A INVESTIGAÇÃO CRIMINAL NA *DARK WEB*[1]

David Silva Ramalho

Abstract: *The rise of technologies aimed at guaranteeing a satisfactory level of anonymity in Web browsing brought forth a type of software which allows Internet users to reach the Deep Web. The advantages of these tools were quickly spotted by cybercriminals and used for malicious purposes in the Dark Web. The present study intends to explain the origins and concept of the Dark Web, as well as to analyse the effectiveness of the legal mechanisms provided by Portuguese Law to respond to these new challenges and ultimately to present some tools which may be useful to counter this type of cybercrime.*

INTRODUÇÃO

Nas primeiras horas do dia 14 de outubro de 2011, o grupo "hacktivista"[2] autointitulado *Anonymous*[3] deu início a um ataque informático, a que chamou

1 O trabalho que ora se apresenta corresponde fundamentalmente ao relatório de mestrado em Ciências Jurídico-Criminais, apresentado na Faculdade de Direito da Universidade de Lisboa, no ano letivo de 2011/2012, no âmbito da disciplina de Direito Processual Penal, sob a regência do Senhor Professor Doutor Paulo de Sousa Mendes, e encontra-se atualizado com elementos factuais e bibliográficos até Outubro de 2012.

2 O termo hacktivism (que resulta da fusão dos termos hacking e activism), apesar de ter sido cunhado em 1996 pelo grupo Cult of the Dead Cow, apenas veio a popularizar-se na segunda metade da primeira década de 2000, tendo vindo a ganhar especial destaque na comunicação social, por via dos ataques

Operação *Darknet*, direcionado ao fornecedor de serviços *Freedom Hosting*, com os propósitos concretizados de tornar inoperacionais cerca de 40 *websites* dedicados à difusão de pornografia infantil – entre os quais o *website Lolita City*, cujo conteúdo se estimava rondar os 100 *Gigabytes*[4] – e de divulgar os *usernames* de vários dos seus utilizadores[5].

Com a informação obtida naquele primeiro ataque[6], os *Anonymous* iniciaram uma investigação privada que consistiu, em grande medida, na pesquisa, em motores de busca, redes sociais e outros *websites* de caráter e conteúdo lícitos, de *usernames* idênticos aos extraídos dos *websites* alojados no *Freedom Hosting*, de modo a aferir se, em ambos os casos, o utilizador era o mesmo.

Com base na informação recolhida, os *Anonymous* anunciaram, no dia 19 de maio de 2012, a conclusão da operação *Darknet V2*, publicando uma lista com informação pessoal dos utilizadores dos *websites* pedo-pornográficos[7] atacados na primeira versão daquela Operação, designadamente o seu nome, profissão, localização, idade, tipo de equipamento informático com que acediam à Internet, preferências de jogos *online*, endereço IP[8] e/ou endereço de correio eletrónico.

---

informáticos perpetrados pelos conhecidos grupos Anonymous e LulzSec. Apesar de o significado do termo não ser unânime, diríamos que o hacktivism consiste no ato de manifestação política/ideológica ocorrida em ambiente digital com recurso a meios técnicos de informática, traduzida no exercício da ação direta, isolada ou concertada, sobre alvos percecionados como, pelo menos parcialmente, responsáveis por uma conduta ou pela criação de um estado de coisas tido como errado, injusto ou imoral à luz das crenças, ideologia ou padrões de moralidade e idoneidade do agente ou do conjunto de agentes participantes.

3 Para uma análise mais detalhada do fenómeno do *hacktivism*, em particular no que concerne ao grupo *Anonymous*, Hampson, 2012: 511-542. Para uma abordagem mais crítica e com especial incidência no fenómeno do *hacktivism* no panorama português, Esteves, 2012: 45-47.

4 Para visualizar os *printscreens* do fórum *Lolita City* divulgados pelos *Anonymous* com os relatos feitos por alguns dos utilizadores daquele *website* acerca das suas atividades sexuais com menores (cujo teor, advertimos desde já, é altamente gráfico e obsceno), Chen, 2011.

5 Para aceder aos 1589 *usernames* divulgados no âmbito desta operação, cf. «*#OpDarknet – Lolita City user dump*», disponível em: <http://pastebin.com/88Lzs1XR> [consultado em: 03.06.2012].

6 Para uma informação mais detalhada do procedimento utilizado para obter a informação pretendida no primeiro ataque, cf. http://pastebin.com/hquN9kg5 [consultado em: 14.09.2012].

7 A referida lista encontra-se disponível em <http://pastehtml.com/view/bykt95v1j.html [consultado em: 03.06.2012].

8 O endereço IP é um código de identificação numérico designado a cada aparelho ligado a uma rede de comunicações eletrónicas num dado momento, comparável a uma morada ou a um número de telefone. Em abstrato, tendo conhecimento do endereço IP e do momento exato em que a ligação à rede foi estabelecida, torna-se possível a um fornecedor de serviço descobrir os dados pessoais do indivíduo que subscreveu o contrato de prestação de serviços que permitiu o acesso à Internet através daquele local. Os endereços IP podem ser estáticos – isto é, manualmente designados a um dispositivo de forma permanente pelo administrador – ou dinâmicos – isto é, atribuídos quer por via do *software*, quer por via de um servidor, designadamente no momento de cada conexão. É este último o que se verifica com mais frequência. – cf. Vaciago, 2012a: 32, 36-37.

O que distingue a Operação *Darknet* (em particular a sua primeira versão) dos restantes ataques informáticos e a torna de especial interesse para o presente estudo é precisamente o facto de ter visado uma área da Internet até então relativamente desconhecida: a *Dark Web*. Um lado da *Web* dedicado à cibercriminalidade, no qual a deteção dos utilizadores se revela potencialmente inviável e cujo acesso é, em geral, limitado àqueles que instalam um *software* específico, como o *Freenet*, o *The Onion Router* ou o I2P[9].

Com a incursão da cibercriminalidade num domínio mais profundo da Internet, no qual a navegação é livre, tendencialmente anónima, cifrada e potencialmente indetetável, multiplicam-se os desafios que a investigação criminal já encontra no domínio da Internet. É neste contexto que nos propomos explicar e analisar o fenómeno da *Dark Web*, procurando identificar os principais problemas que aí se suscitam no âmbito da recolha de prova penal digital, analisando-os do ponto de vista do direito constituído e procurando apresentar alguns meios de resposta que, embora muito longe de serem infalíveis, podem representar um meio apto a reduzir as cifras negras que se verificam neste tipo de criminalidade.

Cumpre, porém, deixar, desde já, a advertência de que, face à escassa atenção que esta matéria tem recebido por parte da doutrina e à inexistência de unanimidade quanto aos conceitos que adiante se tratarão, a terminologia aqui adotada resulta de certas opções metodológicas que, não sendo destituídas de controvérsia, se afiguram adequadas a delimitar adequadamente as realidades em apreço e a minorar as sobreposições conceituais.

I. A *DEEP WEB* E A *DARK WEB*

1. A *Deep Web* e a *Surface Web*

Para uma correta compreensão do fenómeno da *Dark Web*, é necessário começar por distinguir e definir os conceitos de *Surface Web* e de *Deep Web*, também conhecida como *Invisible Web* ou *Hidden Web*[10].

A *Surface Web* pode ser definida como a parte da Internet que é geralmente acessível através dos motores de busca, como sejam o *Google*, o *Bing* ou o *Yahoo!*,

9 Não nos debruçaremos sobre o programa I2P – também chamado de *Invisible Internet Project* – no âmbito do presente trabalho por o mesmo não trazer especificidades práticas de relevo e por a sua utilização ser significativamente menos comum.

10 A terminologia foi inicialmente introduzida por Michael K. Bergman, embora, segundo este autor, tenha sido Jill Ellsworth quem, em 1994, cunhou o termo *Invisible Web*, Bergman, 2001: 1-17.

isto é, será o conjunto de páginas detetadas e escolhidas pelos motores de busca para integrarem os resultados de uma pesquisa[11]. Por outro lado, a *Deep Web* será aquela área da Internet que não é acessível através dos motores de busca e que é composta, entre outras, por páginas que poderão ter sido propositadamente excluídas dos resultados de pesquisas efetuadas em motores de busca[12]; por páginas cifradas ou cujo acesso depende da introdução de uma palavra-passe, como *webmails* ou páginas de *Instant Messaging*, por páginas para as quais nenhum *link* exterior remete (e que, portanto, não são detetadas pelos *crawlers*[13] dos motores de busca), bem como por páginas geradas de forma dinâmica[14] ou simplesmente invisíveis para um motor de busca, designadamente por serem compostas por ficheiros em formato *script* (como *JavaScript* ou *Flash*) ou em formato não-HTML (alguns ficheiros PDF[15], imagens, etc.).

Apesar de inexistirem dados recentes que permitam, com algum rigor, conhecer a exata e atual dimensão de ambas as *Webs*, sabemos que, em 2001, a *Deep Web* tinha uma dimensão que se estimava ser entre 400 a 550 vezes superior à da *Surface Web*[16] (sem contar com *webmails* e *Instant Messaging*) e continuava a crescer a um ritmo superior a esta. Embora parte desse conteúdo seja absolutamente irrelevante, a verdade é que uma grande parte da *Deep Web* é

11 He et al., 2007: 94-101.

12 Para uma explicação sintética do funcionamento dos motores de busca, cf. Sherman & Price, 2007: 282-298.

13 Os *crawlers* são, em síntese, programas informáticos que visam detetar e analisar um conjunto de páginas da Internet e cujo funcionamento se traduz na procura automatizada de *links*, em cada página analisada, que remetam para outras páginas, de modo a que, por via da repetição deste processo, se indexe o maior número possível de páginas interligadas. A repetição deste procedimento por várias páginas da Internet permitirá indexá-las aos motores de busca e torná-las acessíveis no âmbito de uma pesquisa aí efetuada. Existem, contudo, várias especificidades que cada motor de busca pode dar aos seus *crawlers* de modo a que certas páginas apareçam antes de outras ou a que certas páginas não apareçam de todo, Najork, 2009: 3462.

14 As páginas da Internet geradas de forma dinâmica são aquelas que são geradas no momento do acesso por parte do utilizador ou que se modificam em consequência da interação com o utilizador. Por exemplo, as páginas geradas no âmbito de uma pesquisa de um catálogo de uma biblioteca *online* e que surgem apenas para dar resposta aos critérios de pesquisa introduzidos pelo utilizador. Em 2003 estimava-se que haveria 100 vezes mais páginas dinâmicas do que as chamadas páginas estáticas, Handschuh, Volz &Staab, 2009: 42.

15 Embora o Google já consiga, em grande parte dos casos, indexar às suas pesquisas o conteúdo de alguns ficheiros PDF, Casey, 2011: 688.

16 Bergman, 2001: 1.

também composta por bases de dados de valor significativo[17] e por outros acervos de informação que, propositadamente ou não, são *invisíveis* ao utilizador comum no âmbito das suas pesquisas. Em face do valor que certa informação aí contida poderá revestir, têm vindo a ser empreendidos esforços cada vez maiores no sentido de desenvolver mecanismos de penetração e pesquisa na *Deep Web*[18], bem como de indexação de várias das suas páginas na *Surface Web*[19].

2. A navegação na *Deep Web*

2.1. *Freenet*

Em 1999, Ian Clarke, um estudante irlandês na área da Inteligência Artificial e Ciência Computacional da Universidade de Edimburgo, concluiu o relatório final do seu curso dedicado ao tema «*A Distributed, Decentralised Information Storage and Retrieval System*»[20], no qual apresentou um novo método de navegação *online*, executável apenas através da instalação de um *software* específico que permitia ao seu utilizador uma navegação totalmente anónima numa área invisível da Internet[21].

O objetivo de Clarke era o de evitar que a Internet pudesse ser utilizada como instrumento para a monitorização das vidas dos cidadãos[22]. E pretendia fazê-lo através da eliminação do rasto que liga a informação disponibilizada na

17 Incluindo bases de dados de natureza académica nas quais se pode aceder livremente a artigos, dissertações, relatórios, livros e outro tipo de dados, Lewandowski & Mayr, 2006: 530-531. De acordo com dados recentes, estima-se que existam mais de mil milhões de páginas com dados estruturados de relevo, Cafarella, Halevy & Madhavan, 2011: 73.

18 Atente-se, nesta matéria, na atividade desenvolvida pela equipa liderada por Juliana Freire, da Universidade do Utah, que tem como objetivo pesquisar e obter a informação relevante contida em bases de dados da *Deep Web*: Freire/Barbosa, 2010: 145-146.

19 Veja-se, a este respeito, a abordagem da Google na sua tentativa de indexar algumas fontes da *deep Web* à *Surface Web*, Madhavan et al., 2008: 1241-1252 – embora a mesma tenha sido já criticada, ainda que muito brevemente, pela sua alegada ineficiência, por Dong & Li, 2012: 973.

20 Clarke, 1999: 1-45.

21 Um trabalho que, apesar de inovador, apenas lhe granjeou a classificação de "B" por o júri ter entendido que o autor não citou suficiente bibliografia. Acerca da origem e evolução do *Freenet*, v. Beckett, 2009 e a resposta de Clarke: 2009.

22 Curiosamente, cerca de dois anos mais tarde ocorreram dois eventos que viriam a dar particular relevância a esta pretensão: o primeiro foi o reconhecimento público, por parte do Parlamento Europeu, da existência de um sistema norte-americano de interceção de comunicações privadas e comerciais – v. relatório sobre a existência de um sistema global de interceção de comunicações privadas e económicas (sistema de interceção "ECHELON") (2001/2098 (INI)); o segundo foi a assinatura, por parte do Presidente dos Estados Unidos da América, George W. Bush, do USA PATRIOT Act, através do qual passou a permitir-se, precisamente, uma mais fácil monitorização da navegação na Internet.

Internet ao seu autor, assim permitindo o exercício da liberdade de expressão sem receio de qualquer tipo de repressão ou censura.

Após a defesa do seu trabalho, Clarke disponibilizou gratuitamente o *software* por si criado na Internet, batizando-o de *Freenet*, e convidou voluntários para ajudarem à sua implementação e difusão. Assim foi criado o *Freenet Project*, um projeto que visa permitir a comunicação livre e anónima e o acesso irrestrito à informação e ao conhecimento em qualquer área do globo.

Doze anos volvidos desde a sua divulgação inicial e já foram feitos mais de dois milhões de *downloads* do programa *Freenet*, incluindo em países com fortes restrições à liberdade de expressão, nos quais este *software* – não obstante, em certos casos, tenha sido bloqueado – tem sido difundido entre utilizadores e aproveitado como meio de divulgação de material censurado.

A vantagem do sistema desenvolvido por Clarke reside no facto de a informação ser armazenada de forma distribuída, descentralizada e em constante movimento, à medida dos acessos e da necessidade que os utilizadores manifestam em relação a certo tipo de dados. Esta configuração permite que qualquer entidade pública que pretenda bloquear ou apreender os dados informáticos acessíveis através do *Freenet* se veja praticamente impossibilitada de conhecer o local onde os mesmos se encontram armazenados, bem como a origem dos acessos a esses mesmos dados.

