

by **CLJIC**

CYBERLAW

by CIJIC

EDIÇÃO N.º III – FEVEREIRO DE 2017

**REVISTA CIENTÍFICA SOBRE CYBERLAW DO
CENTRO DE INVESTIGAÇÃO JURÍDICA DO
CIBERESPAÇO – CIJIC – DA FACULDADE DE
DIREITO DA UNIVERSIDADE DE LISBOA**





EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e GONÇALO SOUSA

DESIGN & GRAFISMO: ISABEL BAPTISTA e ANTÓNIO OLIVEIRA

DIRECTOR DO CIJIC: EDUARDO VERA-CRUZ PINTO

COMISSÃO CIENTIFICA:

- ALFONSO GALAN MUÑOZ
- ANTÓNIO R. MOREIRA
- DANIEL FREIRE E ALMEIDA
- ELLEN WESSELINGH
- FRANCISCO MUÑOZ CONDE
- MANUEL DAVID MASSENO
- MARCO ANTÓNIO MARQUES DA SILVA
- MARCOS WACHOWICZ
- ÓSCAR R. PUCCINELLI
- RAQUEL A. BRÍZIDA CASTRO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729



NOTAS DO EDITOR:

O presente número assume a responsabilidade de compilar a iniciativa de Novembro passado, no âmbito da I CONFERÊNCIA INTERNACIONAL DE LISBOA SOBRE SEGURANÇA DA INFORMAÇÃO E DIREITO CONSTITUCIONAL DO CIBERESPAÇO. A iniciativa foi do Centro de Investigação de Direito Público do Instituto de Ciências Jurídico-políticas (CIDP-ICJP), da Faculdade de Direito da Universidade de Lisboa (FDUL), em parceria com o Centro de Investigação Jurídica do Ciberespaço (CIJIC), da FDUL, e contou com o apoio do Instituto de Direito Brasileiro (IDB), da FDUL; da AFCEA Portugal; e, do Centro Nacional de Cibersegurança (CNCS). Ao longo de dois dias, a Conferência reuniu especialistas, técnicos, académicos, alunos e demais sociedade civil, num esforço de discussão, assinalável e sempre necessário, subordinado às novas tecnologias e às impactantes alterações que estas vão revelando na sociedade.

A Conferência começou, a 17 de Novembro, com uma comunicação do Contra-Almirante GAMEIRO MARQUES, Diretor-Geral do Gabinete Nacional de Segurança. Seguimos com o painel internacional, onde PETR JIRASEK (Executive Committee Member – Cyber Security & IT Advisor/ AFCEA), Alfonso GALAN MUÑOZ (Professor de Direito Penal/Universidade de Pablo de Olavide, Sevilha, Espanha), IOANNIS IGLEZAKIS (Professor of Law and Informatics/ Faculty of Law at the Aristotle University, Thessaloniki, Grécia) e PAULO Neves EMPADINHAS (Head of Administration/ENISA), trouxeram visões e saberes distintos à abordagem do tema “*Constituição, Estado e Ciberespaço: “Contradictio in Terminis”?*”.

O painel seguinte partiu do tema: “*Estado de Direito Democrático, Informações e Segurança do Estado no Ciberespaço*”. Com os contributos de CASIMIRO MORGADO (SIRP- Sistema de Informações da República Portuguesa), RUI Carlos PEREIRA (Professor ISCSP), José Carlos LOURENÇO MARTINS (Academia Militar), Nuno LEMOS PIRES (Academia Militar), foi-nos aduzida uma prolixa perspectiva quanto às diárias tensões estabelecidas entre o exercício e defesa dos direitos fundamentais, por um lado, e a segurança do Estado, por outro, numa vertente onde a operacionalidade se apresentou como mais-valia considerável.

Ainda no dia 17 de Novembro, pela tarde, contamos com mais duas sessões. Iniciando com “*Constituição Digital e um novo “Bill of Rights” para a Internet*”, RAQUEL Alexandra BRÍZIDA CASTRO (Professora Auxiliar FDUL/ Investigadora Principal/CIDP; CIJIC), ALEXANDRE SOUSA PINHEIRO (Professor Auxiliar/FDUL; Investigador Principal/CIDP; CIJIC), CATARINA SARMENTO E CASTRO (Juíza Conselheira/Tribunal Constitucional), MARIANA MELO EGÍDIO (Assistente Convidada/FDUL; Investigadora Associada/CIDP), presentearam-nos com uma perspectiva garantística, onde a discussão gravitou em torno da necessidade de uma Constituição *digital*, cardápio de direitos e deveres fundamentais, para um cidadão cada vez mais virtualizado, global, do mundo.

