de informação), estando

[17] LEI da Cooperação Judiciária Internacional em Matéria Penal, Lei n.º 144/99, de 31 de Agosto.

por esse motivo a extensão da referida competência fora do alcance dos factos que consubstanciam a exploração sexual de crianças no Ciberespaço.

Efetivamente, no que concerne à aplicação da lei penal portuguesa vigor a regra geral, o princípio da territorialidade, ou seja a lei penal portuguesa apenas é aplicável a factos cometidos em território português ou a bordo de navios ou aeronaves portuguesas. Como exceção a esta regra, prevê-se no Art. 5.º, n.º 1, alínea b) do CP a punição de factos que consubstanciam a exploração sexual de crianças praticados fora do território português desde que o agente seja encontrado em Portugal e não possa ser extraditado ou entregue em resultado de mandado de detenção europeu ou de outro instrumento de cooperação que vincule o Estado Português. Atentas as caraterísticas próprias do Ciberespaço e as características do fenómeno já elencadas, designadamente a dispersão de agentes, recursos e a atuação sob anonimato, a inexistência de fronteiras e a possibilidade de existirem locais no globo em que tais tipos de condutas não são punidas, deveria ser ponderada previsão do CP que conferisse a extensão da competência da lei penal portuguesa a todos os factos relacionados com a exploração sexual de crianças, à semelhança do previsto para a Lciber. Efetivamente, se assim não for, podem-se configurar situações, ocorridas no Ciberespaço que, por ausência de indícios quanto ao lugar da prática dos factos, poderão escapar à punição dos que se dedicam a tais práticas. Preconiza-se, assim, que este tipo de ilícitos passe a integrar o Art. 5.º, n.º 1, alínea a) do CP, prevendo-se a aplicação da lei penal, desde que, para factos ocorridos no estrangeiro estejam em causa menores de nacionalidade portuguesa e para factos ocorridos no teritório nacional sem distinção da nacionalidade do menor.

4.4. Medidas complementares aos sistemas de justiça penal

Apesar do julgamento e condenação penal dos que produzem, distribuem, ou possuem imagens ou material de abuso sexual de crianças ser fundamental para proteger as crianças contra maiores riscos, existem ainda outras medidas que um determinado Estado pode implementar, complementando o seu sistema penal, para combater este problema crescente. Embora seja necessário desenvolver formação especializada direcionada aos profissionais da justiça criminal, incluindo magistrados judiciais e do Ministério Público, advogados, polícias de investigação, oficiais de justiça, peritos informáticos forenses no que concerne à aplicação da lei, à dimensão do fenómeno em concreto, e às técnicas de investigação relacionadas com a aquisição e valoração da prova digital, como parte

necessária de um programa nacional concebido para combater estes crimes, é igualmente necessário estabelecer parcerias tendentes à repressão deste fenómeno.

A sociedade e, em particular, os profissionais do judiciário, devem percecionar que o abuso sexual de crianças, a pornografia infantil e imagens de sexo explícito de crianças são uma e a mesma coisa, e que esses delitos devem ser clara e fortemente denunciados e reprimidos pelo sistema de justiça criminal. Da mesma forma, o aumento da consciencialização pública e implementação de programas de formação sobre a prevalência e a natureza da exploração sexual infantil através de posse, comercialização e consumo de material de abuso sexual de menores, facilita o reporte deste tipo de casos perante as autoridades e incrementa a prevenção geral quanto à prática deste tipo de ações por parte de possíveis infratores.

Com efeito, pese embora a dimensão global do comércio de material de abuso sexual de menores exija respostas globais e concertadas por parte dos governos, de agências e organizações internacionais, regionais e nacionais, o setor privado dever ter também um papel muito relevante a desempenhar no combate a este fenómeno criminal. O setor privado, designadamente as empresas prestadoras de serviços de Internet, os profissionais de tecnologia da informação, as instituições financeiras, a sociedade civil, incluindo organizações não-governamentais, os órgãos de comunicação social, pais e educadores, devem ser encorajados, através de ações de sensibilização, a refletir sobre o papel que poderiam desempenhar na luta contra este tipo crimes, criando-se, por exemplo, mecanismos ágeis e eficazes de reporte de tais tipos de conduta às Autoridades de IC. Deste modo, as entidades nacionais cuja atividade se relacione com o Ciberespaço, sejam organizações públicas ou privadas, devem contribuir para um acompanhamento e acção permanente e eficaz na luta contra as infrações relacionadas com o abuso sexual de crianças no Ciberespaço, em cooperação com fornecedores de serviços Internet e outras entidades privadas.[18]

A natureza cada vez mais interativa de conteúdo *on-line*, as redes sociais, a partilha instantânea de vídeos e imagens na Internet oferecem aos utilizadores novas oportunidades, mas também trazem novos riscos para crianças e jovens. Por exemplo, a convergência tecnológica dos telemóveis e da Internet também tem consequências significativas para a

[18] Nos EUA, por exemplo, foi criado o *"National Center for Missing & Exploited Children*", organização não lucrativa, que configura uma parceria entre o sector público e privado em questões relacionadas com a exploração sexual de crianças no Ciberespaço e o desaparecimento de crianças.

segurança *on-line* o acesso à internet móvel dá às crianças e jovens maior recato na comunicação, torna-os mais autoconfiantes e ao mesmo tempo mais vulneráveis.

A nível internacional, em termos de medidas concretas, é de destacar a iniciativa que levou à criação da "*Virtual Global Taskforce"* (VGT) [19], em 2003, que se constitui como um exemplo referência de cooperação internacional ne repressão da exploração sexual de crianças no Ciberespaço. Esta organização tem como objetivo identificar e localizar o paradeiro de crianças abusadas sexualmente, prestar assistência às crianças em risco, e identificar pessoas que se dedicam a aliciar crianças no Ciberespaço, com vista a sua identificação e monitorização e comparência perante as autoridades. Por outro lado, em resposta aos riscos existentes neste âmbito no Ciberespaço foram criadas pelos Estados, ONG´S e ISP, canais de denúncia e reporte de conteúdos ilegais na Internet, em que se inclui o material de abuso sexual de crianças, como por exemplo, o caso da *"INHOPE – International Association of Internet Hotlines"*, com parceiros em 37 países, designadamente em Portugal. Na Noruega e no Reino Unido, no sentido de aumentar a segurança das crianças, foram criados botões de abuso que podem ser acionados *on-line* por crianças, para relatar qualquer conteúdo ilegal ou assédio sexual. Através de uma parceria entre o "*CEOP- Child Exploitation and On-line Protection Centre*" e a empresa "*Microsoft"* foi também adicionado um botão de reporte de abuso na versão inglesa do "*Windows Live Messenger"*, que pode ser utilizado por crianças quando se encontram a conversar *on-line*, no caso de serem abordadas por terceiros com textos, conversas, imagens, vídeos ou músicas com conteúdos de natureza sexual. A Comissão Europeia desenvolveu o programa *Safer Internet Plus*, com o objetivo de tornar a Internet mais segura para as crianças, contribuindo para o desenvolvimento de filtros, disponibilização de informação e de ferramentas educacionais sobre os riscos associados à utilização da Internet pelas crianças. Como parte desse programa, é celebrado todos os anos um Dia da Internet Segura, cujo objetivo é aumentar a consciência pública sobre as questões de segurança no contexto da utilização de novas tecnologias.

De igual modo, a base de dados de imagens de material de abuso sexual infantil (ICSE DB) da "Interpol", já referida, constitui-se como uma poderosa ferramenta de investigação que permite que os investigadores especializados possam partilhar dados com investigadores de todo o mundo. Esta base de dados utiliza um software sofisticado de comparação da imagem, que permite efetuar conexões entre vítimas e lugares. Esta base

[19]Fazem parte da VGT a Austrália, o Canadá, a Europol, a Interpol, a Itália, a Nova Zelândia, os Emirados Árabes, o Reino Unido e os EUA.

permite ainda que os utilizadores autorizados dos diferentes países possam aceder de forma segura e em tempo real à base de dados, proporcionando respostas imediatas para consultas para identificação das vítimas, a nível nacional e internacional. Esta base de dados contém também informação sobre as vítimas já identificadas e resgatadas, o que evita que outros serviços de investigação desenvolvam diligências inúteis, direcionando os seus esforços para outras vítimas em prol da eficácia da IC deste tipo de casos. De notar, que a identificação de crianças vítimas de abuso sexual por meio de análise de imagem é essencial às investigações, uma vez que muitas vítimas deste tipo de crime raramente apresentam queixa à polícia.

A análise de imagem que conduz à identificação e resgate de centenas de crianças em todo o mundo é um processo altamente especializado e rigoroso que requer uma grande dose de experiência, tempo e tecnologia de última geração. Exige um grande investimento, que muitos países não podem pagar, pelo que a base de dados de imagens da "Interpol", enriquecida por contributos de investigações nacionais, é um instrumento importante e relevante para o sucesso das investigações, à escala global. Através do acesso a esta base de dados, e recorrendo a analistas de imagens, foi possível, até o final de 2011, identificar cerca de 2.500 vítimas de mais de 40 países e 1.377 criminosos.

De referir ainda, que alguns países têm as suas bases de dados de imagens de crianças, que partilham com a "Interpol" e com outros países, indicando-se a título de exemplo os EUA, o Reino Unido, a Itália, a Austrália, entre outros, que procuram fazer um trabalho semelhante ao da "Interpol", mas a nível nacional.

De acordo com a ONU (2009, p. 22) constata-se que apesar dos enormes esforços efetuados em muitos países, até à data nenhum estudo tem sido capaz de medir o impacto do abuso sexual de crianças no Ciberespaço. Além disso, esses esforços têm ocorrido principalmente nos denominados países do hemisfério Norte, pelo que seria desejável expandir e desenvolver essas capacidades a todos os países do globo e, assim, torná-los disponíveis para todas as crianças, numa visão agregada e, se possível, globalizada.

4.5. A cooperação entre organizações e o combate à exploração sexual de crianças no Ciberespaço

O compromisso e os esforços de muitos atores da comunidade internacional, autoridades públicas, ONG´S, do sector privado, designadamente os ISP e do sector de telecomunicações e das empresas emissoras de cartão de crédito, entre outros, conduziram à aplicação de muitas medidas efetivas, tendentes à eliminação da exploração sexual de crianças no Ciberespaço, designadamente: reformas legislativas, desmantelamento de redes

de comercialização de material de abusos sexual de menores, relatórios direcionados aos utilizadores da Internet, limitações no acesso e bloqueio de sites da Internet, apreensões de material de abuso sexual de menores, prisões de predadores sexuais, campanhas de sensibilização, desenvolvimento de software de controlo parental, entre outras iniciativas.

No entanto, apesar destas iniciativas, múltiplas e variadas, a distribuição de material de abuso sexual de menores na Internet, persiste um negócio muito lucrativo, com um valor de mercado estimado em milhares de milhões de dólares americanos. O fácil acesso às novas tecnologias, as constantes alterações nos métodos de produção e padrões de consumo, a que acresce a dimensão internacional da distribuição de material de abuso sexual de crianças, dificultam a luta contra este flagelo.

O número de *website*s dedicados à pornografia infantil está a em crescimento constante em todo o mundo. Entre 2001 e 2004 o número de sites cresceu quase 50%. Em 2004 foram identificados 480.000 *sites* relacionados com este fenómeno. O número de predadores de crianças, ligados à Internet em qualquer momento, é estimado em 750.000. Em 2009, o Centro Nacional de Crianças Exploradas e Desaparecidas (NCMEC), dos Estados Unidos, de um total de 681.275 analisados, detectou 592.044 *website*s com material de abuso sexual de menores. Em 2007 a IWF no Reino Unido recebeu 3.487 relatórios de lugares no Ciberespaço com material de abuso infantil, incluindo 2.755 domínios que contêm imagens de abuso sexual de crianças (80% para fins comerciais e 20% para fins não-comerciais); em 2008, a mesma instituição recebeu 33.947 relatórios, em que se incluem 1.536 domínios que descrevem o abuso sexual de crianças (74% para fins comerciais e 26% para fins não - comerciais, armazenamento ou troca). Constata-se que milhares de novas fotografias e vídeos são carregados para a Internet e todos os dias são realizadas centenas de milhares de pesquisas na Web para imagens de exploração sexual de crianças. É possível que existem pessoas que tenham, em seu poder coleções de mais de um milhão de imagens de crianças vítimas de exploração sexual. Contudo, uma vez que a pornografia infantil é ilegal e objeto de perseguição penal na maioria dos países, é difícil calcular o número de menores que em todo o mundo são vítimas dessas redes, embora as estimativas indiquem entre 10.000 a 100.000 crianças de todas as idades.

O material de abuso sexual de menores ou é produzido off-line para posterior circulação na Internet ou é produzido em tempo real, para espectadores on-line. A produção e distribuição de material de abuso sexual de menores tem um valor estimado pela ONU entre US $ 3.000.000.000 e US $ 20.000.000.000 de dólares americanos (2009, p. 10). Acresce que as imagens disponíveis *on-line* de crianças exploradas sexualmente, além de

crescerem em número, são cada vez mais violentas, pelo que as medidas de combate a este fenómeno, de caráter legal e operacional, se afiguram urgentes tendo em conta o número de vítimas em causa e o efeito que este tipo de práticas provoca nas crianças.

Em síntese a cooperação entre organizações potenciou bons resultados mas a persistência e o crescimento do fenómeno justificam a intensificação de tal cooperação e o rasgar de novos caminhos pelo carácter nefasto de que se reveste a exploração sexual de uma só criança que seja. O fenómeno e o *locus* em questão exigem dos ISP um papel sem alternante.

4.6. Responsabilidade dos ISP

Uma vez que este fenómeno criminal está associado ao Ciberespaço e à Internet, aos ISP deve ser atribuído o papel principal na monitorização e reporte dos conteúdos relacionados com a exploração sexual de crianças.

Nos Estados Unidos e na Austrália, por exemplo, estão previstas sanções para os prestadores de serviços de Internet e proprietários de domínio que não reportarem sites com conteúdos de abuso sexual de menores às autoridades de investigação, num prazo razoável. Na África do Sul um ISP deve tomar todas as medidas necessárias para prevenir a utilização do seus serviços para hospedar ou distribuir material relacionado com a exploração sexual de crianças – o ISP deve notificar essa atividade às autoridades de investigação, bem como os dados da comunicação associada - nome e IP – para além ser obrigado a manter também um registo dessa informação para utilização como prova em processos criminais. Os ISP sedeados na África do Sul estão também obrigados por lei a tomar medidas para bloquear a divulgação deste tipo de imagens. Na Finlândia e na Suécia a polícia pode bloquear sites de pornografia infantil, com o objetivo de impedir a circulação de imagens de exploração sexual de crianças.

