OBSERVARE
Universidade Autónoma de Lisboa

ISSN: 1647-7251
Vol. 6, n.º 1 (Maio-Outubro 2015), pp. 93-107

REGULAÇÃO DO CIBERESPAÇO: CESURISTAS E TRADICIONALISTAS

Lino Santos
lino.santos@cncs.gov.pt
Mestre em Direito e Segurança pela Faculdade de Direito da Universidade Nova de Lisboa. Licenciado em Engenharia de Sistemas e Informática pela Universidade do Minho. Coordenador de Operações no Centro Nacional de Cibersegurança (Portugal)

Resumo

No fantástico *Code and Other Laws of Cyberspace*, o Professor L. Lessig afirma "que algo de fundamental mudou" com o ciberspaço, no que à capacidade do Estado em fazer cumprir a lei diz respeito.

Por um lado a estrutura e as características do ciberespaço colocam algumas dificuldades relacionadas com a competência e a escolha da lei aplicável. Por outro, levanta dúvidas sobre o próprio conceito de soberania, como o conhecemos.

Este trabalho analisa os argumentos daqueles que defendem uma regulação do ciberespaço à margem da soberania do Estado ou dentro de um novo conceito de soberania e de capacidade para fazer cumprir a lei, bem como os argumentos daqueles que rejeitam essa excepcionalidade de tratamento ao ciberespaço.

Palavras chave:

Ciberespaço; Regulação; Auto-regulação; Soberania; Utopia

Como citar este artigo

Santos, Lino (2015). "Regulação do ciberespaço: cesuristas e tradicionalistas". *JANUS.NET e-journal of International Relations*, Vol. 6, N.º 1, Maio-Outubro 2015. Consultado [online] em data da última consulta, observare.ual.pt/janus.net/pt_vol6_n1_art6

Artigo recebido em 31 de Março de 2015 e aceite para publicação em 30 de Abril de 2015

JANUS.NET, e-journal of International Relations
ISSN: 1647-7251
Vol. 6, n.º 1 (Maio-Outubro 2015), pp. 93-107
Regulação do ciberespaço: cesuristas e tradicionalistas
Lino Santos

REGULAÇÃO DO CIBERESPAÇO: CESURISTAS E TRADICIONALISTAS

Lino Santos

Introdução

É incontestável que o ciberespaço introduziu profundas alterações na forma como os cidadãos, as organizações e os Estados se relacionam entre si.

A capilaridade da internet, juntamente com a sua grande cobertura geográfica de acesso e o advento do computador pessoal, deram origem às globalizações da informação e do conhecimento, criando novos espaços de interactividade, partilha e armazenamento de e produtos de mercado, entre os quais destacamos os ambientes virtuais imersivos de lazer, cultura (mundos virtuais), o produto das interacções sociais mediadas pelas tecnologias da informação (redes sociais), ou o local onde é armazenada e processada a informação (*cloud*). Esta diversidade de espaços que representa a riqueza de aplicações do ciberespaço, está na base do seu sucesso e do rápido crescimento da sua utilização.

Este conjunto de espaços assenta no sistema de comunicações global—a internet—ao qual os sistemas de informação e os dispositivos electrónicos de uso pessoal se ligam para realizarem a sua função. Senão criada pelo menos desenvolvida originalmente com objectivos militares, a internet desenvolveu-se como rede académica no final da década de 1980 e rapidamente se assumiu como meio de comunicação de massas em meados dos anos 90. Na sua origem militar, o desenho da internet teve como principal preocupação a resiliência a falhas parciais,[1] resultando numa arquitectura física e numa gestão completamente distribuídas, sem qualquer tipo de ligação com o mapa administrativo das nações.

Cedo o ciberespaço foi idealizado como espaço de liberdade—uma espécie de novo *Far West* global onde nenhum Estado conseguiria aplicar a lei ou manter a ordem. Neste contexto, surgiram duas correntes académicas, antagónicas entre si. A primeira sugere a falência do sistema jurídico para lidar com o ciberespaço e defende a criação de novas formas de regulação, adaptadas às suas especificidades. A segunda sustenta uma inexcepcionalidade de tratamento para esse mesmo ciberespaço e defende que os

[1] Um dos requisitos colocados aos criadores da internet, então designada ARPANET, visava a tolerância a falhas na comunicação entre bases operacionais militares em cenário de destruição parcial das suas infra-estruturas. Composta por uma "teia" (*web*) de ligações entre os vários "nós", (*nodes*) a informação dentro desta rede deveria chegar sempre ao destino desde que existisse um caminho disponível para tal, desta forma reduzindo a criticidade individual de cada "nó" para o contexto global das comunicações.

desafios na sua regulação não são distintos daqueles que foram colocados por outros domínios onde se verificam transações transnacionais.

Este artigo propõe-se apresentar e discutir estas duas correntes, à luz dos desenvolvimentos ocorridos desde a sua formulação inicial, bem como verificar se existe uma tendência ou primazia na utilização de mecanismos de regulação para o ciberespaço.

Características do ciberespaço

Algumas características da arquitectura do ciberespaço colocam sérios desafios de governação deste novo media, bem como de regulação das diversas actividades nele realizadas. Desde logo o ciberespaço aumenta radicalmente a velocidade e a quantidade das comunicações, ao mesmo tempo que reduz ou elimina a distância entre instituições, entre indivíduos, ou mesmo entre nações. As mensagens de correio electrónico ou *sms* são enviadas e recebidas quase instantaneamente, fotografias, videos e artigos de opinião são partilhados e difundidos globalmente quase em tempo real, comprar um livro pela internet é hoje tão fácil e cómodo como fazê-lo numa livraria. Neste contexto, o ciberespaço e a conversão do analógico para o digital vieram aumentar brutalmente a frequência e a velocidade de alguns comportamentos ilícitos já existentes. São exemplo destes a violação de direitos autorais, que sempre existiu, mas que as tecnologias digitais facilitaram e levaram ao extremo.

