O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço

Tenente-coronel
Rui Manuel Piteira Natário

1. Introdução

O que é um cibercrime? Sem reflexão, poderemos imediatamente responder que se trata de um crime cometido no, ou através do, ciberespaço e que pode ser combatido como os outros: com aplicação da lei. Mas saberemos exactamente o que é o ciberespaço? Ou será esta uma palavra que utilizamos de forma natural sem que nunca tenhamos reflectido verdadeiramente sobre o seu significado? Possivelmente, algo de semelhante se passará com a noção de cibercriminalidade, já que o termo é relativamente recente e é indissociável do conceito de ciberespaço. No entanto, sem que por vezes tenhamos verdadeira consciência disso, a cibercriminalidade, nas suas diversas formas, é hoje omnipresente no quotidiano de muitos milhões de cibernautas. Este trabalho traça um percurso evolutivo dos conceitos basilares respeitantes à cibercriminalidade em geral, caracterizando-os e ilustrando as dificuldades legislativas que têm vindo a criar às autoridades. São analisadas sumariamente as principais iniciativas legais em curso para combater este fenómeno e elencadas algumas das suas limitações no combate à moderna criminalidade envolvendo sofisticados meios tecnológicos.

A cibercriminalidade tem vindo a ser objecto de diversos estudos nos últimos anos e é actualmente alvo de grande interesse, tanto por parte do mundo académico como do mundo empresarial, dado o seu crescente impacto negativo em diversas áreas da vida contemporânea. Uma boa parte destes estudos preocupa-se em caracterizar a criminalidade informática e perspectivar as tendências futuras para este flagelo. No entanto, muitos outros estudos têm sido orientados para a procura de respostas legais que permitam melhorar a actuação das autoridades, focando a sua atenção sobre as limitações das actuais molduras criminais, e propondo alternativas. O combate ao cibercrime tem, até aqui, sido uma batalha desigual que opõe a rigidez dos múltiplos

sistemas legais em vigor nos diversos países do mundo, à grande flexibilidade das organizações criminais internacionais. A comunidade internacional tenta responder com diversas iniciativas mas, enquanto a cibercriminalidade for um negócio altamente rentável, a luta vai continuar.

2. O que é o ciberespaço?

Nos últimos anos deu-se um crescimento verdadeiramente explosivo das tecnologias de informação, nomeadamente da Internet. Na sequência desta expansão, o termo ciberespaço passou a integrar o léxico comum, sendo vulgarmente utilizado para descrever o mundo virtual que os utilizadores da Internet visitam quando estão *online*, acedendo aos mais diversos conteúdos, jogando ou utilizando os variadíssimos serviços interactivos que a rede mundial de computadores disponibiliza.

Mas é fundamental distinguir o ciberespaço da infra-estrutura física das redes de comunicação, pois existe uma generalizada confusão conceptual.

As telecomunicações e a informática, a chamada telemática, limitam-se a permitir a comunicação à distância, enquanto o ciberespaço é um ambiente virtual que se serve destes meios de comunicação para o estabelecimento de relações virtuais. Todavia, esta distinção básica não é suficiente para definir e caracterizar o ciberespaço.

2.1. Definições de ciberespaço

Contrariamente à maior parte dos termos informáticos, o ciberespaço não tem uma definição objectiva e universalmente aceite e é apenas um conceito vago utilizado para descrever o mundo virtual dos computadores. A maior parte dos cibernautas, se solicitados a descrever o ciberespaço, irá provavelmente referir-se a computadores pessoais e à Internet. Embora estas tecnologias sejam importantes para a nossa concepção do ciberespaço, é evidente que estes elementos constituem apenas uma pequena parte da globalidade das redes políticas, sociais, económicas, culturais e financeiras que constituem aquilo a que vulgarmente se chama ciberespaço [50]. A génese do termo remonta a 1984 quando foi popularizado por Willian Gibson que o definiu como sendo uma alucinação consensual experimentada diariamente por biliões de utilizadores [21]. Nos anos que se seguiram, foram surgindo outras definições que reflectiam já uma perspectiva onde se cruzava a visão filosófica com a tecnológica. Por exemplo, em 1999, o filósofo Lévy considerou que o ciberespaço era definido como sendo o espaço de comunicação aberto pela interligação mundial dos computadores e das memórias dos computadores. Esta definição incluía o conjunto dos sistemas de comunicação electrónicos, na medida em que transmitiam informações provenientes de

fontes digitais ou destinadas à digitalização [32].

Entretanto, a doutrina oficial dos EUA sobre o ciberespaço foi amadurecendo e evoluindo mas, em 2001, a definição do Departamento de Defesa dos EUA (DoD) sobre a matéria limitava a definição de ciberespaço a um hipotético ambiente em que a informação digitalizada era comunicada através de redes de computadores [42], o que implicava que o ciberespaço era apenas um meio de comunicação de natureza teórica ou imaginária. Neste mesmo ano, o sociólogo espanhol Castells, sem definir exactamente o conceito de ciberespaço, afirmou que a Internet não era apenas tecnologia; era uma ferramenta tecnológica e um método organizacional de distribuição de poder informacional, geração de saber e capacidade de ligação em todas as áreas da sociedade [5].

Numa outra perspectiva, e num documento estratégico de grande importância, em 2003, a Casa Branca definiu o ciberespaço como um sistema nervoso – o sistema de controlo do país, composto por centenas de milhar de computadores, servidores, comutadores, encaminhadores e cabos de fibra óptica interligados que permitia que as infra-estruturas críticas funcionassem [27]. Três anos mais tarde, na sequência dos estudos conducentes à elaboração de uma estratégia militar para actuação no ciberespaço, o DoD definiu o ciberespaço como sendo um domínio caracterizado pela utilização da electrónica e do espectro electromagnético para guardar, modificar e trocar dados através de sistemas em rede e infra estruturas associadas [45]. Continuando apenas focadas na segurança e defesa das redes informacionais do governo e dos militares, as autoridades norte americanas divulgaram, em 2008, duas novas definições oficiais de ciberespaço. No início do ano, a Casa Branca considerou que ciberespaço era a rede interdependente de infra-estruturas de tecnologia de informação, e incluía a Internet, as redes de telecomunicações, os sistemas de computadores, os processadores e controladores embebidos em indústrias críticas [25]. Poucos meses depois, o DoD voltou a rever a sua terminologia considerando agora que o ciberespaço era um domínio global dentro do ambiente de informação, composto pela rede interdependente de infra-estruturas de tecnologia de informação incluindo a Internet, as redes de telecomunicações, os sistemas de computadores e os processadores e controladores neles embebidos [43].

Estas definições, além de reconhecerem o carácter omnipresente do ciberespaço, colocaram-no no âmbito de um ambiente mais vasto, reconhecendo implicitamente as suas profundas ligações ao mundo físico onde estão as pessoas e as infra-estruturas de suporte da sociedade. Tal facto foi espelhado no ano seguinte quando um outro documento da Casa Branca referiu, em aditamento à definição do ano anterior, que a utilização corrente do termo ciberespaço também se referia ao ambiente virtual de informação e interacções entre pessoas [26]. Enquanto na literatura da especialidade continuavam a surgir diversas análises e teorizações sobre o conceito de ciberespaço, em 2009, Kuehl aglutinou os conceitos anteriores introduzindo algumas diferenças subtis, mas muito importantes. Este conceituado especialista considerou que o ciberespaço era um domínio operacional cujo carácter distinto e único era enquadrado pela utilização da electrónica e do espectro electromagnético para criar, guardar, modificar trocar e explorar informação através de sistemas baseados em tecnologia de comunicação de informação interligados e as suas infra-estruturas associadas [30].

Neste momento, o DoD mantém a sua anterior definição [44] e reconhece oficialmente [10] a sua dependência do ciberespaço para o funcionamento efectivo da sua estrutura, referindo explicitamente que opera mais de 15.000 redes e 7 milhões de dispositivos de computação, distribuídos por centenas de instalações em dezenas de países em todo o mundo. Além disso, é hoje unanimemente aceite a noção de que o ciberespaço não se limita à Internet, sendo uma experiência mais vasta, de imersão numa verdadeira plataforma de comunicação a nível global, na qual os participantes acreditam viver em comunidade, e onde muitos deles chegam mesmo a confundir as suas vidas reais com os seus alter egos virtuais.

No plano nacional, a definição do termo também foi evoluindo. Em 2001, a Academia de Ciências definia o ciberespaço como o "espaço onde se estabelece comunicação electrónica", "realidade virtual" [34]. Mais recentemente, a *Larousse* definiu ciberespaço como sendo "o termo utilizado para designar o mundo dos computadores, ligados em rede, e a sociedade de informação em pleno crescimento" [31]. Actualmente, a *Porto Editora* define o ciberespaço como o "espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações"[1] e a *Priberam* define-o como "o espaço ou conjunto das comunidades de redes de comunicação entre computadores, nomeadamente a Internet"[2].

A computação móvel, a utilização permanente de ferramentas de geolocalização e a ligação da Internet a objectos de uso mundano, fazem surgir novas questões. Ou seja, o constante progresso tecnológico leva a que os termos do léxico comum, assim como os termos legais, fiquem desactualizados a um ritmo alucinante. Passados quase trinta anos desde a sua criação, parece ser extremamente difícil definir com clareza e rigor o que é realmente o ciberespaço, facto que ilustra a complexidade do tema e abre caminho a todas as especulações e interpretações.

2.2. Características do ciberespaço

Embora seja aparentemente impossível alcançar um consenso no que diz respeito à definição exacta daquilo a que nos referimos quando falamos de ciberespaço, este ambiente tem algumas características distintivas que lhe conferem um carácter único. Na realidade, são exactamente essas propriedades peculiares que têm sido exploradas de forma nefasta para a prática de diversos tipos de criminalidade.

2.2.1. Libertarismo

A ideia de liberdade da Internet está relacionada com os direitos humanos básicos, nomeadamente com a liberdade de expressão. Muitos têm sido aqueles que têm defendido a noção de que a Declaração Universal dos Direitos do Homem, de 1948, nomeadamente no que diz respeito à liberdade de expressão por qualquer meio, se aplica ao ciberespaço [7]. Esta é uma ideia que ganhou grande divulgação nos anos 90 do século

passado: o conceito de que a Internet e as suas tecnologias formavam um ciberespaço separado do vulgar mundo físico. Esta noção de ciberespaço oferecia uma escapatória, com todas as conotações positivas e negativas associadas; a libertação dos limites da opressão, das instituições e da realidade. É precisamente neste movimento que encontramos a génese do princípio da neutralidade da rede. Embora, por motivos históricos, a Internet tenha sido quase sempre gerida por instituições sedeadas nos EUA, a sua orientação sempre foi independente.