A ideia de armazenamento distribuído e descentralizado sobre a qual assenta o *Freenet* depende da existência de um conjunto de voluntários (os chamados *nodes* ou nódulos[23]) que, com a instalação do *software*, passam a contribuir para a rede através da cedência de alguma da sua largura de banda e de espaço no seu disco rígido[24]. Essa largura de banda será utilizada para promover o funcionamento da rede *Freenet* e o espaço de armazenamento será utilizado para armazenar pedaços da informação e ficheiros colocados na rede *Freenet* pelos vários utilizadores[25].

O facto de estes dados serem armazenados no computador de cada um dos utilizadores de forma cifrada[26] impede que o acesso direto aos mesmos

23 O termo significa, em traços gerais, um ponto de conexão, de redistribuição ou de chegada de uma transmissão de dados.

24 O valor mínimo do espaço a ser disponibilizado varia na medida do espaço de armazenamento de cada disco rígido.

25 Clarke et al., 2002: 40-44.

26 Quanto à eficácia da cifragem para impedir o acesso aos dados protegidos, refere Vaciago que "[é], *na realidade, totalmente inútil tentar prever quanto tempo demoraria a desbloquear dados protegidos por*

(leia-se, a abertura da pasta no computador e pesquisa nos ficheiros armazenados) permita apreender o seu conteúdo. Este mecanismo de cifragem serve fundamentalmente para permitir aos utilizadores do *software* negar conhecimento do material que o *Freenet* colocou no seu computador[27]. Isto significa, por um lado, que o utilizador não terá qualquer conhecimento ou controlo sobre os ficheiros armazenados no seu computador e, por outro, que o teor eventualmente ilícito dos mesmos à partida não implicará qualquer responsabilidade criminal para quem os tiver armazenados no espaço cedido ao sistema *Freenet*.

Para permitir uma maior acessibilidade do conteúdo aos vários utilizadores, os ficheiros disponibilizados no *Freenet* são cifrados, repartidos e distribuídos por vários nódulos e acedidos como se de um normal programa de *peer-to-peer* se tratasse. Portanto, a rede *Freenet* não tem um servidor centralizado no qual se encontram armazenados os dados, mas antes se encontra distribuída pelos vários utilizadores deste *software* que cedem o seu espaço de armazenamento.

O *Freenet* pode funcionar, essencialmente, de dois modos distintos: o modo *Opennet* e o modo *Darknet*, consoante a rede seja composta por toda a base de utilizadores ou apenas por alguns utilizadores que escolheram restringir o acesso à informação ou ficheiros partilhados a um grupo restrito.

Com o desenvolvimento deste programa, Ian Clarke permitiu um processo mais fácil de criação, navegação e difusão de *websites*, *chats* e fóruns, bem como de armazenamento de ficheiros e informações na *Deep Web*. Fê-lo, contudo, criando uma rede autónoma própria dentro da *Deep Web*, invisível a quem não tenha o *software Freenet*, e que permite aos seus utilizadores, de forma anónima, trocarem informações sem correrem o risco de deteção[28].

---

palavra-passe uma vez que, dependendo do tipo de chave de cifragem e de software *de decifragem utilizado, o tempo envolvido poderia variar entre uns segundos até muitos milhares de anos. Uma palavra-passe de 20-bit, por exemplo, permite um milhão de combinações possíveis, sendo que um computador portátil normal com uma capacidade de processamento de cerca de um milhão de computações por segundo, poderia muito bem descobrir a chave de cifragem em menos de um segundo. Contudo, ao mesmo computador demoraria cerca de 2285 anos a desbloquear dados protegidos por uma palavra-passe de 56-bit. Para se ter uma ideia da complexidade da tarefa em termos práticos, temos de considerar o PGP (Pretty Good Privacy), o programa de cifragem mais popular no mercado hoje, que usa uma chave de cifragem de 1024-bit."* (tradução nossa) – Vaciago, 2012a: 123.

27 Quayle, 2009: 250.

28 Para uma explicação do processo técnico utilizado pelo programa *Freenet* na transmissão de comunicações, Clarke et al., 2001a.

2.2. *The Onion Router* (Tor)

Pouco tempo depois da disponibilização ao público da primeira versão do *Freenet* foi divulgado, no âmbito do *13th USENIX Security Symposium* de 2004, um novo *software* com uma finalidade semelhante, apresentado como *Tor: The Second-Generation Onion Router* [29].

Tratava-se de uma nova e aperfeiçoada geração de *onion routing*, uma tecnologia surgida no final da década de noventa, desenvolvida pela Marinha norte-americana, cujo propósito era o de permitir a comunicação anónima e em rede entre os seus utilizadores através do envio de mensagens cifradas entre vários pontos de conexão até um destinatário final. O sistema de *roteamento* assim previsto fora concebido de modo a inviabilizar a interceção da comunicação e o conhecimento do seu conteúdo, origem e destinatário por terceiros não autorizados[30], introduzindo, para tal, pontos intermédios na transmissão, através dos quais a comunicação será enviada sob diferentes camadas de cifragem[31]. Em concreto, quando, numa rede de *onion routing*, os dados são transmitidos para qualquer dos seus elos de ligação, este apenas conseguirá decifrar a informação que lhe permitirá saber qual o próximo elo para onde a comunicação deverá ser enviada, mas não qual o trajeto que a comunicação fez desde a sua origem nem aquele que fará até chegar ao seu destinatário[32] – exceto nos casos em que o elo em causa recebe diretamente a comunicação de um desses pontos.

A proclamada nova geração de *onion routing*, subsequentemente promovida através do Projecto *Tor*[33], visava universalizar o acesso a esta tecnologia e, com

29 Dingledine, Mathewson & Syverson, 2004: 303-320.

30 Weber & Heinrich, 2012: 17.

31 Aliás, o nome *Onion Routing*, por vezes traduzido para a língua portuguesa na infeliz expressão "roteamento cebola", advém precisamente do facto de as comunicações trocadas na rede Tor partirem envoltas em várias camadas sobrepostas de cifragem que são progressivamente removidas à medida que a comunicação é transmitida aleatoriamente ao longo da rede de voluntários.

32 Patil & Lingam, 2012: 31-37, começam por explicar o conceito de comunicação em *Onion Routing* do seguinte modo: «*Imagine standing in a large, crowded room and you are handed a brown paper cylinder with your name on it. The person who hands it to you tells you to peel the paper with your name on it off of the cylinder to expose a new layer with a new name on it –your task is to deliver the cylinder to the person named, tell him to peel that layer of paper off and pass it on to the next person named and tell him to do the same. This goes on until the very center of the cylinder is handed off to the person to whom it is addressed. The idea is that the center of the cylinder contains a message sent to the final recipient by the very first person to hand the cylinder off. But, because the cylinder travelled through so many hands, and along a random path through the crowd, anyone observing the receipt of the final message (or any of the hand-offs at any point along the way, for that matter) has no idea where it came from originally; he or she only saw the final hand-off in a relay of handoffs.*»

33 Inicialmente o termo *Tor* surgiu como uma sigla para *The Onion Router*, embora posteriormente e por vontade expressa do *Tor Project*, tenha passado a ser concebido como uma só palavra.

ela, à semelhança do *Freenet*[34], permitir aos seus utilizadores uma navegação livre, segura e anónima na Internet[35].

O funcionamento do *Tor*, enquanto programa de *Onion Routing* pode resumir-se do seguinte modo: os seus utilizadores formam uma rede na qual alguns dos mesmos funcionam como retransmissores de comunicações. Isto significa que um dado utilizador que queira aceder a um *website* através do *Tor*, liga-se automaticamente à rede de retransmissores *Tor* e esta cria um "túnel" que transporta aleatoriamente a comunicação através da rede *Tor* até ao seu destinatário final – daí que, quanto maior o número de utilizadores, mais difícil será a identificação de cada um[36]. Quando a comunicação finalmente atinge o portal de saída do "túnel", isto é, quando a comunicação parte do último retransmissor da rede *Tor* (o chamado *exit node*) para o fornecedor de serviço[37], encontrar-se-á já desprovida de qualquer camada de cifragem. Adiante-se, porém, que esta remoção da cifragem da comunicação no seu trajeto final não resulta numa desproteção da comunicação e do anonimato do seu autor, uma vez que, mesmo tornando-se possível, em abstrato, nesta fase, a interceção da comunicação e subsequente conhecimento do seu conteúdo, na prática, como veremos, a pessoa cujo sistema informático é utilizado para enviar, a final, a comunicação para o seu destinatário final (o *exit node*) será completamente alheia ao seu conteúdo e, em princípio, não terá qualquer ligação ao seu autor, pelo que, um terceiro que a intercete nesta fase não terá maneira de saber quem a enviou nem qual o trajecto que a comunicação percorreu na rede *Tor*[38].

---

34 A principal diferença entre o *Freenet* e o *Tor* é que, enquanto aquele visa permitir a divulgação e publicação anónimas de informação, à semelhança de, como dizia Ian Clarke, *"uma biblioteca na qual as pessoas podem submeter ou retirar livros de forma anónima"*, funcionando, portanto, como um espaço de armazenamento limitado pelos seus próprios utilizadores, já o Tor funciona como um *browser* que permite uma navegação anónima em qualquer área da Internet, seja na *Surface Web* ou na *Deep Web*, podendo a informação acedida encontrar-se armazenada em qualquer local.

35 Uma nota apenas para ressalvar que o anonimato fornecido pelo *Tor* está dependente da cautela e das medidas tomadas pelo seu utilizador. Assim, a utilização simultânea de certas aplicações, como o *BitTorrent*, ou a configuração descuidada do *browser*, designadamente permitindo a visualização de páginas e ficheiros em formato *Flash* ou *Javascript*, poderão permitir uma mais fácil identificação do autor da comunicação.

36 Facto que poderá suscitar dúvidas quanto à verdadeira intenção dos *Anonymous* em divulgar a existência da *Dark Web* e do programa *Tor*. Na verdade, sabendo que também os *Anonymous* utilizam este programa e que também eles são procurados pelas autoridades, o aumento significativo de utilizadores do *Tor* decorrentes desta publicidade apenas os poderá beneficiar.

37 Todavia, nem todos os utilizadores do *Tor* funcionam como portais de saída (*exit nodes*) da comunicação, mas apenas aqueles que escolherem fazê-lo. Tal deve-se ao facto de, muitas vezes, os utilizadores que se tornam *exit nodes* serem interpelados (por vezes detidos) pelas autoridades para justificarem o teor das comunicações que partiram do seu computador para o servidor (por exemplo, quando alguém utiliza o *Tor* para aceder a pornografia infantil *online* e essa comunicação parte de um *exit node* determinado).

38 Para uma explicação tecnicamente mais detalhada do funcionamento dos sistemas de *onion routing* em geral, com particular incidência no programa *Tor*, Syverson, 2011: 123-137.

3. A incursão da cibercriminalidade na *Deep Web*: a *Dark Web* e as *Darknets*.
O crescente interesse por parte de certos setores da comunidade *online* pelo estudo e aplicação das chamadas "técnicas antiforenses" – ou simplesmente *anti-forensics*[39] – promoveu uma rápida difusão de programas como o *Freenet* e o *Tor*, em virtude do seu potencial para frustrar investigações criminais *online*.

Cedo, as propriedades destes *softwares*, desenhados inicialmente para salvaguardarem a liberdade de expressão e informação dos seus utilizadores, passaram a ser aproveitadas como meio para eliminar o rasto digital dos perpetradores de ilícitos *online*[40]. Daí que, imediatamente após a sua divulgação, o *Freenet* tenha passado a incluir várias páginas dedicadas à difusão de pornografia infantil e de material protegido por direito de autor, bem como ao ensino de técnicas de fabrico de explosivos e à proliferação de grupos terroristas.

Contudo, foi o *Tor* o programa cuja exploração teve mais impacto na evolução da criminalidade na *Deep Web*, facto que se deveu desde logo à sua significativa superioridade em termos de rapidez face ao *Freenet*[41] (não obstante seja, ainda assim, consideravelmente mais lento do que um *browser* normal), bem como à possibilidade que o *Tor* confere aos seus utizadores de navegação num ambiente mais vasto da *Internet* e, em particular, da *Deep Web*.

Assim, pouco tempo após a sua disponibilização, o *Tor* viu surgir diversos *websites* secretos, designados de *hidden services*[42], dedicados a todo o tipo de criminalidade. Começaram, então, a aparecer verdadeiros mercados de droga,

---

39 Apesar de não existir uma definição unívoca do que são técnicas antiforenses, adotaremos a definição utilizada por Ryan Harris por nos parecer ser aquela cuja amplitude será mais suscetível de obter consenso. Assim, as medidas ou técnicas antiforenses serão «*quaisquer tentativas de comprometer a disponibilidade ou utilidade da prova no processo forense. Comprometer a disponibilidade da prova inclui quaisquer tentativas de evitar que a prova venha a existir, de esconder prova existente ou de manipular a prova no sentido de assegurar que a mesma deixe de estar ao alcance do utilizador. A utilidade pode ser comprometida através da obliteração da própria prova ou da destruição da sua integridade*», Harris, 2006: S45.

40 Sublinhe-se, porém, que o *Tor* também é utilizado por forças policiais no âmbito de ações encobertas em ambiente digital, dado que a sua utilização permite esconder o seu endereço IP e ocultar a sua atividade.

41 Ainda que o *Tor* permita uma navegação consideravelmente mais rápida do que o *Freenet*, a verdade é que o seu funcionamento continua a ser consideravelmente mais lento do que a de um *browser* normal - para uma explicação dos motivos desta acrescida lentidão, cf. Dhungel et al., 2010: 1-4.

42 Estes *hidden services* dizem-se *escondidos* porque o seu alojamento é, muitas vezes, impossível de detetar, bem como porque geralmente apenas podem ser acedidos via *Tor* por quem conheça o seu endereço, composto por um conjunto de dezasseis caracteres aleatoriamente dispostos.

documentos falsos e outros materiais ilícitos, como o célebre *The Silk Road*[43] no qual as transações são feitas com recurso a *bitcoins*, ou o mercado de drogas, armas e explosivos chamado *Black Market Reloaded*. Adicionalmente, surgiram mercados *online* dedicados à venda de pornografia infantil ou mesmo de espécies em vias de extinção, bem como inúmeras páginas e fóruns de pornografia infantil e/ou violenta, bem como fóruns dedicados ao canibalismo[44], fóruns *jihadistas*[45] e páginas que comercializavam dados relativos a cartões de crédito obtidos através de esquemas de *phishing*[46].

São, portanto, estas páginas da *Deep Web,* acessíveis somente com recurso a *software* especificamente desenvolvido para induzir o anonimato da navegação *online* e dedicadas à prática, divulgação, aconselhamento para a prática, incitamento ou publicitação de crimes ou à difusão de material de origem criminosa, que compõem, na definição utilizada no presente estudo, a *Dark Web*[47].

---

43 entre a data de conclusão do presente artigo e a sua publicação o The Silk Road foi encerrado, em circunstâncias que permanecem por clarificar, na sequência de uma ação de investigação criminal desenvolvida por entidades norte-americanas.