Por outro lado, como já foi referido, o ciberespaço é aterritorial. Ao contrário dos domínios naturais (ar, mar, terra e espaço), onde os Estados, dentro das suas capacidades, exercem a soberania e aplicam a lei dentro de um território físico relativamente bem definido, no ciberespaço esse exercício levanta problemas de delimitação. Neste mesmo sentido, B. Posen refere-se-lhe como mais um *global common*, comparando-o ao espaço marítimo, aéreo e extra-atmosférico (Posen, 2014: 64). Assim sendo, conceitos clássicos tais como "jurisdição" ou "propriedade"—para dar aqui apenas alguns exemplos—tornam-se difusos quando aplicados ao ciberespaço. A prestação de serviços *on-line* dificilmente cumprirá o quadro legal de todos os Estados onde estes são disponibilizados,[2] criando dificuldades a cada um destes no seu exercício de soberania, começando pela própria escolha da lei aplicável—aplica-se a lei de onde é prestado o serviço, ou aquela de onde são produzidos os efeitos?

Por último, este espaço virtual garante algum grau de anonimato a quem o utiliza, o que levanta, novamente, dificuldades quanto à atribuição dos actos praticados ou à identificação dos seus autores. Um cibernauta português ou localizado em território português pode utilizar um serviço de *blogues* norte-americano para difamar outro cidadão português. Esse mesmo cibernauta pode jogar *on-line* um jogo permitido no país onde o servidor está alojado, mas proibido em Portugal. Pode, ainda, praticar remotamente uma profissão regulada em Portugal, mas não regulada no país onde o serviço é prestado.

O ciberespaço veio igualmente criar um conjunto de novos objectos de protecção jurídica, alargar a esfera de protecção de alguns já existentes, bem como facilitar o surgimento de novos tipos ilícitos. Figuras como como a de identidade digital, múltiplas

[2] J. P. Trachtman refere que a grande novidade do ciberespaço é a de que "dará lugar a mais situações nas quais os efeitos são sentidos em múltiplos territórios em simultâneo" (1998: 569).

identidades, *avatar,* dinheiro virtual ou domínio internet, bem como profissões tais como administrador de sistemas, *blogger* ou programador, ainda hoje não possuem regras que lhes confiram direitos e responsabilidades. Da mesma forma, conceitos tradicionais como o de privacidade viram alargado o seu espectro de protecção jurídica, passando a incluir, por exemplo, o direito ao esquecimento,[3] e o conjunto das acções tipificadas como ilícitas no contexto da pornografia de menores passou a incluir a posse de material desta natureza em formato digital ou a mera vizualização deste.[4] Refira-se ainda a necessidade, cedo percebida, da protecção jurídica dos próprios sistemas que informáticos que materializam o ciberespaço, tratada em regime autónomo na lei do cibercrime.

Estes e outros desafios foram avaliados, na viragem do século, por vários académicos da área do direito. As discussões de então permitem identificar duas tendências divergentes no que respeita à regulação do ciberespaço.

Uma primeira via entende algumas das características distintivas do ciberespaço como suficientes para, por um lado, justificar a inviabilidade da aplicação dos mecanismos de escolha da lei aplicável e da determinação da jurisdição legais existentes e, por outro, advogar um novo paradigma de regulação para o ciberespaço. Contribuem para esta visão, entre outros, Johnson e Post, defendendo a regulação do ciberespaço pelos cibernautas através de mecanismos de auto-regulação (1996; 2002), e Lessig que defende, por sua vez, a regulação pelo "código" e pela arquitectura do ciberespaço (1999; neste como em todos os casos que se seguem, a tradução é minha).

Do outro lado encontram-se aqueles que defendem que os desafios levantados ao direito pelo ciberespaço não são muito diferentes daqueles que foram colocados por outros desenvolvimentos tecnológicos, e que as transações realizadas com recurso a este não diferem de outras transações de características transnacionais, realizadas por outros meios. Os principais partidários desta via são Goldsmith (1998) e Trachtman (1998), que recusam a excepcionalidade do ciberespaço e defendem uma evolução dentro do quadro do direito internacional e através do reforço dos instrumentos supranacionais de regulação.

A discussão académica do tema levou J. P. Goldsmith a apelidar aqueles que, tal como D. Johnson e D. Post, acentuam o cariz extraordinário do ciberespaço e pedem um novo modelo de regulação de "cépticos da regulação" (1998, pp.1199). Por sua vez, Post trata os que advogam que os problemas colocados pelo ciberespaço à capacidade do Estado exercer e fazer cumprir a lei não são assim tão diferentes ou novos, de "inexcepcionalistas" (2002: 1365). Sem desprimor dos respectivos autores, trataremos, doravante, os primeiros como "cesuristas" e os segundos como "tradicionalistas".

---

[3] O art.º 17.º da proposta da Comissão Europeia de regulamento da Protecção de Dados Pessoais refere que "[o] titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento de dados pessoais que lhe digam respeito". Ver *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)*, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf, consultado em Setembro de 2014.

[4] Cf. alínea f) do art.º 20.º da *Convenção para a Protecção das Crianças contra Exploração Sexual*, Resolução da Assembleia da República n.º 75/2012, de 28 de Maio, onde é prevista a criminalização sempre que "[...] aceder, conscientemente, através das tecnologias de comunicação e de informação, a pornografia de menores".