Muitos dos responsáveis pelo desenvolvimento do ciberespaço, particularmente nos seus primórdios, assumiram uma postura claramente libertária, desde a *Electronic Frontier Foundation* (EFF) até às empresas interessadas no comércio electrónico livre da regulação governamental [50]. Em 1996, John Perry Barlow, um dos fundadores da EFF, publicou *online* a famosa *Declaration of the Independence of Cyberspace*[3] num grito de revolta contra as iniciativas legislativas da Casa Branca que, na sua opinião, ameaçavam a independência e soberania do ciberespaço. Primariamente, o libertarismo generaliza um argumento altruísta e universal: todos devem poder fazer tudo aquilo que não causa danos a ninguém. Ou seja, o libertário tenta proteger a liberdade de todos e não apenas a sua [1]. Nesta visão do mundo, o papel da lei deve ser o do guardião: defensor de uma série de caixas que os cidadãos enchem como querem. A lei deve proteger as liberdades, os direitos de propriedade e fazer honrar os contratos, e deve fazê-lo sem questionar os motivos individuais de cada um. Ou seja, o papel do estado deve ser o de proteger a caixa e não o de avaliar o valor do seu conteúdo [1].

Na sequência destas ideias libertárias, alguns teóricos utópicos conceberam a Internet como um espaço de discurso perfeito, uma mente global que apagaria todas as diferenças entre os povos do mundo. Mas a realidade do mundo moderno é bem diferente e parece ser imune a essa ideologia. Existem vários regimes autoritários onde não há respeito pela liberdade *online* e é impossível aceder à Internet sem censura. Há vários exemplos em que o governo utiliza a sua soberania para controlar o ciberespaço doméstico, censurando tudo aquilo que lhe parece prejudicial ao regime. Na China, todos os conteúdos são filtrados através daquilo a que se chama a Grande Firewall e outros regimes despóticos tentaram silenciar os seus dissidentes; desde os protestos pós eleitorais no Irão, em 2009, até aos mais recentes acontecimentos na Primavera Árabe [7].

Por outro lado, nos EUA, o ciberespaço é geralmente considerado como um ambiente onde qualquer tipo de discurso, por mais questionável que possa ser, é permitido tal como seria noutro meio de comunicação protegido pela Primeira Emenda Constitucional [7]. As únicas excepções a esta regra incluem a difamação e a pornografia infantil. No entanto, no ciberespaço, a Primeira Emenda é apenas uma lei local [1] e esta protecção não se estende aos conteúdos alojados fora dos EUA. Embora semelhante, a postura europeia relativamente à liberdade de expressão tem acentuadas diferenças, em particular no que diz respeito à propaganda xenófoba [7]. Um passo importante nesta área foi dado quando o Conselho para os Direitos Humanos das Nações Unidas, em Julho de 2012, adoptou, por consenso, a resolução A/HRC/20/L.13[4] para protecção, garantia e gozo de direitos humanos na Internet. Esta resolução confirma que as pessoas devem ter

online os mesmos direitos que têm *offline*, em particular, a liberdade de expressão.

2.2.2. Geografia

A maior distinção entre o espaço físico e o virtual é a forma como o sentimos e experimentamos: enquanto o primeiro é vivido pela passagem da totalidade do nosso corpo por ele, o segundo, é sentido directamente apenas pelos olhos e ouvidos [50]. Há apenas algumas décadas atrás, o mundo estava dividido em entidades geograficamente delimitadas como casa, rua, escritório ou café, mas o advento da Internet parece ter esbatido toda esta estrutura geográfica. Agora, no ciberespaço, até mesmo a questão de saber onde ocorrem os eventos é claramente uma questão de convenção social [1]. O ciberespaço cria mundos que, à partida, parecem ser contíguos com o espaço geográfico, mas uma análise mais cuidada revela que as leis da física não têm qualquer significado *online*. Isto ocorre porque o ciberespaço é puramente relacional e consiste de diferentes *media*, todos eles sendo construções, ou seja, não são naturais e são apenas resultado da produção dos seus criadores e, em muitos casos, dos seus utilizadores.

A distinção entre o virtual e o real, sem privilegiar o último, tende a idolatrar o primeiro. No entanto, embora os mapas mentais sejam importantes para construção do ciberespaço, este continua a manter grandes ligações com o mundo real onde estão os servidores, e os governos e onde produz efeitos materiais sobre a economia global [50]. A distribuição geográfica dos utilizadores da Internet é muito desigual, tal como pode ser constatado nas taxas de penetração relativa em cada país. Não é surpreendente que a utilização da Internet seja altamente diferenciada à escala mundial, uma vez que esta desigualdade segue os padrões de distribuição da infra-estrutura tecnológica, de desenvolvimento económico, de distribuição de recursos ou de nível de educação [49]. Ou seja, a geografia *online* reflecte as desigualdades *offline*.

2.2.3. Tecnologia

A Internet é, possivelmente, o mais significativo desenvolvimento na história das comunicações, uma vez que liga indivíduos, instituições e tudo e o que está entre eles, de uma forma sem precedentes. Mas a dependência da tecnologia aumentou exponencialmente e o ciberespaço afecta todos os aspectos da vida quotidiana, desde os mais sérios aos mais mundanos. O *Transmission Control Protocol/Internet Protocol* (protocolo TCP/IP), que está na base do funcionamento da Internet, foi adoptado em 1983 e, no ano seguinte, a *National Science Foundation* (NSF) criou ligações baseadas neste protocolo com as maiores universidades dos EUA. Como todos os potenciais utilizadores eram conhecidos e de confiança, a segurança do protocolo nunca foi uma prioridade. Nesta altura, a utilização indevida da rede não era uma preocupação, porque as pessoas que a utilizavam eram as mesmas que a desenvolviam e concebiam, e constituíam um grupo culturalmente homogéneo ligado pelo desejo de ver a rede funcionar [52]. Assim, a Internet primordial não tinha requisitos de segurança; na realidade bastava que um

computador estivesse ligado à rede para ser considerado seguro. O resultado desta génese levou a que o protocolo sobre o qual ainda hoje assenta toda a estrutura de funcionamento da Internet, seja intrinsecamente inseguro. Posteriormente, a redução das tensões internacionais, que ocorreu após o final da Guerra Fria, levou a que a NSF desse inicio à expansão da Internet a outros países e ao público em geral. Na actualidade, o próprio DoD reconhece as vulnerabilidades dos EUA no ciberespaço e assume que há um enorme contraste entre a grande dependência tecnológica e a fraca segurança das tecnologias utilizadas [10].

Paralelamente a esta evolução, surgiram os defensores da ideia que o poder da dispersão geográfica e da tecnologia fariam com que fosse impossível regular a Internet. Entre estes, talvez os mais destacados fossem os *cypherpunks* que acreditavam que os avanços na tecnologia de cifra, em combinação com a arquitectura global da rede, permitiriam uma total emancipação do domínio dos estados [1]. Nesta visão, a utilização de códigos invioláveis, assinaturas digitais e outros sistemas fiáveis, permitiria o florescimento de toda uma actividade económica e cultural à margem da regulação dos governos nacionais. Enquanto as autoridades encaravam esta utilização das tecnologias de cifra como um manto para encobrir actividades ilícitas, para os *cypherpunks* esta revolução digital em direcção à libertação da opressão estatal era, não só inevitável como também desejável. Estas ideias foram sistematizadas num famoso documento de 1993[5], no qual o autor defendeu que, na sociedade da informação, as principais protecções da privacidade seriam tecnológicas e geográficas, e não institucionais.

Consideradas conjuntamente, as características atrás referidas parecem indicar que a tecnologia do meio, a distribuição geográfica dos utilizadores e a natureza do seu conteúdo tornam a Internet particularmente resistente à regulação governamental. O estado é demasiado grande, lento e limitado em termos geográficos e tecnológicos para regular as interacções fugazes de uma cidadania global que ocorrem num meio imprevisível. Vista por este prisma, a Internet é o ambiente ideal para a disseminação da informação e tentar regulá-la é como tentar proibir a evolução natural [1]. Mas há uma outra perspectiva, segundo a qual o ciberespaço não é uma realidade fixa nem predeterminada, funcionando de acordo com princípios e dinâmicas que não podem ser controladas ou alteradas. Sendo uma criação, o ciberespaço é mutável e pode ser transformado [4].

3. O que é o cibercrime?

A conceptualização da cibercriminalidade implica o esclarecimento de algumas questões essenciais onde se inclui a localização dos actos criminais no mundo real e no virtual, que tecnologias estão envolvidas, a motivação dos criminosos e a sua identidade. Uma possível forma de encarar o problema dos cibercrimes pode ser considerá-los apenas como sendo versões digitais de crimes no mundo real, ou seja, seriam crimes tradicionais se não fosse a adição do elemento virtual ou ciberespacial [14]. Mas, na realidade, embora os especialistas da indústria, os académicos e as autoridades governamentais

tenham, ao longo das últimas décadas, divulgado variadíssimas abordagens com vista ao desenvolvimento de definições exactas para as expressões empregues nesta área, continua a não existir uma definição consensual de cibercrime.

3.1. Definições de cibercrime

Em 1989, o Departamento de Justiça dos EUA definia o crime informático (*computer crime*) como sendo qualquer violação da lei criminal que envolvesse conhecimentos de tecnologias de computadores para a sua penetração, investigação ou acusação [29]. Em 1998, Parker distingue crime informático, em que o autor utiliza conhecimentos específicos de tecnologias de computadores, de cibercrime (*cybercrime*), no qual o crime é cometido utilizando a Internet ou requerendo conhecimentos específicos sobre o ciberespaço [38]. Em 2000, durante o 10º Congresso das Nações Unidas para a Prevenção do Crime e Tratamento das Vítimas, foram desenvolvidas duas novas definições. Cibercrime, no sentido estrito, cobriria qualquer comportamento ilegal, conduzido através de meios electrónicos, cujo alvo fosse a segurança de sistemas de computadores e os dados neles alojados. Cibercrime, no sentido lato, cobriria qualquer comportamento ilegal cometido por meio de, ou relacionado com, sistemas ou redes de computadores, incluindo crimes como a posse ilegal e distribuição de informação através de sistemas ou redes de computadores [48].

Em 2001, a Convenção sobre Cibercrime do Conselho da Europa definiu o cibercrime como sendo um vasto leque de actividades que se enquadram em quatro categorias genéricas de crimes relacionados com computadores: (1) violações de segurança; (2) fraude e falsificação; (3) pornografia infantil; e (4) violação de direitos de autor [14]. No mesmo ano, numa proposta alternativa de uma convenção internacional para incrementar a protecção contra o cibercrime e o ciberterrorismo, surgiu uma outra definição que se limitou a definir cibercrime como sendo a conduta respeitante a sistemas cibernéticos que viole os termos da própria proposta de convenção [41]. Em 2002, Furnell fez uma distinção entre a criminalidade em que os computadores são utilizados como uma capacidade de suporte, mas em que a tipologia do crime em si mesmo é anterior ao surgimento das novas tecnologias (fraude ou usurpação de identidade), e outro tipo de criminalidade onde a acção é um produto directo das tecnologias de informação (vírus informáticos ou penetração de sistemas) [17]. Numa outra perspectiva, uma das maiores companhias mundiais na área da segurança informática definiu recentemente cibercrime como sendo qualquer crime cometido utilizando um computador, rede ou dispositivo de *hardware*[6]. No entanto, esta parece-nos ser uma definição demasiado genérica e que cria algumas dificuldades de interpretação e aplicação. A visão instrumental dos computadores, em que estes são uma mera ferramenta, leva a que, no limite, seja cibercrime um atacante que mate alguém utilizando um teclado como arma para cometer a agressão.