Em Portugal não está estabelecida a obrigatoriedade de os ISP monitorizarem conteúdos para detetar os que são afins da exploração sexual de crianças e, por isso, não está legalmente prevista nenhuma sanção caso os ISP não reportem a existência de conteúdos relativos a material de abuso sexual de menores na Internet. Admite-se que a situação descrita resulte de ser considerado que o acesso a esses conteúdos poderia contender com o direito à proteção da privacidade, pese embora, num juízo de ponderação de valores, o valor do direito à privacidade deva ceder perante o valor da proteção das crianças. Efetivamente, tendo em conta as características deste fenómeno, as obrigações do Estado Português perante convenções internacionais em vigor no ordenamento jurídico português,

a dimensão do fenómeno e as consequências deste tipo de práticas para as vítimas, torna-se premente estabelecer a obrigatoriedade do reporte de tais tipos de conteúdos às Autoridades de IC, designadamente ao Ministério Público.

4.7. As crianças e a sua exploração sexual no Ciberespaço

Os efeitos distribuição do material de abuso na Internet são suscetíveis de agravar as consequências do abuso infantil, afetando a recuperação integral das vítimas - as imagens das crianças exploradas sexualmente e divulgadas na Internet, podem de fato nunca desaparecer e essa circunstância tem um efeito devastador sobre as vítimas. Acresce, que muitas vezes as vítimas não querem falar do que passaram ou do que se passou; culpam-se a si mesmas; e, ao saber que outras pessoas podem visualizar as imagens do abuso que sofreram através de um simples "clique", sofrem com maior intensidade e ficam ainda mais abaladas e traumatizadas, necessitando de mais tempo e esforço para recuperar da violência a que foram sujeitas. Além disso, muitos abusadores forçam as vítimas a fingir que estão a gostar da experiência aquando da produção das imagens, razão pela qual a vítima pode temer que a polícia acredite no abusador ao dizer que a vítima é *"que o seduziu"* - neste aspeto, as autoridades de investigação têm de ter sempre presente que as crianças vítimas são sempre forçadas a cometer tais tipos de atos, seja através de violência física ou psicológica. Investigadores da *"ECPAT – Internacional"* referem que *"os profissionais relatam que uma criança nesta situação pode sentir que a existência de imagens a fingir o seu agrado perante a situação, em virtude da humilhação e da violência que experimentaram, pode fazer que estas sintam que parecem cúmplices dos predadores"*. A este dilema adiciona-se um fator traumático adicional que consiste no seguinte: *"para algumas vítimas de abuso, este comportamento torna-se algo tão normal que o seu comportamento pode parecer enganoso"*.

Em suma, a constante circulação de imagens de crianças exploradas sexualmente aumenta exponencialmente o tempo de recuperação das vítimas. Apesar de, num caso concreto, o abuso pode ter acontecido há muito tempo, as vítimas continuam a ser violentadas porque as imagens estão ainda em circulação e são utilizadas para fins de gratificação sexual. Esse fato é agravado pelo medo de que algo de tão pessoal que sucedeu no passado, possa reaparecer em qualquer lugar, a qualquer momento e ser visto por qualquer pessoa. Esta circunstância constitui uma violação sem fim do direito à privacidade, que provoca uma humilhação adicional nas vítimas, que crescem sabendo que aquelas fotografias ou vídeos estarão na Internet para o resto das suas vidas.

Por outro lado, a exposição de crianças à pornografia infantil inspira e influencia as práticas sexuais dos mais jovens, influenciando o seu comportamento sexual, uma vez que o material de abuso passa a constituir a sua principal fonte de informação sobre comportamentos sexuais e serve de exemplo para a sexualidade real. Ou seja, a distribuição deste tipo de material facilita a replicação de comportamentos associados como *"normais*", na medida em que se insensibiliza as crianças quanto a este tipo de práticas - existem redes de troca de material de abuso, que divulgam imagens em que as crianças foram forçadas a sorrir, no sentido de comprovar que aquelas práticas constituem um "*divertimento*" e não uma violência em relação às vítimas.

Para evitar a difusão indevida de material referente à exploração sexual de crianças os tribunais dos Estados Unidos, em processos-crime que contenham material de abuso sexual de crianças, estão obrigados a negar todos os pedidos da defesa para cópia, fotocópia ou reprodução do material apreendido. Em Portugal, o acesso ao material de abuso sexual de crianças constante de processos-crime, é limitado mas carece de despacho fundamentado, numa interpretação conforme à Constituição, tendo em conta a reserva da intimidade da vida privada e o superior interesse da criança.

Perante a constatação da dificuldade em combater este fenómeno, um número crescente de ISP, operadores de telecomunicações móveis e instituições financeiras internacionais têm adotado códigos de conduta numa tentativa de autorregulação associada à repressão da distribuição de material de abuso sexual de menores - estas empresas comprometeram-se a desencadear medidas para combater a distribuição deste tipo de material, implementado diversas medidas, como a instalação de filtros em determinados *sites* que bloqueiam esse tipo de conteúdos, proceder à classificação dos *sites* de acordo com seu conteúdo e fornecer informação às Autoridades de IC sobre *sites* com conteúdo ilegal.

A título de exemplo, refere-se que as operadoras de telecomunicações e instituições financeiras do Reino Unido são membros da IWF que trabalha em cooperação com a indústria de Internet no Reino Unido; com as Autoridades de IC e com vários ministérios para automatizar e inovar na deteção e reporte de conteúdos de exploração sexual de crianças[20]. Este modelo de autorregulação e articulação com as Autoridades de IC poderia servir de exemplo inspirador em Portugal, sobretudo quanto aos aspetos operacionais para o reporte deste tipo de conteúdos – veja-se, como exemplo, o Código de Boas Práticas para os casos de deteção de material de abuso de menores nos locais de trabalho da IWF.

[20] São membro da IWF empresas como a "Vodafone", a "Google", a "Netclean", a "The Uk Cards Association" , a "Image Analyser", entre outras empresas.

Ao nível da articulação com as Autoridades de IC, constitui exemplo de referência, a criação em 2009 da "Aliança Financeira Europeia" para combater a distribuição de material de abuso sexual de menores no Ciberespaço. Esta organização é liderada pelo "CEOP – Child Exploitation and *On-line* Protection Centre" - organização pública do Reino Unido que se ocupa da proteção das crianças contra a exploração sexual – é financiada pela Comissão Europeia, e constitui um grupo informal que reúne intervenientes dos sectores público e privado, incluindo autoridades policiais, operadores financeiros, fornecedores de serviços de Internet, ONG e outros parceiros, que pretendem trabalhar em conjunto na repressão deste fenómeno.[21] Neste caso, as empresas gestoras de cartões de pagamentos, a crédito ou a débito, comprometem-se a bloquear pagamentos sobre aquisições de material de abuso de menores no Ciberespaço, efetuados através dos cartões que tenham emitido, integrando este compromisso na vertente da responsabilidade social das organizações.[22]

Todos estes exemplos estão alinhados, na prática, com a norma ISO 26000 sobre a responsabilidade social das organizações, em prol de um desenvolvimento sustentável da sociedade. A ISO 26000 é um padrão de orientação de atuação, aplicável a todos os tipos organizações, o que significa que não é suscetível de certificação. A responsabilidade social é definida como a assunção da responsabilidade por parte das organizações pelos impactos das suas decisões na sociedade e no meio ambiente, preconizando que as organizações, no âmbito da sua atuação interna e externa, devem orientar a sua atividade tendo sempre em consideração o respeito pelos direitos humanos. No ponto 6.3. da ISO 26000 considera-se que as organizações têm a responsabilidade de respeitar todos os direitos humanos, independentemente de o Estado ser capaz ou não desejar cumprir com seu dever de protegê-los. Essa responsabilidade envolve tomar medidas positivas para evitar a aceitação passiva ou a participação ativa na violação de direitos. Cumprir com a responsabilidade de respeito dos direitos humanos requer diligência e pro-atividade por parte das organizações, que deverão promover a adoção de medidas adicionais, no sentido de assegurar que respeitam os direitos humanos em todas as suas operações.

No âmbito da referida norma da qualidade preconiza-se, em especial, que as organizações e as empresas tenham em conta a proteção conferida às crianças pelos instrumentos da ONU, adotando códigos de conduta e boas práticas de negócio tendentes à

[21] As empresas "MasterCard", "Microsoft", "PayPal" e a "VISA Europa" integram Agência Financeira Europeia. Quanto à vertente de investigação criminal da Agência Financeira Europeia, integram este grupo informal, entre outros, a "Europol" e a "Polícia Nacional dos Correios e Comunicações de Itália".
[22] Comunicado à Imprensa da Comissão Europeia sobre Agência Financeira Europeia, 3 Março de 2009.

proteção das crianças contra a exploração sexual. Esta abordagem deve ser considerada nas organizações nacionais, sobretudo aquelas cuja atividade está relacionada com o Ciberespaço (eg.: ISP, empresas de comunicações, instituições financeiras, fornecedores de serviços de internet sem fio, organização privadas e públicas), independentemente das suas obrigações legais atuais e futuras (Ecpat Sweden Briefing Paper, 2011).

Apesar de terem sido desenvolvidos esforços conjuntos entre o setor Público e o setor privado no combate a este fenómeno, alcançando-se sucesso em investigações com conexões com vários países, é premente aprofundar-se a cooperação judiciária internacional, através da especialização dos operadores judiciários responsáveis por este tipo de casos e empenhar o setor privado, designadamente as empresas prestadoras de serviços no Ciberespaço e com as instituições financeiras, na deteção de conteúdos de exploração sexual de crianças e no bloqueio de pagamentos relacionados com a comercialização de material de abuso sexual de menores, em consonância com obrigações internacionais assumidas pelo Estado Português.

A nível nacional este desiderato será alcançado com maior eficácia se for centralizada a análise do material relativo à exploração sexual de crianças apreendido em investigações criminais desenvolvidas por Portugal, que assegure a difusão do conhecimento, de boas práticas e recomendações deste tipo de casos.

Capítulo 5

Conclusões

A exploração sexual de crianças no Ciberespaço constitui hodiernamente um problema mundial. A sua expressão assume formas diversas. Dentre essas, o comércio de material com imagens de abuso sexual de menores continua a crescer a uma velocidade alarmante. A utilização de computadores e de tecnologia de diversa natureza (correio eletrónico, sites comerciais, salas de conversação online, aplicações peer-to-peer, *webcams)* para cometer crimes relacionados com a exploração sexual de crianças está em crescendo, não tem fronteiras e ocorre em tempo tendencialmente instantâneo. Como fator potenciador do fenómeno assinala-se o recato potenciado pelo uso da Internet e o informalismo da comunicação. Os mais jovens, movidos pela curiosidade, são especialmente vulneráveis e incautos (por inexperiência de vida), suscetíveis de serem facilmente atraídos para uma situação de exploração sexual, sem consciência do significado e consequências dos seus comportamentos. Efetivamente, perante menores pouco informados dos perigos existentes no Ciberespaço contrapõem-se redes internacionais de produtores, comerciantes e colecionadores de imagens de crianças com conteúdo sexual, muitas vezes ligados ao crime organizado (traficantes de produto estupefaciente, traficantes de armas, traficantes de pessoas, etc.) e ao branqueamento de capitais – este tipo de organizações criminosas, a partir de um simples terminal de acesso à Interne, têm facilidade de acesso a um universo mundial de consumidores.

No Ciberespaço não existem fronteiras e pretender conter a comunicação a um espaço nacional é objetivo "fracassado", pelo que as imagens circulam livremente dos fornecedores de material para os consumidores, sem ser necessário um encontro pessoal ou uma entrega física, por contraposição, em certa medida, ao tráfico de droga ou ao contrabando de tabaco.

Os produtores, comerciantes e os colecionadores de material de abuso sexual de menores atuam predominantemente a coberto do anonimato e podem ser encontrados em

qualquer país pelo que todos os países devem desenvolver esforços para reprimir com eficácia este tipo de criminalidade, se mais não fora porque as crianças são o nosso futuro que para ser sustentável carece de agentes saudáveis.

A investigação de quem no ciberespaço desenvolve atividades conexas com a exploração sexual de crianças está confrontada com a dificuldade de rastreio das máquinas que veicularam a atuação dos criminosos. Apesar de existir uma referência ou endereço físico, tendencialmente exclusivo para cada dispositivo digital com capacidade de conexão ao Ciberespaço, a tecnologia não utiliza este endereço físico para encaminhamento das comunicações, mas sim o endereço IP, disponibilizado pelos ISP no momento em que a ligação à Internet acontece. A maioria dos endereços de IP são atribuídos de forma dinâmica, sem que seja necessário configurar o endereço físico de cada dispositivo, verificando-se que o IP pode variar durante a comunicação. Cada vez que alguém se conecta com o Ciberespaço, através de um IP dinâmico, vai ser identificado na rede através de um IP provavelmente diferente, sendo possível, viajar de forma "encoberta", de difícil rastreio atentos os diferentes IP atribuídos.

Como contramedida para as dificuldades de rastreio de máquinas que serviram atores criminais de exploração sexual de crianças, é necessário prever que todos os dispositivos que se conectam à Internet estão devidamente identificados pelo ISP, associando-se este registo aos dados do utilizador registado[23] e da sua localização no momento da comunicação. Estes dados serão guardados pelos ISP durante 1 ano e apenas seriam disponibilizados mediante autorização de um Juiz. Ou seja, seria necessário associar a identificação de uma pessoa a um dispositivo e a uma ligação. No caso dos CyberCafes ou nas redes públicas de acesso livre é recomendável que as pessoas que iniciam uma ligação se autentiquem na rede, através de método seguro de identificação (eg.: certificado digital ou introdução de credenciais de acesso disponibilizadas no momento).

A colaboração dos ISP e das instituições cuja atividade consista na disponibilização de serviços e ou monitorização de conteúdos no Ciberespaço é de extrema relevância na deteção e repressão deste fenómeno. À semelhança dos EUA e da Austrália, deverão ser previstas sanções para os ISP e proprietários de domínio que não reportem, às autoridades IC, *sites* com conteúdos de abuso sexual de menores.

A investigação deste tipo de criminalidade e a dedução da acusação em processo penal deve ser facilitada pela legislação e pela adaptação operacional das autoridades de IC.

[23] Releva-se que o utilizador registado é responsável pelo uso dado ao seu IP mas pode não ser actor criminal, por exemplo, pode ter ocorrido utilização abusiva por terceiro.