Tirando partido da distância temporal em relação a esta discussão, começaremos por abordar os argumentos esgrimidos entre "cesuristas" e "tradicionalistas", para de seguida analisar as duas soluções dominantes para uma melhor regulação do ciberespaço: a auto-regulação e a abordagem supranacional complementar.

Cesurismo vs. tradicionalismo

O termo "cesurismo" — cunhado por Hermínio Martins (Garcia, 2006) — é aqui usado como referência a uma linha de pensamento que tende a tratar os fenómenos como específicos e sem precedentes, de algum modo renunciando ao tempo e à história. É precisamente esta a linha de pensamento dos que, tal como Johnson e Post, concentram sua atenção na novidade que representa o ciberespaço como justificação para a falência do actual modelo de regulação baseado na lei e para uma ruptura com o passado.

A base de argumentação dos "cesuristas" centra-se na aterritorialidade do ciberespaço e, mais concretamente, no facto de as fronteiras bem definidas serem um atributo necessário para a eficácia da aplicação da lei. A relação entre o espaço e a lei, defende Johnson, apresenta múltiplas dimensões. Por um lado, é a lei que permite a um Estado exercer soberania e controlo sobre o seu território—uma espaço bem delimitado e reconhecido por todos—, assim como ao cidadão defender-se da acção do Estado. Por outras palavras, o conceito de fronteira funciona como o limite dentro do qual o Estado faz cumprir a sua lei, bem como aquele fora do qual o cidadão está a salvo dessa acção do Estado.[5] Por outro lado, a relevância jurídica dos efeitos de uma acção - ou da ausência dela - é igual dentro de um mesmo espaço jurídico e, muito provavelmente, diferente entre espaços jurídicos distintos[6]. Por outro, ainda, a legitimidade da lei advém da participação directa ou indirecta dos cidadãos de um Estado na elaboração da lei, perdendo essa legitimidade quando aplicada de outra forma. Finalmente, a eficácia preventiva da lei resulta do conhecimento prévio da lei aplicável ao espaço onde praticamos actos relevantes ou daquela onde esses actos produzem efeitos (Johnson & Post, 1996).

Tendo em conta esta relação entre espaço e lei, os "cesuristas" defendem que a localização geográfica dentro de limites físicos conhecidos—fronteiras—, são essenciais para determinar o conjunto de direitos e responsabilidades da pessoa jurídica, concluindo que o ciberespaço "enfraquece radicalmente [esta] relação entre o fenómeno com significado legal e a localização física" (Johnson & Post, 1996: 1370). Partindo deste pressuposto, os "cesuristas" questionam a competência de um qualquer Estado para a aplicação da lei e da justiça para actos praticados no ciberespaço e levantam reservas sobre a escolha da lei aplicável. Johnson e Post idealizam o ciberespaço como *uno*[7], como um novo plano de acção ou dimensão paralela cuja

[5] É através da lei que um Estado de Direito regula as liberdades e as responsabilidades dos seus cidadãos e instituições. O aplicação eficaz dessa regulação representa um exercicio de soberania.

[6] Mais uma vez o apelo aos princípios de um Estado de Direito, onde a lei deve ser igual para todos. Obviamente esta igualdade aplica-se aos objectos jurídicos desse Estado, já que a lei pode ser diferente entre Estados.

[7] M. Libiki sugere que o ciberespaço não é um media *uno*, mas sim uma "multiplicidade de medias—no mínimo a tua, a deles e a dos outros" (2012: 326) . Também L. Strate, no seu brilhante artigo sobre concepções de ciberespaço, sugere a exeitência de uma multiplicidade de ciberespaços centrada na vivência de cada indivíduo (1999). Note-se igualmente que no quadro ideológico de um único ciberespaço, não faria sentido o conceito de "ciberespaço nacional", comummente utilizado nas várias estratégias

fronteira com o nosso mundo fisico é "feita de écrans e palavras chave" (1996: 1367) onde, uma vez lá dentro, não existem outras barreiras. Uma vez dentro deste ciberespaço, é igual comunicar com o vizinho do lado ou com alguém nos antípodas - aliás, dentro do ciberespaço não existe o conceito de antípodas - e o quadro jurídico que regula essa comunicação, ou não existe, ou é de difícil identificação.

O caso que opôs a Liga Internacional contra o Racismo e anti-Semitismo à gigante norte-americana Yahoo, ilustra bem estas dificuldades . No ano 2000, o cidadão francês Marc Knobel, um activista da luta contra o neo-nazismo, verificou que o *portal* de leilões da Yahoo, estava a vender material neo-nazi. Através da ONG referida, Knobel levou a tribunal a Yahoo - uma empresa sediada na Califórnia - por violação da lei francesa de proibição de tráfico de bens nazis. A primeira reação de um dos co-fundadores da Yahoo, Jerry Yang, foi considerar que o tribunal francês pretendia impor um julgamento numa área sobre a qual não tem controlo. Independentemente desta opinião, o julgamento prosseguiu, com a defesa a centrar a sua argumentação na impossibilidade técnica de distingir o que era apresentado aos clientes franceses da Yahoo daquilo que era apresentado aos restantes, e a acusação, por seu lado, a defender a soberania do Estado francês para se defender da venda de mercadorias nazis ilegais a partir dos Estados Unidos e a questionar o porquê de um regime de excepção para a Yahoo, e para o ciberespaço. O tribunal determinou que a Yahoo violou a lei francesa e ordenou que esta empresa tomasse todas as medidas necessárias para dissuadir e tornar impossível o acesso, por parte de cidadãos franceses, a tais conteúdos. A alegação da Yahoo a respeito da impossibilidade técnica de cumprir a ordem do tribunal, baseada nas idiossincrasias da arquitectura da internet, foi ultrapassada depois de vários *gurus* da internet, entre os quais Vint Cerf, terem apontado soluções técnicas que permitem à Yahoo cumprir a ordem do tribunal (Goldsmith & Wu, 2006: 1-10).