A variedade de abordagens demonstra que há dificuldade em definir com rigor os termos “cibercrime” ou “crime informático”. Estas expressões são utilizadas para descrever um

vasto leque de ofensas que, sendo muito distintas entre si, excluem a aplicação de um único critério que englobe todos os actos nos diferentes contextos legais nacionais e internacionais [20]. O próprio governo norte-americano não parece ter uma definição oficial de cibercrime [14]. Apesar de tudo, a expressão "crimes informáticos" parece ser mais abrangente que a expressão "cibercrime" uma vez que esta última terá, à partida, que envolver a utilização de redes informáticas enquanto a primeira pode estar relacionada apenas com computadores isolados. Além disso, a distinção normalmente feita entre o cibercrime e outras actividades maliciosas provenientes do ciberespaço, tais como o terrorismo e a espionagem, prende-se com a motivação do autor. Nomeadamente, o FBI não tem dúvidas em classificar como cibercrime todas as actividades ilegais no ciberespaço que visem a obtenção de proveitos financeiros ilícitos [14]. Mas, sem uma definição exacta do termo, uma determinada ocorrência pode ser considerada, por exemplo, como um acto terrorista (ou ciberterrorista) o que altera completamente todo o enquadramento da sua investigação, da jurisdição para o fazer e a própria moldura penal aplicável.

Em Portugal, a Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), transpõe para a ordem jurídica nacional a Decisão Quadro n.º 2005/222/JAI, do Conselho da Europa, relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime, do Conselho da Europa, sem, no entanto, definir exactamente o que é "cibercrime". No dicionário *online* da *Porto Editora* descobrimos que o cibercrime é o "crime cometido com o recurso aos sistemas electrónicos e às novas tecnologias de informação"[7] e a *Priberam* define-o como sendo o "crime cometido através da comunicação entre redes de computadores, nomeadamente através da Internet"[8]. À semelhança do que ocorre com a definição de ciberespaço, o cibercrime também não parece ser fácil de definir com exactidão e esse facto é um dos grandes desafios que as autoridades do séc. XXI enfrentam no combate a este fenómeno.

3.2. Características do cibercrime

Apenas uma pequena parcela da cibercriminalidade consiste em ofensas verdadeiramente novas, ou seja, crimes nunca vistos no passado. A maior parte dos cibercrimes são de tipo clássico, mas cometidos com recurso a outros meios. No entanto, toda a cibercriminalidade acaba por ser uma nova criminalidade pois as suas características criam dificuldades nunca antes sentidas pelas autoridades.

3.2.1. Transnacionalidade

O cibercrime não requere proximidade física entre a vítima e o atacante, ou seja, estes podem estar em diferentes cidades e até mesmo em diferentes países. Tudo o que um cibercriminoso necessita é de um computador ligado à Internet e com isto pode cometer uma vasta panóplia de cibercrimes [3]. Um criminoso armado com um computador e uma ligação tem a capacidade para vitimizar pessoas, negócios e governos em qualquer parte

do mundo, cometendo todo o tipo de crimes, desde apoiar o terrorismo internacional até vender pornografia infantil, passando pelo roubo de propriedade intelectual [29]. As restrições territoriais são irrelevantes no ciberespaço, isto é, os cibercrimes não estão confinados por fronteiras nacionais o que implica que, para um cibercriminoso, é tão fácil atacar um alvo nos antípodas como atacar o seu vizinho do lado. Assim, uma grande parte da cibercriminalidade é hoje transnacional, tirando partido das ambiguidades sem fronteiras do ciberespaço para iludir as autoridades nacionais dos diferentes países [49] [3].

3.2.2. Anonimato

Contrariamente ao que ocorre com os criminosos do mundo real, os cibercriminosos conseguem frequentemente manter-se anónimos. Ainda que a polícia consiga identificar a origem dos criminosos, a recolha de provas e a apreensão dos suspeitos podem ser extremamente difíceis, uma vez que o país a partir do qual foi praticado o crime pode recusar-se a colaborar [3]. Este é um aspecto fundamental da cibercriminalidade; como os crimes são cometidos num ambiente virtual, na maior parte dos casos, as provas que os agentes da autoridade têm que recolher são provas digitais intangíveis [2]. Os criminosos podem dificultar ainda mais a tarefa das autoridades utilizando a tecnologia em seu favor para alcançar níveis de anonimato sem paralelo no mundo real, assumindo uma multitude de falsas identidades ou fazendo-se passar por cidadãos inocentes [2]. Todo este véu de anonimato confunde os investigadores e provoca atrasos que, muitas vezes, impedem a apreensão dos verdadeiros culpados [20] [49]. Estima-se que apenas 5% dos cibercriminosos são presos ou condenados, porque o anonimato associado às suas actividades os torna difíceis de capturar, e o novelo de provas que os liga ao crime muito difícil de desenrolar [51].

3.2.3. Tecnologia

O cibercrime nem sempre tem apenas um autor e uma vítima. O cibercrime é crime automatizado e esta característica permite que os criminosos cometam milhares de crimes de forma expedita e sem esforço [3]. Os criminosos podem utilizar a automação para aumentar a escala das suas operações e conseguir, assim, não só criar novas dificuldades à investigação das suas actividades, mas também aumentar os seus potenciais lucros uma vez que o número de vítimas aumenta exponencialmente [19]. Os cibercriminosos do séc. XXI dependem cada vez mais da Internet e de tecnologia avançada para aprimorar as suas actividades ilícitas [49]. Estes criminosos, além de explorarem a rede global para cometerem crimes de tipo tradicional, como a distribuição de droga, ainda exploram o mundo digital para cometer crimes de cariz mais tecnológico, como a usurpação de identidade ou a fraude com cartões de crédito [14].

Outro factor que pode complicar a investigação do cibercrime é a tecnologia de cifragem que protege a informação contra acessos não autorizados. Tal como o anonimato, a

cifragem não é nova, mas a tecnologia dos computadores impulsionou esta área de conhecimento de tal modo, que hoje é possível cifrar qualquer informação com um simples movimento do rato do computador. Esta tecnologia de acesso fácil é utilizada para dificultar o trabalho das autoridades, camuflando eficazmente muitas das comunicações criminosas [19]. Assim, a tecnologia moderna favorece o desenvolvimento de um tipo de criminalidade que se distingue da criminalidade tradicional em dois aspectos essenciais: é muito mais difícil para as autoridades identificar e capturar os criminosos, e estes podem cometer os seus crimes numa escala nunca antes alcançada [2].

3.2.4. Organização

Os cibercriminosos têm vindo a estabelecer alianças com traficantes de droga do Afeganistão, do Médio Oriente e de outras paragens, onde as suas lucrativas actividades ilegais são utilizadas para financiar grupos terroristas. Muitos destes grupos criminosos são transnacionais e os seus membros operam a partir de pontos dispersos por todo o mundo, trabalhando em conjunto para atingir os seus objectivos [51]. De acordo com a Europol, há cerca de 3600 grupos de crime organizado activos no espaço da União Europeia e estes grupos estão cada vez mais organizados em redes com hierarquias flexíveis que tiram pleno partido das tecnologias da Internet e das comunicações móveis [13].

O crime organizado está também a recrutar adolescentes que, gradualmente, deixam a criminalidade de rua e se especializam em diversas actividades ilícitas que podem desempenhar *online* a partir da relativa segurança doméstica. De acordo com um estudo da *McAfee*, estas organizações criminosas estão há alguns anos a recrutar jovens talentos universitários, incentivando-os a desenvolver capacidades em áreas que serão mais tarde exploradas na cibercriminalidade tecnologicamente sofisticada [37]. O FBI considera que os principais autores por detrás da cibercriminalidade são os grupos organizados que atacam essencialmente o sector financeiro, embora estejam a alargar o leque das suas actividades [14]. Estas tendências do crime organizado, tanto de recrutamento jovem como de ameaça sobre as instituições financeiras, são também confirmadas pelas autoridades europeias [18], o que ilustra o carácter verdadeiramente global desta tendência.

3.2.5. Impacto

Não existem dados verdadeiramente fiáveis, nem sobre o número de incidentes, nem sobre o impacto financeiro da criminalidade, e assim é difícil avaliar com rigor a verdadeira dimensão desta ameaça. Além das limitações impostas pela ausência de uma definição clara do que é cibercrime, há também que ter em conta que os dados disponíveis são fornecidos voluntariamente pelas vítimas e algumas preferem não o fazer [14]. Esta ausência de estatísticas, válidas relativas aos danos financeiros causados

pela cibercriminalidade, e a persistente confusão acerca da tipificação exacta destes incidentes, são os maiores obstáculos à existência de uma métrica rigorosa que permita avaliar a verdadeira dimensão e intensidade do cibercrime [51]. Embora todos os estudos sobre a matéria sejam apontados como sendo limitados e parciais, vale a pena ter em conta, apenas como referência, uma estimativa recente [46] que aponta para um número na ordem dos 110 mil milhões de dólares anuais, apenas em vinte e quatro países. Um outro estudo [39], limitado apenas aos EUA, estima que as organizações analisadas perdem, em média, cerca de 9 milhões de dólares por ano. No entanto, este estudo, à semelhança de outros, não define cibercrime e não especifica que critério foi considerado para incluir os incidentes considerados.

Existem numerosas razões que justificam a relutância que as organizações têm em reportar a ocorrência de intrusões nos seus sistemas. A mais vulgar é, obviamente, o medo do que isso possa fazer à sua imagem pública e à sua posição no mercado concorrencial [29]. Esta relutância das empresas, e mesmo dos cidadãos que não reportam as pequenas fraudes de que são vítimas, contribui para que as estimativas sejam todas deturpadas, ou seja, com valores inferiores à realidade [14]. Mas, há ainda uma outra razão para a ausência de dados fidedignos relativos ao cibercrime: muitas vítimas não reportam os incidentes por acreditarem que as autoridades não têm capacidade para apreender os responsáveis [3]. O recente escândalo do *Liberty Reserve* [9] veio pôr a descoberto um extenso rol de situações que ilustram todos os aspectos atrás referidos e que podem perfeitamente ser apenas a ponta de um tenebroso iceberg de esquemas ilícitos à escala global. À data de elaboração deste trabalho, todos os indícios apontam no sentido de se tratar da maior operação de lavagem de dinheiro jamais descoberta.

4. Desafios legislativos

A indústria das tecnologias de informação evoluiu, num relativamente curto espaço de tempo, desde as grandes máquinas que ocupavam salas inteiras até aos modernos dispositivos portáteis para os quais se podem comprar aplicações mais baratas do que uma chávena de café. Este progresso foi acompanhado por grandes desenvolvimentos nos modelos de computação e nas redes de computadores, que culminaram na moderna Internet e nas diversas formas de computação pessoal móvel. Mas estas tecnologias, devido ao seu carácter único e até volátil, criaram novos e complexos desafios legais para indivíduos, negócios e legisladores. É precisamente a natureza inovadora destes desafios que os torna tão difíceis de superar por parte das autoridades e pelos órgãos de polícia criminal.