O dia encerrou com a sessão: “*Intrusividade Tecnológica e Segurança da Informação no Ciberespaço*”. Com ARNAUT MOREIRA (Major-General), CARLOS CALEIRO (Departamento Matemática/ IST), SOFIA VASCONCELOS CASIMIRO (CIJIC), e GONÇALO BAPTISTA de SOUSA (GNS), a demonstração com relativa *facilidade* da concretização de um dado *ciberataque*, teve o condão de catapultar a perspectiva da segurança da informação (e da ulterior continuidade das organizações) para um nível onde o factor humano e a sua imperiosa cibereducação se demonstram fundamentais.

Acelerados pelas discussões do dia anterior, no último dia do evento, a 18 de Novembro, despertamos para o exercício de todas (as discussões prévias) numa *internet* regulada por modelos jurídicos de *governance* propensos a impasses regulatórios sugestivos. “*Os Dilemas Regulatórios da “Internet Governance”*” abriram as hostilidades. PEDRO VEIGA (Coordenador/CNCiber; Professor Catedrático /FCUL), MANUEL S. PEREIRA (ISCTE-IUL), e, ANA Cristina AMOROSO DAS NEVES (Diretora/ Departamento da Sociedade da Informação da Fundação para a Ciência e

Tecnologia), elevaram as perplexidades. Afinal, quem determina o quê, o exercício das nossas liberdades, numa *internet* tida por livre, aberta, sem constrangimentos?

Seguidamente, Luís LIMA PINHEIRO (Professor Catedrático/FDUL), MANUEL DAVID MASSENO (Professor Adjunto/Instituto Politécnico de Beja), e, CLAUDIO LUCENA (Research Centre for The Future of Law/Católica Global School of Law/Investigador FCT/Paraíba State University), concretizaram parte das respostas procuradas (e muitas outras ficaram para futuro) em: “*Os Impactos Jurídicos dos Modelos da “Internet Governance”*”.

A conferência encerrou com os contributos de Sua Excelência, o Secretário de Estado da Presidência do Conselho de Ministros, MIGUEL PRATA ROQUE (Professor Doutor FDUL) e FILIPA CALVÃO (Presidente CNPD – Comissão Nacional de Proteção de Dados; Professora Doutora UCatolica), onde o ideal da defesa e promoção da dignidade humana, também no digital, apaziguou os espíritos mais preocupados com o descerrar imparável da tecnologia disruptiva que nos domina.

O objectivo da Conferência, pressuposto numa aproximação estreita a aspectos de natureza tecnológica e operacional, atentos os novos desafios que o ciberespaço coloca ao Direito, visava um aprofundamento e desenvolvimento multidisciplinar, crucial para o sucesso dos propósitos do Projeto de Investigação que a equipa de investigação do CIDP-ICJP e CIJIC têm vindo a desenvolver. Cumprido o desígnio, exigente nos objectivos alinhavados, é com efeito, onde o destaque vai, de forma assinalável, para o contributo de muitos dos seus oradores-participantes (conquanto os artigos *omissos* ou já foram publicados aqui, ou, sê-lo-ão no futuro), que revelamos a edição de Fevereiro de 2017 da Cyberlaw by CIJIC.

Finalmente, noutro contexto, na prossecução da cientificidade e edições futuras da Revista que temos a honra de editar, sublinhando a efeméride, cumpre-nos, ainda, publicar o primeiro artigo escrutinado ao abrigo do *double peer-review* do Regulamento da Cyberlaw by CIJIC.

Cyberlaw by CIJIC, *Direito: a pensar tecnologicamente*. Boas leituras.