Na linha de argumentação de Johnson e Post relativamente à excepcionalidade do ciberespaço, a autoridade apenas pode ser exercida dentro de um território, questionando estes autores a legitimidade de uma nação regular actividades exercidas noutro território. Também argumentam que as disputas internacionais pela escolha de um quadro jurídico se resolvem pela escolha do quadro do local onde os actos ilícitos são praticados. Estes pressupostos garantem a uniformidade, a previsibilidade e a certeza na aplicação das leis, valores de um Estado de Direito. Porém, o caso acima descrito vem apontar no sentido contrário e dar razão aos "tradicionalistas".

Os "tradicionalistas", cujo mote poderia ser "nada de novo debaixo do sol"[8], defendem, por oposição aos "cesuristas", que o ciberespaço não constitui uma excepção. Para os "tradicionalistas",

> *"[a]s transações no ciberespaço não são diferentes das transações transnacionais ocorridas no espaço real. [...] Elas envolvem*

nacionais de cibersegurança. Ver *The National Strategy to Secure Cyberspace* (2003), disponível em https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, consultado em Setembro de 2014; *ou Italy's National Strategic Framework for Cyberspace Security* (2014), disponível em http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf, consultado em Setembro de 2014.

[8] Eclesiastes 1:9 "O que foi, isso é o que há de ser; e o que se fez, isso se fará; de modo que nada há de novo debaixo do sol."

> *pessoas no espaço real inseridas numa jurisdição, a comunicar com outras pessoas também no espaço real noutras jurisdições"* (Goldsmith, 1998: 1250).

Para J. P. Trachtman o ciberespaço é o meio. A conduta persiste num território, os seus autores encontram-se num território, e o mais importante é que os efeitos - embora mais dispersos do que no passado - continuam também a ser produzidos num território (1998: 568)[9]. Como consequência, o conjunto de princípios e os instrumentos legais tradicionais são capazes de resolver os problemas da escolha da lei e da competência jurisdicional.

A ideia de que o ciberespaço nada traz de novo é sustentada por Goldsmith recorrendo à analogia com outros contextos de comunicação e transação transnacionais. O autor aceita que o mundo esteja a mudar e que o ciberespaço é uma expressão dessa mudança, mas refere que o direito internacional tem evoluído no sentido de responder a estas alterações, nomeadamente "é commumente aceite que [na ausência de soluções consensuais internacionais] uma nação regule, extraterritorialmente, os efeitos locais de uma conduta" (Goldsmith, 1998: 1212) e aponta como exemplo o tema da propriedade industrial.

A outra ideia chave dos "cesuristas" - em género de conclusão - é a de que as dificuldades legais atrás referidas, conjugadas com dificuldades técnicas colocadas pelas características do ciberespaço, tornam impossível a regulação deste por parte dos Estados. Para Johnson e Post o ciberespaço "cria um fenómeno totalmente novo que precisa de ser objecto de regras jurídicas claras, mas que não pode ser regulado, de forma satisfatória, por uma qualquer soberania assente no conceito de território". (1996: 1375) Desta impossibilidade técnica e legal para os Estados exercerem a sua soberania sobre o ciberespaço, emergirão, numa primeira fase, mecanismos de auto-regulação (1996: 1387).

Os "tradicionalistas", por seu turno, defendem que a tecnologia existe e que, como ficou patente no caso que envolveu a Yahoo, mas também nos diversos casos que envolvem a filtragem de conteúdos realizada, pelas mais diversas razões, os Estados conseguem exercer a sua soberania e proteger os cidadãos contra conteúdos ofensivos ou actividades ilícitas (Goldsmith & Wu, 2006: viii). A informação envolvida numa transacção "aparece num território, não por magia, mas por uma acção de hardware e software localizado dentro desse território" (Goldsmith, 1998: 1216) pelo que actuando junto desse hardware e software é possível realizar a função de regulação.

A auto-regulação do Ciberespaço

Esta dualidade de pontos de vista relativamente a um assunto novo que ainda não é percebido na sua plenitude é recorrente. Ao longo da história, o surgimento de novas tecnologias tem originado tomadas de posição que defendem a sua excepcionalidade e o seu futuro papel numa ruptura com o passado e na criação de um mundo melhor - instrumentos da paz universal -, bem como opiniões mais conservadoras que logo

[9] Trachtman rejeita a visão dos "cesuristas" sobre a diminuição de soberania dos Estados provocada pelo ciberespaço: "Não foi o Estado que morreu, mas a velha e moribunda teoria da soberania absoluta sobre o território" (1998: 562).

identificam afinidades com outros episódios ocorridos. Armand Mattelart (2000), na sua *História da Utopia Planetária,* elenca um conjunto de exemplos históricos onde, ao surgimento de uma nova tecnologia, foi criada uma esperança libertadora: a imprensa escrita, o telégrafo, os caminhos de ferro ou a televisão.

