REVISTA PORTUGUESA DE HISTÓRIA DA COMUNICAÇÃO

Francisco Rui Cádima

O (des)controlo da Internet: para uma história da *Darknet*

O (des)controlo da Internet: para uma história da *Darknet*

The (un) control of the Internet: for a history of Darknet

Francisco Rui Cádima (FCSH – Universidade Nova de Lisboa)
frcadima@fcsh.unl.pt

"The Darknet is nothing more than a mirror of society. Distorted, magnified, and mutated by the strange and unnatural conditions of life online"
Jamie Bartlett

"Isto não é só o Wild West, isto é a Sodoma e Gomorra dos tempos modernos"
Jake Wallis Simons

"Todos nós fomos ficando desiludidos quanto à pura democratização da informação e da tecnologia. (O Tor) está a refletir a vida mais de perto, com as suas luzes e as suas sombras."
Bill Buchanan

Resumo
O início do século XXI está a ser marcado, em boa parte, por algo que tem ainda um grau de invisibilidade e de imprevisibilidade acentuado. É já iniludível que no contexto da geopolítica internacional um fator disruptivo complexo, que designaremos genericamente por "ciberguerra", está de certa forma a ensombrar o modo clássico de gerir as relações políticas e económicas no mundo global, diluindo por vezes o próprio conceito de "nação". Um dos "alfobres" deste conflito sem rostos, onde parte desta ameaça se esconde, é justamente a "Darknet". Procuraremos dar neste texto uma imagem dos seus enormes perigos, mas também, paradoxalmente, de algumas das suas virtualidades.

Palavras chave: Internet, darknet, cibercrime, terrorismo, regulação da rede.

REVISTA PORTUGUESA DE HISTÓRIA DA COMUNICAÇÃO

Abstract

The beginning of the 21st century is being largely marked by something that still has a high degree of invisibility and unpredictability. It is already unavoidable that in the context of international geopolitics a complex disruptive factor, generally referred to as "cyberwar", is in a way overshadowing the classic way of managing political and economic relations in the global world, sometimes diluting the very concept of "nation". One of the breeding grounds of this faceless conflict, where part of this threat is hidden, is precisely "Darknet." We will try to give in this text an image of its enormous dangers, but also, paradoxically, of some of its virtualities.

Keywords: Internet, darknet, cybercrime, terrorism, net regulation.

O descontrolo da rede na sua área visível não se compara em nada com o que se passa na sua zona "subterrânea" profunda – referida habitualmente como *Darknet* ou *Dark Web* – um espaço sem regras nem lei, em que a navegação se torna uma imersão no desconhecido, ou mesmo uma aventura perigosa nas zonas mais obscuras da Internet. E o facto é que, por isso mesmo, quer na opinião pública em geral[1], quer nalguns círculos políticos de governação, há quem peça o fim desta espécie de "buraco negro" da rede. Uma grande sondagem divulgada em 2016 pela IPSOS, realizada para o *think tank* canadiano CIGI - The Center for International Governance Innovation, abrangendo cerca de 24 mil pessoas consultadas em 24 países concluía, através de 70% das opiniões expressas, pela necessidade de encerrar esta rede de crime que é, por assim dizer, a mãe de todos os perigos e mercados negros na Internet.

Uma primeira questão que se coloca é saber se esta opinião generalizada no plano global colide ou não com a questão da privacidade na rede e a defesa dos direitos humanos, sobretudo onde os direitos de cidadania são perseguidos por regimes autocráticos ou mesmo pelas ditaduras mais totalitárias. Num segundo momento, convirá apurar se entre o "deve" e o "haver", isto é, entre os benefícios implícitos do sistema e os conteúdos criminosos que o inundam, se se justifica ainda assim a defesa e a manutenção da *Darknet* como excrescência horrenda, paraíso da pedofilia e dos mercados negros, do *malware* e de *botmasters*, do *hacking* e da contrafação de documentos e identidades, mas necessária e vital porque da sua existência e da existência da rede que a acolhe – a "Deep Web", dependerá também, por assim dizer, o princípio da privacidade e do anonimato na rede, de base política, científica ou meramente individual, pessoal. E em terceiro lugar – a manter-se tudo tal como está –, que