Lisboa, Fevereiro de 2017

Nuno Teixeira Castro

INDÍCE:

- «O PAPEL DO DIRIGENTE NO INCREMENTO DA RESILIÊNCIA DIGITAL DAS ORGANIZAÇÕES»

- **GAMEIRO MARQUES** _____Página 10

- «NON-IT PERSPECTIVES OF CYBER SECURITY BY AN IT PROFESSIONAL: CHALLENGES AND FUTURE TRENDS»

- **PETR JIRÁSEK** _____Página 18

- «LOS NUEVOS INSTRUMENTOS DE PREVENCIÓN Y LUCHA CONTRA EL NUEVO TERRORISMO: MALAS NOTICIAS PARA LOS DERECHOS FUNDAMENTALES DE LOS CIUDADANOS»

- **ALFONSO GALÁN MUÑOZ** _____Página 29

- «THE RIGHT TO BE FORGOTTEN: A NEW DIGITAL RIGHT FOR CYBERSPACE»

- **IOANNIS IGLEZAKIS** _____Página 67

- «AS PLATAFORMAS CIBERNÉTICAS PARA A EXPONENCIAÇÃO DO TERRORISMO TRANSNACIONAL»

- **NUNO LEMOS PIRES** _____Página 80

- «PODERES E ACTORES NO CIBERESPAÇO»

- **ARNAUT MOREIRA** _____Página 93

- «CIBERESPAÇO – ESPAÇO ESTRATÉGICO DE CONFLITO»

- **GONÇALO SOUSA** _____Página 108

- «A EXPERIÊNCIA DE ACOMPANHAMENTO DA ICANN»
- **PEDRO VEIGA**_____Página 116

- «ICANN, O “NOVO DEUS” NA INTERNET»
- **MANUEL SILVA PEREIRA**_____Página 121

- «CONTRIBUTOS PARA O DEBATE SOBRE A "GOVERNAÇÃO DA INTERNET"»
- **ANA CRISTINA NEVES**_____Página 136

- «ALGUMAS REFLEXÕES SOBRE A GOVERNAÇÃO E A REGULAÇÃO
DA INTERNET»
- **LUÍS DE LIMA PINHEIRO**_____Página 146

- Artigo peer review: «O PARTILHADOR ENQUANTO “HOMO RECIPROCANS”:
MOTIVAÇÕES E JUSTIFICAÇÕES DOS UTILIZADORES PORTUGUESES E
BRASILEIROS DE INTERNET PARA A PARTILHA NÃO AUTORIZADA DE OBRAS
PROTEGIDAS POR DIREITOS DE AUTOR»
MIGUEL CAETANO_____Página 157

CYBERLAW

by CIJIC



***O PAPEL DO DIRIGENTE NO INCREMENTO DA RESILIÊNCIA
DIGITAL DAS ORGANIZAÇÕES
– GAMEIRO MARQUES***

O PAPEL DO DIRIGENTE NO INCREMENTO DA RESILIÊNCIA DIGITAL DAS ORGANIZAÇÕES

Todos sabemos que estamos na era da Internet das Coisas e das Pessoas (IOT), da *Industrial IOT* (IIOT), da grande mobilidade das pessoas e dos respetivos dispositivos e do advento das cidades inteligentes, e que, de acordo com a Gartner, em 2020 existirão mais de 26 mil milhões de dispositivos ligados à rede.

Neste artigo, e no contexto da hiperconectividade e do “*always on*” que caracterizam a digitalização da sociedade em que vivemos, importa perguntar qual deverá ser o papel do dirigente de uma organização, seja ela pública ou privada, relativamente ao modo como a mesma se comporta e se apresenta no ciberespaço. Será que o dirigente sabe o tipo de pegada digital que a sua organização deixa no ciberespaço? Dá sinal de ser uma entidade que apresenta alto risco quando comparada com outras da mesma área, ou, por outro lado, apresenta evidências de que é resiliente e confiável? Quais as implicações deste seu estado, (seja ele qual for), para as suas atividades? Será que o dirigente sabe, ou se interessa por estes assuntos ou considera que isto é uma coisa para os “informáticos”? Pior ainda, será que nem quer saber?