Como já foi referido, os "cesuristas" estão convencidos de que o ciberespaço é uma destas tecnologias libertadoras. Uma tecnologia suficientemente diferente do mundo real para que a regulação do comportamento humano nesse espaço não possa ser feita através dos mecanismos existentes[10]. Lessig advoga que "algo de fundamental mudou" (1999: 126), para sustentar a sua tese de que no ciberespaço "o código é a lei"; enquanto Johnson e Post defendem que o ciberespaço é dos cibernautas e portanto "aqueles que definiram e usam os sistemas *on-line* têm o interesse em prevenir a segurança do seu território electrónico e de prevenir o crime" (1996: 1383), dando o mote para auto-regulação do ciberespaço.

A ideia de que o ciberespaço dilui o conceito de soberania de Estado, mas também de que os probelmas no ciberespaço devem ser deixados para os cibernautas, encaixa perfeitamente no perfil de "internet-centrismo", como idealizado por E. Morozov (2012). A crença no efeito libertador da internet, mas principalmente a ideia de que tudo se resume, tudo pode ser explicado, ou pode ser feito por via da internet, permite compreender porque razão Johnson e os seus correlegionários defendem regras à parte para o ciberespaço.[11] As teses dos "cesuristas" inserem-se claramente num contexto de euforia da internet e não anteviram nem as alterações societais desencadeadas com as redes sociais na última década, nem a concentração de poder nas mega empresas do sector. Inserem-se no espírito e na ideologia dos primórdios da internet e na vontade dos seus utilizadores de a manter livre de regulação e da intervenção dos Estados ou de manter viva a ideia de que o cibespaço "possa realizar a sua promessa de profunda alavancagem liberatória" (Post, 2000: 1439), vontade essa expressa por grupos como o *Electronic Frontier Foundation*, e por manifestos como a *Declaração de uma Internet Independente,* de John Bralow (1996).

Dentro deste espírito, Johson e Post apontam alguns exemplos práticos de auto-regulação. Este autores sugerem que o sistema de DNS—sistema global de atribuição e gestão nomes internet, coordenado por uma organização internacional sem fins lucrativo, designada de ICANN,[12] estaria a ser redesenhado, num processo de auto-regulação, para acondicionar um conjunto de salvaguardas exigidas pela "propriedade industrial" (1996: 1388). Passados quase vinte anos, podemos avaliar como decorreu este processo. Pese embora a gestão do DNS continue nas mãos do cibernautas, praticamente todos os países europeus liberalizaram as regras de registo de domínios internet, colocando uma maior pressão sobre a gestão dos direitos de propriedade industrial e criando fenómenos como o *cybersquating* — especulação financeira com os nomes internet mais apetecíveis. Existe efectivamente um regime de auto-regulação neste domínio, segundo um modelo de melhores práticas internacionais. No entanto,

[10] Lessig sustenta que a regulação do comportamento humano é realizado pela convergência de quatro forças—quatro reguladores: a lei, o mercado, as normas sociais e, no tocante ao ciberespaço, a arquitectura (1999).

[11] "Os internet-centricos gostam de responder a qualquer questão sobre mudanças democráticas, reformulando-as, antes de mais, em termos da internet, em vez do contexto em que estas ocorrem" (Morozov, 2012: xvi). Um dos alvos favoritos de Morozov é o norte-americano Clay Shirky, (2009), que Morozov qualifica de ciberutópico.

[12] *Internet Corporation for Assigned Names and Numbers*. Ver https://www.icann.org, consultado em Setembro de 2014.

essa auto-regulação revela-se insuficiente e é recorrente o recurso à legislação da propriedade industrial para dirimir conflitos. Note-se, no entanto, que, como sugerido por Johnson, alguns países criarm tribunais arbitrais especializados[13], com o saber-como necessário para tratar as particularidades cibernéticas neste domíno (1996: 1387).

Outro exemplo de auto-regulação como forma de resolução para problema concretos do ciberespaço é-nos exposto por Post relativamente ao crescimento do número de mensagens de correio electrónico não solicitadas, vulgarmente conhecidas como *spam*. Post apresenta-nos como um bom exemplo de auto-regulação ou de como a rede irá funcionar no futuro, uma das várias iniciativas para criação de uma base de dados centralizada de reputação de endereços de correio electrónico ou de servidores de correio electrónico (*Realtime Blackhole List*), alimentada remotamente por voluntários - activistas nas suas palavras (2000: 1440). Este conjunto de voluntários estabelece, em comunidade, um conjunto de regras, às quais todos os participantes no ciberespaço aderem. É, de facto, uma visão linda, mas que a história não confirmou. Desde logo, não surgiu uma, mas várias iniciativas semelhantes que criaram um problema de escolha aos administradores de serviços de correio electrónico. Depois, o regime de voluntariado passou a ser um constrangimento para a qualidade do serviço, pelo que assistimos à mercantilização de alguns destes serviços - o modelo vigente[14]. Por outro lado, nasceram outras formas de solucionar o problema do *spam*. O mercado viu a oportunidade e os gigantes da *cloud*, como a AOL a *Microsoft* e a *google* criaram o *Sender Policy Framework,* o *SenderID* ou, ainda, o *DKIM* - para referir apenas os mais conhecidos -, não existindo, ainda hoje, o "consenso colectivo" preconizado por Post (2000: 1456). Em suma, no que ao tratamento do *spam* diz respeito, podemos afirmar que sofremos de "demasiada" auto-regulação.