4.1. Um novo paradigma de criminalidade

O cibercrime não substitui o crime do mundo real; é adicionado à panóplia de crimes que continuam a ocorrer com rotineira frequência. Até agora, o cibercrime não alterou a tendência de algumas pessoas para a violação, o roubo ou o assassinato no mundo real. A combinação destes dois efeitos cria uma sobrecarga no sistema, uma vez que os recursos existentes para lidar com a criminalidade tradicional não conseguem responder simultaneamente a essa realidade e às novas ocorrências da cibercriminalidade [3]. Como já vimos, o cibercrime pode ser automatizado e os criminosos podem evitar os constrangimentos físicos que limitam o mundo do crime tradicional. Um criminoso pode, com um mínimo de esforço e ainda menos visibilidade, desviar fundos de um banco europeu e colocá-los numa conta *offshore*. O actual modelo de policiamento, que assenta na premissa da reacção efectiva das autoridades a uma ocorrência criminal, é muito menos eficaz contra o cibercrime, porque, nestes casos, a reacção policial ocorre muito depois do crime ter sido perpetrado com sucesso [3]. Além disso, os criminosos podem, com o auxílio da tecnologia, aumentar exponencialmente o número de crimes cometidos num curto espaço de tempo, criando novas dificuldades às autoridades policiais e judiciárias. Há ainda a considerar a dificuldade em traduzir os cibercrimes em ofensas puníveis pela lei. Imaginemos o caso de um vírus informático que provoca milhões de euros de prejuízo. Trata-se de um crime (um vírus), milhares de crimes (milhares de vítimas) ou de milhões de crimes (milhões de euros perdidos)? [3].

Especialmente preocupante é o facto de muitas das ferramentas tecnológicas maliciosas serem de fácil utilização e estarem livremente disponíveis na Internet [19]. No final de 2011, mais de um terço da população mundial (cerca de 2,3 mil milhões de pessoas) estava ligada à Internet e aproximadamente 70% dos lares nos países desenvolvidos tinham acesso a banda larga, a velocidades cada vez mais elevadas e a custos cada vez menores [49]. Todos estes utilizadores, e os outros que continuamente engrossam a imensa multidão anónima de cibernautas, são potenciais vítimas da moderna criminalidade ciberespacial. E qualquer um deles pode, com relativa facilidade, planear e executar um ataque informático com a informação e ferramentas disponíveis na Internet. Esta é uma nova realidade e, como diz Brenner, temos um modelo de aplicação da lei do séc. XX para combater criminalidade do séc. XXI [3].

4.2. Privacidade e anonimato

Como já vimos, o anonimato é das características marcantes da criminalidade no ciberespaço. Uma vez que os cibercriminosos não estão fisicamente presentes na “cena” do crime, a presunção de que foram observados a planear, a cometer ou a fugir do crime, não é válida [3]. Além da dificuldade em seguir as eventuais pistas deixadas pelos criminosos, as autoridades têm também que se debater com a questão do direito à privacidade garantido pelas leis fundamentais dos regimes democráticos, embora existam diferenças consideráveis nos dois lados do Atlântico. Nos EUA, a Quarta Emenda Constitucional impede a busca e apreensão sem justificação, garantindo o direito individual à privacidade. A Europa tem um modelo diferente e esta distinção, nas palavras de Omar Tene é que, nos EUA, a privacidade é aquilo que o individuo considera

privado, e na Europa é aquilo que os legisladores nos dizem que é privado[10].

Assim, a investigação de uma ocorrência, além de ser extremamente dificultada pelas questões tecnológicas intrínsecas a este tipo de criminalidade, esbarra ainda nas questões éticas que rodeiam o respeito pela privacidade dos indivíduos e, até, pelo sigilo das empresas. Muitas companhias que distribuem *software* malicioso, fazem-no a coberto de outras actividades legítimas o que acaba por ser uma importante fonte de financiamento e um disfarce para uma variedade de cibercrimes [51]. Por outro lado, o sigilo empresarial permite que as empresas vítimas de cibercriminalidade escondam essas ocorrências, tentando manter intacta a sua imagem de fiabilidade perante o segmento de mercado onde se inserem. Outra forma de explorar o sigilo empresarial é utilizada por empresas tecnológicas que, num ostensivo desafio à legislação vigente, garantem anonimato total a quem contratar os seus serviços[11].

Como sociedade, queremos que as nossas autoridades recolham informação para prevenir, ou resolver, tantos crimes quanto for possível. No entanto, como indivíduos, queremos que as mesmas autoridades respeitem limites durante este processo de recolha. Isto é, não queremos que as autoridades violem a nossa privacidade individual, a menos que cumpram determinados requisitos legais [3]. Este tenso balanço entre privacidade e segurança em que vivem as sociedades democráticas, tem sido habilmente explorado por organização criminosas, mas também por diversas autoridades governamentais. O recente escândalo da monitorização das comunicações efectuadas pelo governo americano levanta sérias questões sobre a sua legitimidade e o impacto provocado na privacidade dos cidadãos[12].

4.3. Soberania e jurisdição

Quando um cibercrime envolve vítimas que estão num país, e o autor está noutro país, as autoridades não podem simplesmente recorrer aos procedimentos normais de investigação e apreensão. Como o nosso mundo é na realidade um conjunto de espaços soberanos, cada estado nação é uma entidade distinta e exerce soberania absoluta sobre o território que controla. Um mandato judicial emitido nos EUA não tem qualquer validade noutro país, e vice-versa [3]. Embora para os criminosos a Internet não tenha fronteiras, os agentes da autoridade têm que respeitar a soberania das outras nações.

Este problema da recolha de prova e apreensão de criminosos noutro país não é exclusivo da cibercriminalidade. O traço distintivo do cibercrime é a frequência com que esta circunstância ocorre. O que era uma excepção está a tornar-se norma, e a lei não acompanhou esta tendência [3]. Durante muito tempo, os entusiastas da Internet acreditaram que esta seria imune à regulação estatal, não porque os estados não a quisessem regular, mas porque não o conseguiriam fazer, impedidos pelas características atrás elencadas [1]. No entanto, são cada vez mais as vozes que se erguem e afirmam que o ciberespaço é erradamente caracterizado como sendo um domínio que transcende o espaço físico e que, por isso, é imune à soberania dos estados e resistente à regulação

internacional [33]. Apesar de os diferentes sistemas legais e as disparidades na lei serem um enorme obstáculo [29], há quem acredite que o exercício da soberania estatal no ciberespaço é, não só possível, mas essencial para o estabelecimento de uma ciberordem internacional [33].

4.4. Santuários do cibercrime

Outro factor que dificulta a aplicação da lei aos criminosos do ciberespaço prende-se com facto de estes poderem operar a partir de uma localização onde a sua actividade não seja criminalizada ou não seja encarada como motivo para extradição [2]. Por outras palavras, os criminosos podem explorar a existência de refúgios onde as autoridades locais, ou não podem, ou não querem, actuar sobre eles. A atitude da Rússia, relativamente ao cibercrime – perseguir criminosos que atacam alvos domésticos e ignorar os que atacam alvos no estrangeiro –, é um exemplo deste tipo de situação [3]. Uma série de outros pequenos estados também se tornaram centros de actividade do cibercrime internacional. Estas nações são, na prática, santuários para este tipo de criminalidade, permitindo que os criminosos actuem com total impunidade. Se, por vezes, este facto pode ser imputado à falta de capacidade do estado para impor a lei, muitas vezes é também devido à existência de uma cumplicidade entre as autoridades nacionais e as poderosas máfias do crime organizado internacional [7]. O mesmo pode ser dito de outros países onde, por diversas razões, o combate ao cibercrime não é uma prioridade. Estes países têm outras prioridades, como garantir a estabilidade do estado e alimentar o povo, logo a cibercriminalidade não é uma das preocupações prementes, porque os alvos dos criminosos estarão nos países ricos [3].

Como funciona um refúgio do cibercrime? Se imitar o funcionamento de um santuário de secretismo bancário, terá que legalizar o cibercrime, ainda que parcialmente, o que parece ser improvável. Se simular os velhos santuários da pirataria de alto mar, então nem sequer terá leis que criminalizem o cibercrime ou abdicará de as aplicar. De momento, a Rússia parece estar nesta última categoria, ou seja, funciona como um santuário de cibercrime onde a lei é aplicada de forma irregular [3]. O mais conhecido exemplo desta situação é o da famosa *Russian Business Network*, organização criminosa alegadamente responsável por dar cobertura a todos os tipos de cibercriminalidade de forma completamente impune[13]. A continuada exposição pública e denúncia internacional[14] a que esta organização foi sujeita, em finais de 2007, levou a que alterasse as suas operações e saísse de cena. No entanto, notícias recentes dão conta do seu regresso em força, sendo responsável pelo ressurgimento de uma nova versão de uma das grandes ameaças do passado, adaptada para actuar nas modernas redes sociais[15]. Na realidade, o submundo do cibercrime russo é muito vasto e complexo, tal como tem vindo a ser denunciado em diversos relatórios da indústria de segurança [23] [47] [16] [12] que alertam não só para a variedade e número de ameaças provenientes da Rússia, mas também para a dificuldade legal em combater essas mesmas ameaças. Embora num contexto diferente, mas com uma dimensão verdadeiramente assombrosa, a China ocupa igualmente um lugar de destaque entre as nações onde ocorrem actividades

cibercriminosas em larga escala [28]. Por último, existem diversas nações no continente africano onde estas actividades ilícitas estão a desenvolver-se a ritmo assustador [47].

4.5. Investigação

A recolha de provas digitais cria novos desafios e requere novas capacidades. A facilidade com que se alteram, ou apagam completamente, os vestígios da cibercriminalidade é um dos grandes desafios forenses da actualidade [49]. Além disso, as provas digitais podem ser incrivelmente volumosas, o que implica que os investigadores poderão ter que despender muito tempo, espaço de armazenamento e recursos de computação, na análise e identificação de elementos relevantes para um determinado caso [36] [2]. Se os criminosos e as vítimas estiverem localizados em diferentes países, as investigações só podem avançar com a cooperação das autoridades de ambos os estados uma vez que a soberania nacional não permite investigações no interior do território de um país estrangeiro sem a autorização expressa desse mesmo país [20]. Assim, é absolutamente fundamental que a investigação conte com o apoio e participação das autoridades de todos os países envolvidos.