Consultoras internacionais, quando interpeladas sobre como classificam a atitude dos dirigentes da Europa e do continente Norte-americano, quanto aos assuntos relacionados com a resiliência digital das entidades sob a sua responsabilidade, respondem que, de uma forma geral, enquanto no continente europeu o assunto ainda é predominantemente considerado um problema eminentemente tecnológico e portanto algo que deve estar na agenda dos departamentos de IT, nos EUA e no Canadá o tema é claramente um assunto de conselho de administração e tratado como tal em todas as suas vertentes (RH, financeiro, tecnológico, marketing, operações, etc.). Esta forma de ver as coisas, leva, mesmo, a que o mercado na área da formação pós-graduada, quer os EUA quer o Canadá disponibilizem, em algumas prestigiadas universidades norte-americanas, MBA subordinados ao tema cibersegurança, onde se juntam pessoas com diferente formação de base mas que, estudando juntos, contribuem para que as futuras gerações de líderes, independentemente da sua base académica, criem saber para lidar com estes temas, que vão muito para além do meramente tecnológico e que condicionam, de sobremaneira, a atividade, a

reputação e os proveitos das organizações. Se interiorizarmos que, tal como os espaços físicos que fazem parte do nosso ambiente natural (terra, mar, ar, espaço), o ciberespaço é um lugar “habitado” por seres que, não sendo sempre necessariamente reais, têm comportamentos que importa tentar compreender para antecipar, prevenir e agir, perceberemos facilmente que o este tema é muito mais do que um tópico tecnológico, carecendo, por isso, de uma abordagem multidimensional e transversal: *Directors need to understand and approach cyber security as an enterprise-wide risk management issue, not just an IT issue* (Cyber-Risk Oversight Executive Summary, Director’s Handbook Series, 2014 Edition).

Se relativamente às diferentes perceções que existem dos dois lados do Atlântico, o panorama genérico é o que acabou de ser sumariamente caracterizado, no caso do nosso país o assunto ainda é mais peculiar. De facto, de acordo com o *Global Risk Management Survey* de 2015 da *AON Risk Solutions*¹, nas cerca de 1400 entidades que participaram no inquérito, o risco relacionado com a cibersegurança entrou diretamente para o 9º lugar (no continente norte-americano é 5º). A perspetiva futura é que o risco devido a fatores relacionados com estes assuntos suba dois lugares no próximo estudo, previsto ser publicado em 2017. No caso português, também contemplado pela primeira vez no documento, os riscos associados à presença no ciberespaço não emergem com esta relevância no universo das cerca de 60 empresas que participaram na elaboração do relatório.

E qual será a razão que subjaz a este facto? Será porque a comunidade IT usa linguagem muito hermética e por isso difícil de entender pela maioria dos dirigentes? Será por desconhecimento? Ou será antes pela atitude que na generalidade amiúde adotamos, de só darmos efetivamente importância ao que tem visibilidade imediata e retorno no mesmo registo temporal?

É que o dirigente não se pode olvidar de que a organização que dirige não vive isolada, e assim blindada do mundo exterior. Neste nosso mundo, as interações com um cada vez mais amplo e complexo ecossistema, e com agentes que conhecemos e que desconhecemos (pensando conhecer), são constantes e ocorrem de forma permanente. Por estas razões, as fronteiras são difusas e este facto deve enquadrar a forma como se deve gerir o risco associado. Na verdade, e como todos nós sabemos, as organizações de hoje dependem do exterior pois partilham informação com outras entidades, disponibilizam serviços e aplicações ao mundo que as rodeia,

¹http://www.aon.com/grms2015-video/index.html?utm_source=aon.com&utm_medium=vidimlink01&utm_campaign=grms2015

encontrando-se por isso interligadas, levando a que informação explícita e implícita relativamente a si própria esteja dispersa, dentro e fora de portas. A organização é, assim, algo ubíqua, por oposição a existir num só local físico bem determinado.

Simultaneamente, os colaboradores movimentam-se no seio da respetiva comunidade de interesse, utilizando meios remotos para aceder à organização, que passa a ser, numa lógica de gestão do risco, uma entidade virtual, e não apenas física e estruturada num só local ou locais bem definidos.

Paralelamente, e também por causa disso, a informação, designadamente a que nos diz respeito, está dispersa e muitas vezes guardada em condições que não sabemos em locais que desconhecemos, levando a que esteja cada vez mais na ordem do dia os assuntos relacionados com a privacidade e o respetivo equilíbrio com a segurança. Amiúde ouvimos dizer que temos que abdicar da nossa privacidade para preservar a segurança. No entanto, e como princípio fundamental, recomenda-se que não se enverede por esse caminho! O que têm que ser descortinadas é soluções que incrementem a segurança da nossa informação sem comprometer a privacidade!