Numa outra prespectiva do significado de auto-regulação, a tese de Lessig sobre o papel do código na regulação do ciberespaço é ambivalente. Por um lado sustenta uma ideia de que a produção das normas que regulam o ciberespaço reside nos seus arquitectos e programadores e não no Estado. Neste cenário, o poder regulatório encontra-se tanto nas mãos da indústria de telecomunicações, de media e de aplicações para a internet, que através dos seus produtos regem e enformam as condutas no ciberespaço. Mantendo intocáveis os princípios da neutralidade da rede e o não dever de vigilância sobre os conteúdos transitados ou armazenados nas suas infraestruturas, os gigantes dos media digital têm vindo a introduzir, nas suas aplicações, mecanismos de denúncia com vista à remoção de conteúdos ofensivos ou, ainda, mecanismos de reputação para avaliação de risco em transações comerciais entre desconhecidos. Por outro lado a produção de norma também reside nas mãos do cidadão comum, que pode criar uma nova aplicação e, por essa via, produzir norma. Em ambos os casos esta forma de produção de norma pode ser conflituante com outros poderes normativos. Bons exemplos desta auto-regulação são: o *Skype*, um sistema global de comunicações de voz criado por dois jovens nórdicos à margem do quadro regulatório das telecomunicações e em violação de disposições processuais penais, em várias jurisdições, como o regime de intercepção telefónica; ou o *Pretty Good Privacy*,

[13] No caso português, as regras para registo de nomes internet inclui a possibilidade de recurso para um tribunal arbitral especializado. Ver .PT Domain Registration Rules, Chapter VI, disponível em http://www.dns.pt/en/domains-2/domain-rules/chapter-vi/, consultado em março de 2015.

[14] O modelo de negócio de muitas destas RBL passa pela cobrança de uma taxa pela remoção de entradas da lista.

uma plataforma de cifra, desenvolvida por Phil Zimmermann, que violou, entre outras, as leis norte-americanas de exportação algoritmos de cifra. Por outro lado, a tese de Lessig, define o código como o meio para, de uma forma mais eficaz, fazer-se cumprir a lei:

> *"o código substitui a lei através da codificação das regras, tornando-as mais eficazes do que estas eram enquanto meras leis"* (Lessig, 1999: 206).

Ou seja, o Estado pode tirar proveito do código no seu exercício de soberania. Da mesma forma que as empresas codificaram os seus processos de negócio, diminuindo a arbitrariedade e o erro do colaborador, os Estados começam a codificar parte das suas funções - nomeadamente aquelas onde é necessária a interação com o cidadão - com ganhos de eficácia. Um exemplo disto é o actual modelo de colecta de impostos em Portugal, onde a codificação do comportamento dos comerciantes para a emissão de facturas e a codificação do comportamento dos contribuinte para o preenchimento da sua declaração de impostos - o termo "declaração" começa a não fazer sentido - são a própria da lei.

Em sentido contrário à auto-regulação, a arquitectura do ciberespaço veio, igualmente, criar um conjunto de oportunidades para o controlo e a vigilância da sociedade. Os Estados de regime autoritário foram os primeiros a perceber esta possibilidade[15], mas rapidamente a vigilância passiva, a recolha indiscriminada de metadados e o conceito de *big data* no suporte às funções de soberania criaram adeptos um pouco por todo o mundo. Os Estados já perceberam que para um melhor controlo do ciberespaço - o seu e o dos outros, na acepção de M. C. Libiki (2012) - as grandes empresas da indústria da internet podem desempenhar um papel fundamental, seja na arquitectura da topologia dos fluxos de informação, seja no desenho das próprias funcionalidades do serviço. É geopoliticamente relevante, para dar apenas um exemplo, a localização física do motor de busca planetário *google*. Este interesse estratégico adensa-se quando passamos a falar de armazenamento de informação. Por exemplo na disputa entre a *google* e o governo da República Popular da China, em 2010, a última via a primeira como uma componente do poder norte-americano (Klimburg, 2011: 52).

Soberania desagregada

Atentos aos limites do processo de auto-regulação do ciberespaço, vários autores sugerem complementar os mecanismos tradicionais de regulação com uma abordagem supranacional para os problemas mais complexos. Numa perspectiva mais tradicionalista - aquela que não advoga um regime de excepção para o ciberespaço - é comummente aceite uma partilha de poder com outras instituições para melhor responder aos vários desafios de governação global, e não apenas aqueles colocados pelo ciberespaço. Os exemplos mais conhecidos desta forma governação em rede são

[15] Talvez o caso mais evidente deste controlo seja o aparato tecnológico designado de *Great Firewall of China*, uma infra-estrutura tecnológica, alegadamente capaz de monitorizar e de bloquear selectivamente comunicações e conteúdos dentro do ciberespaço chinês e entre este e o resto do mundo, numa espécie de "lápis azul" virtual e em tempo real.

as várias instituições da Organização das Nações Unidas, tais como a Organização Mundial de Saúde ou Organização Mundial do Comércio.

Estas estruturas de resposta aos problemas contemporâneos de governação transnacional têm vindo a ser teorizadas, entre outros, por W. H. Reinicke, que as designou de "redes globais de política pública" (1999) ou por A.-M. Slaughter, que lhes chamou "soberania desagregada" (2009). Os objectivos destas redes entram dentro do conceito de *soft-power* e determinam uma transposição do conceito de soberania centrado na administração do território para uma combinação entre poderes fixados nos Estados e mecanismos supranacionais e descentralizados de articulação entre estes. Estes mecanismos assentam em estruturas que juntam as partes interessadas - *stakeholders* - quer do governo, quer da economia, quer ainda da sociedade civil, para tirar proveito das vantagens das redes na gestão de conhecimento, para partilhar informação e ideias e para coordenar políticas entre si, sem o cunho formal negociado de um tratado" (Mueller, 2010: 40). Estas formas de governo são coincidentes com o conceito de abordagem *multi-stakeholder* preconizada por exemplo no *Internet Governance Forum*, ou nos vários grupos de trabalho da União Europeia.