É difícil cooperar no combate ao cibercrime com base nos tradicionais princípios de assistência legal mútua, uma vez que os requisitos formais e o tempo necessários para estabelecer esta colaboração são muitas vezes um factor retardador das investigações [20]. Além disso, como já vimos, os vestígios de uma acção cibercriminosa podem desaparecer muito rapidamente o que implica que toda a tramitação legal necessária à colaboração internacional tenha que ser expedita, sob pena de ser completamente inútil. Ou seja, os métodos tradicionais de colaboração internacional não funcionam para investigar e combater a cibercriminalidade transnacional [49]. As dificuldades na obtenção de prova digital, na sua preservação e análise têm vindo a ser referidas há vários anos [36] e, embora as ferramentas de pesquisa forense digital tenham evoluído imenso, os problemas continuam a agravar-se em face das cada vez maiores capacidades tecnológicas dos cibercriminosos [11] [8]. Esta tendência é referida pelas Nações Unidas [49] como um dos grandes desafios do combate à cibercriminalidade e a indústria de segurança alerta para o facto de os cibercriminosos estarem a utilizar as ferramentas de segurança em seu proveito próprio, partilhando informação entre si e tornando cada vez mais difícil o trabalho dos investigadores nesta área [35].

A conjugação de todos os aspectos atrás referidos cria novas dificuldades às autoridades que, na esmagadora maioria dos países, não estão preparadas para os enfrentar. Os investigadores têm que ser devidamente treinados na localização, preservação e análise de provas digitais, e têm que ter à sua disposição todas as ferramentas necessárias para desempenhar estas tarefas. Uma vez que a tecnologia está em permanente evolução, e a um ritmo crescente, é absolutamente imprescindível garantir que os investigadores da cibercriminalidade têm acesso a todos os recursos de que necessitam para se manterem a par dos criminosos que perseguem [8] [49]. Trata-se de uma área de investigação relativamente recente e onde não é verdadeiramente possível criar uma tradição, pois o

ritmo de evolução é verdadeiramente estonteante. Em face deste realidade, na opinião de Brenner, é difícil, senão mesmo impossível, para a maioria das forças de segurança, manter um corpo de agentes altamente especializados e equipados para lidar com a cibercriminalidade, em particular com as suas variantes mais sofisticadas e complexas [2].

5. Principal legislação vigente

Todas estas actividades criminosas estão em permanente evolução o que coloca uma constante pressão sobre as autoridades policiais e judiciárias. À medida que a globalização evolui, a necessidade de uma melhor coordenação internacional contra o cibercrime torna-se cada vez mais premente. A nível europeu, a integração de um número cada vez maior de países acentua a necessidade de coordenar os esforços policiais de modo a evitar a fragmentação das acções de combate ao cibercrime. No entanto, embora seja uma responsabilidade de todos, muitos países tardam em adoptar legislação apropriada e esse facto tem criado profundas assimetrias a nível global.

5.1. Convenção do Conselho da Europa

A Convenção do Conselho da Europa (CCE), de 2001, é um marco histórico no combate ao cibercrime é, sem dúvida, o mais importante instrumento legal neste campo. A CCE tem como objectivo facilitar a cooperação internacional, detecção, investigação e penalização da cibercriminalidade e apela ao estabelecimento de uma base comum de actuação legal e judicial.

5.1.1. Descrição

A CCE é o primeiro e único tratado internacional que aborda as lacunas da lei relacionadas com a Internet ou outras redes e requere que os países participantes actualizem e harmonizem as suas leis criminais contra os tipos de cibercriminalidade nela tipificados [51]. A convenção é uma importante ferramenta legislativa internacional, porque compromete os países signatários da mesma forma que um tratado, ou seja, assim que um número significativo de países a ratifique passa a ser aceitável tratá-la como lei geral [29]. Os redactores da CCE acreditavam que as lacunas e conflitos nas leis nacionais diminuíam a capacidade das autoridades para responderem à cibercriminalidade. Assim, a convenção tenta corrigir este facto garantindo que os países ilegalizem os vários tipos de cibercrimes e forneçam às autoridades os instrumentos necessários à investigação da cibercriminalidade [3].

Para estarem abrangidos pela CCE e submetidos às suas disposições, os países têm que a assinar e ratificar formalmente. Ao fazê-lo, assumem que as suas leis domésticas criminalizam as condutas descritas na convenção como constituindo cibercrimes, ou seja, uma panóplia de actividades que, como já vimos, se enquadram em quatro categorias genéricas de crimes relacionados com computadores. A CCE assenta implicitamente no princípio de que todos os países irão, eventualmente, ratificá-la, o que significaria que cada país teria leis do cibercrime completas e consistentes [3]. Além disso, a convenção estabelece critérios jurídicos baseados no princípio da territorialidade. No seu Art.º 22º, a CCE determina que cada parte adoptará medidas, legislativas e de outro tipo, necessárias para estabelecer jurisprudência sobre qualquer violação da lei, quando esta for cometida no seu território, embora sejam também identificadas situações em que este princípio da territorialidade pode ser ultrapassado [15].

5.1.2. Limitações

A noção base da CCE – que a harmonização das leis nacionais irá melhorar a capacidade de actuação das autoridades a nível transnacional – é inatacável. O problema está na sua implementação. A convenção contém quarenta e oito artigos, dos quais, pelo menos, trinta e três implicam a adopção de medidas legislativas ou outro tipo de implementação. Esta tarefa é dificultada pelas diferenças nas leis locais e na cultura de cada país. A convenção foi redigida por europeus que receberam um contributo substancial de juristas norte-americanos [2] e, por isso mesmo, é natural que incorpore noções e procedimentos que não são rotineiros noutras partes do mundo. Isto não significa necessariamente que outros países não a possam implementar; significa apenas que levará muito tempo até que isso aconteça.

A Convenção ficou disponível para assinatura em 23 de Novembro de 2001 mas, na altura da elaboração deste trabalho, quase doze anos depois da sua criação, apenas trinta e nove países a ratificaram, embora outros doze a tenham assinado sem a ratificarem[16]. Tendo em conta que existem neste momento quase duzentos países no mundo, parece-nos legítimo afirmar que, até ao momento, a eficácia da CCE no combate ao cibercrime tem sido muito restrita. Há quem afirme que se trata de uma fase transitória e que o ritmo de ratificações aumentará à medida que todos os países forem tomando consciência da real dimensão da ameaça da cibercriminalidade [3]. No entanto, a realidade parece ser diferente uma vez que, em 2008, a Rússia recusou assinar a Convenção alegando que um dos artigos da mesma ameaçaria a sua soberania [40].

Há outros países que podem menosprezar o cibercrime, uma vez que não são afectados por esse flagelo. Em termos práticos, se os cidadãos de um determinado país não são vítimas, as autoridades desse país não encararão o cibercrime como um problema, especialmente se tiverem a consciência de que as vítimas estão nos chamados países ricos [3]. Alguns especialistas, como Brenner, sustentam que o objectivo de garantir que o maior número possível de países tenha leis adequadas à cibercriminalidade, embora nobre, tem poucas hipóteses de converter o actual modelo de aplicação da lei num meio

eficaz de combater este flagelo [3]. Por último, importa ter presente que a convenção foi baseada na conduta dos cibercriminosos, nos anos de 1990. Entretanto, surgiram novos métodos e técnicas que não se enquadram na tipificação feita na altura e muitos países já reagiram, adaptando as suas leis para dar resposta a esta realidade em permanente mutação. Portanto, a terminologia utilizada na Convenção está ultrapassada e não é adequada para tipificar a ampla variedade de cibercrimes actuais [40]. Ou seja, resumir a cibercriminalidade a violações de segurança, fraude e falsificação, pornografia infantil e violação de direitos de autor é completamente desajustado da realidade contemporânea. Em face destas limitações, e embora continue a ser um instrumento legal de referência a nível internacional, pensamos que, doze anos depois da sua criação, o impacto real da CCE é ainda muito limitado.

5.2. Outras iniciativas

Em 2007, as Nações Unidas lançaram a *ITU Global Cybersecurity Agenda*[17] (GCA) com o intuito de ser uma iniciativa para a cooperação internacional, no sentido de aumentar a confiança e a segurança da sociedade da informação. Todas as medidas enunciadas nos cinco pilares da CGA são essenciais para uma estratégia de cibersegurança, logo, absolutamente incontornáveis no combate ao cibercrime [20]. Em 2009, a ITU lançou o *Draft Cybercrime Legislation Toolkit*, com o propósito de fornecer exemplos de normas e materiais de referência como meios auxiliares na criação de leis e procedimentos harmonizados no âmbito das Nações Unidas. Entretanto, este documento já foi actualizado com as mais recentes análises efectuadas às diversas molduras legais existentes no mundo e está agora disponível com o nome *Understanding Cybercrime: Phenomena, Challenges and Legal Response* [20], num outro formato, mas com os mesmos objectivos.

A nível europeu, embora tenha sido criado na Europol, em 2002, o *High Tech Crime Centre* para a coordenação dos esforços dos diferentes países no combate à nova criminalidade, não se pode afirmar que isso tenha contribuído para a criação de uma verdadeira política europeia de combate ao cibercrime [15]. No entanto, as iniciativas legislativas continuaram a surgir, num esforço continuado de adaptação à nova realidade criminal. Em 2007, a União Europeia (UE) emitiu uma directiva sobre retenção de dados que impõe às companhias de telecomunicações dos estados membros a retenção de um conjunto de dados relativos a todas as comunicações. Os dados têm obrigatoriamente que ser mantidos durante um período que varia entre os seis meses e os dois anos e, em caso de necessidade para a investigação de ofensas sérias, as companhias são obrigadas a disponibilizá-los, assim que, para tal, forem notificadas judicialmente. Esta directiva entrou em vigor em Abril de 2009, data a partir da qual todos os fornecedores de serviço de acesso à Internet na UE têm que obedecer às implementações nacionais da referida directiva [9]. Além disso, no dia 1 de Janeiro de 2013, entrou oficialmente em actividade o *European Cybercrime Centre* (EC3), na Europol, com a missão de melhorar a resposta aos cibercrimes e auxiliar os estados membros e as instituições da UE no desenvolvimento de novas capacidades para a investigação e cooperação com os

parceiros internacionais.

6. O futuro da cibercriminalidade

Como já vimos, a cibercriminalidade reveste-se de um conjunto de características que a tornam uma actividade aliciante, e esse facto tem contribuído para um aumento do número de cibercriminosos e um aumento ainda maior no número de vítimas [3]. Uma vez que os lucros ilícitos são potencialmente muito avultados, alguns grupos de criminosos estão a adoptar práticas empresariais do mundo das tecnologias de informação para desenvolverem mais e melhores ferramentas para as actividades de cibercriminalidade [51]. Relatórios recentes [16] [49] confirmam o agravamento da já referida tendência para o recrutamento de jovens estudantes [51] [37], embora muitas vezes estes não tenham consciência de que nos bastidores das empresas de recrutamento estão grupos de crime organizado. O impacto estimado da cibercriminalidade é apenas a parte visível deste tenebroso icebergue que esconde nas suas profundezes uma enorme rede de interesses criminosos à escala global.