Por outro lado, estamos numa *Knowledge Intensive Society* em que o conhecimento, providenciado pela informação que decorre da combinação dos dados com os respetivos metadados, tem um valor capital. Mas esse valor é tanto mais relevante quanto o soubermos e pudermos partilhar por comunidades que compreendam o valor dessa partilha: “*all of us are smarter than one of us*”².

Todavia, e por causa de tudo isto, os predadores abundam, são cada vez mais sofisticados e complexos. Como o número de dispositivos ligado à rede é cada vez maior, a potencial superfície de ataque é também cada vez mais ampla. E isso deve preocupar-nos. É que, se bem que os registos de ataques deste tipo com efeitos cinéticos sejam ainda escassos, a tendência é claramente para o seu crescimento. E se ocorrerem nas infraestruturas controladas por sistemas SCADA de tecnologia legada, que fornecem serviços essenciais às sociedades, então poderemos vir a ter problemas graves e bem tangíveis.

Por isso, é absolutamente determinante que os dirigentes coloquem a Segurança no topo das prioridades, conferindo-lhes um carácter Estratégico, de modo a que passem a ter visibilidade, ao nível dos órgãos diretivos, sobre indicadores de risco que sejam simples, claros

² Tradução livre de provérbio japonês

e acionáveis, para viabilizar a rápida tomada de decisão. Deste vértice onde se posiciona o dirigente, deverá ser possível não só compreender como está o nível de maturidade da própria organização relativamente à cibersegurança, estabelecendo objetivos e monitorizando a respetiva prossecução, mas também perceber o que se passa no exterior, designadamente no que concerne às entidades com quem a própria organização se relaciona, principalmente aquelas com quem existe a necessidade de interagir para o cumprimento da respetiva missão.

Neste contexto, é possível, hoje em dia, reunir um conjunto de indicadores que podem fornecer uma quantificação do grau de ameaça que representamos para terceiros, incluindo a criticidade que a nossa presença no ciberespaço poderá representar para o normal funcionamento das relações institucionais entre organizações.

Uma das formas que tem vindo a ser desenvolvida para se mostrar ao dirigente, de forma facilmente compreensível, indicadores relacionados com assuntos desta natureza, reside no recurso a um conjunto de parâmetros semelhantes aos que são observados, de uma forma mais consolidada, na avaliação do risco financeiro, os quais são obtidos sem qualquer intrusão na organização que se pretende estudar, mas apenas analisando a respetiva pegada digital no ciberespaço.

Através da observação dessa pegada é possível obter uma classificação de risco, cuja análise é depois possível aprofundar na ótica interna, de modo a que se compreendam as razões subjacentes à pontuação obtida, viabilizando a concretização de medidas tendo em vista a resolução dos problemas identificados. Por outro lado, na ótica externa, a obtenção da classificação das entidades que fazem parte do nosso ecossistema quanto ao respetivo risco, permite posicionar-nos de forma pró-ativa quando essa classificação é baixa, revelando-nos que poderemos importar esse risco para a nossa organização se e quando, por via da nossa atividade, trocamos informação e serviços com terceiros.

Todavia, neste contexto, o papel do dirigente não se confina apenas ao que acabei de mencionar.

Num interessante artigo da Harvard Business Review de Setembro de 2015³ subordinado a este tema, os autores defendem que os CEOs têm um papel determinante no incrementar da resiliência digital das suas organizações, através da conjugação de um conjunto de princípios

3 <https://hbr.org/2015/09/cybersecurity-human-factor-lessons-from-the-pentagon>

gizados para servir um objetivo comum: instituir uma cultura que minimize o ciber risco através da intervenção pró-ativa no fator humano: *“People matter as much, if not more than, technology. We have to get beyond focusing on just a tech piece. It’s about ethos. It’s about culture. It’s about how you train your men and equip your organization, how you structure it and the operational concepts you apply”* (Admiral Mike Rogers, USA Cyber Command).