Os partidários desta abordagem não a consideram uma perda de soberania para os Estados, mas antes uma inevitabilidade para a resolução de problemas globais. Como refere Slaughter,

> *"[p]or mais paradoxal que possa parecer, a medida da capacidade de um Estado actuar como uma unidade independente dentro do sistema internacional—a condição e objectivo de soberania - depende da largura e da profundidade das suas ligações a outros Estados"* (2009: 268).

Os problemas de regulação do ciberespaço não fogem a esta regra. Como refere J. S. Nye Jr. (2010: 3),

> *"o ciberespaço não irá substituir o espaço físico geográfico e não acabará com a soberania dos Estados, mas a difusão de poder no ciberespaço coexistirá e complicará, em grande medida, o que signica exercício de poder neste domínios."*

Neste sentido vários autores defendem uma solução global para um problema global. H. H. Perritt Jr. sugere que

> *"ter em conta o pontencial do [ciberespaço] requer uma evolução das instituições internacionais públicas e privadas de forma a que as regras de atribuição de responsabilidade possam se fazer cumprir com eficácia, mesmo em relação às condutas que não possam ser localizadas territorialmente num Estado em particular"* (1996: 113).

Também Trachtman insiste que "vale a pena idealizar uma solução institucional mais forte" (1998: 569) para a regulação do ciberespaço.

Um das áreas onde esta soberania desagregada tem vindo a produzir efeitos é a do combate ao cibercrime. Muito cedo se percebeu a necessidade de uma abordagem transnacional aos desafios colocados pelo crime nas redes de computadores. Em 1990 a Assembleia Geral das Nações Unidas adoptou uma primeira resolução onde se identifica como necessário o desenvolvimento de formas e instrumentos de cooperação internacional para o combate ao cibercrime[16]. Ainda no quadro da Nações Unidas, e do 11.º congresso sobre prevenção e justiça criminal, realizado em 2005, resultou uma declaração onde foi expressa a necessidade de harmonização legislativa no combate ao cibercrime[17]. A concretização desse objectivo surge em 2004, da reunião dos Ministros da Administração Interna do G8, realizada em Washington, da qual resulta um plano de acção para o combate ao crime *high-tech* onde se destaca o incentivo à adopção, por parte de todos os países, da Convenção para o Cibercrime, do Conselho da Europa, de 2001[18]. Esta Convenção é muitas vezes referida como o primeiro documento de trabalho internacional resultado de uma reflexão profunda sobre o tema (Verdelho *et al.*, 2003). Um dos seus principais objectivos é a harmonização das várias legislações nacionais relativamente a crimes cometidos contra redes de computadores ou crimes de conteúdo nas redes de computadores. Para além do direito penal material, a Convenção visa, igualmente, uma cooperação transnacional mais eficaz, para o que contribui com um conjunto de institutos de direito processual penal e com a criação de instrumentos de cooperação judiciária transnacional.

Ainda no quadro das Nações Unidas, foram feitas algumas tentativas, sem sucesso, para celebrar um acordo com vista à limitação do uso de ciberarmas por parte de um Estado. Por desconfiança na eficácia de tal acordo — nomeadamente quanto à possibilidade de verificação —, ou porque simplesmente não existe vantagem estratégica para si, este acordo tem sido rejeitado sistematicamente pelos Estados Unidos (Clark & Knake, 2010: 219-225).

No mesmo sentido e como resposta a uma crescente centralidade do ciberespaço na actividade terrorista - seja como instrumento, seja como potencial alvo -, a União Europeia prepara-se para aprovar medidas tendentes a um maior controlo e vigilância da actividade *jihadista* na internet. De entre estas, destacam-se a criação de uma unidade especial, dentro da Europol, para monitorização da internet e o reforço da

[16] Resolução A/RES/45/121, *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, disponível em http://www.un.org/documents/ga/res/45/a45r121.htm, consultado em Maio de 2014. Dessa resolução resultou um manual sobre prevenção e controlo de crimes relacionados com computadores. Ver *United Nations Manual on the Prevention of Computer-related Crime*, disponível em http://www.uncjin.org/Documents/irpc4344.pdf, consultado em Maio de 2014. Em 2000, a mesma Assembleia Geral adoptou uma nova resolução em matéria de combate à utilização criminosa de tecnologias da informação, onde se reforça a necessidade de os Estados membros assegurarem que os seus regimes legais não criem zonas francas para o exercício de actividades criminosas desta natureza e apela a uma maior cooperação na investigação criminal e judiciária transnacional. Ver Resolução A/RES/55/63, *Combating the criminal misuse of information technologies*, disponível em http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf, consultado em Maio de 2014.

[17] Ver *Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice*, "Declaração de Bangkok", disponível em http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf, consultado em Maio de 2009.

[18] Texto integral em http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, consultado em Maio de 2009. Para um sumário da génese e objectivos da Convenção sobre o Cibercrime, ver http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm, consultado em Maio de 2014.

cooperação público-privada com os principais gigantes de *social media*, como o *Facebook* ou o *Twitter*, para a eficácia dessa monitorização[19].

Outro exemplo de soberania desagregada para uma melhor regulação do ciberespaço surgirá com a nova directiva da União Europeia para a segurança das redes e da informação que, previsivelmente, será aprovada ainda em 2015. Na proposta de directiva[20] é prevista a criação de *fora* para a partilha de informação e de boas práticas, para a articulação na resposta a incidentes de cibersegurança, bem como para a articulação entre autoridades nacionais de cibersegurança, numa abordagem *multi-stakeholder*.