Nesse sentido, é necessário promover a implementação de medidas adotadas internacionalmente e preconizadas em textos internacionais subscritos por Portugal, que garantam:

- A supressão imediata das páginas eletrónicas que contenham ou difundam material de abuso sexual de menores sediadas em território nacional, preservando-se os respetivos registos de criação, acesso e manutenção para cedência às autoridades IC, em articulação com os ISP e outras entidades de monitorização de conteúdos no Ciberespaço;
- O bloqueio imediato do acesso a páginas eletrónicas que contenham ou difundam material de abuso sexual de menores sediadas fora do território nacional, em articulação com os ISP e outras entidades de monitorização de conteúdos no Ciberespaço;
- A comunicação das referências de *websites* com material de abuso sexual de menores detetadas pela IC aos ISP, às entidades de monitorização de conteúdos no Ciberespaço e entidades financeiras, de forma a operacionalizar o bloqueio e acesso aos respetivos conteúdos, e outrossim permitir que as entidades bancárias possam impedir pagamentos através de cartões de débito e crédito pela utilização e visualização desse material. Esta divulgação exigiria forte cooperação judiciária internacional em matéria penal, sob pena de os esforços de um país serem manifestamente inúteis, face à ausência de fronteiras no Ciberespaço e a diversidade de jurisdições envolvidas;
- A comunicação por parte dos ISP e de outras entidades que desenvolvam a sua atividade no Ciberespaço às autoridades de IC de sites com material de abuso sexual de menores;
- A comunicação por parte de entidade bancárias dos pagamentos efetuados com cartões de débito e de crédito associados a *sites* com material de abuso de menores às autoridades de IC;
- A vigilância preventiva de conteúdos no Ciberespaço tendente a identificar material de abuso sexual de menores, mediante autorização prévia do Ministério Público e acordo do Juiz de Instrução Criminal;
- O desenvolvimento e incremento de ações encobertas direcionadas para a prevenção e investigação criminal deste fenómeno;

- A construção de uma base de dados, tutelada pelas autoridades de IC, designadamente pelo Ministério Público, com material relacionado com o abuso sexual de menores, apreendido nas investigações, transmitidos ou disponibilizados através de tecnologias de informação ou comunicação, como fotografias, vídeos e identificação de *websites*, que permitisse, através de análise de dados, identificar vítimas, agressores, recursos do Ciberespaço (locais) e a troca de informação com entidades de IC estrangeiras, designadamente o Eurojust, a Europol e a Interpol;
- A construção de capacidades operacionais de tratamento e análise centralizado de informação, recolhida no âmbito da prova digital tratada em sede de processo-crime relacionado com a exploração sexual de crianças no Ciberespaço e sua posterior disseminação pelas autoridades de IC, nacionais e estrangeiras, em articulação com a atividade de prevenção criminal.

As medidas elencadas permitiriam debelar as dificuldades com que a IC se debate na investigação do fenómeno da exploração sexual de crianças no Ciberespaço, em prol da eficácia na prossecução de um objetivo comum - a proteção das crianças contra a exploração sexual. Das medidas elencadas merece destaque, pela globalidade do fenómeno, a intensificação da cooperação internacional neste domínio.

No que concerne à IC deste fenómeno, embora não estejam instituídas ou sejam recomendadas práticas a adotar a nível nacional, foi possível detetar regras essenciais a observar aquando da aquisição e manuseamento da prova eletrónica. Essas regras são as seguintes:

- As ações desencadeadas pelas forças policiais ou seus agentes não devem alterar os dados guardados num computador ou num dispositivo de armazenamento que possa ser apresentado em tribunal como prova;
- Em circunstâncias excecionais, caso se considere necessário aceder aos dados originais mantidos num computador ou num dispositivo de armazenamento de dados, essa pessoa deve ter competência legal e técnica para o fazer e poder apresentar provas, explicando a relevância e as implicações das suas ações;
- Deve ser criada e preservada uma linha de auditoria ou outro registo de todos os processos aplicados a elementos de prova eletrónicos informáticos. Um terceiro independente deve poder examinar esses processos e obter o mesmo resultado;

- A pessoa responsável pelo processo (responsável do processo: magistrado do Ministério Público e ou magistrado judicial) deve assumir a responsabilidade global pela observância da lei e dos presentes princípios.

Às regras enunciadas importa relevar também as questões emergentes da manutenção da *"cadeia de custódia da prova"* também identificada como *"cadeia probatória*". Há que salvaguardar e proteger, de forma documentada, a informação digital apreendida para que não possa alegar-se que foi modificada ou alterada durante o processo de investigação.

O princípio da necessidade de manutenção da cadeia de custódia da prova também se verifica se a prova é eletrónica. Com a prova eletrónica (imagens de discos e memória, arquivos de dados e ficheiros executáveis, etc.) a prática consiste em obter *"hashes"* (vulgo assinaturas digitais) da informação no momento da sua recolha, de modo que possa comprovar-se em qualquer momento se essa prova foi modificada, o que se deve observar aquando da efetivação da "cópia de trabalho", no âmbito da realização de perícias informáticas forenses e na análise da prova digital apreendida durante a IC.

Nos termos do disposto no Art. 151.º do CPP a *"a prova pericial tem lugar quando a perceção ou a apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos".* Só o perito nomeado pela autoridade judiciária pode produzir uma perícia no âmbito do processo penal. À semelhança do que sucede noutros países, na determinação para a realização de perícia informática forense no âmbito da investigação da exploração sexual de crianças no Ciberespaço, a autoridade judiciária e o perito nomeado devem ter em especial consideração a reserva da intimidade da vida privada das crianças – deve ser assegurado que terceiros não têm acesso a informação que coloque em causa a reserva da intimidade da vida privada das vítimas, adotando-se regras de segurança de informação que que visem evitar a sua difusão.

A prova pericial distingue-se do exame. Este visa a deteção de vestígios. A perícia visa a avaliação especializada desses vestígios. O exame não subentende a existência de especiais conhecimentos técnicos, ao contrário da perícia. A prova pericial distingue-se igualmente do parecer da autoria de um técnico, uma vez que a realização destes não pressupõe a nomeação no processo por parte da autoridade judiciária.

Associada à realização da perícia informática forense encontra-se a análise forense.

O objetivo da análise forense é estabelecer o que se passou (o quê?), quem o fez (quem?), quando ocorreu (o quando?), como aconteceu (como?). No caso de abuso sexual de crianças no Ciberespaço, importa procurar obter os registos de acesso à Internet, as pesquisas realizadas na Internet, os sites visitados, os ficheiros de vídeo e imagens

guardadas no computador, os ficheiros enviados para outros destinatários, a identificação das vítimas, a existência de jogos ou de material de entretenimento de menores, os registos de pagamentos de vistas a *sites* contendo material de abuso sexual de menores e todos os dados que permitam confirmar ou infirmar a existência de indícios probatórios da prática de crime, entre outros elementos relevantes.

Deste modo, face à tecnicidade da IC no Ciberespaço todos os que intervêm em processos-crime relacionados com este fenómeno, designadamente as autoridades judiciárias e os OPCs, devem dominar as técnicas de apreensão, busca e de análise pericial da prova digital, tendo em vista a manutenção da cadeia da custódia da prova, para o que necessitam de formação e, em permanência, de apoio pericial e técnico especializado.

Os efeitos decorrentes da distribuição do material de abuso na Internet são suscetíveis de agravar as consequências do abuso infantil, afetando a recuperação integral das vítimas – as imagens das crianças exploradas sexualmente e divulgadas na Internet, podem de fato nunca desaparecer e essa circunstância tem um efeito nefasto sobre as vítimas, necessitando de mais tempo e esforço para recuperar da violência a que foram sujeitas. A recuperação é agravada pelo medo de que algo de tão pessoal que sucedeu no passado, possa reaparecer em qualquer lugar, a qualquer momento e ser visto por qualquer pessoa. Esta circunstância constitui uma violação sem fim do direito à privacidade, que provoca uma humilhação adicional nas vítimas, que crescem sabendo que aquelas fotografias ou vídeos estarão na Internet para o resto das suas vidas.

Perante a constatação da dificuldade em combater este fenómeno, e independentemente das obrigações legais, um número crescente de ISPs operadores de telecomunicações móveis e instituições financeiras estrangeiros têm adotado códigos de conduta numa tentativa de autorregulação associada à repressão da distribuição da de material de abuso sexual de menores, reportando esses conteúdos à IC. Ou seja, uma vez que este fenómeno criminal está associado ao Ciberespaço e à Internet, aos ISP deve ser atribuído o papel principal na monitorização e reporte dos conteúdos relacionados com a exploração sexual de crianças.

Em Portugal não está estabelecida (!) a obrigatoriedade de os ISP monitorizarem conteúdos para detetar aqueles que são afins da exploração sexual de crianças e, por isso, não está legalmente prevista nenhuma sanção caso os ISP não reportem a existência de material de exploração sexual de menores na Internet. Admite-se que a situação descrita resulte de ser considerado que o acesso a esses conteúdos poderia contender com o direito à proteção da privacidade, pese embora, num juízo de ponderação de valores, o valor do

direito à privacidade deva ceder perante o valor da proteção e do superior interesse da crianças. Efetivamente, tendo em conta as características deste fenómeno, as obrigações do Estado Português perante convenções internacionais em vigor no ordenamento jurídico português, a dimensão do fenómeno e as consequências deste tipo de práticas para as vítimas, torna-se premente estabelecer a obrigatoriedade do reporte de tais tipos de conteúdos às Autoridades de IC, designadamente ao Ministério Público e assegurar, em articulação com as instituições financeiras o bloqueio de pagamentos relacionados com a comercialização deste tipo de material.

Em suma, a coordenação e articulação entre as autoridades dos diversos países, a partilha de recursos humanos e técnicos e de informação sobre o fenómeno, e um compromisso coletivo a nível internacional, envolvendo parceiros públicos e privados, são fatores indispensáveis para possibilitar investigações de sucesso e a repressão eficaz deste fenómeno e, assim, garantir maior segurança para as crianças no Ciberespaço.

Bibliografia

Ac. do TRP, de 2010-11-17 – **Crimes Sexuais, Procedimento Criminal, Legitimidade, Perícia**. [Em Linha]. Proc. 5/04.2AILSB.P1. Des. José Manuel Araújo Barros et al.. [Consult. 2012-06-10]. Disponível em WWW: <URL: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/256aafd83866bd22802577f9004dc505?OpenDocument&Highlight=0>.

Ac. do TRL, de 2011-01-11 – **Correio Eletrónico, Apreensão de Correspondência, Juiz de Instrução Criminal.** [Em Linha] Proc. 5412/08.9TDLSB-A.L1-5, Des. Ricardo Cardoso et al. [Consult. 2012-06-05]. Disponível em WWW: <URL: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?>.

Ac. do TRL, de 2011-01-18 – **Comunicações Eletrónicas, Segredo de Telecomunicações, Difamação.** [Em Linha] Proc. 3142/09.3PBFUN-A.L1-5, Des. Filomena Clemente Lima et al.. [Consult. 2012-05-05]. Disponível em WWW: <URL: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/0e870e9e2782243380257839005785c2?OpenDocument&Highlight=0,comunica%C3%A7%C3%B5es,electr%C3%B3nicas,sigilo>.

Ac. do TRL, de 2011-03-22 – **Agente Encoberto, Agente Infiltrado, Agente Provocador.** [Em Linha] Proc. 182/09.2 JELSB, Des. Nuno Gomes da Silva et al. [Consult. 2012-05-05]. Disponível em WWW: <URL: http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/e324710ede9b8ed88025788b00345015?OpenDocument>.

Ac. do TRL, de 2011-09-15 – **Localização Celular, Proibição de Valoração de Provas, Prova Testemunhal, Prova Pericial, Prova Oral, Alegações Orais, Novos Meios de Prova.** [Em Linha]. Proc. 1154/07.0POLSB.L1-9, Des. Carlos Benido et al. [Em Linha]. [Consult. 2012-06-25]. Disponível em WWW: <URL: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d579fa3f98618d4e802579140039375f>.

Ac. do TRL, de 2012-03-29 **Comunicações Eletrónicas, Autorização Judicial, Juiz de**

Instrução Criminal, Segredo das Telecomunicações. Proc. 744/09.1S5LSB-A.L1-9, Des. João Carrola et al. [Em Linha]. [Consult. 2012-06-10]. Disponível em WWW: <URL: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/3fadd3f921c9d658802579e2004500c9?OpenDocument&Highlight=0>.

ACPO – Association of Chief Police Officers – **Good Practice Guide for Computer-Based Electronic Evidence** – Official release version. Supported by 7Safe Information Security, 2007, pág. 22. [Em Linha]. [Consult. 2012-06-07]. Disponível em WWW: <URL: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf>.

ALBUQUERQUE, Paulo Pinto de – **Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção dos Direitos do Homem**. 2ª ed. actualizada, Lisboa: Universidade Católica Editora, 2008.

ALBUQUERQUE, Paulo Pinto de – **Comentário do Còdigo Penal à luz da Constituição da República e da Convenção dos Direitos do Homem.** 2ª ed., Lisboa: Universidade Católica Editora, 2010.

BLACHMAN, Nancy, Jerry – **?Google Guide making search even easier (**2012a). [Em Linha]. [Consult. 2012-06-07]. Disponível em WWW: <URL: http://www.googleguide.com/advanced_operators.html>.

BLACHMAN, Nancy, Peek, Jerry Peek and Bergson-Michelson, Tahsa - **?Google Guide making search even easier** (2012b). [Em Linha] - [Consult. 2012-06-07]. Disponível em WWW: <URL: http://www.googleguide.com/advanced_operators_reference.html>.

CARR, John, e Hilton, Zoë - **Coalition on Internet Safety: Digital Manifesto - Action for Children**. [Em Linha]. London, 2009, p. 29. [Consult. 2012-04-07]. Disponível em WWW: <URL: www.chis.org.uk/uploads/02b.pdf>.

CASEY, Eoghan - **Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet**, 3.ª ed, Oxford, Elsevier, 2011.

CÓDIGO de Processo Penal, **Decreto-Lei n.º 78/87, de 17 de Fevereiro** - versão consolidada [Em Linha]. [Consult. 2012-04-07]. Disponível em WWW: <URL: http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=199&tabela=leis>.

CÓDIGO Penal, **Decreto-Lei n.º 48/95, de 25** de Março - versão consolidada [Em Linha] - DR I Série, 170 (2007-09-04), 6201-6258. [Consult. 2012-03-09]. Disponível em WWW: <URL: http://dre.pt/pdf1sdip/2007/09/17000/0618106258.pdf>.

COMISSÃO Europeia - **Comunicação da Comissão ao Parlamento Europeu, ao**

Conselho, ao Comité Económico Social Europeu e ao Comité das Regiões – Uma Agenda Digital para a Europa (2010) [Em Linha]. [Consult. 2012-03 09]. Disponível em WWW: <URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PT:PDF>.

COMISSÃO Europeia - **Comunicado à Imprensa da Comissão Europeia sobre Agência Financeira Europeia**, 3 março de 2009. [Em Linha]. [Consult. 2012-08-20]. Disponível em WWW: <URL: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/342&format=HTML&aged=1&language=PT&guiLanguage=fr>.