[1] Clara Barata (2016). "Sondagem diz que 70% dos cidadãos querem fechar a dark net". *Público* online, 29/03/2016. https://www.publico.pt/tecnologia/noticia/sondagem-diz-que-70-dos-cidadaos-quer-fechar-a-dark-net-1727470.

fazer então do ponto de vista societal, qual o debate a estabelecer, ou o conhecimento específico que é necessário passar aos internautas neste novo contexto. E, sobretudo, qual o tipo de vigilância e de controlo legal que os países e a comunidade internacional devem aprofundar para combater essa invisível *Darknet* que se está a espalhar pela rede como uma espécie de mancha de óleo…

História e *media*

Comecemos por um breve enquadramento histórico, para procurar melhor situar o complexo fenómeno. A *Darknet* surge, já neste século XXI, quando investigadores da Marinha norte-americana procuram construir uma rede que lhes possibilite total invisibilidade e total secretismo no acesso à rede e aos diversos *websites*, tendo desde início objetivos claramente institucionais e de segurança interna, por assim dizer.

Paul Sylverson, matemático da Universidade do Indiana e colaborador da Marinha norte-americana para a construção da "rede anónima" está verdadeiramente na origem do projeto uma vez que consegue autonomizar a nova rede do sistema aberto da World Wide Web. Em Agosto de 2004 Sylverson anuncia em San Diego, no Simpósio de Segurança Usenix, juntamente com Roger Dingledine e Nick Mathewson, membros do MIT - Massachusetts Institute of Technology que então desenvolviam o projeto Free Haven, aquilo que viria a ser a porta de entrada para a rede-sombra: o Tor - The Onion Router um *browser* destinado a todos os que pretendem não só entrar na *Darknet*, como para todos os que preferem navegar anónimos. Na prática, o Tor encripta os dados do utilizador, não sendo possível identificar a origem ou o IP do internauta. Segundo o próprio Sylverson, o objetivo estratégico da investigação "era permitir aos funcionários do Governo americano visitarem *websites* públicos para reunir informação sem que ninguém soubesse que a Marinha estava à procura daquelas coisas". [2]

Um tanto paradoxalmente, para que o modelo funcionasse, era fundamental que se tornasse popular, isto é, não poderia ficar fechado e circunscrito apenas a funcionários do Estado, dado que dessa forma a rede e os seus utilizadores seriam mais facilmente identificados.

É criado então o Tor, hoje com mais de 150 milhões de *downloads*, segundo se estima. Mas, outro aspeto paradoxal nesta questão é uma certa esquizofrenia que existe nas autoridades americanas relativamente ao Tor. Se, por um lado o financiam, por outro lado atacam-no, como no caso da NSA, procurando detetar e identificar utilizadores-alvo, bloquear *websites*, etc. Ou como no caso do FBI, que detém *software* malicioso para rastrear e infetar determinados sites e os seus visitantes, como tem sido o caso, nomeadamente, em matéria de comércio de droga e de pornografia infantil. Bill Buchanan, especialista em segurança

[2] Jake Wallis Simons (2014), "A rede secreta". *Público* online ,19/10/2014. https://www.publico.pt/tecnologia/noticia/a-rede-secreta-1673221. Acedido em 2/4/2016.

eletrónica da Edinburgh Napier University compreende esta estranha duplicidade do governo norte-americano:

> "Eles continuam a ter de monitorizar as ameaças. E mais importante, querem canais secretos para seu próprio uso. Mas, se é para serem quebrados, preferem que sejam eles a qualquer outra pessoa. É assim que se mantêm na vanguarda da tecnologia[3]."

Ao contrário dos norte-americanos, por exemplo na Rússia, Putin parece não desejar nenhum tipo de confusão nesta matéria. Terá inclusive um prémio de quatro milhões de rublos para quem conseguir fazer implodir esta rede.