44 Uma palavra para referir quanto a esta matéria, a título exemplificativo, o célebre e macabro caso do Canibal de Rotemburgo, o qual, apesar de ter ocorrido antes da divulgação destes *softwares*, teve lugar tecnicamente na *Deep Web*. Em síntese, num fórum dedicado ao canibalismo e propositadamente não indexado aos motores de busca, Armin Meiwes colocou uma mensagem na qual referia estar à procura de um homem bem constituído entre os 18 e os 30 anos para o matar e comer. Poucos meses depois, Bernd Huergen Brandes, de 43 anos, respondeu do seguinte modo: *"ofereço-me a ti e deixar-te-ei jantar o meu corpo vivo"*. Após algumas semanas de discussão dos pormenores por correio eletrónico, Brandes apresentou-se em casa de Meiwes onde acabou por ser parcialmente comido vivo, até finalmente ter sido decapitado e armazenado numa arca frigorífica para servir de alimento ao homicida durante os meses que se seguiram. Meiwes acabaria por vir a ser preso e condenado a prisão perpétua – para uma análise deste caso e respetivo enquadramento jurídico-penal na temática dos limites do consentimento como causa de justificação, v. Bergelson, 2008: 723-726.

45 O que tem, aliás, motivado um trabalho notável de desenvolvimento tecnológico com vista à recolha de informação relacionada com grupos terroristas na *Deep Web* por parte do Laboratório de Inteligência Artificial da Universidade do Arizona, Chen, 2012.

46 Existem relatos de muitos outros tipos de criminalidade na *Deep Web* mas que, por se nos afigurarem menos plausíveis e por não dispormos de informação fidedigna quanto à sua existência, não incluiremos no presente estudo.

47 Apesar de ser usual distinguirem-se vários níveis dentro da *Dark Web*, cujo acesso seria progressivamente mais difícil à medida que nos aproximamos do nível mais profundo (a chamada *Mariana's Web*), a verdade é que a existência de uma hierarquização desta natureza é altamente contestada. Por esse motivo, e sem prejuízo de reconhecermos a existência de áreas mais facilmente acessíveis do que outras dentro da *Dark Web*, abster-nos-emos de tecer quaisquer ulteriores considerações acerca da existência destes níveis e limitaremos as nossas referências às áreas da *Dark Web* que consultámos durante o nosso estudo ou cuja existência é afirmada por fontes fidedignas.

O termo *Dark Web* não deve ser confundido com o termo *Darknet* uma vez que a *Darknet* é antes uma rede virtual estabelecida entre vários utilizadores, inacessível a terceiros e que funciona através de uma rede de telecomunicações pública, neste caso a Internet, que visa a partilha de informações e ficheiros em formato digital[48] sem, contudo, permitir que, quer os endereços de IP dos seus membros, quer o teor das comunicações entre si estabelecidas, possam ser descobertos. Pense-se, por exemplo, na existência de um grupo de indivíduos de várias nacionalidades que se conhecem, confiam uns nos outros, e decidem partilhar imagens de pornografia infantil em formato de *peer-to-peer* uns com os outros, sem que qualquer outra pessoa possa aceder a esses dados, estabelecendo para tal uma rede de partilha privada – neste caso estaremos perante uma *Darknet* na *Dark Web*.

4. As *bitcoins*

A navegação anónima na *Dark Web* cedo se deparou com uma fragilidade da maior importância: a impossibilidade da manutenção do anonimato nas transações *online*.

Com efeito, a partir do momento em que se efetua uma transação na Internet, torna-se necessária a intervenção de uma entidade bancária externa à relação contratual para que esta providencie pela transferência do montante pecuniário do vendedor para o comprador. Isto significa que um indivíduo que navegue de forma anónima na Internet e pretenda adquirir um produto *online* (por exemplo, um livro banido no seu país) terá, à partida, de recorrer a uma entidade bancária para poder efetuar o pagamento, o que, em última análise, permitirá a sua identificação.

Para fazer face a esta e a outras, dificuldades, em 2008, Satoshi Nakamoto[49] publicou um trabalho intitulado «*Bitcoin: a Peer-to-Peer Electronic Cash System*»[50], onde apresentou a sua ideia para a criação de uma *cifromoeda* (*cryptocurrency*) descentralizada que funcionasse em rede, num sistema de *peer-to-peer* e com recurso a tecnologia de cifragem, com o intuito de que todas as transações decorressem de forma anónima entre as duas partes envolvidas: a *bitcoin* (฿).

48 Os termos foram, inclusivamente, utilizados sem rigor no caso da Operação *Darknet* que, na verdade, incidiu sobre a *Dark Web* e, possivelmente, sobre várias *Darknets*.

49 Cuja verdadeira identidade permanece desconhecida.

50 Nakamoto, 2008.

O funcionamento do sistema *bitcoin* depende da instalação prévia, por parte de alguns dos seus utilizadores com conhecimentos técnicos que o permitam (os chamados *miners*), de um *software* específico que colocará parte da capacidade de processamento central ou visual dos seus computadores (CPU ou GPU) ao serviço da rede *bitcoin*, mantendo-a ativa. Em contrapartida, cada um destes utilizadores habilita-se a receber um dos lotes de 50 novas *bitcoins* entregues a cada 10 minutos[51]. A entrega destes lotes de *bitcoins* funciona com base no lançamento automático, pelo sistema *bitcoin*, de uma espécie de *puzzles* de cifragem (chamados de *hash*) para a rede de *miners*, os quais, por sua vez, terão parte da sua capacidade de processamento afeta à sua resolução. Assim, o primeiro computador, ou conjunto de computadores, a descodificar aquele *puzzle* com recurso ao *software* apropriado receberá o lote de *bitcoins* correspondente. Todavia, para que o sistema consiga manter a periodicidade dos lotes, à medida que aumenta o número de utilizadores da rede e, consequentemente, aumenta a capacidade de processamento afeta à resolução dos *puzzles*, também aumenta a sua complexidade – daí que atualmente a resolução destes *puzzles* não seja feita com recurso a um só computador, mas antes a redes cada vez maiores de computadores de voluntários (as chamadas *mining pools*)[52].

Para os utilizadores tecnicamente menos proficientes, a maneira mais fácil de obter *bitcoins* será comprando-as junto de uma das lojas de câmbio de *bitcoins*, como a *Mt. Gox*, *bitomatPLN*, *virwoxSLL*, *britcoinGBP*, *bitmarketEUR*, *bcmPPUSD*, e a *thUSD*, e armazenando-as na sua carteira digital.

Cada transação (compra ou doação) efetuada com recurso a *bitcoins* é automaticamente enviada para a rede de *peer-to-peer* para validação e permanentemente registada de forma descentralizada e anónima na rede, assim criando um bloco de dados relativo a cada transação que permite verificar a validade daquela *bitcoin* e evitar que a mesma *bitcoin* possa ser gasta duas vezes[53].

O valor da *bitcoin* flutua consoante a procura da mesma. Assim, enquanto em fevereiro de 2011 cada *bitcoin* valia cerca de $0.87, em maio do mesmo ano, na sequência de uma reportagem da revista *Forbes*, o valor disparou para $8.89 e, em junho, após a revista Gawker ter publicado uma reportagem na qual

51 Grinberg, 2011: 163.

52 Cf. http://www.weusecoins.com/ [consultado em 06.10.2012].

53 Para uma explicação detalhada de toda a evolução das *bitcoins*, v. Wallace, 2011.

associou as *bitcoins* ao tráfico de droga *online*, subiu para os 27$[54]. Estima-se que o seu valor venha a aumentar no futuro, uma vez que o sistema *bitcoin* se encontra programado para deixar de produzir moeda a partir dos 21.000.000 de *bitcoins*[55].

Até agora, e ressalvados alguns percalços, a *bitcoin* tem-se revelado uma verdadeira moeda, apta a fazer face às flutuações do mercado, sendo cada vez mais aceite em todo o tipo de transações *online*. Tem, naturalmente, o mérito de ter sido a primeira *cifromoeda* a conseguir ultrapassar as dificuldades técnicas do "duplo-gasto" da mesma moeda, bem como de conseguir um nível de divulgação tão amplo que permite ao seu titular obter com relativa facilidade qualquer bem que pretenda adquirir sem necessitar de divulgar quaisquer dados que permitam a sua identificação[56].

II. A RECOLHA DE PROVA NA *DARK WEB*

Delimitadas, em traços gerais, as coordenadas fácticas e técnicas da criminalidade na *Dark Web*, haverá agora que enquadrar juridicamente a recolha de prova na *Dark Web*, à luz dos instrumentos processuais consagrados na Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro).

Ao longo do presente capítulo debruçar-nos-emos separadamente sobre a eficácia da aplicação, no contexto da *Dark Web*, em primeiro lugar, das medidas dedicadas à obtenção de dados informáticos armazenados num sistema informático, em segundo lugar, da interceção de comunicações e, por fim, do recurso ao agente encoberto em ambiente digital. O nosso objetivo, nesta sede, será o de analisar em que medida é que estes mecanismos permitem ultrapassar as etapas necessárias à recolha de prova em ambiente digital, em particular as etapas relativas à identificação do suspeito e à deteção e apreensão dos conteúdos visados.

---

54 Assim, um indivíduo do Tennessee que se autointitulava de *KnightMB* que detinha 371.000 *bitcoins*, viu o valor das mesmas aumentar de 322.770$ para mais de dez milhões de dólares.

55 Porém, para facilitar a divulgação da moeda mesmo após a cessação da sua emissão, a *bitcoin* incorpora a possibilidade de ser dividida até à casa do milionésimo de *bitcoin*, uma unidade monetária que foi denominada de *satoshi*, em homenagem ao criador da moeda.

56 O anonimato que a *bitcoin* fornece não é, porém, completo, e para ser totalmente eficaz deverá ser conciliado com outros mecanismos.

1. A obtenção de dados informáticos armazenados num sistema informático

Imagine-se, então, que, no âmbito de uma investigação criminal a uma rede de pornografia infantil, localizada na *Dark Web*, na qual se incluem menores portugueses, se inicia uma investigação criminal com vista à descoberta dos participantes nas imagens ou vídeos e das pessoas que os divulgaram. Pergunta-se, face aos instrumentos legais disponíveis, como proceder à recolha de prova neste contexto?

A Lei do Cibercrime coloca à disposição do investigador cinco medidas processuais para a investigação criminal em ambiente digital que permitem obter dados informáticos armazenados num sistema informático[57]:

a) A preservação expedita de dados informatizados, prevista no 12.º e, em matéria de cooperação internacional, no art. 22.º;

b) A revelação expedita de dados de tráfego, prevista no 13.º e, em matéria de cooperação internacional, no art. 22.º;

c) A injunção para apresentação ou concessão do acesso a dados, prevista no art. 14.º e, em matéria de cooperação internacional, no art. 26.º;

d) A apreensão de dados informáticos, prevista no art. 16.º e, em matéria de cooperação internacional, no art. 24.º;

e) A apreensão de correio eletrónico e registos de comunicações de natureza semelhante, prevista no art. 17.º;

Ora, tendo em conta que a análise da eficácia da medida cautelar de preservação expedita de dados (a) no contexto da *Dark Web* se nos afigura redundante face ao que se dirá na exposição referente à revelação expedita de dados de tráfego (b), à injunção para apresentação ou concessão de acesso a dados (c) e à apreensão de dados (d), não cremos que a mesma mereça uma análise individualizada, pelo que não a abordaremos no presente capítulo (exceto enquanto pressuposto necessário da revelação expedita de dados de tráfego). Por outro lado, tendo em conta que a apreensão de correio eletrónico e registos de natureza semelhante (e) é desprovida de especificidades de relevo no âmbito da *Dark Web*, também nos absteremos de a analisar em separado.

57 Sobre esta matéria escrevemos já mais desenvolvidamente, cf. Ramalho, 2014.

1.1. A revelação expedita de dados de tráfego

O primeiro dos meios de obtenção de prova (ainda que a título cautelar) cuja eficácia cumpre apreciar no âmbito da *Dark Web* – e que pressupõe a aplicação prévia da medida cautelar de preservação expedita de dados – será, então, a preservação e revelação expedita de dados de tráfego[58], isto é, ao abrigo da definição constante da al. *c)* do art. 2.º da Lei do Cibercrime[59] (doravante LC), dos "*dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente*".

Este meio consiste, em síntese, na imposição, aos fornecedores de serviço, da preservação e divulgação dos dados de tráfego relativos a uma determinada comunicação, assim permitindo identificar, entre outros elementos, o trajeto percorrido pela comunicação.

Acontece que, como tivemos ocasião de referir, o programa *Tor* está especialmente desenhado para impedir que essa identificação seja efetuada, pois que, ao criar um "túnel" para o envio da comunicação, faz com que o fornecedor de serviço deixe de receber os pedidos de acesso a quaisquer *websites* diretamente do utilizador.

Assim, se for ordenada a revelação dos dados de tráfego a partir da origem da comunicação (do *node* inicial), antes da sua entrada no "túnel", será impossível descobrir a quem a mesma se destina. Se, por outro lado, a revelação da origem da comunicação for solicitada, tendo como única referência o *exit node*, então será igualmente impossível ao investigador descobrir a proveniência da mesma, qual o trajeto que fez e até qual o seu tamanho e hora de expedição (isto porque, como se verá, o *Tor* adotou um mecanismo de atraso e de alteração dos tamanhos dos pacotes de dados). Deste modo, se o investigador pretender fazer um trajeto reversivo a partir do fornecedor de serviço utilizado para aceder a um *website* até à origem da comunicação, ver-se-á confrontado com uma impossibilidade técnica em virtude de o trajecto ter ocorrido de forma aleatória e cifrada por uma rede de utilizadores *Tor*.

---

58 Diríamos, porém, que esta medida se revela pouco relevante quando incida sobre fornecedores de serviços, dado que, nos termos do art. 6.º da Lei n.º 32/2008, de 17 de julho, os fornecedores de serviços já se encontram obrigados a guardar os dados de tráfego por um ano, pelo que haverá pouca necessidade de requerer a preservação expedita destes dados àquelas entidades.

59 Lei n.º 109/2009, de 15 de setembro.

Destarte, num contexto de investigação em que se pretende reconstituir o trajeto por via reversiva da comunicação, a única informação que, em regra, poderá ser acessível ao investigador dirá respeito ao "nódulo" de saída da comunicação, isto é, incluirá apenas os dados de tráfego do sistema informático no qual se encontra instalado o *Tor* e que, enquanto retransmissor final, recebeu a comunicação do "túnel" e a reencaminhou automaticamente para o destinatário final. Mas estes dados não revestirão qualquer utilidade, uma vez que este retransmissor será um mero utilizador do *Tor* que desconhecerá o teor da comunicação que automaticamente passou pelo seu computador[60].

Apesar de o *Freenet* funcionar de maneira diferente em relação ao *Tor*, a verdade é que os obstáculos colocados ao investigador serão essencialmente os mesmos. O facto de o utilizador aceder a informação armazenada de forma cifrada nos computadores de utilizadores diferentes permitirá apenas, na melhor das hipóteses, saber que a dada hora um sistema informático se ligou a vários outros. Tendo em conta que a informação armazenada nos vários computadores é sucessivamente modificada e redistribuída para outros utilizadores, tal informação revelar-se-á inútil, uma vez que não permitirá ligar o visado ao conteúdo ilícito.

Daqui se retira que preservação e revelação expedita de dados de tráfego dificilmente revestirá qualquer utilidade para o investigador no âmbito da *Dark Web*.