6.1. Crime organizado

O cibercrime está cada vez mais organizado [49] e assume gradualmente um carácter de negócio internacional [16]. Existem, há vários anos, diversas ofertas de cibercriminalidade para aluguer [51], e esta tendência agravou-se recentemente para dar resposta a uma crescente procura de um leque cada vez mais variado de clientes, desde indivíduos até grupos terroristas [49] [16] [13]. É hoje evidente que há diversos grupos terroristas a tirar partido da Internet para difundir as suas mensagens e recrutar novos elementos para a sua causa. Da mesma forma, estas organizações terroristas exploram a cibercriminalidade como forma de financiamento das suas actividades e aliam-se a grupos de cibercriminosos para alcançar objectivos comuns [51].

Actualmente, à semelhança do que ocorre em qualquer empresa, o cibercrime evoluiu até ser uma hierarquia complexa de dirigentes, engenheiros e simples operários. Os bastidores destas organizações são complexos e incluem sofisticados núcleos de pesquisa e desenvolvimento que criam códigos informáticos maliciosos por encomenda [16]. O cibercrime está solidamente estabelecido, bem equipado e ricamente financiado. Emprega uma multidão de simples funcionários, fornecedores e parceiros [23] [28] e está num constante processo de produção de novas formas de iludir as mais recentes ferramentas de segurança, levar a potenciais vítimas a instalar *software* malicioso, ou simplesmente roubar-lhes informação sensível [16]. É expectável que o cibercrime continue a desenvolver-se e organizar-se em poderosas estruturas como as que se encontram hoje dispersas em diversos países do antigo bloco soviético e outras que se

espera que surjam em África [47] e na América do Sul [18].

6.2. Sofisticação tecnológica

Os ataques cibernéticos são, cada vez mais, concebidos para roubarem informação sem deixarem atrás de si nenhum tipo de vestígios que possam alertar imediatamente as vítimas. As autoridades, a indústria e as empresas limitam-se a responder às ameaças emergentes, criando novas defesas, mas não conseguem antever com prever com rigor quais as novas ferramentas que serão utlizadas pelos cibercriminosos. Como já vimos, o constante esforço de pesquisa dos malfeitores e a criatividade dos programadores que contratam, produzem novos resultados a um ritmo avassalador. A cibercriminalidade irá explorar intensivamente o novo paradigma da computação na nuvem[18]. Muitas empresas, indivíduos, e até governos, têm beneficiado significativamente da mudança das suas necessidades de computação para a nuvem. Mas a computação na nuvem é igualmente atractiva para os cibercriminosos que têm explorado as redes sociais e outros serviços gratuitos em seu proveito [47]. Por outro lado, este novo modelo de computação sobrecarrega ainda mais o sistema legal, uma vez que se avolumam as disputas sobre jurisdição, protecção de dados, propriedade intelectual, responsabilidade e outros. É inquestionável que todos estes avanços tecnológicos irão criar novos desafios aos profissionais da lei [24].

Os criadores de *software* malicioso já utilizam uma grande variedade de ferramentas para atingir os seus objectivos. Portanto, parte dos desenvolvimentos nesta área irão certamente concentrar-se no aperfeiçoamento das ferramentas existentes, criando novas formas de responder às novidades introduzidas pela indústria de segurança. Nesta categoria estão os conjuntos de *software* (*exploit kits*) prontos a utilizar que, periodicamente, são actualizados e reforçados com novas capacidades e formas de iludir os órgãos de polícia criminal nos seus esforços forenses [47] [35]. Assim, as tendências actuais vão no sentido do desenvolvimento e aperfeiçoamento de métodos que permitam atingir as vítimas sem levantar suspeitas, além do incremento da cooperação entre diversos grupos de criminosos, partilhando informação tecnológica relevante [47].

6.3. Computação móvel

O volume de aplicações maliciosas para dispositivos móveis pode triplicar em 2013, acompanhando o crescimento explosivo deste mercado. Embora os fabricantes se esforcem por melhorar a segurança dos seus dispositivos, está em curso em verdadeira corrida às armas entre os cibercriminosos e a indústria de segurança [47]. Estudos recentes [12] estimam que o número de utilizadores de serviços bancários a partir de plataformas móveis irá ultrapassar os 500 milhões já em 2013, o que é um indicador claro de que essa será uma das áreas preferenciais de actuação da criminalidade informática. Existe também uma tendência para utilizar os dispositivos móveis como forma de pagamento (*mobile wallet*), impulsionada por alguns dos principais agentes do mercado.

Embora tenham já sido descobertas diversas vulnerabilidades no protocolo de comunicação utilizado [22], a massificação deste serviço parece inevitável, pois é uma área de negócio apetecível para muitas empresas, apesar de ser do conhecimento público que os cibercriminosos, como sempre, estão à espreita. Há ainda um grande número de outras ameaças para as plataformas móveis, algumas enviadas mesmo por *sms* [12].

Outro factor que reforça o dramático crescimento das ameaças sobre a computação móvel é a crescente tendência conhecida como BYOD[19]. Embora as empresas encarem esta tendência com entusiasmo, pois permite-lhes poupar dinheiro, a verdade é que cria todo um novo problema de segurança [12]. Se, por exemplo, um funcionário pode aceder a todos os recursos da sua empresa através de um *smartphone* que está infectado com um *software* malicioso, este acesso pode resultar num roubo de informação sensível [6]. Assim, o imenso número de dispositivos móveis é uma oportunidade que os atacantes não irão desvalorizar, até porque nalguns países são já a principal forma de aceder à Internet [22].

6.4 Novos alvos

O estilo de vida digital em que os consumidores alegremente mergulham, liga-os cada vez mais à Internet e leva-os a aderir a novas tecnologias que são passíveis de ser exploradas de forma nefasta. Hoje em dia, muitos aparelhos de TV têm acesso à Internet e permitem o aluguer de filmes, consultas bancárias, etc.. Os sistemas operativos destes dispositivos não são concebidos segundo uma lógica de segurança, mas sim de facilidade de utilização e isso pode ser facilmente explorado pelos cibercriminosos [47]. À medida que a tecnologia evolui, mesmo os dispositivos que eram simples se tornam agora mais complexos e capazes de disponibilizar novas formas de comunicar. Embora todas estas inovações, quando usadas correctamente, possam simplificar a nossa vida, criam também novas oportunidades para a criminalidade tecnologicamente evoluída [12]. Os dispositivos móveis, as aplicações, e as redes sociais estão cada vez mais integrados, o que cria novas vulnerabilidades e oportunidades. As novas tecnologias como o pagamento de serviços com o *smartphone*, ou a integração do GPS para ligar a nossa vida digital e a nossa vida real, criam todo um novo leque de possibilidades para comprometer a nossa segurança e a nossa privacidade [35].

A rápida adopção do BYOD, a utilização de múltiplos dispositivos por utilizador, a migração para a *cloud*, e todas as outras novidades que surgem constantemente, criam uma rede ciberespacial inteligente mas que tem imensas vulnerabilidades, tantas quantas as que cada utilizador tem. À medida que os ataques se tornam cada vez mais sofisticados, são capazes de infectar multidões em silêncio, sem discriminar indústria, negócio, país ou cidadão. A superfície de ataque cresce todos os dias e os cibercriminosos exploram todas as oportunidades que lhes são oferecidas, cada vez que um individuo utiliza um dispositivo para entrar na rede da sua empresa ou para aceder à sua conta bancária [6]. Como já referimos, o continente africano está a tornar-se a nova base para o cibercrime sofisticado. Os estrangeiros, forçados a escapar das autoridades dos seus

países onde a aplicação da lei é mais eficaz, estão a procurar refúgio junto dos cibercriminosos africanos à medida que a infra-estrutura da Internet no continente continua a desenvolver-se. O cibercrime desenvolve-se em áreas onde a aplicação da lei é ténue, especialmente se os criminosos contribuírem para a economia local e não atacarem alvos domésticos. A aplicação de leis contra o cibercrime é particularmente difícil em países em vias de desenvolvimento e, por isso, o cibercrime é uma verdadeira indústria em crescimento em África [47].

7. Soluções propostas

Estão em discussão diversas abordagens técnicas e legais para responder aos desafios atrás apresentados. As propostas variam desde a imposição de filtros aos resultados dos motores de busca, para que não disponibilizem as ferramentas para a prática da cibercriminalidade, até à limitação legal dos acessos indevidos a determinados conteúdos. O debate acerca das respostas legais vai desde a criminalização da produção, divulgação, venda, ou mesmo posse de ferramentas informáticas concebidas primariamente para a prática de ataques tecnologicamente sofisticados. Mas, como seria de esperar, estes controlos colidem muitas vezes com o espirito intrinsecamente libertário da Internet e este conflito, entre os aspectos políticos, éticos e económicos da sociedade *online*, tem dado origem a diversas formas de resistência organizada e a inúmeras questões legais.

7.1. Restrições tecnológicas

A Internet foi originalmente concebida como uma rede militar, numa lógica descentralizada e com uma arquitectura que lhe permitiria manter as suas principais funções intactas mesmo que alguns dos seus elementos falhassem. Como esta rede nunca foi destinada a facilitar qualquer tipo de investigação criminal, nos últimos anos têm sido desenvolvidas e implementadas diversas soluções técnicas, e as respectivas molduras legais, que permitem controlar o tráfego da Internet, nomeadamente bloquear o acesso a conteúdos ilegais alojados fora do país [19]. A solicitação aos fornecedores de serviço para a remoção de determinados conteúdos é normalmente eficaz, mas isto só fará com que os utilizadores mal-intencionados se mudem para outro fornecedor. A proliferação de uma vasta oferta de serviços fará com que no futuro seja cada vez mais difícil bloquear conteúdos ilegais por esta via [47].

A imposição de controlos baseados em filtragem é na realidade uma ilusão, pois os utilizadores minimamente esclarecidos podem facilmente evitar os filtros com o recurso a técnicas de cifragem que permitem comunicação anónima, escapando assim à censura dos fornecedores de serviço e das autoridades. Esta prática é corrente entre os

cibercriminosos que, inclusivamente, desenvolvem as suas próprias ferramentas para comunicarem em total liberdade. Uma campanha contra este tipo de comunicação só será eficaz com um esforço concertado a nível internacional, de modo garantir que os recursos da rede global não são utilizados de forma indesejada.

7.2. Novas medidas legais

A discussão das soluções legais para enfrentar os desafios da cibercriminalidade centra-se, inevitavelmente, sobre a harmonização da legislação a nível internacional e sobre o incremento da cooperação em assuntos do foro cibercriminal. Embora o assunto continue a ser amplamente discutido, e esteja longe de ser consensual, têm surgido diversas propostas com vista a atingir o objectivo de ter ferramentas legais verdadeiramente eficazes para enfrentar o previsível futuro do cibercrime. Além disso, há também uma crescente consciencialização para a necessidade de adoptar um modelo de policiamento que permita combater com eficácia a cibercriminalidade transnacional.

7.2.1. Tribunal internacional

O juiz Schjolberg considera que a investigação criminal e a condenação do cibercrime, baseadas em legislação internacional, necessitam de um tribunal internacional para o efeito. Na sua visão, a instituição de um tribunal deste tipo seria o garante de uma justiça universal. Este tribunal (*International Criminal Tribunal for Cyberspace*) seria baseado numa decisão do Conselho de Segurança das Nações Unidas e a escolha natural para a sua localização seria Haia [40].