A primeira grande vaga de *disclosures* emergem também na *Darknet* com a Wikileaks. Julian Assange, aliás, defende exatamente que a criptografia é fundamental para a proteção da privacidade do cibernauta de forma a impedir a vigilância dos cidadãos por empresas, órgãos policiais ou pelos próprios governos, tal como sucedia aliás na era analógica, em que se verificava uma inviolabilidade da experiência e da vivência do indivíduo. Para ele, a encriptação tinha naturalmente os dois lados da moeda, mas na sua opinião era fundamental garantir o anonimato e facilitar e incentivar os denunciantes de forma a se expor ou a "abrir" os segredos não divulgados da governação.

Julian Assange começa por ser conhecido como *hacker* no final dos anos 80, então sob o nome Mendax. Fica depois também associado às proto-*darknets*, uma vez que ele próprio dava nome a um personagem designado de "Proof", membro ativo das listas de discussão *cypherpunk* nos anos 1993-94. Por essa altura, Eric Hughes divulgava "A Cypherpunk's Manifesto", onde acentuava exatamente a questão de base:

> "Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."[4]

Mais tarde, em 1997, Assange apoia a pesquisa de Suelette Dreyfus quando esta publica a obra *Underground - Hacking, madness and obsession on the electronic frontier*, onde são descritas múltiplas experiências pioneiras neste começo da Internet-sombra. Dreyfus expunha então o seu ponto de partida:

---

[3] Jake Wallis Simons, op. cit.

[4] "A Cypherpunk's Manifesto" by Eric Hughes (1993). http://www.activism.net/cypherpunk/manifesto.html. Acedido em 11 de Abril de 2016.

> "I came upon the brave new world of computer communications and its darker side, the underground, quite by accident. It struck me somewhere in the journey that followed that my trepidations and conflicting desires to explore this alien world". [5]

Essencialmente, a *Darknet* é crime, contém e comercializa os conteúdos absolutamente terríveis do digital, sobretudo no plano da pornografia infantil, do tráfego de órgãos e de estupefacientes, e também, claro, no plano do terrorismo. O tema das "redes negras", apesar daquilo que representam e da impressionante dimensão que atingem, não tem sido suficientemente analisado, por exemplo, nos *media* tradicionais, pelo menos tendo como referência o caso português. Num rápido levantamento dos artigos publicados em Portugal sobre o assunto identificamos muito poucos trabalhos com uma boa contextualização do problema[6]. O artigo de Meruje e Fonseca referia que na altura as estimativas existentes, que reportavam a 2001 e ao estudo da BrightPlanet, apontavam para uma dimensão desta rede 500 vezes maior do que Internet "de superfície", e enumeravam as múltiplas situações que fazem dessa *Web* escondida – e ao fim e ao cabo deste planeta que habitamos, – uma espécie de "aldeia global" do terror e das piores experiências da espécie humana.

Deep Web vs. Darknet

Estamos então a falar de uma "galáxia sem sítio, sem IP, sem morada, sem rasto, onde os motores de busca vulgares não têm acesso. Um mundo onde é possível tudo o que na WWW não é".[7] E onde, através do principal motor de busca, o Google, apenas se consegue chegar a 0,03 por cento da informação disponível online – no total, com referência a dados de 2016, a cerca de 4,66 mil milhões de páginas apenas na internet de "superfície", na "pequena" Web de todos conhecida… Sendo que, em termos de tráfego, estamos por assim dizer na "zettabyte era"[8] da Internet, estimando-se que no final de 2016 o tráfego global da Internet atinja os 1.1 zettabytes e, no final 2019, os 2 zettabytes/ano. Uma referência também para os dados conhecidos sobre as línguas dominantes nos URLs da *deep web* lideradas pelo russo (41.40%) e seguidas do inglês (40.74%). Em português, há apenas 1,25% das páginas, pouco mais do

[5] Suelette Dreyfus and Julian Assange (1997). *Underground — Hacking, madness and obsession on the electronic frontier*. Kew: Mandarin/Reed Books Australia. www.underground-book.net.