COMPROMISSO e **Plano de Acão de Budapeste contra a Exploração Sexual de Crianças com fins Comerciais** - Conferência Preparatória do 2.º Congresso Mundial contra a Exploração Sexual das Crianças com Fins Comerciais (20 -21 de Novembro de 2001). [Em Linha]. [Consult. 2012-07-07]. Disponível em WWW: <URL: http://www.coe.int/t/dghl/standardsetting/children/Budapest_Commitment_and_Plan_of_Action.pdf>.

COMPROMISSO Mundial de Yokohama contra a Exploração Sexual das Crianças com Fins Comerciais - 2**.º Congresso Mundial contra a Exploração Sexual das Crianças com Fins Comerciais** (17 -20 de Dezembro de 2001). [Em Linha] [Consult. 2012-07-07]. Disponível em: WWW <URL: http://www.ecpat.net/EI/Global_yokohama.asp>.

Conselho Consultivo do Ministério Público de 2009-10-08, Parecer: 3060, **Segredo de Justiça, Segredo Bancário**, (…) Acesso a documentos (…), Cons. António Leonel Dantas et al. [Em Linha]. [Consult. 2012-06-07]. Disponível em WWW: <URL: http://www.dgsi.pt/pgrp.nsf/7fc0bd52c6f5cd5a802568c0003fb410/34156d46d2de0da9802575dd00313e6d?OpenDocument&Highlight=0>.

CONSELHO da Europa - **Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais** - assinada em Lanzarote em 25 de Outubro de 2007. Aprovada pela Resolução da Assembleia da República n.º 75/2012, de 28 de Maio. DR I Série, 103 (2012-05-28). [Consult. 9 Març. 2012]. Disponível em WWW: <URL: http://www.coe.int/t/dghl/standardsetting/children/Source/LanzaroteConvention_por.pdf>.

CONSELHO da Europa - Convenção do Conselho da Europa Relativa à Luta contra o Tráfico de Seres Humanos, aberta à assinatura em Varsóvia, em 16 de maio de 2005 – DR I Série 9 (14-01-2008), 412-441. Aprovada pela Resolução da Assembleia da República n.º

1/2008, de 14 de Janeiro. Em linha [Consult. 2012-06-06]. Disponível em WWW: <URL: http://dre.pt/pdf1sdip/2008/01/00900/0041200441.PDF>.

CONSELHO da Europa - **Convenção Europeia sobre o Exercício dos direitos da criança** – Estrasburgo, 25 de Janeiro de 1996. Em linha [06-06-2012]. Disponível em WWW: <URL: http://conventions.coe.int/treaty/en/Treaties/Html/160.htm>

CONSELHO da Europa - **Convenção para a Proteção dos Direitos do Homem e Liberdades Fundamentais**. [Em Linha]. [06-Consult. 2012-06-06]. Disponível em WWW: <URL: http://www.dgpj.mj.pt/sections/relacoes-internacionais/copy_of_anexos/tribunal-europeu-dos_1/downloadFile/attachedFile_f0/Convencao_Europeia_dos_Direitos_do_Homem.pdf?nocache=1203004099.16>.

CONSELHO da Europa - **Convenção sobre o Cibercrime** – Budapeste, 23 de Setembro de 2001 – Aprovada pela Resolução da Assembleia da República n.º 88/2009, de 15 de Setembro. [Em Linha]. [Consult. 2012-06-06). Disponível em WWW: <URl: http://dre.pt/pdf1sdip/2009/09/17900/0635406378.pdf>.

CONSELHO da Europa, – Uma estratégia Nacional integrada – **Directrizes do Conselho da Europa sobre as estratégias nacionais integradas de proteção das crianças vítimas de violência**. [Em Linha]. [Consult. 2012-06-06]. Disponível em WWW: <URL: http://www.coe.int/t/dg3/children/news/guidelines/A4%20Recommendation%20CM%20protection%20of%20children%20_POR_BD.pdf>.

COUNCIL of Europe - Committee of Ministers – **Recommendation N.º R (91) 11 of Ministers to Member States concerning sexual exploitation pornography and prostitution and trafficking in, children and young adults.** [Em Linha]. [Consult. 2012-06-06]. Disponível em WWW: <URL: http://www.copii.ro/files2/31_RecomandareaCE_11_1991.pdf>.

COUNCIL of Europe - Committee of Ministers – **Recommendation N.º R (2001) 16 of Ministers to Member States on the protection of children against sexual exploitation**. [Em Linha]. [Consult. 2012-06-07]. Disponível em: WWW: <URl: https://wcd.coe.int/ViewDoc.jsp?id=234247>.

COUNCIL of Europe - **Explanatory Report - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse** [Em Linha]. [Consult. 2012-03-09]. Disponível em: WWW <URL: http://conventions.coe.int/Treaty/EN/Reports/Html/201.htm>.

COUNCIL of Europe - Recommendation 1882 - Parlamentary Assembly, Council of Europe. **The promotion of Internet and online media services appropriate for minors**, 2009. [Em Linha]. [Consult. 2012-03-09]. Disponível em WWW: <URL: http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta09/EREC1882.htm>.

COUNCIL of Europe - Report. Doc. 11924 - Parlamentary Assembly, Council of Europe, Committee on Culture, Science and Education - **The promotion of Internet and online media services appropriate for minors**, 2009. (Em Linha].[Consult. 2012-03-10]. Disponível em WWW: <URL: http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc09/EDOC11924.ht>

COUNCIL OF EUROPE Treaty Series - No. 201 – **Convenção do Conselho da Europa para a Protecção de crianças contra a exploração sexual e os abusos sexuais**, 2012. DR I Série [Em Linha]. [Consult. 2012-06-6]. Disponível em WWW <URL: http://www.coe.int/t/dghl/standardsetting/children/Source/LanzaroteConvention_por.pdf>.

COUNCIL of the Inspectors General on integrity and efficiency - **Guidelines on Undercover Operations,** June 2010. [Em Linha] [Consul. 2012-07-11].Disponível em WWW: <URL: http://www.ignet.gov/pande/standards/invprg1211appj.pdf>.

DECLARAÇÃO e **Programa de Acção de Estocolmo contra a Exploração Sexual das Crianças com Fins Comerciais** - 1.º Congresso Mundial contra a Exploração Sexual das Crianças com Fins Comerciais, - Estocolmo - 27 a 31 de Agosto de 1996. [Em Linha]. [Consult. 2012-07-07]. Disponível em WWW: <URL: http://www.ecpat.net/EI/Global_stockholm.asp>.

DECRETO-LEI nº 176/2007, de 8 de Maio – **Lei das Comunicações Eletrónicas**. DR I Série, 88 (2099-3001. [Em Linha]. [Consult. 07-06-2012]. Disponível em WWW: <URL: http://dre.pt/pdf1sdip/2007/05/08800/29993001.pdf>.

DIAS, Maria do Carmo Saraiva de Menezes da Silva - **Crimes Sexuais com Adolescentes**, 1.ª ed., Lisboa, Almedina, 2006 - ISBN 972-40-2730-9

ECPAT - End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes, Sweden - **The Commercial Sexual Exploitation of Children**, 1.ª ed., Stockholm: ECPAT Sverige an Jurge Forlag AB, 2011 - ISBN 978-91-7223-447-5, pág. 154.

EICHENWALD, Kurt – **Trough his webcam, a boy joins a sordid online world**. New York Times, (2005-12-19). [Em Linha] [Consult. 2012-06-12]. Disponível em WWW: <URL: http://www.nytimes.com/2005/12/19/national/19kids.ready.html?pagewanted=all>.

ETHEREAL – **A Network Protocol Analyser** [Em Linha]. [Consult. 2012-05-28]. Disponível em WWW: <URL: http://www.ethereal.com/>.

FERRARO, Monique Mattei and CASEY, Eoghan - **Investigating Child Exploitation and Pornography - The Internet, The Law and Forensic Science**, 1.ª ed., Elsevier Academic Press, 2005, Oxford,- ISBN - 13:978-0-12-163105-5.

G-8 Justice and Home Affairs Ministers (24.05.2007) - **Ministers' Declaration: Reinforcing the International Fight Against Child Pornography**. [Em linha]. [Consult. 2012-07-22]. Disponível em WWW: <URL: http://www.canadainternational.gc.ca/g8/ministerials-ministerielles/2007/child_porno-enfant_porno.aspx?lang=eng&view=d>.

GIBSON, William - **Neuromancer**, The Berkley Publishing Group, a division of Penguin Putnam Inc. – New York, 1984.

GOOGLE – **Google Alert FAQS**. [Em Linha] -[Consult. 2012-06-07]. Disponível em WWW: <URL: http://www.google.pt/support/alerts/bin/answer.py?hl=pt-PT&answer=71057&rd>.

GOOGLE - **Google Inside Search**. [Em Linha]. [Consult. 2012-06-07]. Disponível em WWW: <URL: http://support.google.com/websearch/bin/answer.py?hl=en&answer=136861>.

GOOGLE mail – **página inicial de ajuda do google** – cabeçalhos de mensagem. [Em Linha]. [Consult. 2012-06-20]. Disponível em WWW: <URL: http://support.google.com/mail/bin/answer.py?hl=pt-BR&answer=22454>.

INTERPOL – **Victim Identification**. [Em Linha]. [Consult. 2012-07-22]. Disponível em WWW: <URL: http://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification>.

IWF **– Código de Boas Práticas para os casos de deteção de material de abuso de menores nos locais de trabalho**. [Em Linha]. [Consult. 2012-08-20]. Disponível em WWW: <URL: http://www.iwf.org.uk/resources/best-practice-guide>.

IWF - Internet Watch Foundation, Annual and Charity Report, 2006 e 2010, Cambridge, UK, 2007 and 2011, (2007 e 2010) [Em Linha]. [Consult. 2012-04-05]. Disponível em WWW: <URL: www.enough.org/objects/20070412_iwf_annual_report_2006_web.pdf> e WWW: <URL: http://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf>

LEI da Cooperação Judiciária Internacional em Matéria Penal - **Lei n.º 144/99, de 31 de**

Agosto, DR I Série, 203 (1999-08-31), 6012-6040. [Em Linha]. [Consult. 2012-08-27. Disponível em WWW: <URL: http://www.gddc.pt/legislacao-lingua-portuguesa/portugues/Lei144-99rev.html>.

LEI da proteção dos dados pessoais - **Lei n.º 67/98**, DR I Série, 247 (5536-5546). [Consult. 08-06-2012]. Disponível em WWW: <URL: http://dre.pt/pdf1sdip/1998/10/247A00/55365546.pdf>.

LEI da Proteção dos Dados Pessoais nas Comunicações Eletrónicas - **Lei n.º 41/2004, de 18 de Agosto**, DR I Série, 194 (5241-5245). [Consult. 08-06-2012]. Disponível em WWW: <URL: http://www.dre.pt/pdfgratis/2004/08/194A00.PDF>.

LEI das Comunicações Eletrónicas - **Lei n.º 5/2004, de 10 de Fevereiro**, DR I Série, 34, (788-821). [Em Linha]. [Consult. 07-06-2012]. Disponível em WWW: <URL: http://dre.pt/pdfgratis/2004/02/034A00.pdf>.

LEI do Cibercrime - **Lei n.º 109/2009, de 15 de Setembro**. [Em Linha]. [Consult. 2012-03-09]. DR I Série, 179 (2009-09-15), 6319-6325. Disponível em WWW: <URL: http://www.cnpd.pt/bin/legis/nacional/LEI109-2009-%20CIBERCRIME.pdf>.

LEI do Comércio Eletrónico - **Decreto-Lei n.º 7/2004, de 7 de Janeiro**, DR I Série, 5 (70-78). [Em Linha]. [Consult. 08-06-2012]. Disponível em WWW: <URL: http://www.dre.pt/pdf1s/2004/01/005A00/00700078.pdf>.

LEI n.º 32/2008, de 17 de Julho – [Em Linha]. [Consult. 2012-03-09]. DR I Série, 179 (2009-09-15), 6319-6325. Disponível em WWW: <URL: http://www.umic.pt/images/stories/legislacao/Lei%2032_2008.pdf>.

LEITE, Inês F.- Pedofilia - **Repercussões das Novas Formas de Criminalidade na Teoria Geral da Infracção**. 1ª ed., Coimbra: Almedina, 2004, págs. 15 e 16.

MEDARIS, Michael and Girourad, Cathy – **Protecting Children in Cyberspace – The ICAC Task Force**. [Em Linha]. Juvenile Justice Bulletin Program, U.S. DOJ - Department Of Justice – Office of Justice Program – Office of Juvenile Justice and Delinquency Prevention, .2002. [Consult. 2012-08-20]. Disponível em www <URL:. https://www.ncjrs.gov/pdffiles1/ojjdp/191213.pdf>

NP – Norma Portuguesa 4438 - **Informação e documentação, Gestão de Documentos de Arquivo, Parte 2: Recomendações de Aplicação** - IPQ – Instituto Português da Qualidade, Almada, Portugal, 2005.

NSPCC - NATIONAL society for the prevention of cruelty to children – **People convicted of child abuse image offences**. Press releases (2011-07-27). [Em Linha]. [Consult. 2012-

04-05]. Disponível em WWW: <URL: http://www.nspcc.org.uk/news-and-views/media-centre/press-releases/2011/11-07-27-Child-sexual-abuse-images-convictions/11-07-27-Child-sexual-abuse-images-convictions_wdn83516.html>.

OIT – Organização Internacional do Trabalho - **Convenção n.º 182, Relativa à Interdição das Piores Formas de Trabalho das Crianças e à Acão Imediata Com Vista À Sua Eliminação**. – adotada pela Conferência Geral da OIT - Organização Internacional do Trabalho em 17 de Junho de 1999 - Aprovada, para ratificação, pela Resolução da Assembleia da República n.o 47/2000, em 25 de Maio de 2000. [Em linha]. [Consult. 2012-06-06]. Disponível em WWW: <URL: http://www.ilo.org/public/portugue/region/eurpro/lisbon/pdf/conv_182.pdf>.

OLAF – Office Européene de Lutte Anti - Fraud - Informações sobre os procedimentos de informática forense do OLAF. [Em Linha]. [Consult. 2012-06-20]. Disponível em WWW: <URL: http://ec.europa.eu/anti_fraud/documents/forensics-leaflet/external_pt.pdf>.

ONU - **Convenção Sobre os Direitos da Criança** - . Adoptada pela Assembleia Geral nas Nações Unidas em 20 de Novembro de 1989 e ratificada por Portugal em 21 de Setembro de 1990. Em Linha [06-06-2012]. Disponível em WWW: <URL: http://www.unicef.pt/docs/pdf_publicacoes/convencao_direitos_crianca2004.pdf>.

ONU – Human Rights Council – **Report of the Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography**, Najat M'jid Maalla, (13-07-2009), A/HRC/12/23. [Em Linha]. [Consult. 2012-06-21]. Disponível em WWW: <URL: http://www.unhcr.org/refworld/docid/4ab0d35a2.html>.