1.2. A injunção para apresentação ou concessão do acesso a dados.

Existem essencialmente duas vias através das quais a injunção para apresentação ou concessão do acesso a dados poderia, em abstrato, ser utilizada no contexto em apreço: a primeira, mais óbvia, seria a apresentação da injunção junto do fornecedor de serviço; a segunda consistiria na apresentação da referida injunção ao administrador da rede informática que tenha sido utilizada pelo visado no acesso à *Dark Web*, por exemplo, uma rede empresarial que tenha sido utilizada por um trabalhador para aceder a *hidden services* na *Dark Web*[61].

60 É, porém, relativamente frequente que os utilizadores do *Tor* que funcionam como retransmissores finais, sejam interpelados e por vezes detidos em virtude de comunicações de natureza ilegal que acedem a um fornecedor de serviço a partir do seu computador – cf. Kaspersen, 2009: 1-26.

61 Verdelho, 2009: 739.

Reportando-nos à primeira das vias apresentadas, cumpre, antes de mais, distinguir duas sub-hipóteses: em primeiro lugar, aquela em que, nos termos do n.º 1 do art. 14.º da LC, se pretenda obter o acesso a dados específicos armazenados num determinado sistema informático, *in casu*, num fornecedor de serviço na aceção da segunda parte da al. *d)* do art. 2.º da LC[62] (ou seja, enquanto "*qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respetivos utilizadores*"), e, em segundo lugar, aquela em que se pretenda obrigar o fornecedor de serviço a revelar os dados constantes das als. *a)* a *c)* do n.º 4 do art. 14.º, desta feita devendo o conceito de fornecedor de serviço ser entendido nos termos da primeira parte da al. *d)* do art 2.º da LC (isto é, enquanto entidade que "*faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático*"). Assim, enquanto a primeira destas sub-hipóteses poderá incidir sobre o fornecedor de serviço no qual se encontra alojado um determinado *hidden service* com material ilícito na *Dark Web*, já a segunda reportar-se-á ao fornecedor de serviço do qual é assinante ou cliente o indivíduo cuja ligação foi utilizada para aceder à *Dark Web*.

Ora, no caso de estarmos perante uma injunção a ser apresentada perante o fornecedor de serviço que armazena o material visado (primeira sub-hipótese), haverá, em primeiro lugar, que detetar onde se localiza o mesmo, o que, como vimos, a menos que não tenham sido tomadas medidas de segurança adequadas, poderá revelar-se tecnicamente impossível. Por outro lado, trata-se de uma medida que apenas poderá produzir efeitos num contexto em que os dados (essencialmente de conteúdo) visados sejam efetivamente transmitidos para o fornecedor de serviço. Deste modo, esta injunção seria insuscetível de produzir efeitos no caso das *darknets*, incluindo no caso do *Freenet*, caso se pretendesse obter dados de conteúdo, uma vez que estes são transferidos e armazenados diretamente nos computadores dos vários membros da rede, muitas vezes de forma cifrada, sem que o fornecedor de serviço tenha acesso aos mesmos.

Já no que concerne à injunção apresentada junto do fornecedor de serviço do qual é assinante ou cliente o indivíduo cuja rede foi utilizada para aceder à *Dark Web* (segunda sub-hipótese), também se afigura que a mesma, à partida, será de diminuto relevo prático. Isto porque a sua utilização pressupõe que seja possível ao fornecedor de serviço determinar qual o sistema informático a

62 Acerca da aplicabilidade desta previsão também aos fornecedores de serviços, embora reportando-se ao art. 18.º da CsC no qual o mesmo foi inspirado, Gercke, 2011: 427.

partir do qual partiu a comunicação relativa ao acesso à *Dark Web*, o que, como se viu, para um utilizador cauteloso do *software* utilizado, será dificilmente praticável. Aliás, a utilização desta medida, na melhor das hipóteses, permitiria, novamente, descobrir apenas os dados relativos à última pessoa do "túnel" do *Tor*, a partir da qual foi retransmitida a comunicação enviada pelo verdadeiro visado para a *Dark Web*, ou, quando muito, no caso do *Freenet*, quais os computadores aos quais o utilizador acedeu para obter a informação pretendida (e nunca o seu conteúdo, uma vez que esses dados se encontram cifrados).

No que respeita à segunda hipótese *supra* enunciada, relativa à apresentação da referida injunção ao administrador da rede informática que tenha sido utilizada pelo visado no acesso à *Dark Web*, verifica-se que a mesma, novamente, parte do pressuposto de que a parte mais difícil neste tipo de investigações já foi efetuada: a identificação do suspeito ou da origem da comunicação.

Todavia, mesmo na eventualidade de essa informação prévia já estar no poder da autoridade judiciária – caso em que não estaremos verdadeiramente perante uma recolha de prova no contexto da investigação criminal na *Dark Web*, mas antes num sistema informático *offline* e, portanto, fora do escopo do presente estudo –, esta medida apenas poderá ter algum efeito útil caso o visado tenha descurado algumas técnicas antiforenses no seu sistema informático isto é, caso o visado tenha feito o *download* dos ficheiros visualizados para o sistema informático em causa sem os ter cifrado e caso não tenha configurado o seu *browser* para se abster de guardar qualquer informação relativa aos *websites* visitados, designadamente em *cache*[63] ou sob a forma de *cookies*[64] e, ainda, caso não o tenha igualmente programado para eliminar todos os dados após o fim da sessão.

Assim, a utilidade prática desta medida, especialmente no caso de utilizadores cautelosos do *software* referido, também se revela reduzida.

63 O *web cache* será, em síntese, um mecanismo de armazenamento temporário de ficheiros automaticamente requeridos para visualizar uma página da Internet de modo a permitir que, de cada vez que a página é reaberta, o computador não tenha de fazer novamente o *download* de todos os seus elementos mas antes possa recorrer aos que já tem em memória, Santos, Bessa & Pimentel, 2008: 243-244.

64 Os *cookies* são, em traços gerais, ficheiros que alguns *websites* colocam no disco rígido do computador de quem os visita de modo a poderem recordar-se de algo acerca desse cibernauta numa visita futura. Estes ficheiros poderão ser utilizados, por exemplo, para permitir que o utilizador, ao navegar num dado *website*, não seja sempre confrontado com os mesmos anúncios ou não seja constantemente obrigado a fazer *log in* – cf. Vacca, 2005: 565.

1.3. A apreensão de dados informáticos

Reportar-nos-emos agora à última medida processual prevista na Lei do Cibercrime para obtenção de dados armazenados num sistema informático: a apreensão de dados informáticos.

A apreensão de dados informáticos poderá decorrer de uma pesquisa a um sistema informático (art. 15.º, n.º 1, da LC), de uma extensão dessa pesquisa a um outro sistema informático acessível através do primeiro (art. 15.º, n.º 5, da LC), ou de outro acesso legítimo a um sistema informático (art. 16.º, n.º 1, da LC).

Acontece que, para a efetivação da apreensão de dados, em qualquer uma daquelas modalidades, torna-se novamente necessário o empreendimento prévio de medidas que permitam descobrir esses mesmos dados, ou seja, é necessário que se saiba em que sistema informático estão armazenados os dados visados, a partir de que sistema são os mesmos acessíveis (se possível, a partir de que sistema foram efetivamente acedidos[65]) ou como aceder a esses dados.

Ora, a resolução desta difícil questão prévia implica que o investigador se encontre numa posição privilegiada, quer porque tem acesso ao computador do visado, quer porque saberá da existência e do *link* de um *website* na *Dark Web*, quer ainda porque logrou infiltrar-se numa *Darknet*. A superação desta questão pressuporá a execução prévia de outras atividades de investigação (como o recurso às ações encobertas, possivelmente acompanhadas do recurso a buscas *online*, ou, de forma mais rigorosa, de recurso a *malware* como meio de obtenção de prova), cujo sucesso geralmente estará dependente da possibilidade técnica da sua utilização (em páginas de mera divulgação de imagens ou vídeos sem lugar a interação, de pouco servirá o recurso a ações encobertas), de faltas de cuidado[66] por parte do visado, da vontade do visado (por exemplo, autorizando o acesso aos dados) ou de uma denúncia que inclua aquelas informações.

A segunda possível questão prévia a superar antes de proceder à apreensão dos dados informáticos visados traduz-se na obtenção das credenciais (nome de utilizador e palavra-passe) que permitem o acesso aos *websites* não publicamente acessíveis ou às *darknets*, o que poderá ocorrer, em princípio, numa de quatro situações: (i) o suspeito divulga essa informação voluntariamente; (ii) no momento da realização da pesquisa ao sistema informático inicial do

65 Cumpre, porém, não esquecer que a identificação deste sistema não significa que o utilizador do mesmo seja responsável pelos acessos à *Dark Web*. Recorde-se que é possível que haja outra pessoa a servir-se da rede *wireless* do suspeito ou que o sistema informático em causa se encontre infetado por *malware* que permite o seu controlo por um terceiro, como nos casos das *botnets* e dos *rootkits* – cf. Vaciago, 2012a: 56.

66 Algo que é relativamente comum nos casos de tráfico de pornografia *online*, Gercke, 2011: 66.

visado (por exemplo, o computador), esses *websites* ou *darknets* encontram-se abertos; (iii) as credenciais já se encontram inseridas, por defeito, no sistema informático inicial no momento em que se tenta aceder aos *websites* ou às *darknets*; (iv) ou, por fim, as credenciais foram obtidas no decurso da atividade de investigação, designadamente por se encontrarem escritas num local acessível ao investigador ou por terem sido empreendidas medidas prévias que permitiram o conhecimento das mesmas (por hipótese, caso tenham sido obtidas por via de uma ação encoberta em ambiente digital, designadamente com recurso a *malware*, nos termos do art. 19.º da LC).

Admitindo que se ultrapassam estes dois obstáculos iniciais, o investigador, nos primeiro e segundo casos *supra* referidos – quando pretenda apreender dados a partir de um sistema informático determinado ou de outro sistema acessível através daquele – terá de começar por apreender os dados armazenados no sistema informático inicial, isto é, na generalidade dos casos, terá de apreender o computador a partir do qual se acedeu à *Dark Web* ou então terá de realizar uma *bitstream copy* do disco[67], ao abrigo do n.º 7 do art. 16.º da LC[68].

Os dados a apreender incluem, para além do material de teor objetivamente criminoso (como eventuais ficheiros de pornografia infantil), todos os ficheiros criados, enviados, recebidos ou eliminados[69] recuperáveis que permitam associar o utilizador do computador à atividade ilícita perpetrada ou descoberta *online*.

Todavia, a apreensão deste tipo de vestígios resultará, como se referiu anteriormente, de uma nova falta de diligência por parte do utilizador do sistema informático em causa, uma vez que facilmente poderia ter armazenado os

---

67 Face aos riscos do ponto de vista da integridade da prova e da completude da recolha decorrentes da mera apreensão de alguns dados informáticos, é recomendável a preservação de todo o conteúdo do disco através da realização de uma *bitstream copy*. Trata-se de uma duplicação exata de todo o conteúdo de um sistema informático que permite evitar a perda de quaisquer elementos probatórios, à exceção daqueles que apenas podem ser recolhidos quando o computador esteja ligado (como a informação sobre os programas que se encontram a correr ou sobre as contas de utilizador abertas no momento da pesquisa), Casey, 2011: 383 e 482.

68 Sempre com o respeito pelas regras e técnicas mais avançadas disponíveis da Ciência Forense Digital – Vaciago, 2012a: 54-66.

69 À exceção dos casos em que se utiliza *software* próprio para eliminar definitivamente os ficheiros apagados pelo utilizador, como o *Eraser* ou o *CCleaner*, o mero ato de enviar um ficheiro para a reciclagem do computador e de esvaziar esta pasta não permite a remoção definitiva do ficheiro do sistema informático no qual se encontra. Na verdade, "[...] *quando se apaga um ficheiro isso não quer dizer que se remove o seu conteúdo do disco. É meramente removido o apontador a esse ficheiro. Os dados são armazenados em* clusters *, que são unidades constituídas por um conjunto de* bits. *Pelo facto das partes de um ficheiro não serem sempre armazenadas em* clusters *contíguos de um disco, sem uma ordem aparente e em diferentes localizações, a remoção dos já referidos apontadores faz com que a reconstituição de um ficheiro seja difícil de ser concretizada.",* Santos/Bessa/Pimentel, 2008: 240.

ficheiros num suporte autónomo cifrado[70]. Por outro lado, tendo em conta que a configuração certa (e, no caso do *Tor*, a configuração configurada por defeito), do *software* utilizado para aceder à *Dark Web* permite a eliminação do "rasto" do percurso desenvolvido *online*, também aqui teria de ter havido uma falta de cuidado por parte do utilizador (ou mesmo uma conduta ativa no sentido de reduzir as suas defesas, no caso do *Tor*) ao não promover a eliminação automática do histórico, *cookies* e *cache*.

Porém, este é apenas o procedimento a adotar diretamente no sistema informático objeto da pesquisa e cujos dados se pretendem apreender. Haverá ainda que proceder à recolha, por via remota, dos dados acessíveis apenas através deste sistema ou acessíveis diretamente com recurso às credenciais certas, ou seja, haverá que recolher a prova disponível em rede, seja na *Dark Web* – leia-se, no servidor no qual se encontra alojado o *website* na *Dark Web* –, seja numa *darknet*. Este tipo de recolha oferece problemas acrescidos, uma vez que a prova se encontra armazenada em rede numa situação de extrema volatilidade. Assim, no caso dos *websites*, qualquer administrador, ou o utilizador responsável pelo *upload* dos ficheiros visados, poderá eliminar os dados visados e, no caso das *darknets*, especialmente das mais pequenas, os utilizadores que partilham os ficheiros poderão facilmente eliminá-los da rede[71].

Acresce que, para proceder à recolha de prova num *website* ou numa *darknet* de acordo com as regras forenses digitais que permitem validar tecnicamente, com segurança, a apreensão dos dados informáticos, é conveniente tomar prévio conhecimento da localização física do sistema informático no qual aquele se encontra alojado (o que, como se viu, poderá revelar-se impossível), quer para inclusão da sua menção no despacho inicial que autoriza a pesquisa que precederá a apreensão dos dados (art. 15.º, n.º 1 da LC), quer para concessão da autorização para extensão da pesquisa dirigida a um sistema informático inicial para o sistema no qual se encontram os dados pretendidos (at. 15.º, n.º 5), quer ainda para que a recolha da prova possa ser adequadamente validada do ponto de vista da Ciência Forense Digital, assim se garantindo a cadeia de

70 No caso em que os ficheiros pretendidos se encontrem cifrados, não é admissível, à luz do direito à não autoincriminação, no ordenamento jurídico português, a imposição ao arguido da divulgação da palavra-passe que permite a decifragem, Pinto, 2010: 91-116.