[6] Vejam-se nomeadamente os trabalhos de Miguel Meruje e Patrícia Fonseca, "Deep web - O mundo secreto da internet", *Visão*, nº 991, de 1/3/2012; de Ricardo Nabais, "Bem-vindos ao submundo da internet", *Sol*, de 16/02/2015; de Luís Pedro Cabral (2015), "Buraco Negro". *Expresso* – E, Revista, 24 de dezembro.

[7] Luís Pedro Cabral (2015), "Buraco Negro". Expresso – E, Revista, 24 de dezembro de 2015.

[8] 1 zettabyte são 10^{21} bytes, para se ter uma ideia um pouco mais aproximada, um zettabyte equivale a 36 mil anos de vídeo de alta definição.

que foi verificado em catalão (1,12%).[9] Refira-se que esta percentagem muito elevada do russo tem a ver também com a existência de fóruns a que se acede pelo Tor ou pelo I2P (Invisible Internet Project, rede anónima *peer-to-peer*), não relacionados com atividades criminosas.

Convém estabelecer a diferença necessária relativamente à *Deep Web*, que é, essa sim, a grande galáxia na sombra da internet de superfície, também utilizada por redes sociais, universidades, bases de dados, etc., no fundo, uma rede disponível para todos os internautas, mas que não é indexada pelos motores de busca conhecidos – Google, Yahoo, Bing, etc. Mas que é utilizada por exemplo pelo Facebook[10]. Ou pela Web of Science. Ou mesmo pelas mensagens instantâneas. O acesso ou a utilização deste tipo de conteúdos[11] tem, à partida, um carácter essencialmente inócuo. O mesmo não acontecerá com a navegação por áreas e IPs escondidos, apenas acessíveis através do Tor, que para além de ser um *software* de navegação permite basicamente a qualquer utilizador estar *online* de forma segura e anónima. Daí que importe esclarecer se a *deep web* é efetivamente uma plataforma essencial para a privacidade na rede, isto é, se a internet "de superfície" não será suficiente para garantir essa mesma privacidade, ou se haverá, pelo contrário, absoluta necessidade de aceitar essa sua extensão nociva que é a "rede invisível".

Na verdade, o que está hoje em jogo, pensando nomeadamente no rápido desenvolvimento dessa zona negra que é a *Darknet*, é o que desse submundo criminal está a contaminar a camada de superfície, isto é, a vida das pessoas, a economia, os direitos humanos, etc. Perante a expansão acelerada do *Darknet* são desde logo novos desafios políticos que se colocam, sendo certo que este é um problema de muito complexa gestão, que terá naturalmente importantes implicações pelos efeitos que gera no plano da defesa da privacidade, da segurança, no plano do desenvolvimento e no equilíbrio global das sociedades modernas. Como é referido no relatório do Wilson Center: *"This understandable and legitimate privacy interest in the Deep Web's anonymity (or at least greater user control over anonymity) does not mean that states should turn a blind eye to the entire Deep Web."*[12] A questão é, portanto, o que – e como – monitorizar, como controlar algo que se está a tornar num ecossistema "do mal" e que assume dimensões muito preocupantes.

---

[9] Vincenzo Ciancaglini et altri (2015) *Below the Surface: Exploring the Deep Web*. TrendLabs research paper. Irving: Trend Micro, 2015, p. 10.

[10] Lorenzo Franceschi-Bicchierai (2014), "Facebook is now available through Tor for ramped-up privacy". *Mashable*, October, 31. http://mashable.com/2014/10/31/facebook-tor/#M_8BRSxJUgqc.

[11] How to Access the Deep Net - Working Links to the Deep Web: https://sites.google.com/site/howtoaccessthedeepnet/working-links-to-the-deep-web.

[12] Daniel Sui et altri (2015) The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. Washington: Woodrow Wilson International Center for Scholars, p. 10. https://www.wilsoncenter.org/sites/default/files/deep_web_report_october_2015.pdf

Terrorismo

As questões relacionadas com o terrorismo estão, obviamente, entre as que maior controlo têm tido por parte dos rastreadores do sistema. Também por isso mesmo, a presença do terrorismo na *darknet* está a tornar-se num fenómeno algo atípico no atual contexto de desenvolvimento da rede invisível.