ONU - **Protocolo Facultativo relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil** – Adoptado e aberto à assinatura pela Assembleia Geral das Nações Unidas em 25 de maio de 2008 – Aprovado pela Resolução da Assembleia da República n.º 16/2003, de 5 de Março. [Em linha]. [Consult. 2012-06-06]. Disponível em WWW: <URL: http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhuniversais/protocolo-crian%E7as2.html>.

PARLAMENTO Europeu - **Directiva do Parlamento Europeu e do Conselho relativa à Luta Contra o Abuso e a Exploração Sexual de Crianças e a Pornografia Infantil** - substitui a Decisão-Quadro 2004/68/JAI do Conselho. [Em linha]. [Consult. 2012-06-11). Disponível em WWW: <URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:PT:PDF>.

PARLAMENTO Europeu - **Directiva do Parlamento Europeu relativa à Luta contra o**

Abuso e a Exploração Sexual de Crianças e a Pornografia Infantil, 2011 [Em Linha]. [Consult. 2012-03. 09]. Disponível em: WWW: <URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:PT:PDF >.

PGDL – Atualidades -Uso do Facebook. Condenação em pena de prisão. Ministério Público de Sesimbra. (29-05-2012) [Em Linha]. [Consult. 06-07-2012]. Disponível em WWW: <URL: http://www.pgdlisboa.pt/pgdl/novidades/nov_main.php?ficha=26&pagina=&destaque=>.

PINHO, Carlos – **Os problemas interpretativos da Lei n.º 32/2008, de 17 de Julho**. Rev. do Mini. Público, ano 33, pág. 91. ISSN 0870-6107.

SILVA, Germano Marques da.- **Curso de Processo Penal**. 2ª ed., Vol. Lisboa, Editorial Verbo, 1999.

SISTEMA de Segurança Interna - **Relatório Anual de Segurança Interna**, 2011. [Em Linha]. [Consult. 2012-06-21]. Disponível em WWW: <URL: http://www.portugal.gov.pt/media/555724/2012-03-30_relat_rio_anual_seguran_a_interna.pdf>.

TAVARES, Raquel. - **Combate à Pornografia Infantil na Internet – caso português**. GDDC – Gabinete de Documentação e Direito Comparado. [Em Linha]. [Consult. 2012-08-20]. Disponível em WWW: <URL: http://www.gddc.pt/direitos-humanos/temas-dh/Pedofilia.html>.

TINK, Palmer e STACEY, Lisa - **Just One Click: Sexual abuse of children and young people through the Internet and mobile phone technology**, Barnardo´s, Ilford, UK – United Kingdom, 2004.

VERDELHO, Pedro. **A nova Lei do Cibercrime**. Scientia Ivridica. Revista de Direito Comparado Português e Brasileiro. Braga. ISNN 0870 – 8185. Tomo LVIII, 320 (8 Outubro-Dezembro 2009).

Website da IWF – **Internet Watch Foundation**. [Em Linha]. [Consult. 2012-06-21]. Disponível em WWW: URL:. http://www.iwf.org.uk/>.

Website Ethereal – **A Network Protocol Analyser.** [Em Linha]. [Consult. 2012-05-28]. Disponível em WWW: <URL: http://www.ethereal.com>.

Website Wireshark – **A Network Protocol Analyser.** [Em Linha]. [Consult. 2012-05-28]. Disponível em WWW: <URL: http://www.wireshark.org/>.

Apêndice 1

Glossário

abusador sexual - Qualquer pessoa que ofende sexualmente crianças ou se envolve em qualquer atividade sexual com uma criança.

abuso sexual infantil em linha - produção, distribuição, disponibilização ou visualização de pornografia infantil (fotografias ou vídeo); solicitação *on-line* de crianças e jovens para a produção de material de abuso infantil, mediante conversas de natureza sexual ou outra atividade *on-line* de cariz sexual, designadamente para atrair a criança para um encontro off-line, para fins de atividade sexual com esta

armazenamento de dados digitais - processo pelo qual os dados são copiados para um computador, a partir da Internet ou de outra fonte, como um disco rígido, um telefone ou outros dispositivos de armazenamento de dados. Os dados são normalmente transferidos para um computador para acesso, guarda, visualização posterior, e incluem arquivos de texto, fotografias, vídeos e música.

banda larga - uma conexão de alta capacidade que facilita a conexão através da Internet e permite uma troca mais rápida de arquivos grandes dimensões, como vídeos, jogos e programas informáticos (software).

blog - Sites com entradas ou "posts", incluindo textos e imagens, normalmente exibidas em ordem cronológica. Blogs inteiros ou “postagens” em particular podem ser públicos e disponíveis para todos, ou privados e disponíveis apenas para utilizadores que estão autorizados pelo proprietário do blog / autor.

browser - Um programa de software que é selecionado pelo consumidor e utilizado para localizar e mostrar páginas na World Wide Web (páginas web). Navegadores mais populares incluem o Windows Internet Explorer, Firefox, Google Chrome, Safari e Opera.

ciberespaço - o universo virtual compartilhado do mundo "redes de computadores”. O termo foi criado por William Gibson no seu romance intitulado “Neuromancer”, em 1986.

consola de jogos - Um dispositivo usado para jogar jogos eletrónicos, especialmente jogos de vídeo, como Sony PlayStation ou Nintendo Wii. O jogador normalmente interage

com o jogo através de um dispositivo portátil; as consolas mais recentes permitem que o utilizador se conecte diretamente à Internet.

conteúdo gerado pelo utilizador - materiais e meios de comunicação criados por utilizadores da Internet e não por empresas, de que são exemplo a "Wikipedia" e o "Youtube"

criança - todas as pessoas com idade inferior a dezoito anos, salvo nos casos em que nos termos da lei aplicável à criança a maioridade seja alcançada antes.

criptografia - processo mediante o qual os dados são convertidos para um formato ou código que não pode ser lido ou utilizado por uma pessoa ou por um computador sem a chave adequada para descodificá-lo.

e-grupos - um grupo que é controlado centralmente e comunica coletivamente por e-mail; podem oferecer serviços de um "opt-out" ou "opt-in" com base no qual um indivíduo escolhe a participar depois de ter sido convidado a participar do grupo.

e-mail - abreviatura de "correio eletrónico" - uma ferramenta que permite que alguém envie uma mensagem, ou "email" a outra pessoa ou outras pessoas com "caixas de correio eletrónico" conectadas através de uma rede de comunicações como a Internet.

Endereço de Internet Protocol (IP) - Uma sequência de dígitos usados para representar um computador na Internet. Este conjunto de dígitos pode ser comparado a um número de telefone ou número de identificação de uma máquina. Os endereços IP podem ser temporários (dinâmicos) ou fixos. De qualquer modo, estão diretamente ligados a uma máquina específica que foi ligada à Internet num determinado momento ou período temporal. Por esta razão, os endereços IP são de importância fulcral na proteção da criança e de todos os crimes que se preparam, desenvolvem ou praticam em linha, ou em qualquer outro tipo de investigação criminal com conexão com o Ciberespaço.

exploração sexual comercial de crianças - prostituição infantil, pornografia infantil e, bem assim a participação de uma criança em espetáculos pornográficos. Inclui-se o recrutamento, mediante a utilização da força física ou a prática de atos que causem receio contra a vida e a integridade física da criança ou de terceiros, de modo a que a criança seja constrangida a participar em espetáculos pornográficos ou a sujeitar-se a atos de natureza sexual. Inclui-se no conceito a circunstância de o agente se aproveitar de outra forma de exploração de uma criança com tais fins e objetivos, de forma livre e consciente, bem assim assistir ao abuso sexual ou atividades sexuais da criança, mesmo sem ter de participar ou solicitar crianças para fins sexuais.

filtro - um mecanismo para detetar e bloquear o acesso a determinado material. A maioria dos pacotes de segurança infantil de software utiliza um componente de deteção e bloqueio de determinados dados. O programa pode ser concebido para funcionar num computador pessoal individual ou pode ser aplicado a uma rede de computadores. Muitas vezes a componente de deteção e acesso a determinados dados é oferecido gratuitamente como uma parte integrante de um computador ou sistema operacional. Este tipo de programas pode vir integrado num pacote de conectividade de um utilizador a um ISP. Também têm sido desenvolvidos para telefones celulares e consolas de jogos.

grooming em linha - um processo ou conjunto de atividades destinado a atrair as crianças, através de comportamento sexual, conversas ou outros meios a fim de torná-lo(a) mais vulnerável ao abuso sexual.

grupo de avisos ou "newsgroups" - fórum de comunicações eletrónicas com mensagens de acolhimento e artigos ligados a um assunto ou tema comum. Os participantes podem optar por participar no grupo de avisos e visualizar as mensagens no serviço de notícias disponibilizado a todos os participantes ou recebê-las através de correio eletrónico. Os membros/utilizadores participam dos "newsgroups" lendo as mensagens e também ao respondê-las.

imagens de abusos - 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.

Internet - rede mundial de centenas de milhares de redes de computadores interconectados, utilizando um conjunto comum de protocolos de comunicação e partilha de um esquema de endereçamento comum. A Internet facilita a transmissão de mensagens de e-mail, arquivos de texto, imagens e muitos outros tipos de informações entre computadores.

Internet Service Provider (ISP) - Uma empresa comercial que fornece aos utilizadores acesso direto à Internet, geralmente mediante o pagamento de uma determinada quantia monetária ou uma taxa. Empresa que fornece serviços de Internet, tais como hospedagem de e desenvolvimento de sítios web.

jogos multiplayer online papel playing (MMORPG) - jogos em linha que podem ser jogados por um grande número de jogadores em simultâneo. Também por vezes referido como massively multiplayer *on-line* (MMO) ou massively multiplayer *on-line* games (MMOG).

mensagens instantâneas (IM) - texto baseado em serviço de comunicações semelhante a uma sala de conversação. A principal diferença é que as salas de conversação são normalmente espaços públicos onde qualquer pessoa pode participar, enquanto os sistemas de mensagens instantâneas geralmente dependem de uma "lista de amigos" ou de alguma outra lista de pessoas predeterminadas pelo utilizador. Apenas as pessoas na lista podem comunicar com o utilizador, ou seja, cada utilizador controla quem pode dirigir-lhe ou enviar mensagens instantâneas. O Google Chat, o MSN - Microsoft Messenger e o Twitter são exemplos de serviços de mensagens instantâneas. Os sítios web de redes sociais (ver definição abaixo) disponibilizam uma função de mensagens instantâneas.

mundos virtuais - ambientes tridimensionais simulados, disponíveis em linha, habitados por jogadores que interagem uns com os outros através de avatares (ícones que representam uma pessoa móveis no ciberespaço). Second Life, ou mais popular entre os jovens, o Second Life Teen, são exemplos de mundos virtuais.

on-line - ligação a uma rede de computadores ou à Internet; qualquer atividade ou acesso a serviço que está disponível através da Internet. Uma pessoa está "*on-line*" quando está registada numa rede de computadores, ou quando tenha ligado um computador ou outro dispositivo à Internet. O termo *"offline"* descreve a atividade que não é feita *on-line*, bem como a condição de estar desconectado da Internet.

partilha de vídeo – semelhante a partilha de fotografias (veja acima), mas para vídeos. Estes vídeos são muitas vezes gerados pelo utilizador.

pedófilo - categoria diagnóstica referindo a uma orientação sexual exclusiva para crianças pré-púberes.

peer-to-peer (P2P) - software que permite transmissão de dados diretamente de um computador para outro através da Internet, normalmente sem a necessidade de envolver um servidor de terceiros.

pornografia infantil ou material de abuso sexual de menores - 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.

programa de computador para partilha de fotografias - uma aplicação que permite aos utilizadores disponibilizar na Internet (upload), visualizar e partilhar fotografias – os utilizadores podem permitir quer o acesso público ou privado.

prostituição infantil - utilização de uma criança em atividades sexuais mediante

contrapartida monetária ou qualquer outra forma de retribuição.

provedor de serviço eletrónico (ESP) ou provedor de serviços online (OSP) - qualquer empresa, organização ou indivíduo que oferece um serviço através da internet. Geralmente este termo é usado para distinguir um ESP ou um OSP de um Internet Service Provider (ISP) que, historicamente, disponibiliza apena o acesso ou a conectividade à Internet.

sala de conversação ou de "chat" - "salas de reuniões virtuais" onde as pessoas podem comunicar umas com as outras digitando mensagens em tempo real. A maioria das salas de conversação concentra-se num tópico específico, mas alguns são mais gerais e são criados as pessoas a conhecerem outras pessoas.

serviço de mensagens curtas (SMS) - O serviço de mensagens de texto comum disponível no telefones móveis, outros dispositivos portáteis e computadores.

sexting - forma de mensagens de texto / mensagens de texto (ver definição abaixo) em que as pessoas enviam imagens de natureza sexual ou textos sexualmente explícitos.

sítios de redes sociais (SRS) – disponibilização de funcionalidades em linha, as quais permitem aos utilizadores criar perfis, públicos ou privados, e formar uma rede de amigos. As redes sociais permitem que os utilizadores interajam com amigos através de meios privados e públicos, tais como mensagens e mensagens instantâneas, e coloquem conteúdos gerado pelo utilizador, como fotos e vídeos. Exemplos de SRS são o Facebook, o HI5, o MXit, o Myspace e o Orkut.

smartphones – telemóveis portáteis que incorporam um sistema operacional completo e são capazes de aceder à Internet. Em muitos aspetos, funcionam como pequenos computadores, com mais memória e écrans maiores do que os telefones comuns.

solicitação de crianças para fins sexuais - proposta intencional, através de tecnologias de informação e comunicação, de um adulto em relação a uma criança (que não tenha atingido a idade legal para atividades sexuais) com a finalidade de se envolver em atividades sexuais ou produzir pornografia infantil.

Tecnologias da Informação e comunicação (TIC) - qualquer dispositivo de comunicação ou programa informático, incluindo rádio, televisão, telemóveis, sistemas de satélite e computador, hardware de rede e software, bem como serviços associados e aplicações como videoconferência e ensino à distância.

upload - O processo de transmissão de dados de um utilizador de uma máquina s para um servidor.

Usenet - Um serviço de Internet, onde milhares de newsgroups estão localizados.

venda de crianças - qualquer ato ou transação pelo qual uma criança é entregue por uma pessoa a outra mediante contraprestação monetária ou qualquer outra forma de retribuição.

webcam - uma câmara de vídeo que integra um computador ou está ligada a um computador, que esteja conectado à Internet.

World Wide Web (WWW) - Um sistema baseado em hipertexto para encontrar e aceder a dados na Internet. As páginas web podem estar ligadas a outros documentos ou sistemas de informação. A Web é uma parte da Internet e nem todos os servidores na Internet fazem parte da web.

Apêndice 2 - Diagrama de Validação

QC: Tendo em consideração a transferência para o Ciberespaço de parte da atividade delituosa relativa à exploração sexual de menores é possível implementar procedimentos de IC que, com eficácia, acautelem a aquisição de prova digital e potenciem a condenação dos que se dedicam a tais tipo de práticas criminosas?