Na aplicação destes princípios, e dado que cada entidade é única, os dirigentes deverão levar em consideração dois tipos de fatores. O primeiro é o tipo de atividade e o respetivo grau de vulnerabilidade a ciberataques: uma entidade financeira, uma indústria altamente competitiva, um prestigiado centro de investigação serão mais propensos a ser alvos de ataques. O segundo é a natureza dos seus colaboradores. Se, por exemplo, estes forem predominantemente da geração Y ou *millennials*, estarão habituados a trabalhar a partir de casa em ambientes colaborativos fazendo várias coisas ao mesmo tempo, o que aporta outro tipo de desafios no alcançar do objetivo que acima referi (porque a superfície de exposição ao risco é maior) que é o de, repetindo, minimizar o ciber risco através da intervenção pró-ativa no fator humano.

Aquele conjunto de princípios baseia-se nos que orientam os comportamentos nas *High-Reliability Organizations* (HRO) e resumem-se no seguinte:

Simplicidade (Integridade) **organizacional** (SMART Simplicity) – Ser simples não é simples. Tendencialmente combatemos a complexidade com mais complexidade. Temos estruturas que funcionam em silos, não cooperam e por isso tendem a ter menos resilientes. Também por isso têm dificuldade em colaborar e a trabalhar em rede. Quando se coopera chega-se mais longe e gastam-se menos recursos. Nas organizações complexas os processos de deteção e reporte de incidentes, quando existentes, são intrincados, lentos e pouco eficientes, quando o que se pretende nestas situações é rapidez e clareza. A organizações complexas, correspondem arquiteturas informacionais e físicas difíceis de compreender e por isso de explicar e de administrar. São, por isso, mais vulneráveis. Nestas organizações é difícil saber com clareza qual é e onde está a informação mais relevante para a organização e assim, aquela que importa proteger prioritariamente.

Conhecimento e treino – Se as pessoas da organização possuírem sólida formação sobre o ecossistema, incluindo a sua arquitetura, as suas vulnerabilidades e os procedimentos para operar os sistemas, estarão mais habilitados a reconhecer algo que evidencie um comportamento anómalo e assim agir de forma eficaz e atempada perante esse facto. Para se atingirem estes níveis de proficiência não basta saber; tem que se treinar

regularmente em exercícios concebidos para representar cenários cada vez mais complexos e assim adestrar a organização a fazer face a situações anómalas. E é o conjunto organização, estrutura, pessoas que é treinado e avaliado. Não as pessoas de per si. Os resultados desses exercícios devem ser avaliados e apresentados ao *board*, para decisões subsequentes.

Ainda neste âmbito, releva-se a necessidade de se conhecer com profundidade o novo Regulamento Geral de Proteção de Dados⁴ e a Diretiva SRI⁵ (*Network and Information Security Directive*) da ENISA e as suas implicações, sobretudo se estivermos a falar de entidades que providenciam quer serviços essenciais para a sociedade, quer serviços de comunicações eletrónicas. É muito importante que os órgãos diretivos fomentem o incremento do saber dos seus recursos relativamente a estes dois importantes documentos.

Redundância – Qualquer ação que represente um alto risco não deverá ser realizada apenas por uma única pessoa, devendo ser monitorizada por alguém que possa interferir proactivamente, caso o procedimento em causa não seja o correto.

Atitude de irreverência construtiva – Compreendendo-se que questionar o *status quo* não é um comportamento muito fácil de fomentar e de aceitar na nossa sociedade, sobretudo em estruturas muito hierarquizadas, deverá ser encorajado um comportamento que leve a que aqueles que operam e administram os sistemas, se interroguem sobre o respetivo comportamento (sobretudo quando ele é estranho). Esta atitude visa acelerar a compreensão do que está na origem de tal situação, de modo a viabilizar a tomada atempada das ações corretivas, antes da dimensão do problema ser tal que dificulte a respetiva resolução. A esta atitude contrapõe-se a complacência perante os factos ou mesmo a indiferença. Se os dirigentes investirem na criação uma cultura de *accountability*, que permita a quem tomou as decisões ter visibilidade sobre os resultados alcançados, poderemos almejar a que haja mudanças significativas neste âmbito.