No que diz respeito à ligação entre a *darknet* e o terrorismo, talvez haja então algumas ideias feitas que não correspondem totalmente à realidade. O que não significa que possa ser diminuída a vigilância. A crer num estudo realizado por Daniel Moore e Thomas Rid[13] conclui-se que as organizações terroristas não têm estado tão interessadas quanto se imagina em usar os recursos e serviços da rede anónima. Nos últimos anos tem-se assistido, aliás, a um intenso rastreamento e a ataques, quer por parte das principais agências de segurança ocidentais, quer por parte de "kacktivistas", contra as atividades do Daesh na *darknet*.

Em consequência, e também por opção estratégia de estarem mais presentes na internet de superfície, em muitos casos estes grupos radicais e terroristas não usam a *darknet*. Moore e Rid desenvolveram um sistema de rastreio na *web* que lhes permitiu analisar cerca de 300 mil endereços ocultos na rede através do Tor. Verifica-se uma presença esmagadora de conteúdos ilícitos na *darknet*, sendo que os usos mais comuns se concentram nas drogas, financiamento ilícito, pornografia envolvendo violência, crianças e animais. Os autores confirmam, no entanto, uma diminuição da presença do extremismo islâmico nesta rede:

> "Jihadis tend to use the internet for at least two general purposes: public-facing activities (propaganda, recruitment and sharing advice) and non-public-facing activities (internal communication, and command and control). The darknet's propaganda reach is starkly limited, not least because novices may be deterred by taking an 'illicit' step early on, as opposed to simple, curious Googling. Hidden services, secondly, are often not stable or accessible enough for efficient communication; other platforms seem to meet communication needs more elegantly. Islamic militants do commonly use the Tor browser on the open internet, however, for added anonymity."[14]

O que significa que em matéria de propaganda e recrutamento os terroristas usam a rede aberta na maior parte das vezes, em particular as plataformas de todos conhecidas como o You Tube, o Twitter ou o Facebook, ou mesmo *websites* em inglês. Veja-se, por exemplo, o caso de uma organização taliban que desenvolveu uma aplicação Android, primeiro na língua local, em *pashto*, e depois em inglês, *app* essa que chegou inclusivamente a estar disponível

[13] Daniel Moore e Thomas Rid (2016) "Cryptopolitik and the Darknet". Survival: Global Politics and Strategy. February–March 2016. Pages: 7-38. Volume: 58.
[14] Daniel Moore e Thomas Rid, op. cit., pp. 21-22.

na Play Store, tendo sido posteriormente removida pela Google. Tratava-se claramente de uma ação de reforço de propaganda *online*, tal como era aliás enunciado pela própria organização, que considerava que a *app* era *"part of our advanced technological efforts to make more global audience"*.[15]

A verdade é que o Estado Islâmico tem tido grande capacidade de gerir as redes sociais e *chatrooms* sobretudo para efeitos de recrutamento *online*. É por essa via que tem tido algum sucesso o efeito persuasor da sua estratégia de "agit-prop", tanto no plano local, como no âmbito global, como é aliás bem conhecido no Ocidente. Chegou ao ponto de ter inclusivamente manuais para os seus militantes saberem como despistar as centrais de informação ocidentais enquanto usavam o Twitter.[16] Pode mesmo dizer-se que o IS, segundo especialistas na matéria[17], domina como nenhum outro grupo extremista as redes sociais. Onde a Al-Qaeda, através dos seus líderes, utilizava as mensagens de vídeo gravadas, divulgadas por vezes várias semanas depois de terem sido gravadas, com um discurso político-religioso enrodilhado e confuso, o Estado Islâmico soube adotar rapidamente uma linguagem de auto-promoção panfletária suportada na "utopia" de uma nova fé e de um novo mundo, com um maior poder de sedução face aos seus frágeis alvos, sobretudo jovens nas margens da sociedade, sem perspetivas algumas de futuro e, portanto, muito sugestionáveis.