QD1 – Na dimensão do Ciberespaço existem limitações às investigações deste tipo de casos?

QD2 – A nível nacional são seguidos procedimentos e metodologias de investigação padrão e estão alinhados com o que é adotado a nível internacional?

QD3 – Existem metodologias de atuação comuns reconhecidas como melhores práticas para a investigação deste tipo de criminalidade?

H1 - O Ciberespaço confronta a investigação criminal com dificuldades novas que, em paralelo com outros fenómenos de natureza global, exigem resposta que, para ser eficaz, tem de ser global.

H2 – A complexidade deste fenómeno e a IC neste âmbito confronta-se a nível nacional quer com a ausência de padrões de atuação quer com as dificuldades decorrentes de uma incipiente cooperação internacional.

H3 – A articulação com autoridades internacionais e com as entidades responsáveis pela monitorização dos conteúdos no Ciberespaço - prestadores de serviço neste domínio e autoridades com competências de IC - são dimensões estruturantes do acervo das melhores práticas de IC deste tipo de casos.

QD1	Na dimensão do Ciberespaço existem limitações às investigações deste tipo de casos?	§§ 2 e 4 de 2.1.; § 3 de 2.2.; § 3 de 2.3. e § 3 de 2.9; § 2 de 2.4. e § 2 de 2.9 ; § 5 de 2.5., § 2 de 2.9, 2.9.7., 2.9.8., 2.6.1., 2.6.2. e 2.6.3., § 1. de 2.6.3.; § 2 e 5. de 2.8., § 2 de 2.9. e § 5 de 2.9.10.	**H1**	O Ciberespaço confronta a investigação criminal com dificuldades novas que, em paralelo com outros fenómenos de natureza global, exigem resposta que, para ser eficaz, tem de ser global	**C**
QD2	A nível nacional são seguidos procedimentos e metodologias de investigação padrão e estão alinhados com o que é adotado a nível internacional?	2.9.6.-2.9.10.; 3.1.; § 5 de 3.3. e §§ 5 e 6 de 3.4., 3.6. e § 2 de 3.7., 3.8. e 3.9.	**H2**	A complexidade deste fenómeno e a IC neste âmbito confronta-se a nível nacional quer com a ausência de padrões de atuação quer com as dificuldades decorrentes de uma incipiente cooperação internacional.	**C**
QD3	Existem metodologias de atuação comuns reconhecidas como melhores práticas para a investigação deste tipo de criminalidade?	2.9.6.-2.9.10.; § 1 de 4.2. e § 3 de 4.5.; §§ 1 e 4 de 4.1.; § 1 de 4.3.; §§ 4, 6 e 7 de 4.4.; § 5 de 4.4.; 4.6.	**H3**	A articulação com autoridades internacionais e com as entidades responsáveis pela monitorização dos conteúdos no Ciberespaço - prestadores de serviço neste domínio e autoridades com competências de IC - são dimensões estruturantes do acervo das melhores práticas de IC deste tipo de casos.	**C**

QD – Questão Derivada H – Hipótese C - Confirmada

TEMA A exploração sexual de crianças no Ciberespaço Aquisição e valoração de prova forense de natureza digital		
QUESTÃO CENTRAL Tendo em consideração a transferência para o Ciberespaço de parte da atividade delituosa relativa à exploração sexual de menores é possível implementar procedimentos de IC que, com eficácia, acautelem a aquisição de prova digital e potenciem a condenação dos que se dedicam a tais tipo de práticas criminosas?		
Da caracterização do Ciberespaço, do enquadramento jurídico internacional e interno que incide sobre a exploração sexual de crianças e dos casos de IC analisados, conclui-se que o *locus* em causa se caracteriza pela sua dimensão mundial e global, que a utilização de computadores e de tecnologia de diversa natureza está em crescendo, pela inexistência de controlo efetivo sobre o material de exploração sexual de crianças, pelo tendencial anonimato dos que se dedicam a tais tipo de práticas e rapidez de difusão de tais práticas neste *locus*, com as inerentes dificuldades para a IC, a exigirem coordenação entre autoridades de IC em articulação e coordenação com os ISP e entidades de monitorização de conteúdos, a um nível global.	Apreciando os casos nacionais analisados, verificando-se a omissão de dados estatísticos nacionais sobre o fenómeno, tendo em conta a complexidade do fenómeno e do ambiente em causa, constatando-se a relativa falta de especialização dos operadores judiciários e dos investigadores criminais em geral, concluímos pela ausência de padrões institucionalizados de atuação da IC, por uma relativa ineficácia da cooperação internacional e nacional quanto à repressão deste fenómeno, designadamente quanto à identificação de vítimas de crime.s	Face à dimensão global do fenómeno, apreciando os exemplos internacionais na abordagem à repressão da exploração sexual de crianças analisados, verificamos a existência de experiências de sucesso entre as autoridades de IC, designadamente com a Interpol e entidades de IC nacionais e, bem assim, a construção de relações proveitosas para a IC no que concerne a mecanismos de reporte e bloqueio de conteúdos ilegais por parte dos ISP e empresas de telecomunicações, a que se alia a coordenação com entidades financeiras no que concerne ao bloqueio de pagamentos de conteúdos relacionados com a aquisição de material de abuso sexual de menores, pelo que concluímos pela imprescindibilidade da existência de uma articulação investigatória entre autoridades de IC dos diversos países e atuação concertada com os prestadores de serviços no âmbito do Ciberespaço e também as instituições financeira, a concretizar em sede legal e operacional.

PARA MELHORAR A IC DA EXPLORAÇÃO SEXUAL DE CRIANÇAS NO CIBERESPAÇO
COOPERAÇÃO JUDICIÁRIA INTERNACIONAL: **Reforço** da coordenação internacional entre autoridades de IC em articulação com as entidades de monitorização de conteúdos no Ciberespaço a um nível global, com a constituição de unidades funcionais de IC nacionais, especializadas na exploração sexual de crianças no Ciberespaço.
PREVENÇÃO CRIMINAL: **Vigilância** preventiva de conteúdos no Ciberespaço tendente a identificar material de exploração sexual de menores. **Desenvolvimento** e incremento de ações encobertas direcionadas para a prevenção e investigação criminal deste fenómeno.
ARTICULAÇÃO E COORDENAÇÃO: **Comunicação** por parte dos ISP e de outras entidades que desenvolvam a sua atividade no Ciberespaço às autoridades de IC de *websites* com material de abuso sexual de menores. **Comunicação** por parte das entidades bancárias dos pagamentos efetuados com cartões de débito e de crédito associados a *websites* com material de abuso de menores. **Construção** de capacidades operacionais de tratamento e análise centralizado de informação recolhida no âmbito da prova digital tratada no âmbito dos processos-crime, com posterior disseminação de boas práticas e informação pelas autoridades de IC (nacionais e internacionais), em articulação com a atividade de prevenção criminal. **Construção** de uma base de dados, tutelada pelas autoridades de IC, com material relacionado com o abuso sexual de menores, apreendido nas investigações, transmitidos ou disponibilizados através das TIC, como fotografias, vídeos, e identificação de *website*s, que permitisse, através de análise de dados, identificar vítimas, agressores, recursos do Ciberespaço (locais) e a troca de informações com entidades de IC estrangeiras, designadamente o Eurojust, a Europol e a Interpol. **Comunicação** das referências de *websites* com material de abuso sexual de menores detetadas pela IC aos ISP, às entidades de monitorização de conteúdos no Ciberespaço e entidades financeiras, de forma a operacionalizar o bloqueio e acesso a esses conteúdos, e permitir que as entidades bancárias impeçam o pagamentos através de cartões bancários pela utilização e visualização desse material. Esta divulgação exigiria forte cooperação judiciária internacional em matéria penal, sob pena de os esforços de um país serem manifestamente inúteis, face à ausência de fronteiras no Ciberespaço e a diversidade de jurisdições envolvidas.
FORMAÇÃO E ESPECIALIZAÇÃO: As autoridades judiciárias e os OPC´S devem dominar as técnicas de apreensão, busca e de análise pericial da prova digital, tendo em vista a manutenção da cadeia da custódia da prova, para o que necessitam de formação e, em permanência, de apoio pericial e técnico especializado, em prol da eficácia das investigações.

Apêndice 3

Ações encobertas *on-line*

Breve enquadramento legal

No que concerne à investigação criminal da exploração sexual de crianças no Ciberespaço, o artigo 19.º, alínea b) da LCiber permite o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, relativamente a crimes cometidos por meio de um sistema informático, desde que se verifiquem os seguintes pressupostos:

- o crime sob investigação seja punido, em abstrato, com pena de máximo superior a 5 anos de prisão, ou;
- os crimes sob investigação sejam cometidos de forma dolosa por meio de um sistema informático, contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, apesar de punidos com pena inferior a 5 anos de prisão.

As acões encobertas afiguram-se-nos extremamente relevantes para a identificação dos agentes que cometem violência sexual contra as crianças no Ciberespaço, atenta o anonimato oferecido pelas TIC e a complexidade que este fenómeno encerra, pelo que é relevante efetuar uma breve análise do regime jurídico aplicável a este tipo de método de aquisição probatória e, outrossim, referir aspetos operacionais a observar na realização deste tipo de diligência.

Nos termos do Artigo 1.º, n.º 2 da Lei n.º 101/2001, de 25 de Agosto que regula o regime jurídico das ações encobertas para fins de prevenção e investigação criminal, as ações encobertas são aquelas que são desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sobre o controlo da PJ-Polícia Judiciária, com ocultação da sua qualidade e identidade. Nos termos do Artigo 3.º, n.º 1 do regime jurídico das ações encobertas para fins de prevenção e investigação criminal estas estão sujeitas aos seguintes requisitos:

- devem ser adequadas aos fins de prevenção e repressão criminais identificados em concreto, nomeadamente a descoberta de material probatório e;
- proporcionais quer àquelas finalidades quer à gravidade do crime em investigação.

No que concerne à autorização estatui o Artigo 3.º, n.º 3 que a realização de uma ação encoberta no âmbito de inquérito-crime depende de prévia autorização do competente magistrado do Ministério Público, sendo obrigatoriamente comunicada ao juiz de instrução, considerando-se a mesma validada se não for proferido despacho de recusa nas 72 horas seguintes. No caso de a ação encoberta decorrer no âmbito da prevenção criminal, é competente para a autorização o juiz do Tribunal Central de Instrução Criminal, mediante proposta do Ministério Público junto daquele (Artigo 3.º, n.º 5 da Lei n.º 101/2001), no caso o DCIAP – Departamento Central de Investigação e Ação Penal.

O referido regime jurídico demonstra ainda preocupação quanto à proteção do agente encoberto. Preocupação evidenciada desde logo na parte em que determina que o relato da ação encoberta apenas é junto ao inquérito, nos casos em que a autoridade judiciária o reputar como indispensável em termos probatórios. É também apenas nesse caso (ser reputado absolutamente indispensável) que a lei admite a possibilidade de, a título excecional, e mediante decisão fundamentada, que o agente encoberto seja autorizado a prestar depoimento, preservando a identidade fictícia e beneficiando do regime aplicável à proteção de testemunhas previsto na Lei n.º 93/99, de 14 de julho.

Quanto ao regime da responsabilidade pelos atos praticados pelo agente encoberto prescreve o artigo 6.º que não é punível a conduta do agente encoberto que, no âmbito de uma ação encoberta, consubstancie a prática de atos preparatórios ou de execução de uma infração em qualquer forma de comparticipação diversa da instigação e da autoria, sempre que esteja assegurada a devida proporcionalidade com a finalidade da mesma.

A Lei n.º 144/99, de 31 de Agosto – Lei da Cooperação Judiciária Internacional em matéria penal, estabelece no Artigo 160.º - B da Lei n.º 144/99, de 31 de Agosto, que os funcionários de investigação criminal de outros Estados podem desenvolver ações encobertas em Portugal, com estatuto idêntico ao dos funcionários de investigação criminal portugueses e nos demais termos da legislação aplicável. A ação encoberta depende, neste caso, de pedido baseado em acordo, tratado ou convenção internacional e da observância do princípio da reciprocidade. Nos termos do disposto no n.º 3 do Artigo 160.º-B da referida lei é competente para a autorização o juiz do Tribunal Central de Instrução

Criminal, mediante proposta do Ministério Público junto daquele, no caso do DCIAP – Departamento Central de Investigação e Ação Penal.

Como referimos, as ações encobertas em linha são um dos meios suscetíveis de ser utilizados na investigação criminal relativa à exploração sexual de crianças no Ciberespaço, com vantagens no que concerne à proteção dos investigadores e na redução do risco de aviso aos criminosos, de que estão a ser recolhidos elementos probatórios da sua atividade. Os investigadores podem assumir identidades falsas, quer fazendo-se passar por uma criança quer fingindo que são um agressor sexual, com o objetivo de recolher prova para a investigação em curso.

Porém, apesar da previsão do regime jurídico das ações encobertas para fins de prevenção e investigação criminal, não foram detetados durante a recolha de dados, a utilização deste tipo de método de recolha de prova no âmbito da exploração sexual de crianças no Ciberespaço.

De referir que a Jurisprudência e a doutrina distinguem entre a atuação do agente encoberto e a do agente provocador. O agente provocador será o membro do órgão de polícia criminal ou alguém a seu mando que pela sua atuação enganosa determina eficazmente ao autor a vontade de praticar o crime que antes não tinha representado e o leva a praticá-lo, verificando-se que sem essa intervenção a atividade delituosa não teria ocorrido. A vontade de delinquir surge ou é reforçada no autor, não por sua própria e livre decisão, mas como consequência da atividade de outra pessoa, o membro do órgão policial. ou de terceiro que atua sob direção daquele. O agente infiltrado - polícia ou agente por si comandado - é aquele que se insinua nos meios em que se praticam crimes, com ocultação da sua qualidade, de modo a ganhar a confiança dos criminosos, com vista a obter informações e provas contra eles, mas sem os determinar à prática de infrações. Neste caso, o agente não suscita a infração, introduz-se na organização com o objetivo de descobrir e fazer punir o criminoso, não atuando para dar vida ao crime, antes contribuindo para a sua descoberta.

Face ao caráter intrusivo deste meio de recolha de prova, deve considerar-se que as ações encobertas são um meio de investigação a usar com parcimónia e o modo como se desenvolvem deve ser objeto de aprofundado escrutínio, devendo apenas ter lugar após ter sido efetuado um juízo de *ultima ratio*, à semelhança do que sucede com as interceções telefónicas – o mesmo é dizer que as ações encobertas apenas poderão ser desencadeadas quando existir um juízo fundamentado de que todos os meios de prova tipificados no CPP são manifestamente inúteis e ineficazes para determinada investigação.