71 Considerando que as *darknets* funcionam em sistema de *peer-to-peer*, haverá que recorrer às técnicas forenses de recolha de prova aplicáveis a estes sistemas. Contudo, os problemas técnicos que o uso de programas indutores de anonimato e o desconhecimento da real localização física de cada um dos sistemas informáticos que compõem a rede, pode tornar a recolha de prova numa tarefa praticamente impossível – cf. Taylor et al. 2011: 650-651.

custódia[72]. A este facto há que aduzir o problema de que, quando a pesquisa incide sobre uma *Darknet*, o próprio processo de descoberta de informações relativas à mesma pode ser confundido pela respetiva *Firewall* como uma tentativa de estudo das suas fragilidades, o que poderá resultar na emissão de um alerta automático para o seu administrador com a informação de que um terceiro se encontra a tentar recolher informação sobre aquela rede[73], o que, por sua vez, poderá levar a que o administrador tome medidas no sentido da remoção dos ficheiros da rede ou do aumento das suas defesas.

Em suma, a apreensão de dados informáticos será um meio de obtenção de prova potencialmente importante, mas apenas na medida em que o investigador disponha de informação prévia acerca do *link* para os *websites* visados, do sistema informático no qual se irão apreender os dados em causa ou, por fim, das credenciais de acesso aos mesmos, o que implica a execução de medidas prévias que permitam essa descoberta.

1.3.1. O acesso a dados informáticos publicamente acessíveis

Apesar de alguma doutrina optar por definir o conceito de dados informáticos publicamente acessíveis como aqueles cujo acesso não depende da introdução de uma palavra-passe[74], cremos que o conceito terá de ser interpretado de forma um pouco mais abrangente.

Com efeito, para a exclusão de alguns dados desta categoria, não basta que os mesmos careçam da introdução de um nome de utilizador e de uma palavra-passe, mas antes se torna necessário que a obtenção dessas credenciais não seja concedida ao investigador nas mesmas circunstâncias em que o seria a qualquer outro cibernauta. Na verdade, em vários *websites* (como os já referidos *The Silk Road* e *Black Market Reloaded*) o acesso depende da obtenção prévia, mediante um mero registo imediato, de um nome de utilizador e de uma palavra-passe, acessíveis a qualquer utilizador sem nenhum tipo de controlo. Nestes casos, inexiste qualquer motivo para se considerar que os dados acessíveis após esse registo não devam também ser considerados como publicamente acessíveis para efeitos de recolha de prova digital.

---

72 Sobre a suficiência da impressão de *snapshots* das páginas *web* visadas apenas a título de recolha de prova cautelar, Casey, 2011: 687.

73 *Idem*, p. 636.

74 Gercke, 2011: 470, Vaciago, 2012a: 119.

No âmbito da *Dark Web* afigura-se que este método é de uma utilidade superior[75], dado que certos utilizadores do *software* necessário para aceder a estes *websites* se sentem escudados pelo anonimato que esta tecnologia lhes permite e se abstêm de esconder a sua atividade *online*, assim disponibilizando largas quantidades de ficheiros de conteúdo criminoso a todos os frequentadores dessas páginas, sem qualquer restrição.

Aliás, constata-se que uma pesquisa alternada entre os motores de busca da *Surface Web* e alguns *websites* da *Deep Web* (designadamente o *The Hidden Wiki*) permitem a qualquer utilizador do *Tor* conhecer, sem grande esforço, os *links* para *hidden services* da *Dark Web* com conteúdos tão diversificados quanto a difusão de pornografia infantil, a troca de experiências pessoais dos vários utilizadores sobre condutas sexuais pedófilas, o incitamento à violência sexual contra adultos e menores, o ensino de técnicas de rapto de menores, o tráfico de droga, a venda e o ensino de fabrico de explosivos ou o recrutamento de homicidas a soldo. Nestas páginas são disponibilizados ficheiros, muitas vezes enviados pelos utilizadores responsáveis pela prática dos ilícitos em causa, cuja recolha poderá, como se verá, conter informação essencial para a investigação criminal.

Assim, e tal como resultou claro do método utilizado pelos *Anonymous* na Operação *Darknet* V2, afigura-se-nos que a realização de uma pesquisa pelos motores de busca da *Surface Web* e os *websites* da *Dark Web* poderá produzir resultados de valor inestimável no combate a este tipo de cibercriminalidade.

2. A interceção de comunicações

À semelhança do que referimos quanto à quase totalidade dos meios de obtenção de prova abordados neste capítulo, o recurso à interceção em tempo real de dados de tráfego e/ou de conteúdo pressupõe, desde logo, o conhecimento prévio da identidade do suspeito ou de «*pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes do suspeito ou, no mínimo, da identidade da vítima do crime*» (embora no âmbito da *Dark Web* esta última hipótese seja menos provável), nos termos do art. 187.º, n.º 4 do CPP, aplicável *ex vi* do art. 18.º, n.º 4 da Lei do Cibercrime.

75 No âmbito da *Surface Web* este meio tem sido sobejamente utilizado com resultados positivos. A este respeito, veja-se o caso de Vito Roberto Palazzolo, fugitivo durante mais de 30 anos em virtude das suas implicações com a Máfia, que foi capturado pela Interpol em Janeiro de 2012 na sequência de informação por si colocada no Facebook que indicava que se encontrava na Tailândia.

Ora, como facilmente se depreenderá a partir do que se vem dizendo acerca do *software* que permite aceder à *Dark Web*, a interceção de dados de conteúdo para obtenção de prova da prática de ilícitos nesta área da Internet não surtirá qualquer efeito útil quando vise dados de conteúdo enviados a partir do sistema informático que origina a comunicação, uma vez que todas as comunicações enviadas se encontrarão, à partida, cifradas e, portanto, serão inacessíveis para qualquer outro que não o seu destinatário final.

Aliás, a única fase em que a comunicação deixará de se encontrar cifrada será, no caso do *Tor*, entre o momento em que sai do "túnel" e o momento em que chega ao seu destinatário (quer esse destinatário seja um *website* ou outra pessoa). Assim, na eventualidade de estarmos perante uma comunicação bilateral na *Dark Web*, apesar de a comunicação enviada se encontrar cifrada, em princípio a resposta recebida a essa comunicação já se encontrará decifrada (salvo se o utilizador tiver tomado medidas antiforenses adicionais no sentido da cifragem também destes dados[76]) e, por isso, em certos casos, admitimos que possa ser intercetada. Assim, se A envia uma mensagem a B através do *Tor* e se se pretende intercetar a mensagem do A no momento em que ela entra no "túnel", a medida não surtirá efeito em virtude de a comunicação do A se encontrar cifrada. Porém, se se conseguir intercetar a resposta do B, então a interceção, pelo menos em teoria, poderá surtir efeito, uma vez que, durante o trajeto percorrido pela comunicação de B desde que sai do *exit node* até que chega ao conhecimento do A, esta, em princípio, não se encontrará cifrada.

Resta, portanto, concluir que, apesar de estarmos novamente perante uma medida processual de aplicação e utilidade residuais nos casos em que se desconheça a identidade do visado, ainda assim, em certos casos, a sua utilização permitirá a obtenção de dados com valor probatório de relevo.

3. As ações encobertas em ambiente digital

Numa curiosa inversão de papéis, a Lei do Cibercrime veio colmatar uma grave lacuna na Convenção sobre Cibercrime ao consagrar, no seu art. 19.º, o recurso a ações encobertas em ambiente digital.

Embora, a nosso ver, o legislador pudesse ter sido mais cauteloso na remissão genérica para o regime da Lei n.º 101/2001, de 25 de agosto, designadamente atentando, de forma mais detalhada, nas especificidades da investigação criminal

76 Plaintext over Tor is still plaintext, 2010, Morozov, 2011: 169-170.

em ambiente digital[77], cremos que o passo dado por este art. 19.º da Lei do Cibercrime vai no sentido certo, ao reconhecer a necessidade do recurso a métodos de investigação criminal mais agressivos em relação a uma criminalidade que tem beneficiado largamente da ineficácia dos restantes meios disponíveis.

Trata-se de uma medida há muito utilizada nos Estados Unidos da América[78], com resultados surpreendentemente positivos, em especial no combate ao jogo ilegal, ao tráfico de droga[79], à pornografia infantil[80] e à pedofilia *online*[81], e que se tem revelado de valor inestimável na prevenção e repressão deste tipo de cibercriminalidade[82].

Daí que, recentemente, a União Europeia tenha vindo a sugerir a sua implementação nas várias legislações nacionais através da Diretiva 2011/92/UE, do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia

77 Por exemplo, não faz qualquer sentido a remissão para o regime da atribuição de identidade fictícia ao agente encoberto, previsto no art. 5.º da Lei n.º 101/2001, de 25 de agosto, quando a ação encoberta decorra em ambiente digital. Significará isto que para a criação de uma ou mais contas de utilizador para aceder a uma sala de *chat* ou para a criação de um ou mais perfis fictícios no *Facebook*, tenha de ser proferido, de cada vez, despacho do Ministro da Justiça, mediante proposta do Diretor Nacional da PJ?

78 A este respeito há que realçar o célebre caso do *Dark Market*, um fórum *online* dedicado à compra e venda de identidades roubadas e, principalmente, de dados relativos a cartões de crédito. Ao longo de dois anos, o Agente Especial J. Keith Mularski do FBI conseguiu infiltrar-se na organização, ascender a uma posição de chefia dentro do *site* e recolher informação suficiente para levar à detenção de dezenas dos seus membros. Aliás, a infiltração foi conseguida com tanto sucesso que a dada altura havia dois agentes infiltrados de duas agências governamentais diferentes a investigar-se um ao outro – v. o muito interessante relato de Glenny, 2011.

79 Casey, 2011: 691-692.

80 Marco Gercke qualifica o recurso às ações encobertas no combate à pornografia infantil como "vital", uma vez que a maior parte do material pedo-pornográfico é transmitido em fóruns fechados protegidos por palavras-passe, Gercke, 2011: 66.

81 De acordo com um estudo feito em 2006, em 76% das detenções ocorridas na sequência do recurso a um agente encoberto com o objetivo de detetar pedófilos, o agente envolvido apresentou-se em certos *chats* ou fóruns como sendo um menor, sendo que apenas 4% das detenções ocorreram na sequência de tentativas de compra ou de venda de menores ou de sexo com menores. – Mitchell, 2011: 267-281. Com efeito, as ações encobertas em que o agente se faz passar por menor em salas de *chat* ou outras plataformas *online* são essenciais para o combate a este tipo de criminalidade e, acima de tudo, para demover potenciais "predadores sexuais" de desenvolverem a sua atividade ilícita na *Internet*. Há casos em que, inclusivamente, os investigadores criminais se reúnem com menores de modo a poderem dominar e utilizar expressões típicas da sua geração, Urbas, 2010: 414.

82 Não partilhamos, em geral, das dúvidas de constitucionalidade suscitadas aqui por Benjamim Silva Rodrigues, exceto no que respeita à utilização de ações encobertas pela prática dos crimes consagrados no título IV do CDADC, uma vez que se nos afigura serem tipos de ilícito desprovidos de um desvalor e de uma intensidade axiológica tal que justifique o recurso a uma medida tão gravosa – Rodrigues, 2010: 455-456 e Rodrigues, 2011: 533.

infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho, em cujo Considerando 27 consta que "[o]*s responsáveis pela investigação e pela ação penal relativas aos crimes referidos na presente diretiva deverão dispor de instrumentos de investigação eficazes* […] *Se for caso disso, e de acordo com a legislação nacional, tais instrumentos deverão também incluir a possibilidade de as autoridades policiais utilizarem uma identidade falsa na Internet*.».

A eficácia do recurso às ações encobertas estende-se ao âmbito da *Dark Web*, onde tem revelado resultados que não encontram paralelo em qualquer outro meio de investigação criminal. A sua principal vantagem reside no facto de permitir ultrapassar os obstáculos à descoberta da identidade e localização dos autores dos crimes e respetivas vítimas, através da persuasão dos próprios suspeitos a ceder elementos que permitam a sua identificação.

Atente-se, nesta matéria, ao célebre caso do "Monstro de Riga", em que um agente encoberto do FBI conseguiu persuadir um frequentador de *chats* e *fóruns* dedicados à pedofilia *online* a enviar-lhe uma fotografia onde figurava um indivíduo adulto a abusar sexualmente de uma criança de 18 meses. Uma mera análise visual da fotografia permitiu descobrir que a criança tinha na sua mão um coelho de peluche, que rapidamente veio a ser identificado como *Miffy*, o conhecido personagem de livros infantis holandeses, o que veio a permitir um redirecionamento da investigação para a Holanda. Aí, com recurso à divulgação das imagens do menor (devidamente editadas) na zona onde se suspeitava que a camisola que este envergava fora vendida, veio a ser descoberta a sua identidade e, subsequentemente, a do seu agressor, o qual havia sido seu *babysitter*[83]. Após identificação e imediata detenção do agressor, veio a descobrir-se que o mesmo frequentava vários *websites* e fóruns dedicados à pornografia infantil na *Dark Web*, o que permitiu à polícia holandesa infiltrar-se em alguns deles, recolhendo todos o material probatório aí localizado e promovendo o seu encerramento[84].

Este exemplo permite demonstrar que, para a investigação da criminalidade na *Dark Web*, o recurso às ações encobertas é fulcral, uma vez que, não só permite que, através de um processo de integração numa dada comunidade *online*, os membros das redes criminosas descurem as suas defesas[85] e cometam

83 McKim, 2012.

84 Cf. Dutch police infiltrate child abuse network, 2011.

85 Embora, em certos casos, para aceder a alguns dos *websites* mais fechados com conteúdo ilícito, seja necessário ganhar a sua confiança com a prática de factos ilícitos. Atente-se, a este respeito, no caso do *W0nderland Club*, a maior rede de pornografia infantil a nível mundial no ano de 2001, cujo acesso apenas era disponibilizado a quem disponibilizasse 10.000 imagens de abusos sexuais de menores. Neste caso, o

erros que permitam a sua identificação, como permite recolher ficheiros que, como se verá, poderão conter informação escondida de importância superior.

Todavia, a desvantagem desta medida reside na insuscetibilidade de o recurso ao agente encoberto poder produzir qualquer efeito útil em *websites* que não permitem interação entre os seus membros ou frequentadores, como sejam aqueles onde apenas constam imagens ou vídeos de conteúdo ilícito para visualização ou *download*, sem possibilidade de inserção de comentários.

III. NOVOS CONTRIBUTOS DA CIÊNCIA FORENSE DIGITAL E SEU ENQUADRAMENTO PROCESSUAL PENAL

Comprovada a genérica ineficácia dos meios de obtenção de prova disponíveis na Lei do Cibercrime para fazer face às peculiaridades da criminalidade na *Dark Web*, cumpre agora aferir da eventual utilidade de alguns dos novos contributos da Ciência Forense Digital e da possibilidade, fáctica e jurídica, da sua aplicação em sede de investigação criminal.

A nossa análise será feita com base em dois momentos distintos da investigação criminal: o primeiro relativo à identificação do suspeito, o segundo relativo à análise dos dados apreendidos.

Nem todos estes contributos visam combater especificamente a criminalidade na *Dark Web*, mas todos eles oferecem respostas que poderão revelar-se de alguma utilidade neste âmbito, pelo que caberá aqui analisá-los separadamente, enquadrando-os devidamente na lei processual penal portuguesa e aferindo da sua admissibilidade jurídica e eficácia técnica.