A ética, o bem e o "apesar de"

Posto perante a questão ética na rede, Sylverson, o criador do Tor, defendia-se alegando que é sobretudo um cientista e não um político, mas que "no geral, o Tor tem sido uma força do bem",[18] que até na Primavera Árabe teria sido decisivo, por exemplo, segundo Sylverson, em determinado momento a única comunicação que saía do Egipto era justamente através da Tor.

Poder-se-ia dizer que também os defensores da privacidade na Internet e os seus principais criadores, de Tim Berners-Lee a Vincent Cerf, têm uma certa condescendência relativamente à rede negra e às suas virtualidades, se é que elas verdadeiramente existem… Cerf, por exemplo, respondendo a uma pergunta de Gina Smith – "What do you regret?" – respondia: *"The fact that the net is abused is something I regret. Then again, there is far more utility than*

---

[15] Daid Z. Morris (2016), "Taliban Launches Smartphone App to Recruit and Spread Propaganda". Fortune online, April 3, 2016. http://fortune.com/2016/04/03/taliban-launches-smartphone-app/.

[16] Pierluigi Paganini (2014), "The ISIS has released a manual for its militants, titled 'How to Tweet Safely Without Giving out Your Location to NSA', that explain how avoid surveillance". Security affairs online, November, 3. http://securityaffairs.co/wordpress/29801/intelligence/isis-twitter-use-manual.html.

[17] "IS Has 'Mastered Social Media' Like No Other Extremist Group". *Voice of America* online. October 21, 2015. http://www.voanews.com/content/islamic-state-has-mastered-social-media-like-no-other-extremist-group/3017239.html

[18] Jake Wallis Simons, op. cit.

harm in it. We need to make sure we are always emphasizing freedom".[19] E o próprio J. D. Lasica, no seu livro intitulado precisamente *Darknet*[20] havia sido muito claro relativamente aos obstáculos que o sistema industrial de *media* e *new media* criava à livre circulação de conteúdos, pondo em perigo as liberdades digitais do cidadão. Para Lasica, na *"darknet"* residia toda a esperança e a promessa de futuro na Web:

> "Darknet nos alerta que podemos estar avanzando hacia un mundo donde los medios digitales personales acaban siendo bloqueados y controlados por la industria, un futuro donde la red no sirve al usuario sino a los intereses de los conglomerados y multinacionales mediáticas y a la industria discográfica. Cada vez hay más actividad en la Internet abierta que se está viendo empujada a la clandestinidade – hacia la Darknet – si continúa la actual tendencia en contra de la innovación".[21]

Ainda que por outras palavras, o mesmo era dito, sensivelmente na mesma altura, quer por Lawrence Lessig, no seu *Free Culture*[22], quer por Dan Gillmor, em *We the Media*[23]. Ou um pouco mais tarde por Matthew Hindman, no seu livro *The Myth of Digital Democracy*.[24]
Mas a *darknet*, sendo uma rede estratégica para determinados objetivos de segurança – também eles sempre algo obscuros – e para situações que envolvem movimentos políticos clandestinos e dissidentes, sobretudo em países que perseguem os ativistas que lutam pelos direitos humanos, o certo é que, como referimos, alberga na sua pesada sombra tudo o que de pior há ao cimo da Terra. E a dúvida que nos assalta é efetivamente porque é o Estado norte-americano o principal financiador desta mesma rede? Mistério, provavelmente mais perverso ainda do que a própria rede que suporta… Ou, porventura, não tanto, mas uma opção difícil por manter um canal que, em última instância, serve os objetivos geo-estratégicos e políticos dos próprios Estados Unidos. Refira-se no entanto, que as autoridades, no plano global, estão, naturalmente, muito atentas a tudo o que se passa nas *darknets*. Prova disso foi uma das ações mais significativas, ocorrida a 5 e 6 de Novembro de 2014, quando cerca de 400