Schjolberg propõe um estatuto provisório para este tribunal, nos termos do qual este teria o poder de acusar e condenar pessoas responsáveis pela violação das leis internacionais contra o cibercrime. Estaria assim satisfeita a necessidade, por si identificada, de ter um organismo supranacional para garantir igualdade de tratamento a todos os cibercriminosos, independentemente da sua nacionalidade ou do local a partir do qual cometeram os crimes. Além disso, a criação deste tribunal seria um sinal das Nações Unidas para a comunidade internacional, no sentido de globalizar e coordenar os esforços no combate ao cibercrime.

7.2.2. Polícia internacional

Conjuntamente com o tribunal internacional, Schjolberg considera que deveria ser criada uma agência (*Global Virtual Taskforce*) com a participação de todas as entidades interessadas, desde a indústria até à Interpol, trabalhando em cooperação contra o cibercrime [40]. Numa lógica similar, Brenner sugere a criação de uma polícia global (*World Cybercrime Police*) para combater o cibercrime transnacional como sendo a forma

ideal de lidar com este flagelo [3]. Contudo, esta especialista tem consciência da impraticabilidade de tal solução, pelo menos num futuro próximo. Segundo ela, os estados são protectores da sua soberania e, portanto, é improvável que abdiquem da sua autoridade e concordem com a criação desta força policial mundial. Como esta polícia teria jurisdição sobre crimes cometidos por, e contra, cidadãos de diversas nações, iria retirar aos estados uma parte da sua soberania. Brenner conclui que os países do mundo actual não estão preparados para isso e, provavelmente, os seus cidadãos também não [3].

No entanto, em 2014, entrará em funcionamento em Singapura o novo complexo da Interpol (*Global Complex*), do qual fará parte o *Digital Crime Centre,* especialmente orientado para a análise forense, pesquisa e desenvolvimento e todo o tipo de suporte ao combate à cibercriminalidade internacional. Schjolberg considera que Singapura poderia ser uma localização alternativa para o tribunal por si proposto, uma vez que a proximidade de uma grande agência de investigação poderia ser potenciada para conseguir que muitos dos crimes que agora ficam impunes, fossem punidos [40].

Seguindo uma linha de raciocínio um pouco diferente, Clarke propõe, como solução para resolver o problema dos santuários do cibercrime, a criação de um centro internacional (*Cyber Crime International Investigative Center*) dedicado à investigação destas actividades [7]. Na sua visão, este centro seria criado por um pequeno grupo de nações com o objectivo de manter uma base de dados de incidentes, operar uma equipa de especialistas forenses (*Significant Cyber Crime Response Squad*) e coordenar em tempo real a resposta a quaisquer ataques. O centro proposto por Clarke seria diferente da Interpol, na medida em que os estados considerados como santuários não fariam parte da organização, e seria diferente dos actuais CERT[20], porque a sua actividade estaria orientada para a resolução de crimes, a identificação e captura de criminosos, e a obtenção de condenações.

7.2.3. Nova lei transnacional

São inúmeras as vozes que se erguem em defesa da criação de novos instrumentos jurídicos de âmbito internacional. Embora possa ser defendido que esta legislação já existe, a verdade é que, por exemplo, a CCE não resolve os problemas relativos à jurisdição aplicável, uma vez que se baseia no princípio da territorialidade [15]. Ou seja, a CCE pode desempenhar um papel importante neste processo legislativo mas não poderá ser a única solução [3], uma vez que não é o instrumento adequado para a captura e punição de casos de cibercrime internacional [15]. Clarke, consciente das limitações da actual CCE, considera que a solução normativa ideal seria a criação de uma outra convenção global, que actualizasse e reforçasse a convenção de 2001 e fosse o suporte legal à actuação investigativa da organização operacional por si sugerida [7].

A título ilustrativo das dificuldades de harmonização nesta área, citamos o episódio no qual, em 2011, foi apresentado às Nações Unidas um documento de trabalho

(*International Code of Conduct for Information Security*) onde a China, a Rússia, o Tajiquistão e o Uzbequistão apelavam aos outros estados para que concordassem com a limitação da disseminação de informação que incite ao terrorismo, secessionismo, extremismo ou que ataque a estabilidade política, económica e social além do ambiente cultural e espiritual de outros países. Embora a fundamentação apresentada para esta limitação tenha sido exactamente o combate a várias formas de criminalidade *online*, o documento foi de imediato rejeitado por um grande número de estados democráticos [7], uma vez que, para estes, a censura não é condição *sine qua non* para a a cibersegurança. Estas diferenças culturais continuam a ser um grande obstáculo à criação de uma estratégia global, pois há grandes distinções a nível internacional sobre quais devem ser os pressupostos legislativos a aplicar ao cibercrime.

8. Conclusões

As dificuldades legais do combate à cibercriminalidade têm a sua génese na definição exacta daquilo que a lei tenta regular, pois parece não ser possível definir com exactidão, nem "onde" decorrem os crimes, nem por que "meio" são cometidos. A multiplicidade de definições nesta área, algumas delas contraditórias entre si, leva-nos a afirmar que a legislação do cibercrime tenta regular uma variedade de actividades ilícitas, mal tipificadas e em permanente mutação, que decorrem num ambiente virtual, difuso e mal definido. O ritmo de evolução tecnológica é explorado de forma a permitir uma torrente de inovações criminais, cada vez mais sofisticadas, o que dificulta imenso a tarefa de criar uma moldura legal ajustada à sua regulação. Assim, no combate à cibercriminalidade, não é fácil preencher o tipo criminal, ou seja, cumprir todos os requisitos da lei para que uma pena possa ser aplicada, visto que a lei está frequentemente desajustada da realidade.

Partindo do princípio que, tudo o que não é punido pela lei é legal, então boa parte da moderna criminalidade informática escapa à alçada das legislações existentes, nomeadamente, as que derivam mais directamente da adaptação da CCE. O mundo moderno, incluindo Portugal, enferma de um conjunto de fragilidades legais que decorrem da utilização de uma moldura criminal obsoleta e incapaz de responder aos desafios da moderna criminalidade cibernética. A cibercriminalidade é um camaleão ameaçador que se transfigura com cada inovação tecnológica e evolui com uma velocidade que os mecanismos legais são completamente incapazes de acompanhar. Pelo contrário, uma revisão dos instrumentos jurídicos é um processo burocrático moroso, que dificilmente poderá acompanhar todas as *nuances* da criminalidade informática. Ou seja, o formalismo da lei não consegue opor-se à criatividade dos criminosos.

É necessária a adopção de um quadro legal mais flexível que permita uma resposta em tempo real aos incidentes e possibilite a imediata recolha de provas. O verdadeiro desafio para os sistemas criminais nacionais é combater o atraso existente entre o aparecimento

das novas ameaças e a implementação das necessárias emendas à lei criminal existente. À medida que a tecnologia avança, este desafio ganha vez mais relevância e torna-se mais exigente. O progresso galopante da tecnologia permite aos criminosos explorar todas as novidades técnicas para criar novas formas de obter lucros ilícitos, enquanto os órgãos de polícia criminal ainda estão a receber formação para combater as novidades do ano anterior.

Paralelamente, todas as mudanças tecnológicas em curso potenciam o aparecimento de novos riscos de segurança. A rápida adopção do BYOD faz esbater as fronteiras entre os dispositivos institucionais e os privados, o que abre uma imensa janela de oportunidades para que criminosos penetrem no ambiente das empresas e cria um novo problema legal. As empresas, aliciadas pela poupança, encorajam a utilização de dispositivos pessoais, mas não estão de todo preparadas para lidar com casos de comprovada violação de segurança provocada por essa mesma utilização. Por outro lado, a disseminação do *cloud computing* faz com que empresas e indivíduos acedam a recursos partilhados com níveis de segurança e termos de serviço, no mínimo, questionáveis. A crescente vulgarização de sistemas com grande sofisticação tecnológica leva a que estes sejam frequentemente adquiridos por, e distribuídos a, utilizadores muito pouco conscientes do seu real poder e de todas as suas vulnerabilidades. A exploração destas oportunidades leva a que o cibercrime seja cada vez mais sofisticado do ponto de vista tecnológico, estando mesmo muitas vezes na vanguarda do desenvolvimento de novas ferramentas e soluções.

Com base em todos os indicadores disponíveis, parece-nos ser óbvio que o volume, intensidade e impacto do cibercrime parecem destinados a aumentar no futuro. Esta tendência justifica-se, não só pelo facto de ser uma actividade altamente lucrativa, mas também porque a comunidade internacional não foi até aqui capaz de encontrar respostas à altura deste desafio. Além disso, a superfície de ataque aumenta constantemente à medida que a Internet se torna cada vez mais essencial à vida diária e o número de potenciais vítimas não pára de crescer. Sendo claro que a cibercriminalidade, nas suas diferentes facetas, é hoje um negócio altamente rentável, é de esperar que continue a atrair cada vez mais jovens talentos em busca de lucro fácil. A existência de organizações criminosas transnacionais, frequentemente apoiadas em estados que lhes servem como refúgio, é uma realidade a que a comunidade internacional, demasiado enredada nos jogos da *realpolitik*, parece ser incapaz de responder com uma estratégia concertada.

Embora se possa argumentar que o ciberespaço, apesar das suas características libertárias, não é imune à soberania dos estados, a verdade é que estamos ainda longe do dia em que será possível criar um mecanismo eficaz de controlo global que não interfira com as liberdades individuais dos cidadãos. Uma solução parcial pode passar por limitar o acesso livre às ferramentas que hoje estão na Internet e que podem ser utilizados para fins criminosos. O problema é que isto colide com a liberdade de expressão e debatemo-nos de imediato com o velho problema ético de avaliar em que medida estes valores são absolutos ou podem ser relativizados em prol do bem-estar comum. Nesta mesma linha de raciocínio, a hipótese de admitir a monitorização das comunicações dos cibernautas é uma situação que nos recorda o clássico dilema de saber até que ponto estaremos

dispostos a abdicar da nossa privacidade em prol de um ilusório sentimento de segurança. Por um lado, podemos argumentar que esta polémica não passa de uma valorização do conceito de segurança do estado em detrimento do binómio privacidade/anonimato, valor basilar nas democracias ocidentais. Por outro lado, não podemos deixar de invocar o clássico dilema de Juvenal quando se questionava *Quis custodiet ipsos custodes*[21]?

Embora sejam inequívocas as vantagens operacionais da existência de uma polícia de carácter global, pensamos que tal não será exequível num futuro próximo. Na realidade, o ciberespaço, embora sendo um ambiente virtual, é um reflexo do sistema político internacional, onde prevalecem as rivalidades e se digladiam interesses unilaterais. Divergências políticas e interesses geoestratégicos impedem a consolidação de uma verdadeira legislação internacional. Embora os governos e as instituições internacionais estejam conscientes da necessidade de articular uma resposta global a estas ameaças, outros valores se sobrepõem e a cibercriminalidade continua a prosperar. Se no mundo ocidental, com tradições culturais semelhantes, é difícil chegar um consenso, a nível global, não nos parece que tal venha a ocorrer nos próximos anos. Ou seja, no presente contexto geopolítico, a criação de uma lei transnacional eficaz, e a consequente harmonização das diferentes leis nacionais, parecem-nos ser tarefas de difícil realização.