1. A identificação do suspeito na *Dark Web*

A principal dificuldade sentida na investigação criminal na *Dark Web* é, precisamente, a da incapacidade de os meios técnicos e processuais actualmente disponíveis permitirem descobrir eficazmente a origem do conteúdo ou comunicação de teor criminoso.

Com efeito, e como já se referiu, o anonimato que o *software supra* referido confere aos seus utilizadores funciona, simultaneamente, como segurança para aqueles que escolhem exercer a sua liberdade de opinião em regimes ditatoriais

---

recurso ao agente encoberto poderia revelar-se impossível ao abrigo do art. 6.º, n.º 1, da Lei n.º 101/2001, de 25 de agosto, aplicável *ex vi* do proémio do n.º 1 do art. 19.º da LC, uma vez que tal consubstanciaria a prática, em autoria imediata, de um crime de divulgação de pornografia de menores, p. e p. no art. 176.º, n.º 1, al. *b)* do CP. Acerca do *W0nderland Club*, seu funcionamento e encerramento, cf. Frank, Westlake & Bouchard, 2010: 2, Clough, 2010: 250.

e como garantia de impunidade para aqueles que escolhem utilizá-lo na prática de factos ilícitos. Daí que a descoberta de novos meios que permitam revelar a identidade dos seus utilizadores se possa revelar perigosa e talvez até, ponderados os benefícios e malefícios, indesejável.

Por esse motivo, de cada vez que uma falha em qualquer um destes *softwares* é detetada, os responsáveis pelos seus desenvolvimento e manutenção tendem a lançar, num espaço de horas, novas atualizações ou conselhos de utilização que frustram a sua futura exploração pelas forças policiais ou pelos governos em regimes ditatoriais.

No presente tópico procuraremos enquadrar técnica e juridicamente alguns dos meios que permitem identificar, com maior ou menor precisão, a autoria da colocação de um dado conteúdo na *Dark Web*.

1.1. Análise textual na *Dark Web*

Na sequência dos eventos ocorridos a 11 de setembro de 2001, o Laboratório de Inteligência Artificial da Universidade do Arizona iniciou um projeto intitulado de *Dark Web Project*[86], liderado por Hsinchun Chen, cujo objetivo é o de recolher e analisar todo o conteúdo gerado por grupos dedicados ao terrorismo internacional, incluindo *websites*[87], fóruns, salas de *chat*, blogues, redes sociais, vídeos, entre outros[88], na *Dark Web*.

A abordagem adotada tem incidido em duas fases distintas: em primeiro lugar, a identificação e recolha do conteúdo visado, em segundo lugar, a análise desse conteúdo com vista ao estabelecimento de uma correlação entre os vários textos e, se possível, à identificação de uma autoria comum dos mesmos.

No que concerne à primeira fase, a mesma tem-se baseado na utilização de *crawlers* especificamente desenhados para recolher ficheiros e informação em determinados *websites* na *Dark Web*, sendo certo que, tendo em conta a

86 Porém, na terminologia adotada pela Universidade do Arizona, o termo *Dark Web* reporta-se somente à área da Internet utilizada por grupos extremistas para promover o ódio e a violência, em particular, grupos terroristas. Assim, a *Dark Web* será «*a porção da World Wide Web utilizada para ajudar a alcançar os objetivos sinistros de terroristas e extremistas*». Apesar de esta definição englobar tanto a *Surface Web* como a *Deep Web*, é nesta área que se tem focado o estudo da Universidade do Arizona – cf. Chen, 2012: p. 45, Chen, 2008: 1347 e 1349.

87 Só em 2005, na sequência da exploração de informação obtida por fontes governamentais, este projeto permitiu a identificação de 104 websites criados por quatro dos maiores grupos terroristas internacionais – Al-Gama'a, al-Islamiyya, Hizballa, Al-Jihad, e a Jihad Palestino-Islâmica – e a subsequente análise de todas as suas páginas e extração de todos os hyperlinks aí contidos – cf. Xu & Chen, 2008: 61.

88 Chen, 2012: v.

inexistência de motores de busca que permitam a descoberta e entrada nestes *websites*, a utilização dos *crawlers* pressupõe uma «*human-assisted approach*»[89] prévia por parte dos investigadores, isto é, pressupõe uma investigação e infiltração prévias. Contudo, a verdadeira inovação fornecida pela Universidade do Arizona à Ciência Forense Digital, reside no método desenvolvido para proceder à análise do conteúdo textual recolhido.

Aproveitando trabalhos anteriores na área da linguística sobre estilometria[90], isto é, a análise estatística do estilo literário, o projeto *Dark Web* desenvolveu uma técnica de análise textual intitulada de *Writeprints*. As *Writeprints* funcionam, então, como um meio de identificação, análogo às impressões digitais (*fingerprints*), e que se traduz na deteção da autoria comum de vários textos através de uma análise do estilo de escrita. Esta análise funciona com base na deteção de padrões de escrita em quatro vetores: um vetor léxico, que tem em conta o número total de palavras por frase e de distribuição das palavras em função do seu comprimento; um vetor sintático, que se refere a padrões na construção de frases, como a pontuação; um vetor estrutural que lida com a organização e disposição do texto, como a utilização de saudações e assinaturas, o número e a média de comprimento dos parágrafos; e, por fim, um vetor de conteúdo específico, que lida com palavras-chave tidas como importantes num tópico específico[91], como sejam termos relacionados com pornografia infantil ou pirataria informática[92]. Após uma primeira sujeição do texto a uma análise automatizada, com base naqueles vetores, a informação será processada, informatizada e utilizada na comparação daquele escrito inicial com vários outros textos, com vista à deteção de uma autoria comum para todos ou alguns deles.

A utilização deste método – o qual, adiante-se, tem demonstrado uma eficácia que chega aos 95%[93] – permite detetar padrões de escrita de utilizadores anónimos na *Dark Web* (embora somente em língua inglesa, árabe e nos dialetos chineses) e compará-los com textos disponíveis na *Surface Web*, cuja origem será, à partida, mais fácil de identificar.

89 Chen, 2012: 46.

90 Abbasi & Chen, 2008: 1-27.

91 Chen, 2012: 411.

92 Li, Zheng & Chen, 2006: 76-82.

93 Chen, 2012: 6.

Assim, transpondo este método para o contexto em análise, havendo, por parte do investigador, um conhecimento prévio da existência de um fórum dedicado, por hipótese, à troca e comentário de material e experiências de natureza pedo-pornográfica na *Dark Web*, a utilização das *Writeprints* poderia permitir a identificação do estilo de escrita de um dado utilizador em vários outros fóruns, possivelmente, na *Surface Web*, assim levando à sua identificação.

Ponderando uma eventual utilização das *Writeprints* no ordenamento jurídico português, verifica-se que inexiste qualquer obstáculo (a não ser de natureza fáctica, em virtude da eventual dificuldade em obter o *software*, especialmente em língua portuguesa, bem como a formação necessárias à sua utilização) à sua consagração na prática forense enquanto meio de prova, em particular sob a forma de prova pericial, nos termos dos arts. 151.º e seguintes do CPP.

Com efeito, se a identificação do autor de vários textos na *Dark Web* for possível com recurso a *Writeprints*, e tendo em conta que a realização (e explicação) do procedimento conducente à conclusão daquela autoria comum carece de especiais conhecimentos técnicos, afigura-se-nos que a nomeação de pessoa idónea para proceder, por intermédio do *software* apropriado, à análise textual que compõe o objeto de estudo, permitirá equacionar a subtração do juízo assim emitido à livre apreciação do julgador (nos termos do art. 163.º, n.º 1 do CPP) e permitirá fortalecer a perceção ou apreciação dos factos que fundamentam a identificação da autoria de um facto praticado na *Dark Web*.

1.2. Os ataques de *fingerprinting*

Durante a curta existência do *Tor*, têm sido várias as tentativas de contornar as suas propriedades indutoras de anonimato. Não obstante o potencial prejuízo que esta atividade possa ter a curto prazo para os utilizadores *legítimos* do *Tor*, a verdade é que a constante sujeição deste *software* a testes e ataques cada vez mais avançados, permite que a equipa do Projeto *Tor* proceda a uma *blindagem* do mesmo[94] e previna a exploração futura dessas lacunas em prejuízo dos seus utilizadores.

Entre essas tentativas, destacam-se os ataques de *fingerprinting*. Em termos genéricos, os ataques de *fingerprinting* consistem em tentativas de reconhecimento da origem do tráfego *online*, independentemente do facto de o seu

94 Por exemplo, no dia 13 de setembro de 2011 o Irão criou um filtro que detetava o tráfego *Tor* e bloqueava o acesso a esta rede. No espaço de 24 horas o Projeto *Tor* lançou uma nova versão do *Tor* que permitiu contornar aquele bloqueio.

conteúdo se encontrar cifrado e de o utilizador visado utilizar programas indutores de anonimato.

O ataque mais comum de *fingerprinting* consiste na monitorização do tráfego da rede *Tor* e na comparação entre o volume do pacote de dados enviado a uma dada hora por um utilizador *Tor* e o volume de dados que posteriormente abandona o último "nódulo" da rede. Por exemplo, imagine-se que A pretende aceder a um determinado *website* através do *Tor*. Este acesso será feito através do envio de um pedido, por parte do sistema informático de A, àquele *website*. A entidade monitorizadora do tráfego *Tor* verá, então, um pacote de dados a ser enviado pelo computador de A para o computador de B, outro utilizador do *Tor* e o segundo nódulo do *túnel*. O computador de B, por sua vez, enviará então a comunicação para o computador do C (o *exit node* da comunicação *Tor*), o qual enviará a comunicação, já sem cifragem, para o fornecedor de serviço que permitirá o acesso ao *website*. Neste momento, a entidade monitorizadora da rede *Tor* constatará que àquela hora, saiu um pacote de dados do computador de A, seguida da partida de um pacote de dados ligeiramente menor do computador de B, seguida de uma comunicação decifrada com um volume muito próximo daquela que partiu do computador de C para o fornecedor de serviço. Com base na proximidade cronológica das sucessivas transmissões dos dados e no tamanho do pacote de dados enviados, seria possível estabelecer um nexo entre a comunicação inicial e a comunicação final[95].

Contudo, dois problemas surgem, desde logo, na utilização desta técnica – sem contar, naturalmente, com o problema óbvio da dificuldade técnica em monitorizar todos os nódulos da rede *Tor*. A primeira é que o Projeto *Tor* passou a incluir, na transmissão das suas comunicações, um atraso aleatório que dificulta seriamente o estabelecimento de uma ligação entre a comunicação enviada a partir de qualquer nódulo e o seu ponto de origem. A segunda consiste na extrema dificuldade técnica da execução de um ataque deste género, em particular quando estivermos perante utilizadores informados e cautelosos que consigam aumentar, por outras vias, a proteção do seu anonimato.

Uma segunda versão deste ataque consiste na análise prévia do volume do pacote de dados necessário para aceder a um determinado *website* e na monitorização de nódulos específicos da rede *Tor* com vista à comparação entre os pacotes de dados enviados e aqueles necessários para aceder ao catálogo de *websites* previamente estabelecido. Contudo, a verdade é que, esta vulnerabilidade já foi

95 Vacca, 2005: 652.

colmatada pelo Projeto *Tor* através da criação dos seus *Pluggable Transports*, os quais *mascaram* o tráfego *Tor* e lhe conferem a aparência de tráfego normal.

No entanto, as técnicas de *fingerprinting* são várias, muitas delas de elevada complexidade técnica, sendo que, em certos casos – de acordo com o Projeto *Tor* –, a sua utilização já permitiu inutilizar o anonimato fornecido pelo *Tor*.

Neste sentido, afigura-se-nos que a resposta a empreender pelas entidades estatais poderá passar pelo estabelecimento das (cada vez mais apetecíveis em matéria de cibercrime) parcerias público-privadas com entidades especializadas[96] em questões técnicas relacionadas com as tecnologias da informação (designadamente Universidades), de modo a permitir explorar o terreno fértil das técnicas de *fingerprinting*, especialmente porque a sua utilização apenas carece do acesso aos dados de tráfego, o que já se encontra previsto a nível comunitário[97] pela Diretiva n.º 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

1.3. O recurso ao *malware*[98] e a *hyperlink sting operations*

A dificuldade no combate à cibercriminalidade tem levado à generalização da adoção de medidas progressivamente mais invasivas e, dir-se-ia mesmo, agressivas, com o intuito de aumentar a eficácia da ação penal numa área dominada pelas cifras negras. Entre essas medidas encontram-se o recurso ao *malware* e a *hyperlink sting operations*, que optámos por abordar sinteticamente no mesmo tópico, em virtude da similitude de princípio subjacente a ambos.

O *malware*, como o próprio nome indica, consiste num programa informático (*software*) malicioso (*malicious*) que, nas modalidades que aqui relevam, permite monitorizar à distância a atividade desenvolvida num determinado sistema informático. Trata-se de um programa instalado de forma secreta e insidiosa no sistema informático visado (por exemplo, através de acesso físico ao sistema informático visado ou disfarçado de atualização do *Windows* ou

96 Acerca da importância das parcerias público-privadas em matéria de combate à pirataria, cf. Masson, 2009: 295-304.

97 Exceto nos países que ainda não transpuseram esta Diretiva ou naqueles em que a mesma foi declarada inconstitucional, como na Alemanha, Roménia e República Checa.

98 Para uma análise mais detalhada do enquadramento técnico, histórico e jurídico do *malware* à luz da Lei do Cibercrime, v. o nosso *O uso de malware como meio de obtenção de prova em processo penal*, em curso de publicação na presente Revista.

de *cookie*) e que o infeta de modo a permitir a recolha de informação e dados introduzidos pelo utilizador, subsequentemente reenviando-os para o órgão de polícia criminal ou autoridade judiciária competente[99].

O uso de *malware* pelas forças policiais ganhou especial dimensão no ano de 2001, altura em que foi divulgada a existência do *malware* norte-americano *Magic Lantern*, tendo mais tarde dado origem ao *Computer and Internet Protocol Addresss Verifier* (CIPAV)[100], e que consistia num *keylogger*[101] instalado no computador de indivíduos – localizados ou não nos EUA – suspeitos de estarem relacionados com atividades criminosas, em particular de natureza terrorista[102].

Porém, a modalidade mais invasiva de *malware*[103] publicamente conhecida a ser utilizada por forças policiais viria a ser divulgada, com um grande impacto na comunicação social[104], na Alemanha, em 2011, por um grupo *hacker* intitulado de *Chaos Computer Club*[105]. Este programa, entretanto vendido também à Áustria, viria a ser apodado de *Bundestrojaner*[106] e consiste numa espécie de

99 Neste sentido, Pinto de Albuquerque, 2011: 502.

100 Este software viria a ser divulgado em 2007 através da publicitação de um pedido de mandado apresentado pelo Agente Especial do FBI Norman Sanders no âmbito de um processo em que se procurava detetar o autor de várias ameaças de bomba. Para consultar uma cópia digitalizada do documento, v. http://www.wired.com/images_blogs/threatlevel/files/timberline_affidavit.pdf [consultado em 04.10.2012].

101 Trata-se de um *software* que visa gravar informação que identifica as teclas premidas pelo utilizador de um sistema informático, com vista à monitorização e documentação da atividade empreendida neste, bem como à obtenção das palavras passe e outras informações relevantes que tenham sido introduzidas através do teclado.