---

[19] Gina Smith, "Daily Dozen: 12 Questions for Vint Cerf, 'Father of the Internet'". aNewdomain, 8/2/2016. http://anewdomain.net/2016/02/08/daily-dozen-12-questions-vint-cerf-father-internet/. Acedido a 2/4/2016.
[20] J. D. Lasica (2006), Darknet: La guerra de las multinacionales contra la generación digital y el futuro de los médios Audiovisuals. Madrid: Nowtilus.
[21] J. D. Lasica, op. cit., p. 13.
[22] Lawrence Lessig (2006) *Free Culture - How big media uses technology and the law to lock down culture and control creativity*. NY: The Penguin Press.
[23] Dan Gillmor (2006) *We the Media, Grassroots Journalism by the People, for the People*. NY: O'Reilly Media.
[24] Matthew Hindman (2009), *The Myth of Digital Democracy.* New Jersey: Princeton University Press.

websites e mercados negros do Tor foram fechados pelas autoridades norte-americanas, incluindo o Silk Road 2.0, o Cloud 9 e o Hydra.

Se é um facto que existem já algumas ferramentas legais para o controlo e a monitorização do cibercrime, por exemplo nos Estados Unidos, com o Computer Fraud and Abuse Act (CFAA), o facto é que no plano internacional muito haverá ainda a fazer neste domínio. Quer isto dizer que não há nenhum tratado que integre de forma global o conjunto de problemas e perigos que o cibercrime envolve hoje, designadamente no novo contexto da *Darknet*. Existe, desde 2001, a Convenção de Budapeste sobre Cibercrime, no âmbito do Conselho da Europa, que já prevê um conjunto de penalizações em matéria de pornografia, de propriedade intelectual, etc., mas as questões emergentes, relacionadas com a operacionalidade do sistema de monitorização e controlo, da circulação da informação entre países, e da harmonização jurídica no plano global, quando estão em presença questões de segurança também elas globais, está a tornar-se um obstáculo preocupante quer para o legislador quer para a sociedade em geral. O facto é que as grandes resistências ao aprofundamento do quadro jurídico global têm vindo sobretudo da China e da Rússia, pelo que até agora mantém-se a situação de indefinição:"*international consensus on law and policy regarding cyberwar and cyberespionage is so far elusive".* [25]

Conclusão

Do que se trata então é de, em primeiro lugar, compreender e estudar o fenómeno, ver qual o seu potencial "legal" e atuar de forma colaborativa e transnacional, reprimindo os grupos e as máfias que gerem as iniciativas e *websites* maliciosos, tal como no mundo físico é reprimida qualquer tipo de atividade criminal ou de comércio ilegal.

A questão é que estamos numa fase em que, muito provavelmente, o controlo da *Darknet* já será tarefa praticamente impossível para o legislador, o regulador e as entidades policiais e de segurança. Como dizia Jamie Bartlett, a Darknet "is going mainstream". A ser assim, do que se trata então é de começar, tão cedo quanto possível, a minorar os danos. As principais agências de segurança, nos EUA e no UK, nomeadamente, já estão no terreno há algum tempo. Mas é grande o risco de ver, por exemplo, nações mais suscetíveis de ver interesse comercial na rede negra aproveitarem as suas facilidades, ao invés de investirem na monitorização das suas atividades ilegais.

A falta de colaboração entre Estados, neste âmbito, tenderá a alimentar e a dar cada vez maior força a uma gigantesca bola de neve negra e invisível. Porventura, permitindo que o submundo do crime ganhe pela primeira vez na história do planeta, embora num espaço virtual obscuro, uma ascendência sobre os cidadãos do mundo e o conceito que temos de licitude, a partir, justamente, dos impérios que se vão construindo na *darknet*. E a verdade é

[25] Daniel Sui et altri (2015), op. cit., p. 12.

que no plano global nos estamos a aproximar perigosamente, como nunca terá acontecido no passado, da linha que separa o bem do mal.

Bibliografia

BARATA, Clara (2016): *Sondagem diz que 70% dos cidadãos querem fechar a dark net*. *Público* online, 29/03/2016. https://www.publico.pt/tecnologia/noticia/sondagem-diz-que-70-dos-cidadaos-quer-fechar-a-dark-net-1727470. Acedido a 30 de março de 2016.