Medidas de autoproteção do agente encoberto

As ações encobertas acarretam risco significativo para a vida e integridade física dos investigadores, para as suas famílias, amigos e para as vítimas dos crimes, pelo que este tipo de atividade de investigação e prevenção criminal apenas é desenvolvido a título excecional em relação a crimes graves, complexos e suscetíveis de grande dano social, em que os agentes do crime atuam com grande proficiência, organização e mestria. Nesse sentido, de modo a minorar riscos evitáveis nas ações encobertas no Ciberespaço, é importante que o investigador esteja familiarizado com os mecanismos de ocultação de identidade em linha e do mesmo modo conhecer a estratégia e as ações desenvolvidas pelos criminosos (de modo a evitar que seja detetado e monitorizado pelos agentes do crime).

Da mesma forma, com o objetivo de salvaguardar informação pessoal como o nome, a morada e número de telefone, à semelhança do *modus operandi* utilizado por alguns abusadores, devem ser utilizados endereços IP que não estão ligados aos investigadores encobertos de qualquer forma.

Indicam-se algumas estratégias que os criminosos utilizam para colocar em causa os investigadores, caso seja revelada a sua identidade do agente encoberto:

- Ameaças de morte efetuadas por telefone;
- -Ameaças de morte efetuadas através de comunicações eletrónicas;
- Assédio constante, através de chamadas telefónicas;
- Queixa à inspeção do serviço a que pertencem por má conduta pessoal e profissional;
- Queixas ao Ministério Público e às Autoridade Policiais;
- Vigilância sobre os movimentos do agente encoberto;
- Gravação vídeo dos movimentos do agente encoberto/investigador, mesmo que não esteja de serviço (eg.: encontros familiares, sociais, etc.);
- Envio de imagens do investigador para militantes da organização criminosa;
- Propositura de ações de responsabilidade civil;
- Instigação a grande exposição mediática do investigador por parte dos suspeitos;
- Mensagens de ódio colocadas na Internet, que motivam por sua vez grande quantidade de chamadas telefónicas;
- Cancelamento de reserva de viagens de avião efetuadas pelo investigador, através do computador;

- Elaboração de dossiers extensíssimos sobre os investigadores e as testemunhas, incluindo informação digital com o nome, a morada, a identidade do cônjuge ou familiar, a data e local de nascimento, ações cíveis, descrição do veículo e número da carta de condução, com difusão dessa informação em websites e na comunicação social;
- Colocação à venda de casas de testemunhas, com envio pelos suspeitos da conta do anúncio da venda para a testemunha pagar;
- As testemunhas recebem na sua residência produtos que não encomendaram, com cartas ameaçadoras por parte dos suspeitos;
- Envio de centenas de convites por computador para uma festa de aniversário ou para um churrasco em casa da testemunha.[24]

Deste modo, quem efetua o trabalho de agente encoberto deve seguir um conjunto de regras preestabelecidas num *protocolo de atuação*, e assegurar-se de que estão preparadas e criadas e condições que lhe permitam defender-se a nível legal, profissional e pessoal de eventuais ataques dos suspeitos ou da organização criminosa[25].

Assim, o investigador encoberto nunca deve fornecer informação pessoal, deve ter apoio legal disponível e o apoio dos seus superiores hierárquicos, de forma a evitar ser um alvo para o criminoso, quando este for preso. Torna-se assim necessário que o investigador, quando atua com ocultação da sua qualidade, construa uma identidade totalmente nova, cuidando que não utiliza a identidade de uma pessoa real.

Utilização de equipamento pessoal

É extremamente relevante que o investigador, quando atua ocultando a sua qualidade e identidade em linha, não utilize o seu equipamento pessoal quando desenvolve a sua atividade, uma vez que tudo o que fizer no decurso da investigação é suscetível de ser descoberto mais tarde. Sobretudo nas investigações encobertas em linha, em que há necessidade de utilizar um computador e uma ligação à Internet, é fator de risco elevado utilizá-lo para enviar mensagens de correio eletrónico privadas, aceder ao sistema de

[24] Council of the Inspectors General on integrity and efficiency - Guidelines on Undercover Operations. 2010.

[25] Nos termos do Artigo 6.º (isenção de responsabilidade) da Lei n.º 101/2001, de 25 de Agosto, 1 - Não é punível a conduta do agente encoberto que, no âmbito de uma ação encoberta, consubstancie a prática de atos preparatórios ou de execução de uma infração em qualquer forma de comparticipação diversa da instigação e da autoria mediata, sempre que guarde a devida proporcionalidade com a finalidade da mesma. 2 - Se for instaurado procedimento criminal por ato ou atos praticados ao abrigo do disposto na presente lei, a autoridade judiciária competente deve, logo que tenha conhecimento de tal facto, requerer informação à autoridade judiciária que emitiu a autorização a que se refere o n.º 3 do artigo 3.º

"*homebanking"*, efetuar pesquisas e, inclusive, ver pornografia, pois tais atividades podem ser facilmente detetadas pelos suspeitos e colocar em causa a credibilidade do investigador e da prova recolhida depois no inquérito.

De referir, que nem todas as autoridades policiais têm os recursos necessários para efetuar operações encobertas em linha, pelo que se deve assegurar a aquisição e manutenção dessas capacidades antes de se iniciar uma ação encoberta em linha.

Acresce que algumas organizações pretendem exercer a função de *"watchdog"* no que concerne à pornografia infantil e ao abuso sexual de crianças no Ciberespaço, o que pode conduzir a becos sem saída em termos de aquisição de prova, sendo certo que a prova recolhida por esses meios, subtraída a um controlo judiciário legalmente definido, terá pouco ou nenhum valor em Tribunal, existindo, inclusive, a possibilidade de que essas práticas, certamente bem-intencionadas, possam acarretar consequências criminais para os seus autores

De notar, que ao evitar-se o envolvimento do computador pessoal num caso de investigação criminal, utilizando-se equipamento dos Órgãos de Polícia Criminal ou do Ministério Público, especialmente adquirido e preparado para o efeito, com ligações seguras e limitações de acesso, existe maior benefício para a deteção de indícios da atividade delituosa, assegurando-se a manutenção da cadeia de custódia da prova, por não-contaminação com outras atividades em linha, não relacionadas com a investigação. Efetivamente, todas as comunicações efetuadas em linha, todas as sessões em linha na Internet e, bem assim, ficheiros acedidos são suscetíveis de constituir prova e que toda essa informação poderá ser auditada ou objeto de perícia, e consequentemente avaliada e validada pelas Autoridades Judiciárias, com a inerente sujeição ao contraditório legal por parte dos suspeitos.

Preparação das ligações de Internet e do telefone de contacto

No âmbito das ações encobertas em ambiente digital é necessário assegurar que as ligações de Internet e o telefone de contato não sejam suscetíveis de ligação à identidade real do investigador. No caso de o suspeito pretender contactar o investigador durante as ações encobertas, não lhe poderão ser facultado os contactos telefónicos do agente, do seu local de trabalho ou da sua casa pessoal. É necessário utilizar um telefone seguro, que não permita que o suspeito efetue trabalho de pesquisa que lhe permita identificar o agente, a família deste ou os seus amigos. Utilizando-se um telefone de serviço é necessário assegurar que o número se não encontra registado em nome do OPC encarregue da investigação ou de outra instituição oficial que, enquanto tal, possa ser facilmente

identificada, alertando o suspeito sobre a ocultação da identidade e da qualidade da pessoa com quem estabelece conversação. O suspeito para tentar identificar a identidade real da pessoa com quem está a conversar em linha pode sempre efetuar pesquisas na Internet de nomes e números de telefone, pelo que é desaconselhável indicar contactos relacionados com a Polícia, com o Ministério ou com os Tribunais.

No que concerne às ligações de Internet utilizadas mas ações encobertas é necessário garantir que o suspeito não possa proceder à identificação do investigador criminal através de obtenção de dados junto da empresa fornecedora de serviços de Internet. Se for necessário utilizar contas de Internet pessoais ou institucionais é necessário pedir especificadamente ao ISP para não fornecer qualquer tipo de informação sobre os dados desta.

É igualmente necessário garantir métodos de pagamento não rastreáveis (eg.: cartões de crédito, contas bancárias e ordens de transferência com ocultação da verdadeira qualidade e identidade), linhas telefónicas com ocultação do número de ligação e locais para receber correspondência de forma anónima (eg.: apartados dos correios), garantindo-se, ao mesmo tempo, que informação pessoal sobre a identidade real na Internet não é detetada através de visitas a sítios web que tentam capturar esse tipo de informação.

Ocultação da identidade *on-line*

Apesar de as ações encobertas *on-line* serem dispendiosas e exigirem muito tempo e dedicação à investigação criminal, são muito úteis no caso de inexistirem outras alternativas de investigação – é o caso, por exemplo, de o anonimato ser um obstáculo à identificação do suspeito ou quando for necessário confirmar uma informação ou uma ligação de um indivíduo em concreto a uma atividade no Ciberespaço.

É necessário utilizar um computador dedicado à ação encoberta com a capacidade em termos aplicacionais de registar permanentemente todas as atividades desenvolvidas e capturar o ambiente em linha. No caso de ser utilizado apenas um computador para operar várias ações encobertas é necessário utilizar discos externos portáteis de forma a evitar a transferência de dados de provas e identidades fictícias entre vários processos.

De igual modo, é necessário utilizar serviços de ligação à Internet e outros serviços disponibilizados que garantam a ocultação de dados verdadeiros sobre o agente encoberto e ter especiais cautelas com a divulgação de informações através de trocas de arquivos (por exemplo: documentos do Word com informações de registo internas ao OPC ou ao Ministério Público), quer seja através da Internet ou de trocas de correio eletrónico / e-mail. De notar, que as aplicações Java e certos componentes do ActiveX podem ser

executados no computador sem o utilizador se aperceber e podem divulgar uma ligação, o endereço IP real e outras informações que podem conduzir à revelação da identidade do investigador encoberto, com sérios prejuízos para este, para as vítimas e para a investigação.

Aspetos operacionais a considerar numa investigação em linha

Se o objetivo da ação encoberta é o de recolher indícios que confirmem ou infirmem a participação de determinado suspeito na exploração sexual de crianças no Ciberespaço através de contacto em salas de conversação virtuais é prudente verificar, de antemão, se os mecanismos de gravação e de recolha de outros dados estão a funcionar corretamente.

De igual modo é necessário efetuar trabalho de pesquisa prévia sobre o suspeito, no que respeita aos seus interesses, códigos de conversação, locais e temas de interesse, interesses literários, o que procura nas suas vítimas, entre outros aspectos relevantes que permitam conhecer a sua personalidade – quanto mais informação existir sobre o suspeito e sobre eventuais indivíduos ou grupos com que se relaciona, maiores serão as probabilidade de êxito de recolha da prova. Caso inexista empatia ao nível da linguagem utilizada na conversação, os suspeitos não vão confiar no agente encoberto e rapidamente o excluem da conversação.

Adicionalmente deverão ser treinadas e simuladas o maior número de contingências possíveis e ter definidas regras de atuação para o caso de o suspeito pretender, por exemplo, contactar telefonicamente com o investigador - quem receber a chamada deve estar preparado para responder sobre determinada informação biográfica do investigador encoberto e sobre a conversação mantida com o suspeito. Do mesmo modo, não é de descurar a eventual interceção de comunicações no inquérito propriamente dito, mediante autorização prévia do Juiz de Instrução Criminal, nos termos e para os efeitos do disposto no Artigo 187.º, n.º 1 do CPP.

É de considerar manter com o suspeito contacto através de correio eletrónico, no sentido de capturar os cabeçalhos das mensagens e detetar a sua localização através do IP.

De qualquer modo, é de ter em conta que não é possível no âmbito de acção encoberta enviar imagens de pornografia de menores ou aceder remotamente a um computador, mas apenas e só, neste último caso, no decurso do inquérito, uma vez cumpridas as formalidades legais, ou seja com autorização do Juiz de Instrução Criminal mediante promoção no processo pelo Ministério Público.

Algumas regras essenciais a observar nas ações encobertas

Uma vez que as CMC facilitam a exploração sexual de crianças no Ciberespaço, os investigadores criminais, os magistrados judiciais e do Ministério público debatem-se com novos desafios no que concerne ao estabelecimento de boas práticas ou *guidelines* a observar no âmbito da atuação com ocultação da identidade e qualidade do agente. Embora esta seja uma matéria em constante evolução, até pelo meio cibernético em que este tipo de ações se desenvolvem, em constante mutação e desenvolvimento, importa procurar indicar algumas regras base a observar neste tipo de diligência probatória, uma vez que a fronteira entre as investigações encobertas e a provocação para a prática de crime é muito ténue.

Face à sensibilidade e grau de intrusão que as ações encobertas podem alcançar, bem assim o perigo real que existe para a vida, a tranquilidade e integridade física quer dos investigadores quer das crianças vítimas, importa tentar elencar regras procedimentais de atuação geral, que preservem o anonimato dos investigadores e das crianças, relativamente a organizações que se dediquem a este tipo de práticas, identificando-se as seguintes regras:

- Omissão de comportamentos ou atos que não sejam suscetíveis de ser documentados ou relatados perante as Autoridades judiciárias, perante o defensor do suspeito ou em sede de julgamento;
- Proibição de envio de pornografia de menores, pornografia entre adultos, imagens com conteúdo erótico, fotografias do investigador ou de crianças através da Internet ou por qualquer outro meio;
- Obrigação de registar todas as actividades em linha, com indicação da data e hora. É essencial nestes casos que exista uma documentação completa e precisa do que for acontecendo durante a investigação;
- Proibição de trabalhar a partir de casa ou com utilização do computador pessoal;
- Facultar a liderança da comunicação ao suspeito;
- Avaliar as ameaças e as oportunidades de um encontro pessoal com o suspeito, em termos de aquisição da prova;
- No caso de descobrir que o suspeito está sujeito a outra jurisdição internacional, remeter imediatamente o caso ou promover articução com autoridades de IC estrangeiras.[26]

[26] OFFICE of the Attorney General, Washington D.C., USA, - **The Attorney´s General Guidelines on Federal Bureau of Investigation Undercover Operations**. [Em Linha] [Consult. 2012-07-12]. Disponível em WWW: <URL: http://www.fas.org/irp/agency/doj/fbi/fbiundercover.pdf>

Apêndice 4

Breve incursão sobre o abuso sexual de crianças no Código Penal

Abuso Sexual de crianças com idade inferior a 14 anos

Nos termos do disposto no Art. 171.º, n.º 1 do CP *"quem praticar ato sexual de relevo com ou em menor de 14 anos, ou o levar a praticá-lo consigo ou com outra pessoa, é punido com pena de prisão de 1 a 8 anos"*, estabelecendo o n.º 2 do referido preceito normativo que *"se o agente tiver cópula, coito anal ou coito oral com menor de 14 anos é punido com pena de prisão de 3 a 10 anos"*. O bem jurídico protegido pela norma incriminadora consiste na proteção da autodeterminação sexual das crianças menores de 14 anos, uma vez que se presume que tais condutas sobre as vítimas daquela idade prejudicam gravemente o seu desenvolvimento e personalidade. Este tipo de crime configura-se, assim, como um crime de perigo abstrato,[27] uma vez que não se exige a verificação do referido prejuízo do desenvolvimento para a personalidade para que o crime seja considerado consumado.