102 Acerca da utilização destes métodos de obtenção de prova, atente-se na seguinte excerto da decisão proferida no âmbito do caso *United States v. Scarfo*: "*we must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes*", Woo & So, 2002: 533.

103 Não incluímos aqui, naturalmente, os já célebres vírus *Stuxnet* e *Flame*, uma vez que o seu âmbito de aplicação material se reporta à espionagem e não à investigação criminal.

104 Já anteriormente, em 2008, o Tribunal Constitucional Alemão declarara inconstitucional a Lei da Renânia Norte-Vestefália que introduzia a utilização de *malware* como meio de obtenção de prova, fundamentando-o, entre outros motivos, no facto de esta não respeitar o princípio da proporcionalidade. Simultaneamente, o Tribunal reconheceu o direito fundamental à garantia da confidencialidade e integridade dos sistemas informáticos (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). – para uma análise mais detalhada da decisão deste tribunal cf. Ortiz Pradillo, 2011: 376-377 e, por todos, Vaciago, 2012a: 125-129. Altamente crítico das tendências legislativas do Tribunal Constitucional Alemão, em particular no que concerne à limitação do âmbito de aplicação das buscas *online* (através do recurso a *malware*), cf. Rogall, 2009: 123-124.

105 Rosenbach, 2011.

106 Para uma análise mais detalhada da origem e funcionamento do *Bundestrojaner* e da utilização deste tipo de programas pela Suíça e pela Áustria, v., por todos, Weber & Heinrich, 2012: 60-65.

malware enviado para o computador do suspeito sob a forma de uma comum atualização de *software* e que, após instalação, permite gravar as chamadas *Skype*, monitorizar toda a atividade do suspeito na Internet, gravar as palavras-passe por ele inseridas e, inclusivamente, ativar o *hardware* do computador do visado, utilizando os seus microfones e a *webcam* para gravar sons e tirar fotos que "subsequentemente" serão enviadas para as autoridades[107].

Ora, apesar de o uso deste tipo de *software* gerar questões complexas relativas ao princípio da lealdade e da proporcionalidade face ao conflito com o direito à reserva da intimidade da vida privada, a verdade é que a sua utilização tem-se alastrado pelos vários ordenamentos jurídicos e a sua consagração já foi, inclusivamente, sugerida no citado Considerando n.º 27 da Diretiva 2011/92/EU do Parlamento Europeu e do Conselho, nos termos seguintes: "[o]*s responsáveis pela investigação e pela ação penal relativas aos crimes referidos na presente diretiva 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 investigações financeiras, tendo em conta, nomeadamente, o princípio da proporcionalidade e a natureza e gravidade dos crimes investigados*".

Porém, dando como assente a existência de norma legal habilitante do recurso ao *malware*, no plano do direito constituído[108], a verdade é que os moldes que a sua aplicação na *Dark Web* teria de revestir revelam peculiaridades que poderão comprometer a sua admissibilidade no plano legal e constitucional. Com efeito, enquanto o *malware* geralmente utilizado por algumas polícias pressupõe uma identificação prévia do suspeito e o envio daquele *software* sob a forma de uma atualização de um outro programa, na *Dark Web* este procedimento será, na prática, mais difícil, pois o investigador não tem conhecimento da identidade do visado – exceto, talvez, do seu nome de utilizador num dado *website* ou fórum ou do *browser* por este utilizado – e, por outro lado, o envio de atualizações via *Tor* ou *Freenet* por esta via afigura-se não só tecnicamente difícil, como suspeito para o comum utilizador destes *softwares*.

107 Vaciago, 2012b: 8-11.

108 Embora com as reservas no plano da sua constitucionalidade que referimos no nosso estudo sobre *O uso de malware como meio de obtenção de prova em processo penal,* publicado na presente revista.

As alternativas serão, então, a implantação de *malware* em ficheiros com títulos que induzam a ideia de que neles se inclui conteúdo ilegal e sua subsequente divulgação em *websites* e fóruns dedicados à sua partilha, na esperança que algum utilizador faça *download* do mesmo e infete o seu próprio computador[109].

Este procedimento assemelha-se em muito àquele utilizado pelo FBI, em 2008, no caso das *hyperlink sting operations*, embora, neste caso, esse método tenha sido utilizado na *Surface Web*. As *hyperlink sting operations* consistem na publicitação, por parte de um órgão de polícia criminal, de *hyperlinks* que supostamente dariam acesso a conteúdo de natureza pedo-pornográfica, mas que, na realidade, uma vez acedidos, apenas servem para dar conhecimento ao FBI do endereço de IP da ligação a partir da qual partiu a comunicação[110]. Ora, a possibilidade de estes ficheiros e *hyperlinks* serem reenviados entre vários cibernautas, sem qualquer referência ao seu conteúdo, por via de vários tipos de comunicações eletrónicas (pense-se, por exemplo, no utilizador que copia o *link* ou reenvia o ficheiro com o título alterado para um terceiro sem fazer menção ao seu conteúdo), permite que o acesso aos mesmos nem sempre manifeste uma intencionalidade de acesso ao conteúdo ilícito, mas antes se traduza no mero acesso a um *hyperlink* ou no *download* de um ficheiro sem conhecimento do seu conteúdo.

Assim, na medida em que a colocação de ficheiros infetados com *malware* policial em *websites* e fóruns da *Dark Web* se poderia revelar uma atividade de natureza provocadora[111], com um potencial excessivamente gravoso, com elevados índices de falibilidade e potencialmente violadora do princípio da proporcionalidade no confronto entre os interesses sacrificados[112] e aqueles que se visam salvaguardar, cremos que o recurso a *malware* não poderá ser utilizado.

2. Análise de dados informáticos apreendidos na *Dark Web*

Admitindo, porém, que o investigador consegue aceder a um fórum ou *website*, ou mesmo a uma *darknet*, na *Dark Web* e aí recolhe ficheiros informáticos

109 É precisamente para evitar a infeção do computador do utilizador do *Tor* e para prevenir a utilização de *software* que permita divulgar o seu IP que este programa apresenta sempre o mesmo aviso quando é feito o *download* de qualquer ficheiro ou programa: *"An external application is needed which could compromise your identity."*

110 McCullagh, 2008.

111 Comparável à do agente provocador, designadamente para aqueles que defendem a consagração futura do malware como "polícias digitais" automáticos, Vaciago, 2012b: 10-11, Vaciago, 2012a: 129.

112 Assim, Rodrigues: 2010: 474.

disponíveis para *download*, haverá que analisar qual a informação, para além da decorrente da mera visualização do ficheiro, que poderá ser recolhida e reaproveitada a partir dos mesmos.

Para isso, optámos por abordar na presente secção as duas técnicas que se nos afiguram como de maior relevância e expressividade na extração de informação apta a permitir uma maior eficácia no combate à criminalidade na *Dark Web*: a primeira, mais conhecida e comummente utilizada, e a segunda, mais recente e especificamente direcionada para o combate à pornografia infantil.

2.1. O uso de *metadata*

O acesso a ficheiros armazenados em rede, incluindo na *Dark Web*, poderá permitir a extração de *metadata*[113] relevante, isto é, a extração de *dados sobre os dados* recolhidos, como sejam a data e hora em que o ficheiro foi criado, modificado[114], acedido e/ou escrito, quem tinha permissão para a ele aceder e qual o nome[115] constante do computador/*software* do seu autor e/ou da última pessoa que o editou[116]. Em certos casos, se estivermos perante fotografias, o próprio ficheiro pode conter o número de série da máquina fotográfica utilizada, bem como detalhes acerca da garantia desse aparelho, ou mesmo, em máquinas mais modernas, em *smartphones* ou *tablets*, poderá permitir o

113 Para uma análise esquematizada e de cariz mais técnico sobre os vários tipos de *metadata*, cf. Guo & Slay, 2010: 307.

114 No célebre caso "Garlasco", foi graças ao recurso a *metadata* que o acusado veio a ser definitivamente absolvido pelo Tribunal de Assize de Milão, a 6 de dezembro de 2011. O caso pode, muito sinteticamente, resumir-se do seguinte modo: Alberto Stasi era o principal suspeito do homicídio da sua noiva Chiari Poggi, que ocorrera algures entre as 10h30m e as 12h de 13 de agosto de 2007. Stasi defendeu-se, alegando que, àquela hora, se encontrava ao computador a escrever o seu trabalho final de curso. Para provar esse facto, entregou às autoridades o seu computador, ainda ligado, para que pudessem confirmar o seu álibi. A polícia, sem qualquer respeito pelas mais elementares regras forenses, acedeu a 39.000 dos 56.000 ficheiros gravados no disco rígido, alterou 1.500 ficheiros (entre os quais o trabalho final de Stasi) e criou 500 novos ficheiros, para além de terem ligado vários dispositivos USB ao computador sem qualquer preocupação com eventual contaminação da prova. Foi necessária a nomeação de um painel de peritos que, através de análise de *metadata*, concluíram que, entre as 10h37m e as 12h20m o computador do acusado esteve ininterruptamente em uso, Vaciago, 2012a: 29.

115 Por exemplo, Dennis Rader, o assassino conhecido como BTK (nome que deriva do seu *modus operandi* e que significa *bind, torture and kill*), foi identificado em 2004 (30 anos após o seu primeiro homicídio e 10 anos desde o último) através de metadata inserido num documento Word por si enviado numa disquete para uma estação televisiva. Após a análise do *metadata* contido no ficheiro, o FBI descobriu que o autor documento tinha como primeiro nome Dennis, tendo inclusivamente encontrado um *link* para uma Igreja Luterana, o que, adicionado ao facto de se saber que o suspeito tinha um jipe *Cherokee* preto e ao facto de os crimes ocorrerem em *Wichita*, permitiu identificar Dennis Rader, diácono de uma igreja luterana em *Wichita*, como o autor dos homicídios.

116 Cohen, 2007: 1.

acesso a *geo-tags* que revelam a localização do aparelho que captou a imagem no momento em que a fotografia foi tirada[117].

A identificação deste tipo de dados poderá, não só permitir a identificação de algum dos anteriores detentores daquele ficheiro, do seu autor e localização, como poderá ainda identificar, num conjunto de várias fotografias, uma origem comum, caso as mesmas tenham sido tiradas com recurso a uma só máquina fotográfica. Esta última informação poderá permitir confrontar o número de série da máquina fotográfica utilizada para tirar uma fotografia de teor ilícito disponibilizada na *Dark Web* com aquele constante de *metadata* colocado em fotografias localizadas na *Surface Web*, de teor mais inócuo, assim facilitando a identificação do seu autor.

Porém, o problema da valoração do *metadata* prende-se com a facilidade com que o mesmo poderá ser alterado por qualquer utilizador, voluntária ou involuntariamente, em particular quando seja recolhido a partir de uma localização *online*, o que lhe retira força probatória. Daí que a sua recolha, para além de ter de obedecer às regras da Ciência Forense Digital, tenha de ser conjugada com outros fatores de cariz indiciário, como a associação do nome de utilizador sob o qual um dado ficheiro foi colocado na *Dark Web*, com a eventual utilização desse mesmo nome associado a outro ficheiro colocado na *Surface Web* com conteúdo a nível de *metadata* semelhante.

A recolha, análise e aferição da credibilidade deste tipo de informação terá de vir sempre acompanhada de um juízo técnico de natureza pericial que permita atribuir-lhe o devido valor a nível probatório, sempre tendo em conta a facilidade da sua contaminação e a necessidade de a conjugar com outros elementos para fundar qualquer juízo condenatório em sede penal.

2.2. *PhotoDNA*

Em 2009 a *Microsoft*, em parceria com a Universidade de Dartmouth, desenvolveu um *software* que veio a chamar de *PhotoDNA*, cujo objetivo era o de facilitar a deteção e remoção das piores imagens de pornografia infantil disponíveis *online*.

O funcionamento do *PhotoDNA* assenta na descoberta de um conjunto de características únicas em cada fotografia que permitem distingui-la de qualquer outra imagem e que são identificáveis mesmo após aquela ter sido alterada, ter

117 Friedland &Sommer, 2010.

perdido definição ou ter sido redimensionada[118]. A extração desta informação visa permitir detetar cópias de certas imagens previamente analisadas em sistemas informáticos como computadores ou servidores. Assim, com base na recolha de uma fotografia com conteúdo pedo-pornográfico e subsequente extração do seu *PhotoDNA*, torna-se possível – com 100% de fidedignidade – detetar cópias dessa imagem em servidores e, desejavelmente, identificar o indivíduo que as detém ou que as disponibilizou.

Trata-se de uma tecnologia que foi inicialmente cedida ao *National Center for Missing & Exploited Children* (NCMEC), uma vez que este centro contém mais de 65 milhões de imagens e vídeos de exploração sexual infantil, e que entretanto já veio a ser instalada nos servidores da própria *Microsoft*, bem como, desde 2011, do *Facebook*, estando prevista a sua gradual implementação no motor de busca *Bing*, no *Skydrive* e no *Hotmail*. Face à finalidade prosseguida por este *software*, o mesmo tem sido cedido de forma gratuita às polícias que assim o solicitem.

Analisando agora a utilidade deste *software* no que concerne à análise de dados informáticos recolhidos na *Dark Web*, verifica-se que a extração de *PhotoDNA* a partir de fotos recolhidas, por exemplo, em *hidden services* do *Tor* dedicados à difusão de pornografia infantil, permitirá a sua subsequente utilização no rastreamento de cópias dessas imagens em servidores que forneçam serviços na *Surface Web*, como os do *Facebook*, assim permitindo identificar alguns dos proprietários desse tipo de material.

Na medida em que seja tecnicamente possível excluir dos dados abrangidos pela pesquisa as mensagens de correio eletrónico ou registos de natureza semelhante e desde que se vise a apreensão de dados determinados no âmbito de um processo criminal previamente instaurado e devidamente direcionado à investigação de infrações concretas e não à mera *pesca* de conhecimentos fortuitos, não cremos que existam objeções de natureza legal ou constitucional à sua utilização no âmbito de uma pesquisa de dados informáticos, nos termos do art. 15.º da Lei do Cibercrime.

Em todo o caso, a instalação por iniciativa das entidades privadas que forneçam serviços *online* – como sucedeu no caso do *Facebook* –, designadamente de alojamento de *websites*, deste tipo de *software* com vista à imposição do cumprimento dos seus termos de serviço e à supressão de material com

118 A este respeito veja-se a página da Internet disponibilizada pela *Microsoft* com a explicação do *PhotoDNA*, acedida e consultada em 15-10-2012, no endereço http://www.microsoft.com/en-us/news/presskits/photodna/.

pornografia infantil dos seus servidores, quando seguida de uma denúncia da deteção daquele material ao Ministério Público, poderá revelar-se como um exemplo extremamente profícuo de parceria público-privada no combate ao cibercrime e como o método mais eficaz de utilização do *PhotoDNA*.