Conclusões

Repetidamente, o surgimento de cada nova tecnologia tem originado tomadas de posição que defendem a sua excepcionalidade e a ruptura com o passado. Como sugere Trachtman,

> *"talvez porque a tecnologia seja tão exuberante, existe uma tendência para defender que as alterações que observamos nos conceitos de soberania, Estado, jurisdição e lei, sejam todas causadas pelo ciberespaço"* (1998: 561).

O mesmo já havia acontecido quando surgiu o telefone ou o telégrafo ou ainda a rádio.

Grande parte das dificuldades sentidas na regulação e na aplicação da lei no ciberespaço devem-se a alterações profundas na sociedade - catalizadas por este mesmo ciberespaço -, tais como o adensar da globalização e o consequente aumento das transacções transnacionais ou a velocidade do desenvolvimento tecnológico. Por outro lado, o ciberespaço apresenta características distintas e ambivalentes que vieram colocar grandes desafios aos Estados para a sua regulação, mas também oportunidades para uma maior vigilância da sociedade. Não se trata, pois, de um problema de excepcionalidade, mas antes de uma gestão de oportunidade - libertária, económica, política - para os vários vários actores envolvidos.

Passados quase vinte anos sobre o trabalho de Johnson e Post, *Law and borders: The rise of law in cyberspace*, ainda não é absolutamente claro o caminho definido para a sua regulação. Dependendo dos interesses de cada Estado (económicos ou securitários), temos situações onde prevalence uma maior auto-regulação (interesse económico) e outros onde se identifica uma crescente vigilância e controlo da sociedade (interesse securitário), resultando numa fragmentação do ciberespaço em ciberespaços.

---

[19] Ver *EU proposes terror unit to tackle online jihadis*, Financial Times, 11 de Março de 2015, disponível em http://www.ft.com/intl/cms/s/0/4d93b7f0-c804-11e4-9226-00144feab7de.html, consultado em Março de 2015.

[20] Ver *COM(2013) 48 final, Proposta de Directiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:PT:PDF, consultado em Setembro de 2014.

Podemos afirmar igualmente que, face a estas duas tendências o ciberutopianismo não passa disso mesmo - de uma utopia.

> *"É fácil demais argumentar que que a regulação do ciberespaço pertence à sociedade do ciberespaço."* (Trachtman, 1998: 568)

As duas abordagens aqui tratadas - a auto-regulação e a soberania desagregada - coexistem e muito provavelmente continuarão a coexistir. Como vem expresso na Estratégia de Cibersegurança holandesa, de 2011, no capítulo de princípios orientadores: "auto-regulação se possível, legislação e regulação se necessário"[21].

Por último e considerando as dificuldades aqui enunciadas de um Estado, *de per si*, realizar, quando necessária, esta regulação, observamos o surgimento das redes transnacionais de governação, e o reforço do papel destas na agenda política. O conceito de soberania absoluta centrado na administração do território encontra-se em diluição e os problemas globais são tratados nestas estruturas transnacionais. É necessária uma abordagem global para problemas globais.

Referências bibliográficas

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Disponível em https://projects.eff.org/~barlow/Declaration-Final.html, consultado em Setembro de 2014.

Clark, R. A. & Knake R. K. (2010). *Cyberwar – The next threat to national security and what to do about it.* New York: HarperCollins

Garcia, J. L. (2006). Introdução: Razão, tempo e tecnologia em Hermínio Martins. In M. V. Cabral, J. L. Garcia, & H. M. Jerónimo (Eds.), *Razão, tempo e tecnologia: estudos em homenagem a Hermínio Martins* (pp. 13– 47). Lisboa: Imprensa de Ciências Sociais.

Goldsmith, J. L. (1998). Against cyberanarchy. *The University of Chicago Law Review*, 65(4), 1199–1250.

Goldsmith, J. L. & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*. New York: Oxford University Press.

Johnson, D. R. & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48, 1367–1402.

Klimburg, A. (2011). Mobilising cyber power. *Survival*, 53(1), 41–60.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic books.

Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *I/S: A Journal of Law and Policy for the Information Society*, 8, 321–336.

Mattelart, A. (2000). *História da Utopia Planetária*. Bizâncio.

[21] Ver *The National Cyber Security Strategy (NCSS)*, disponível em https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011, consultado em Setembro de 2014.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. New York: PublicAffairs.

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. Mit Press.

Nye Jr, J. S. (2010). *Cyber power*. Technical report, Belfer Center for Science and International Affairs, Harvard Kennedy School.

Perritt Jr, H. H. (1996). Jurisdiction in cyberspace. *Villanova Law Review*, 41(1), 1–128.

Posen, B. R. (2014), *Restraint: A New Foundation for US Grand Strategy*. London: Cornell University Press.

Post, D. G. (2000). What Larry doesn't get: Code, law, and liberty in cy- berspace. *Stanford Law Review*, 52, 1439–1459.

Post, D. G. (2002). Against'against cyberanarchy'. *Berkeley Technology Law Journal*, 17, 1365–1387.

Reinicke, W. H. (1999). The other world wide web: global public policy networks. *Foreign Policy*, 117, 44–57.

Slaughter, A.-M. (2009). *A new world order*. New Jersey: Princeton University Press.

Shirky, Clay (2009), *Here Comes Everybody. The power of organizing without organisations*, Penguin Books.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, 63(3), 382–412.

Trachtman, J. P. (1998). Cyberspace, sovereignty, jurisdiction, and moder- nism. *Indiana Journal of Global Legal Studies*, 5(2), 561–581.

Verdelho, P., Bravo, R., & Lopes Rocha, M. (2003). *As Leis do Cibercrime*, volume I. Lisboa: Centro Atlântico.