Os dirigentes poderão dar o exemplo adotando esta atitude de irreverência construtiva, suscitando um conjunto de seis questões⁶ ao seu “conselho de administração” e exigindo, naturalmente, as respetivas respostas:

4 <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>

5 https://www.cncs.gov.pt/content/files/diretiva_2016_1148.pdf

6 <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx>

1. *Existe, ou não, um enquadramento (framework) para a cibersegurança na Organização?*
2. *Quais os cinco maiores riscos de cibersegurança na Organização?*
3. *Qual o nível de adestramento e de sensibilização dos colaboradores?*
4. *As ameaças externas e internas são levadas em linha de conta, quando se planeiam investimentos de cibersegurança?*
5. *Qual é o modelo de governo destes assuntos?*
6. *No caso de um incidente de comprometimento grave da informação mais importante da Organização, existem procedimentos formalizados, testados e treinados?*

Em termos de conclusão diríamos que a construção de uma cultura de alta confiabilidade e resiliência digital vai requerer a atenção do dirigente e do seu *board*, incluindo alterações, quer nos processos de governo da entidade, quer naqueles que enquadram a atividade da organização. Os investimentos na criação de conhecimento permanente e acionável sobre o ciber risco do seu ecossistema e o incremento, quer do saber dos colaboradores, quer das oportunidades de treino das equipas para fazer face eficazmente a situações anómalas, terá retorno na resiliência digital da organização, na sua reputação e assim na criação de valor para a sociedade.

A realidade é clara: se o dirigente não leva a sério estas questões, a sua organização também não o fará. Podem estar certos que o CEO da Target, que foi despedido em 2014 depois do roubo de informação relativa a 70 milhões de cartões de crédito dos seus clientes, bem gostaria agora, de ter tido antes, uma atitude diferente a este respeito.

CYBERLAW

by CIJIC



***NON-IT PERSPECTIVES OF CYBER SECURITY BY AN IT
PROFESSIONAL: CHALLENGES AND FUTURE TRENDS
- PETR JIRÁSEK***

NON-IT PERSPECTIVES OF CYBER SECURITY BY AN IT PROFESSIONAL: CHALLENGES AND FUTURE TRENDS *

ABSTRACT:

This article discusses the cyber security from non-technological perspectives and tries to draw attention to the fact that cyber security is a multidisciplinary field, as well as to explain some threats and challenges that cybersecurity in modern society brings.

Keywords: Cyber security, Threat, Vulnerability, Human factor, Legislation, Trust, Cooperation, Critical information infrastructure

RESUMO:

Neste artigo discutiremos a questão da cibersegurança a partir de perspectivas não-tecnológicas, tentando focar a atenção na sua multidisciplinariedade. Procuraremos ainda explicar algumas ameaças e desafios que a cibersegurança implica na sociedade moderna.

Palavras-chave: Cibersegurança, Ameaças, Vulnerabilidades, Factor humano, Legislação, Confiança, Cooperação, Infra-estruturas de informação crítica

** Petr Jirásek is the Chairman of the Czech Cyber Security Working Group and a Member of AFCEA International Cyber Committee, with more than 25 years' experience in IT and cyber security. He worked on several government and industry IT projects. He is a co-founder of the Czech Cyber Security Working Group and for almost 20 years an organizer of the professional events for security community in the Czech Republic and East Central Europe. Mr. Jirásek is a co-author and an author of several books and papers focused on security and cyber-related topics, he is a co-author of the official Czech Cyber Security Glossary.*

PREAMBLE

Constant and rapid progress in the field of ICT brings new opportunities for the society but also new security challenges. Combination of increased dependence on ICT which is not flawless with human failure or intentional damage makes mitigation of damages more complicated. The emergence of new technologies brings new opportunities for the development of the society but also new vulnerabilities and new demands for the security of ICT and the whole society. [1]

Increased dependence on ICT enhances the vulnerability of the state and its citizens to cyber-attacks. These attacks may be motivated by crime, economic profit or terrorism and may be used to destabilize society. Leaks of strategic information, infringements into ICT of state institutions or strategic companies may endanger the interests of the Czech Republic. Examples show a rapid and diverse development in the field of cyber security. Attacks against ICT are more complex and sophisticated. These attacks are aimed at various targets and waged by various means. Also, the nature of attackers and their motives is changing. Parts of the critical infrastructure (CI), crucial for the functioning of the state, are becoming a target of attacks more and more often. [1]

Protection of critical information infrastructure (CII) is one of the main priorities in cyber security. This infrastructure is the main part of the CI and is becoming more and more important. Both private and public spheres have to create conditions for closer cooperation based on information sharing. It is also a fact that in modern societies the private sectors own the great majority of CII.