Em suma, o futuro combate à cibercriminalidade terá forçosamente que ser a resultante de um equilíbrio entre o respeito pela liberdade dos cidadãos e a implementação de mecanismos de controlo, balanceados pela manutenção da independência da rede. Este cenário terá que assentar numa nova moldura legal internacional que acautele todos os interesses geopolíticos, salvaguardando as respectivas diferenças culturais entre estados. É este o desafio, verdadeiramente titânico, que toda a comunidade internacional tem que enfrentar.

Bibliografia

[1] Boyle, J. 1997. Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors. *University of Cincinnati Law Review*. 66, (1997), 177–205.

[2] Brenner, S.W. 2004. Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law and Technology*. 9, (2004).

[3] Brenner, S.W. 2010. *Cybercrime: Criminal Threats from Cyberspace*. Praeger Publishers.

[4] Brenner, S.W. 2002. Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law & Technology*. 4, (2002).

[5] Castells, M. 2001. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford University Press.

[6] Cisco 2013. *Annual Security Report*. Cisco Systems, Inc.

[7] Clarke, R.A. 2012. *Securing Cyberspace Through International Norms: Recommendations for Policymakers and the Private Sector*. Good Harbor Security Risk Management, LLC.

[8] Davidoff, S. and Ham, J. 2012. *Network Forensics: Tracking Hackers Through Cyberspace*. Pearson Education.

[9] Deibert, R. et al. eds. 2010. *Access controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press.

[10] DoD 2011. *DoD Strategy for Operating in Cyberspace*. U.S. Department of Defense.

[11] EC-Council 2010. *Computer Forensics: Investigating Network Intrusions and Cyber Crime*. Cengage Learning.

[12] ESET 2012. *Trends for 2013: Astounding growth of mobile malware*. ESET Latin America's Lab.

[13] EUROPOL 2013. *EU Serious and Organised Crime Threat Assessment*. European Police Office.

[14] Finklea, K.M. and Theohary, C.A. 2013. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Congressional Research Service, The Library of Congress.

[15] Foggetti, N. 2008. Transnational Cyber Crime, Differences between National Laws and Development of European Legislation: By Repression. *Masaryk University Journal of Law and Technology*. 2, (2008), 31.

[16] Fortinet 2012. *2013 Cybercrime Report*. Fortinet Inc.

[17] Furnell, S. 2002. *Cybercrime: Vandalizing the information society*. Addison-Wesley Boston.

[18] Gendarmerie, F.N. 2011. *Prospective Analysis on Trends in Cybercrime from 2011 to 2020*. French National Gendarmerie.

[19] Gercke, M. 2010. Challenges in Developing a Legal Response to Terrorist Use of the Internet. *Defence Against Terrorism Review*. 3, (2010).

[20] Gercke, M. 2012. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. International Telecommunication Union.

[21] Gibson, W. 1984. *Neuromancer*. Ace Science Fiction Books.

[22] GIT 2013. *Emerging Cyber Threats Report 2013*. Georgia Institute of Technology.

[23] Goncharov, M. 2012. *Russian Underground 101*. Trend Micro Inc.

[24] Harris, A. 2012. *The Legal Standing of Data in a Cloud Computing Environment*. Dublin Institute of Technology.

[25] House, W. 2008. Cybersecurity Policy, National Security Presidential Directive 54/Homeland Security Presidential Directive 23.

[26] House, W. 2009. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.

[27] House, W. 2003. National Strategy to Secure Cyberspace.

[28] Jianwei, Z. et al. 2012. *Investigating China's Online Underground Economy*. University of California, Institute on Global Conflict and Cooperation.

[29] Keyser, M. 2003. The Council of Europe Convention on Cybercrime. *Journal of Transnational Law & Policy*. 12, (2003), 287–327.

[30] Kuehl, D.T. 2009. From Cyberspace to Cyberpower: Defining the Problem. F.D. Kramer et al., eds. Potomac Books, Inc. 24–42.

[31] Larousse ed. 2011. *Larousse Enciclopédia Moderna*. Circulo de Leitores.

[32] Lévy, P. 1999. *Collective Intelligence: Mankind's Emerging World in Cyberspace*. Perseus Books.

[33] Liaropoulos, A. 2013. Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *Proceedings of the 8th International Conference on Information Warfare and Security*. (Mar. 2013).

[34] Lisboa, A. das Ciências de ed. 2001. *Dicionário da Língua Portuguesa Contemporânea*. Editora Verbo.

[35] Lyne, J. 2012. *Thirteen Trends for 2013*. Sophos Ltd.

[36] Marcella, A.J. and Greenfield, R.S. eds. 2002. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Taylor & Francis.

[37] McAfee 2007. *Virtual Criminology Report: The Next Wave*. McAfee Incorporated.

[38] Parker, D. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. John Wiley & Sons.

[39] Ponemon 2012. *2012 Cost of Cyber Crime Study: United States*. Ponemon Institute.

[40] Schjolberg, S. 2012. An International Criminal Court or Tribunal for Cyberspace (ICTC). *EastWest Institute*. (2012).

[41] Sofaer, A.D. and Goodman, S.E. eds. 2001. *The transnational dimension of cyber crime and terrorism.* Hoover Institution Press, Stanford University.

[42] Staff, J. 2001. *Joint Publication 1-02, Dictionary of Military and Associated Terms*. Department of Defense.

[43] Staff, J. 2008. *Joint Publication 1-02, Dictionary of Military and Associated Terms*. Department of Defense.

[44] Staff, J. 2013. *Joint Publication 1-02, Dictionary of Military and Associated Terms*. Department of Defense.

[45] Staff, J. 2006. *National Military Strategy for Cyberspace Operations*. Department of Defense.

[46] Symantec 2012. *2012 Norton Cybercrime Report*. Symantec Corporation.

[47] Trend 2012. *Security Threats to Business, the Digital Lifestyle, and the Cloud*. Trend Micro Inc.

[48] UN 2000. Crimes related to computer networks: Background paper for the workshop on crimes related to the computer network. *10th UN Congress on the Prevention of Crime and the Treatment of Offenders*. (2000).

[49] UNODC 2013. *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.

[50] Whittaker, J. 2004. *The Cyberspace Handbook*. Taylor & Francis Group.

[51] Wilson, C. 2008. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congressional Research Service, The Library of Congress.

[52] Zittrain, J.L. 2006. *The Generative Internet*. Harvard Law Review Association.

---

[1] Definição de ciberespaço, disponível em http://www.infopedia.pt/pesquisa.jsp?qsFiltro=0&qsExpr=ciberespa%C3%A7o. Infopédia, *Porto Editora*, consultado em 30 de Maio de 2013.

[2] Definição de ciberespaço, disponível em http://www.priberam.pt/dlpo, Dicionário *Priberam* da Língua Portuguesa, consultado em 30 de Maio de 2013.

[3] Disponível em http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration, consultado em 26 de Maio de 2013.

[4] United Nations, Human Rights Council, Resolution A/HRC/20/L.13, 29 de Junho de 2012, disponível em http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement, consultado em 30 de Maio de 2013.

[5] Hughes, Eric, *A Cypherpunk's Manifesto*, 9 de Março de 1993, disponível em http://www.activism.net/cypherpunk/manifesto.html, consultado em 12 de Junho de 2013.

[6] *What is Cybercrime?*, Symantec Corporation, disponível em http://us.norton.com/cybercrimedefinition/promo, consultado em 28 de Maio de 2013.

[7] Definição de cibercrime, disponível em http://www.infopedia.pt/pesquisa.jsp?qsFiltro=0&qsExpr=cibercrime, Infopédia, *Porto Editora*, consultado em 30 de Maio de 2013.

[8] Definição de cibercrime, disponível em http://www.priberam.pt/dlpo, Dicionário *Priberam* da Língua Portuguesa, consultado em 30 de Maio de 2013.

[9] Santora, Mark e Rashbaum, William, *Online Currency Exchange Accused of Laundering $6 Billion*, The New York Times, 29 de Maio de 2013, disponível em http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?, consultado em 30 de Maio de 2013.

[10] Tene, Omar, *Privacy in Europe and the United States: I Know It When I See It,* Center for Democracy and Technology, disponível em https://www.cdt.org/blogs/privacy-europe-and-united-states-i-know-it-when-i-see-it, consultado em 3 de Junho de 2013.

[11] CyberBunker Stay Online Policy, disponível em http://www.cyberbunker.com/web/stay-online-policy.php, consultado em 6 de Junho de 2013.

[12] Savage, Charlie, and Wyatt, Edward, *U.S. Confirms That It Gathers Online Data Overseas,* The New York Times, 6 de Junho de 2013, disponível em http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html, consultado em 6 de Junho de 2013.

[13] Krebs, Brian, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, The Washington Post, 13 de Outubro de 2007, disponível em http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html, consultado em 6 de Junho de 2013.

[14] Warren, Peter, *Hunt for Russia's web criminals*, The Guardian, 15 de Novembro de 2007, disponível em http://www.guardian.co.uk/technology/2007/nov/15/news.crime, consultado em 6 de Junho de 2013.

[15] Perloth, Nicole, *Malware That Drains Your Bank Account Thriving on Facebook*, The New York Times, 3 de Junho de 2013, disponível em http://bits.blogs.nytimes.com/2013/06/03/malware-that-drains-your-bank-account-thriving-on-facebook/, consultado em 3 de Junho de 2013.

[16] Listagem em: http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG, consultado em 5 de Junho de 2013.

[17] A ITU (*International Telecommunication Union*) é a agência das Nações Unidas especializada nas tecnologias de informação e comunicação.

[18] A expressão "computação na nuvem" (*cloud computing*) refere-se a um novo conceito de consumo de tecnologia através da Internet que assenta na lógica da partilha de recursos através da rede. Ou seja, o *cloud computing* consiste essencialmente em tirar partido das capacidades de armazenamento e processamento de computadores e servidores partilhados e interligados por meio da Internet para ter acesso a um conjunto variado de serviços, disponíveis a qualquer momento e em qualquer lugar, independentemente da plataforma de acesso, com a mesma facilidade de tê-los instalados nos computadores pessoais.

[19] BYOD é uma sigla inglesa para *Bring Your Own Device* (Traga o Seu Próprio Dispositivo). Este fenómeno tem uma crescente popularidade um pouco por todo o mundo e está directamente relacionado com o surgimento de um número cada vez maior de dispositivos de computação móvel bastante avançados. O BYOD implica que os funcionários possam utilizar os seus próprios dispositivos (*smartphones, tablets* ou

laptops) no ambiente laboral e com eles possam aceder aos recursos da rede da empresa.

[20] *Computer Emergency Response Teams.*

[21] Quem guardará os guardas?