O CP prevê igualmente como tipo legal de ilícito a prática de atos sexuais efetuados perante menor ou na atuação sexual sobre ele, independentemente de o seu corpo ser tocado. Assim, dispõe o n.º 3 do referido preceito normativo que é punido com pena de prisão até 3 anos quem: i) importunar menor de 14 anos, praticando o ato previsto no Art. 170.º[28] ou ii) atuar sobre menor de 14 anos, por meio de conversa, escrito, espetáculo ou objeto pornográfico. Agrava a sua conduta se o agente praticar os atos atrás descritos com intenção lucrativa, caso em que é punido com pena de prisão de (6) seis meses a (5) cinco anos, nos termos do disposto no n.º 6 do Art. 171.º do CP.

O espetáculo, o escrito, a conversa são pornográficos quando são idóneos a excitar sexualmente a criança, tendo-se em conta o seguinte:

[27] ALBUQUERQUE, Paulo Pinto de – Comentário do Còdigo Penal à luz da Constituição da República e da Convenção dos Direitos do Homem, p. 534.
[28] Refere o Art.º 170.º do Código Penal que é punido com pena de prisão até um ano ou com pena de multa até 120 dias "quem importunar outra pessoa praticando perante ela atos de carácter exibicionista ou constrangendo-a a ato de natureza sexual (…), se pena mais grave lhe não couber por força de outra disposição legal".

- a conversa pornográfica materializa-se na troca de palavras mantidas pelo agente com a criança ou com terceiro diante da criança de modo adequado a excitar sexualmente a vítima;
- o escrito pornográfico é o texto redigido de modo adequado a excitar sexualmente a criança. O texto deve ser elaborado em língua compreendida pela criança, podendo ser lido ou dado a ler à criança. O texto pode ser redigido pelo agente ou por terceiro sendo irrelevante o suporte (papel ou informático) em que se encontra fixado;
- o espetáculo pornográfico é o encontro de várias pessoas com vista a presenciar ou intervir em ato adequado a excitar sexualmente a criança. O espetáculo não tem de ser público, nem remunerado, sendo suficiente que decorra aberto a espectadores, isto é, a terceiros que apenas têm o propósito de assistir ao cto. O espetáculo pode ser visual ou sonoro, como é o caso das *hotlines* - o agente pode intervir no espetáculo ou ser mero espectador ou ouvinte;
- o objeto pornográfico é a coisa idónea a excitar sexualmente a vítima. O objeto pode ser um desenho, uma fotografia, um filme ou uma gravação de som ou qualquer outro objeto. A atuação sobre a criança com objeto pornográfico consiste na exibição do objeto à criança, sem que o agente tenha contacto com o corpo da criança. Com efeito, a situação de atuação sobre o corpo da criança com objeto pornográfico é mais grave: constitui ato sexual de relevo punível nos termos do disposto no Art. 171.º, n.º 1 do CP, e quando houver introdução vaginal ou anal do objeto pornográfico pela criança no agente ou pelo agente na criança, a conduta em apreço é subsumível à previsão do Art. 171.º, n.º 2 do CP (abuso sexual).[29]

Abuso Sexual de crianças dependentes com idade entre os 14 e os 18 anos

Dispõe o Art. 172.º, n.º 1 do CP que *"quem praticar ou levar a praticar"* ato sexual de relevo, cópula, coito anal, coito oral ou introdução vaginal ou anal de partes do corpo ou objetos, relativamente a menor entre 14 e 18 anos, que lhe tenha sido confiado para educação ou assistência, é punido com pena de prisão de (1) um a (8) oito anos. Se as condutas acima descritas se referirem a importunação de menor ou atuação sobre menor entre 14 e 18 anos dependente o agente é punido com pena de prisão até (1) um ano, vendo agravada a sua conduta se atuar com intenção lucrativa, uma vez que tal conduta passa a

[29] ALBUQUERQUE, Paulo Pinto de – Comentário do Còdigo Penal à luz da Constituição da República e da Convenção dos Direitos do Homem. p. 536 a 543.

ser punido com pena de prisão até (3) três anos ou multa, conforme os termos do disposto nos n.ºs 2 e 3 do Art. 172.º do CP. O bem jurídico protegido pela incriminação é a liberdade de autodeterminação sexual do menor entre 14 e 18 anos.

O tipo objetivo consiste na prática consensual de ato sexual de relevo com menor (incluindo a cópula, coito anal, o coito oral e a introdução vaginal), de importunação sexual de menor ou de atuação sobre menor por meio de conversa, escrito, espetáculo ou objeto pornográficos. A especialidade da incriminação do Art. 172.º reside na confiança do menor para educação ou assistência ao agente. A confiança do menor pode resultar da lei, de decisão judicial, de contrato ou de relação de facto, ou seja, inclui todas aquelas pessoas a quem o menor tenha sido entregue para educação ou assistência médica ou social, desde que inexista internamento do menor.[30]

Abuso Sexual de crianças com idade entre os 14 e os 16 anos

Nos termos do disposto no n.º 1 do Art. 173.º do CP *"quem, sendo maior, praticar ato sexual de relevo com menor entre 14 e 16 anos, ou levar a que ele seja praticado por outrem, abusando da sua inexperiência, é punido com pena de prisão até dois anos ou com pena de multa até 240 dias"*, estatuindo o n.º 2 do referido preceito normativo que *"se o ato sexual de relevo consistir em cópula, coito oral, coito anal ou introdução vaginal ou anal de partes do corpo ou objetos, o agente é punido com pena de prisão até três anos ou com pena de multa até 360 dias"*. O bem jurídico protegido pela incriminação é a liberdade de autodeterminação do adolescente (menor entre 14 e 16 anos de idade) em face de um processo fraudulento e enganoso de sedução utilizado pelo agente. O crime em apreço é um crime específico próprio uma vez que a ação só é punível se for praticada por pessoa maior de idade. O abuso da inexperiência consiste na exploração, pelo agente da falta de experiência de vida do adolescente e, designadamente, da falta de conhecimento básico sobre a vida sexual. Para apurar a inexperiência deve ter-se em conta o nível de maturidade, a condição psíquica e o grau educacional da vítima.

Pornografia de menores

Nos termos do disposto no Art. 176., n.º 1º do CP quem: i) utilizar menor em espetáculo pornográfico ou o aliciar para esse fim; ii) utilizar menor em fotografia, filme ou gravação pornográficos, independentemente do seu suporte, ou o aliciar para esse fim; iii) produzir, distribuir, importar, exportar, divulgar, exibir ou ceder, a qualquer título ou por qualquer meio, os materiais previstos na alínea anterior; iv) adquirir, ou detiver materiais previstos

[30] Existindo internamento a conduta típica é subsumível aos termos do disposto no Art.º 166.º do CP.

na alínea b) com o propósito de os distribuir, importar, exportar, divulgar, exibir ou ceder; é punido com pena de prisão de (1) um a (5) cinco anos.

Nos termos do n.º 2 do referido preceito normativo, caso os atos acima descritos sejam praticados com intenção lucrativa ou profissionalmente o agente é punido com pena de prisão de (1) um a (8) oito anos.

Nos termos do n.º 3 do referido preceito normativo quem praticar os atos descritos profissionalmente e com intenção lucrativa utilizando material pornográfico com representação realista do menor é punido com pena de prisão até 2 anos.

Nos termos do disposto no n.º 4 do Art. 176.º quem detiver fotografia, filme ou gravação pornográficos de menos menor, independentemente do seu suporte é punido com pena de prisão até um (1) ano ou com pena de multa.

Esta disposição inclui deste modo quatro crimes distintos:

- a utilização de menor de 18 anos em espetáculo, fotografia, filme ou gravação pornográficos;
- a produção, a distribuição, a importação, a exportação, a divulgação, a exibição, a cedência de materiais pornográficos de menor de 18 anos;
- a aquisição ou detenção de materiais pornográficos com o propósito de distribuir, importar, exportar, divulgar, exibir ou ceder esses materiais de menor de 18 anos;
- a aquisição ou detenção de materiais pornográficos de menor de 18 anos.

Na ausência de indícios sobre o autor ou autores dos atos retratados no material (abuso sexual em sentido próprio) que circula no Ciberespaço a que se associa a dificuldade de identificação das vítimas, intui-se que este tipo de ilícito será o que com maior frequência será objeto da IC em Portugal, no que concerne à exploração sexual de crianças no Ciberespaço.

Apêndice 5

Preservação da Prova Forense digital

Uma vez finalizada a perícia informática forense sobre dados digitais e face ao decurso do tempo para a conclusão dos processos-crime, que podem ter delongas de vários anos (desde que se inicia a investigação até decisão do Tribunal Constitucional), e não obstante o relatório pericial ser atualmente efetuado em suporte papel e junto ao respetivo processo-crime, é de considerar tomar medidas de preservação digital da informação apreendida, que fundamentam e suportam as conclusões da perícia.

Com efeito, a rápida taxa de obsolescência tecnológica, inerente à indústria informática, levanta problemas críticos de preservação de informação, operacionalmente indispensável aos inquéritos crimes no âmbito das perícias informáticas forenses realizadas, caso estes tenham um longo período de pendência - considera-se que o período é longo quando ultrapassar 7 anos, de acordo com recomendações da DGARQ – Direção Geral de Arquivos. [31]

Deste modo, a preservação digital pode ser definida como o conjunto de atividades ou processos responsáveis por garantir o acesso continuado a longo prazo à informação existente em suportes digitais. Consiste na capacidade de garantir que a informação digital permanece acessível, com capacidade probatória, de modo a ser interpretada no futuro, assegurando a manutenção do conteúdo intelectual, forma, estilo, aparência e funcionalidade dos dados.

Tendo em conta o tipo de dados tratados nas perícias informáticas forenses no âmbito da exploração sexual de crianças no Ciberespaço, a temática a preservação digital assume-se assim como requisito a considerar no âmbito da Segurança da Informação dos dados, em termos de confidencialidade, integridade, autenticidade e disponibilidade:

- a *confidencialidade*, traduz-se na implementação de uma política de gestão de perfis de acesso, nos termos da qual só acede à informação de um inquérito crime quem tem

[31] Barbedo, Francisco, et al. – Recomendações para a produção de planos de preservação digital - DGARQ – Direcção Geral de Arquivos, p. 17, 2011.

legitimidade e necessidade em termos organizacionais e funcionais, ou seja, no caso de terceiros ao processo, mediante despacho prévio de autorização da autoridade judiciária – Artigo 89.º do CPP;

- a *integridade* assegura que o conteúdo da informação produzida não foi alterado de forma propositada ou acidental;

- a *disponibilidade* assegura o acesso à informação produzida sempre que necessário, que permita eliminar em tempo útil a informação que já não é necessária às investigações, designadamente pelo decurso do tempo ou por esta já não ser necessária por extinção do procedimento criminal;

- a *autenticidade* da informação eletrónica permite identificar inequivocamente o responsável pela sua produção, o propósito e em que termos esta foi produzida e o controlo exclusivo por parte do possuidor ou possuidores dessa informação.

Constata-se, assim, que o armazenamento de documentos de arquivo eletrónicos relativos a perícias informáticas forenses requer uma planificação adicional e a definição de estratégias que previnam a sua perda, implementando-se:

a) Sistemas de salvaguarda de dados (backup) que se traduzem num método de copiar documentos eletrónicos, de valor idêntico aos originais, que previne a sua perda em caso de falhas de hardware ou de software. É conveniente que estes sistemas incluam um plano que preveja a execução regular de cópias, a realização de cópias múltiplas em diferentes suportes, o armazenamento disperso das cópias obtidas e a garantia do acesso rotineiro e urgente às cópias;

b) Procedimentos de manutenção para prevenir danos físicos no suporte – as imagens da informação apreendida podem necessitar ter que ser copiadas para versões mais recentes do mesmo suporte (ou para outros novos suportes) no sentido de prevenir a corrupção dos dados – de notar, que a desatualização do hardware e software pode afetar a capacidade de interpretar os documentos eletrónicos.[32]

Assim, os suportes digitais apreendidos, tendo em conta as necessidades de preservação da prova, apenas devem ser entregues aos arguidos ou aos proprietários dos suportes digitais, após o *terminus* do processo, ou seja, com o trânsito em julgado da decisão de julgamento, ou na impossibilidade de o Ministério Público reabrir o inquérito caso surjam novos elementos de prova, nos termos do disposto no Artigo 279.º, n.º 1 do CPP e desde que não tenham sido instrumento da prática de crime, o que, em principio não se configura

[32]NP – Norma Portuguesa 4438 - Informação e documentação, Gestão de Documentos de Arquivo, Parte 2: Recomendações de Aplicação.

na exploração sexual de crianças no Ciberespaço, uma vez que os dispositivos digitais, contendo material de abuso sexual de menores integram o conceito de instrumento para a prática de crime.

As estratégias de preservação da informação digital mais comuns são as seguintes:

a) *preservação de tecnologia* – exige a conservação e manutenção de todo o software e hardware necessários à correta apresentação da informação digital;

b) *emulação* – corresponde à utilização de um software – o *emulador* – capaz de reproduzir o comportamento de um programa informático que, à partida, seria incompatível;

c) *monitorização de suportes e formatos* – prevê processos de verificação automática, manual e semiautomática da informação digital;

d) *encapsulamento* – consiste em preservar, juntamente com o objeto digital, toda a informação necessária e suficiente para permitir o futuro desenvolvimento de conversores, visualizadores ou emuladores (por exemplo, a descrição formal e detalhada do objecto preservado);

e) *transposição de formatos e suportes* (Migração e transferência de suportes) – refere-se à transferência de informação contida num determinado suporte ou formato para outro suporte ou formato mais atualizado. O principal objetivo desta estratégia é evitar a obsolescência tecnológica, mantendo a informação compatível com as novas tecnologias que surjam, de forma a permitir a sua interpretação sem necessidade de recorrer a técnicas não convencionais.

Apesar de se encontrarem referenciadas algumas desvantagens quanto à Migração e transferência de suportes, por questões de segurança, deve optar-se por esta metodologia de preservação digital dos dados apreendidos e dos relatórios das perícias informáticas forenses realizadas, por ser a técnica mais aplicada até à data e a única que tem vindo a dar provas da sua eficácia, no que concerne às estratégias de preservação digital mais utilizadas.[33]

[33]Barbedo, Francisco - A Preservação Digital na AP – O Papel do Órgão de Gestão da Política Arquivística Nacional.