BARTLETT, Jamie (2015): "How the mysterious dark net is going mainstream". Conference - TED Global London. Filmed Jun 2015. https://www.ted.com/talks/jamie_bartlett_how_the_mysterious_dark_net_is_going_mainstream?language=en. Acedido em 7 de abril de 2016.

BARTLETT, Jamie (2015): *The Dark Net*, London, Windmill Books.

CABRAL, Luís Pedro (2015): Buraco Negro. *Expresso – E*, Revista, 24 de dezembro.

CIANCAGLINI, Vincenzo et altri (2015): *Below the Surface: Exploring the Deep Web*. TrendLabs research paper, Irving, Trend Micro, p. 10. https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf.

DREYFUS, Suelette e ASSANGE, Julian (1997): *Underground — Hacking, madness and obsession on the electronic frontier*, www.underground-book.net. First Published 1997, Kew, Mandarin/Reed Books Australia.

FRANCESCHI-BICCHIERAI, Lorenzo (2014): *Facebook is now available through Tor for ramped-up privacy*. *Mashable*, October, 31. http://mashable.com/2014/10/31/facebook-tor/#M_8BRSxJUgqc. Acedido a 3 de março de 2016.

GILMOR, Dan (2006): *We the Media, Grassroots Journalism by the People, for the People*, NY, O'Reilly Media.

HINDMAN, Matthew (2009): *The Myth of Digital Democracy*, New Jersey, Princeton University Press.

HUGHES, Eric (1993): *A Cypherpunk's Manifesto*. http://www.activism.net/cypherpunk/manifesto.html. Acedido em 11 de abril de 2016.

LASICA, J. D. (2006): *Darknet: La guerra de las multinacionales contra la generación digital y el futuro de los médios Audiovisuals*, Madrid, Nowtilus.

LESSIG, Lawrence (2006): *Free Culture - How big media uses technology and the law to lock down culture and control creativity*, NY, The Penguin Press.

MERUJE, Miguel e FONSECA, Patrícia (2012): Deep web - O mundo secreto da internet. *Visão*, nº 991, de 1 de março.

MOORE, Daniel e RID, Thomas (2016): Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy*, February–March 2016, Volume 58: 7-38.

MORRIS, Daid Z. (2016): Taliban Launches Smartphone App to Recruit and Spread Propaganda. *Fortune* online, April 3. http://fortune.com/2016/04/03/taliban-launches-smartphone-app/. Acedido a 4 de abril de 2016.

NABAIS, Ricardo (2015): Bem-vindos ao submundo da internet, *Sol*, de 16 de fevereiro.

SIMONS, Jake Wallis (2014): A rede secreta, *Público* online, 19/10/2014. https://www.publico.pt/tecnologia/noticia/a-rede-secreta-1673221. Acedido em 2 de abril de 2016.

SMITH, Gina (2016): Daily Dozen: 12 Questions for Vint Cerf, 'Father of the Internet'. *aNewdomain*, 8/2/2016. http://anewdomain.net/2016/02/08/daily-dozen-12-questions-vint-cerf-father-internet/. Acedido a 2 de abril de 2016.

SUI, Daniel et altri (2015): The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box, *Washington, Woodrow Wilson International Center for Scholars*: 10. https://www.wilsoncenter.org/sites/default/files/deep_web_report_october_2015.pdf. Acedido a 14 de março de 2016.

"How to Access the Deep Net - Working Links to the Deep Web" (s/d). Google sites. https://sites.google.com/site/howtoaccessthedeepnet/working-links-to-the-deep-web. Acedido a 24 de março de 2016.

"IS Has 'Mastered Social Media' Like No Other Extremist Group" (2015). *Voice of America* online. October 21. http://www.voanews.com/content/islamic-state-has-mastered-social-media-like-no-other-extremist-group/3017239.html. Acedido a 5 de abril de 2016.

PAGANINI, Pierluigi (2014), The ISIS has released a manual for its militants, titled 'How to Tweet Safely Without Giving out Your Location to NSA', that explain how avoid surveillance. *Security affairs online*, November, 3. http://securityaffairs.co/wordpress/29801/intelligence/isis-twitter-use-manual.html. Acedido a 28 de março de 2016.