CONCLUSÕES

O combate ao cibercrime e a recolha de prova em ambiente digital enfrentam hoje dificuldades técnicas e jurídicas sem precedentes e, diríamos, sem paralelo em qualquer outra área do Direito Penal. A proliferação de técnicas antiforenses que impedem a deteção dos agentes do crime, aliada a uma conceção territorialmente limitada da Internet que por vezes impossibilita a recolha, em tempo útil, do material probatório necessário à sua prossecução penal, tornam o mundo *online* num campo de eleição, não só para a prática de atos subsumíveis ao conceito de cibercrime, mas também para a promoção de atos que transcendem a realidade da Internet e que, graças a ela, permanecem invisíveis aos olhos do sistema.

O surgimento da *Dark Web* vem confrontar a realidade jurídica com um novo nível de criminalidade cuja gravidade só agora começa a ser publicamente revelada e que permite aos seus agentes, com um grau mínimo de conhecimentos técnicos, permanecerem invisíveis e potencialmente indetetáveis aos olhos de quaisquer entidades.

Para se conseguir uma eficácia mínima no combate a esta criminalidade, haverá que recorrer aos meios técnicos disponibilizados pela Ciência Forense Digital, quer através da sua apropriação pelos órgãos de investigação criminal (no caso português, a PJ), quer através do recurso a instrumentos legais que permitam, como *ultima ratio*, recorrer a métodos de investigação criminal *online* mais invasivos e mais agressivos.

Todavia, a longo prazo a resposta deverá passar pela criação de parcerias público-privadas com entidades dotadas dos recursos e dos conhecimentos técnicos que permitam obter meios mais aptos a detetar este tipo de criminalidade, ainda que sempre com a devida cautela e parcimónia para não prejudicar os legítimos utilizadores dos *softwares* indutores de anonimato.

Em todo o caso, a verdade é que a realidade técnica e jurídica atualmente existente e que se estima vir a perdurar nos anos que se avizinham, juntamente com o constante aperfeiçoamento dos meios técnicos utilizados na prática do cibercrime, não oferecem meios adequados para combater esta criminalidade e, por esse motivo, a *Dark Web* continuará a ser sinónimo de *cifras negras*.

BIBLIOGRAFIA

Abbasi, Ahmed & Chen, Hsinchun

2008 "Writeprints: A Stylometric Approach to Identity-Level Identification and Similarity Detection in Cyberspace", *ACM Transactions on Information Systems*, Vol. XXVI, n.º 2, pp. 1-27.

Attfield, Philip

2005 "United States v Gorshkov – Detailed Forensics and Case Study; Expert Witness Pesperctive", *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering*, IEEE Computer Society Washington, DC, USA, pp. 3-26.

Beckett, Andy

2009 "The dark side of the Internet", disponível em: http://www.guardian.co.uk/technology/2009/nov/26/dark-side-internet-freenet [consultado em: 09.06.2012].

Bergman, Michael K.

2001 "The Deep Web: Surfacing Hidden Value", *Journal of Electronic Publishing*, Vol. VII, n.º 1, pp. 1-31.

Bergelson, Vera

2008 "Autonomy, Dignity, and Consent to Harm", *Rutgers Law Review*, Vol. LX, n.º 3, pp. 723-736.

Cafarella, Michael J., Halevy, Alon & Madhavan, Jayant

2011 "Structured Data on the Web", *Communications of the ACM*, Vol. LIV, n.º 2, pp. 72-79.

Casey, Eoghan

2011 *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet*, 3.ª ed., Califórnia: Elsevier.

Chen, Adrian

2011 "Vigilante Hackers wage war on Underground Kiddie Porn", disponível em: http://gawker.com/5851459/vigilante-hackers-wage-war-on-underground-kiddie-porn [consultado em: 03.06.2012].

Chen, Hsinchun

2012 *Dark Web –Exploring and Data Mining the Dark Side of the Web*, Nova Iorque: Springer,

Chen, Hsinchun, et al.

2008 "Uncovering the Dark Web: A Case Study of Jihad on the Web", *Journal of The American Society for Information Science And Technology*, Vol. LIX, n.º 8, pp. 1347-1359.

Clarke, Ian
1999 *A Distributed, Decentralised Information Storage and Retrieval System,* disponível em: https://freenetproject.org/papers/ddisrs.pdf [consultado em: 09.06.2012].
Clarke, Ian, et al.
2001 *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, disponível em: http://www.facweb.iitkgp.ernet.in/~niloy/COURSE/Autumn2010/UC/Resource/freenet1-big.pdf [consultado em: 01.09.2012]
2002 "Protecting Free Expression Online with Freenet", *IEEE Internet Computing* (Janeiro-Fevereiro de 2002), pp. 40-49.
2009 *The Guardian writes about Freenet*, disponível em: http://blog.locut.us/2009/11/26/the-guardian-writes-about-freenet/ [consultado em: 09.06.2012]
Clough, Jonathan
2010 *Principles of Cybercrime*, Cambridge: Cambridge University Press.
Cohen, Kevin
2007 "Digital Still Camera Forensics", *Small Scale Digital Device Forensics Journal*, Vol. I, n.º 1, pp. 1-8.
Constantin, Lucian
2012 "Dutch Government to let law enforcement hack foreign computers", disponível em: http://www.computerworlduk.com/news/security/3406221/dutch-government-to-let-law-enforcement-hack-foreign-computers/ [consultado em: 26.10.2012].
Dingledine, Roger, Mathewson, Nick & Syverson, Paul
2004 "Tor: The Second-Generation Onion Router", *Proceedings of the 13th USENIX Security Symposium – August 9-13, 2004*, The USENIX Association, disponível em: http://static.usenix.org/event/sec04/tech/full_papers/dingledine/dingledine.pdf [consultado em: 09.06.2012].
Dong, Yongquan & LI, Qingzhong
2012 "A Deep Web Crawling Approach Based on Query Harvest Model", *Journal of Computational Information Systems*, Vol. VIII, n.º 3, Hong Kong: Binary Information Press, pp. 973–981.
Dhungel, Prithula, et al.
2010 "Waiting for Anonymity: Understanding Delays in the Tor Overlay", *Proceedings of the 10th IEEE Conference on Peer-to-Peer Computing*, pp. 1-4.
Esteves, Pedro
2012 "Hacktivismo, transpondo a fronteira entre a liberdade de expressão e o cibercrime", *Segurança e Defesa*, n.º 21, pp. 45-47.

Frank, Richard, Westlake, Bryce & Bouchard, Martin
2010 "The Structure and content of Online Child Exploitation Networks", *Proc. 16th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*.

Freire, Juliana & Barbosa, Luciano
2010 "Siphoning Hidden-Web Data through Keyword-Based Interfaces: Retrospective", *Journal of Information and Data Management*, Vol. I, n.º 1, pp. 145–146.

Friedland, Gerald & Sommer, Robin
2010 "Cybercasing the Joint: On the Privacy Implications of Geo-Tagging", *ICSI Technical Report* disponível em: http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf [consultado em: 14.06.2012]

Gercke, Marco
2011 *Understanding Cybercrime: A Guide for Developing Countries*, ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector, 2.ª ed., Genebra: ITU.

Glenny, Misha
2011 *Dark Market – Cyberthieves, Cybercops and You*, London: Bodley Head.

Grinberg, Reuben
2011 "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science and Technology Law Journal*, Vol. IV, n.º 1, pp. 160-210.

Guo, Yinghua & Slay, Jill
2010 "Data recovery function testing for digital forensic tools", *Advances in Digital Forensics VI - IFIP Advances in Information and Communication Technology,* pp. 297-311.

Hampson, Noah C. N.
2012 "Hacktivism, Anonymous & a New Breed of Protest in a Networked World", *Boston College International and Comparative Law Review*, Vol. XXXV, n.º 2, pp. 511-542.

Handschuh, Siegfried, Volz, Raphael & Staab, Steffen
2003 "Annotation for the Deep Web", *IEEE Intelligent Systems*, Vol. XVIII, n.º 5, New Jersey/USA: IEEE Educational Activities Department Piscataway, pp. 42-48.

Harris, Ryan
2006 "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", *Digital Investigation - The International Journal of Digital Forensics & Incident Response*, Vol. III – Suplemento, Elsevier Ltd, pp. S44-S49.

He, Bin et al.
2007 "Accessing the Deep Web: A Survey", *Communications of the ACM*, Vol. L, n.º 5, New York/USA, pp. 94-101.

Kaspersen, Henrik W. K.
2009 *Cybercrime and Internet Jurisdiction*, *Discussion paper* elaborado no âmbito do *Project on cybercrime* do Conselho da Europa, disponível em: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2009)%20draft%20discussion%20paper%20Cybercrime%20and%20jurisdiction.pdf [consultado em: 10.09.2012].

Lewandowski, Dirk & Philipp, Mayr
2006 "Exploring the academic invisible web", *Library Hi Tech*, Vol. XXIV, n.º 4, Germany: Emerald, pp. 529-539.

Li, Jiexun, Zheng, Rong & Chen, Hsinchun
2006 "From fingerprint to writeprint", *Communications of the ACM*, Vol. XLIX, n.º 4, ACM Nova Iorque, pp. 76-82.

Madhavan, Jayant, et al.,
2008 "Google's Deep-Web Crawl", *Proceedings of the VLDB Endowment*, Vol. I, n.º 2, New Zealand: ACM, Inc., pp. 1241-1252.

Masson, Laurent
2009 "Parcerias público-privadas: a única forma eficiente de combater a pirataria", in Palma, Maria Fernanda, Silva Dias, Augusto & Sousa Mendes, Paulo (coord. científica), *2.º Congresso de Investigação Criminal*, Coimbra: Almedina, pp. 295-304.

McCullagh, Declan
2008 "FBI posts fake hyperlinks to snare child porn suspects", *disponível em:* http://news.cnet.com/8301-13578_3-9899151-38.html [consultado em: 14.10.2012].

McKim, Jennifer B.
2012 "Led by an innocent into a web of evil", disponível em: http://www.boston.com/business/articles/2012/07/29/led_by_an_innocent_into_a_web_of_evil/?page=9 [consultado em 20.09.2012].

Mitchel, Kimberly J., et al.
2011 "Investigators using the Internet to apprehend sex offenders: findings from the Second National Juvenile Online Victimization Study", *Police Practice and Research: An International Journal*, Vol. XIII, n.º 3, Nova Iorque: Routledge – Taylor & Francis Group, pp. 267-281.

Morozov, Evgeny
2011 *The Net Delusion – The dark side of Internet Freedom*, Nova Iorque: Public Affairs.
Najork, Marc
2009 "Web Crawler Architecture", in Liu, Ling & Özsu, M. Tamer (eds.), *Encyclopaedia of Database Systems*, Parte 23, Springer Verlag USA, pp. 3462-3465.
Nakamoto, Satoshi
2008 *Bitcoin: A Peer-to-Peer Electronic Cash system*», disponível em: http://www.cs.kent.edu/~JAVED/class-P2P12F/papers-2012/PAPER2012-p2p-bitcoin-satoshinakamoto.pdf [consultado em: 1.10.2012].
Ortiz Pradillo, Juan Carlos
2011 "Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain", *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. XIX, n.º 4, pp. 363-396.
Patil, Nilesh Madhukar, Lingam, Chelpa,
2012 "Anonymous Connections and Onion Routing", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. II, n.º 2, pp. 31-37.
Pinto, Lara Sofia
2010 "Privilégio contra a auto-incriminação versus colaboração do arguido", in Beleza, Teresa Pizarro & Costa Pinto, Frederico (coord.), *Prova Criminal e Direito de Defesa – Estudos sobre teoria da prova e garantias de defesa em processo penal*, Coimbra: Almedina.
Pinto de Albuquerque, Paulo
2011 *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4.ª ed., Lisboa: Universidade Católica Editora.
Quayle, Ethel
2009 "Assessment of Internet Sexual Abuse", in Calder, Martin C. (ed.), *Sexual abuse assessments: Using and developing frameworks for practice*, Lyme Regis: Russell House Publishing, 2009, pp. 250-263.
Radio Netherlands Worldwide
2011 "Dutch police infiltrate child abuse network", disponível em; http://www.expatica.com/nl/news/local_news/dutch-police-infiltrate-child-abuse-network_172736.html [consultado em: 20.09.2012].
Ramalho, David Silva
2014 "A recolha de prova penal em sistemas de computação em nuvem", em curso de publicação na *Revista de Direito Intelectual*.

Rodrigues, Benjamim Silva
2010 *Da Prova Penal, Tomo II, Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, Lisboa: Rei dos Livros.
2011 *Da Prova Penal – Tomo IV – Da Prova –Electrónico– Digital e da Criminalidade Informático-Digital*, Lisboa: Rei dos Livros.
Rogall, Klaus
2009 "A nova regulamentação da vigilância das telecomunicações na Alemanha", in Palma, Maria Fernanda, Silva Dias, Augusto & Sousa Mendes, Paulo (coord. científica), *2.º Congresso de Investigação Criminal*, Coimbra: Almedina, pp. 117-143.
Rosenbach, Marcel
2011 "The shady past of Germany's Spyware", *Spiegel Online International*, disponível em http://www.spiegel.de/international/germany/trojan-trouble-the-shady-past-of-germany-s-spyware-a-792276.html [consultado em 28.08.2012].
Santos, Paulo, Bessa, Ricardo & Pimentel, Carlos
2008 *Cyberwar – O Fenómeno, as tecnologias e os actores*, Lisboa: FCA.
Sherman, Chris, Price, Gary
2007 *The Invisible Web: Uncovering Sources Search Engines Can't See*, 7.ª ed., Information Today, Inc., New Jersey, USA.
Syverson, Paul
2011 "A peel of onion", *Proceedings of the 27th Annual Computer Security Applications Conference*, ACM, New York, USA, pp. 123-137.
Taylor, Mark, et al.
2011 "Digital evidence from peer-to-peer networks", *Computer Law & Security Review*, Vol. XXVII, n.º 6, pp. 647-652.
Tor Project Blog,
2010 "Plaintext over Tor is still plaintext", *TOR PROJECT BLOG*, disponível em: https://blog.torproject.org/blog/plaintext-over-tor-still-plaintext, [consultado em: 19.09.2012].
Urbas, Gregor,
2010 "Protecting Children from Online Predators: The Use of Covert Investigation Techniques by Law Enforcement", *Journal of Contemporary Criminal Justice*, Vol. IV, n.º 26, pp. 410-425.
Vacca, John R.
2005 *Computer Forensics –Computer Crime Scene Investigations*, 2.ª ed., Massachusetts: Charles River Media, Inc.

Vaciago, Giuseppe,

2012a *Digital Forensics, Italian Criminal Procedure and Due Process Rights in the Cyber Age*, Torino: G. Giappichelli Editore.

2012b "Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics", *Cyberlaws 2012: The Third International Conference on Technical and Legal Aspects of the e-Society*, pp. 7-12.

Verdelho, Pedro

2009 "A nova lei do Cibercrime", *Scientia Ivridica*, Tomo LVIII, n.º 320, Braga: Universidade do Minho, pp. 717-759.

Weber, Rolf H. & Heinrich, Ulrike I.

2012 *Anonymization*, 1.ª ed., Nova Iorque: Springer, 2012.

Woo, Christopher & So, Miranda

2002 "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance", *Harvard Journal of Law & Technology*, Vol. XV, n.º 2, pp. 521-538.

Xu, Jennifer & Chen, Hsinchun

2008 "The Topology of Dark Networks", *Communications of the ACM*, Vol. 51, n.º 10.