PREÂMBULO

O progresso constante e acelerado no campo das TIC acarreta novas oportunidades para a sociedade, mas também novos desafios de segurança. A combinação de uma cada vez maior dependência destas, com falhas humanas ou danos intencionais, torna a mitigação dos riscos daí derivados muito mais complicada. Se as novas tecnologias comportam, por um lado, um leque alargado de novas oportunidades para o desenvolvimento da sociedade, por outro lado, também implicam novas vulnerabilidades e novas exigências tanto para a segurança das TIC como para toda a sociedade. [1]

A aditiva dependência das TIC aumenta a vulnerabilidade do Estado e, por sinal, dos seus cidadãos a ciberataques. Estes ataques podendo ser motivados por crime, lucro económico ou terrorismo, podem ainda ser perpetrados para desestabilizar toda a sociedade. Fugas de informação

crítica, violações diversas à política das TIC quer de instituições estatais quer de empresas estratégicas, ameaçam os superiores interesses da República Checa. Os ciberataques denotam uma especial e cada vez maior complexidade e sofisticação. Dirigidos a múltiplos alvos e por variadíssimos meios, a própria natureza dos ciberatacantes e dos seus motivos tem-se alterado. Sendo vários os exemplos que atestam este risco no campo da cibersegurança, destacaríamos os perpetrados contra infra-estruturas críticas (IC), cruciais para o funcionamento do Estado. [1]

A protecção das infra-estruturas de informação crítica (CII) é uma das principais prioridades da cibersegurança. Não negligenciando o facto de que nas sociedades modernas os sectores privados possuem a grande maioria da CII, é crucial que as esferas privada e pública criem condições para uma cooperação mais estreita com base na partilha de informação.

CYBER SECURITY

Cyber security is not only about technology. Cyber security is a multidisciplinary field, including legal environment, human factor (sociology, psychology), education, technical aspects (IT, cryptography, etc.), diplomacy, cooperation, and so on.

There are several terminologies what cyber security exactly is. The first official national cyber security terminology was created in the Czech Republic by the Czech Cyber Security Working Group [2]. It brings to common understanding what cyber security is, what it includes. It helps to understand how to act. Unfortunately, only a few societies around the world created and agreed on such common terminology, which forms a basis for cooperation and brings about the fundamentals for legal environment.

CAN LAWS AND STANDARDS SOLVE THE SITUATION?

Our cyber space has many similarities with road traffic. We have roads (network lines), cars (computers), and we have people here, some good and some bad drivers (users), pirates. We can see a great parallel between these two spaces: road traffic space and cyber space.

Considering the fact that digital society is globalized and cyber-attacks are crossing state, cultural and legislative boundaries, it is often not obvious which jurisdiction should be applied to them. Close international cooperation is therefore needed also in the area of legislation. [1]

Laws regulating road traffic began hundreds of years before the automobile was even invented. The first kind of law regarding road traffic was passed in England in 1555 [3]. In 1686, the first known Traffic Regulation Act in Europe was established by King Peter II of Portugal [4]. The first International traffic code was proposed in 1909 and agreed by most countries by 1949 [5]. Since then we have roads with signs, lights at the crossroads and other helpful indicators, we have cars with proper homologations and car plates, we have trained people with driving licenses, and we have regulators and controllers as state administration, police, etc.

Unfortunately, still we have people dying on the streets, people driving drunk or without a driving license, we have accidents, we have technical issues, we have people intentionally violating traffic and other laws. We still have a lot of such issues.

For all of these reasons we need a legislation framework, standards and regulators to control and protect our critical infrastructure. Nevertheless, we have to understand that legislation itself will not solve the possible cyber threats and other issues easily. All this will take time,

unfortunately. For road traffic it took already 461 years and still we have new threats and challenges. Nevertheless, proper laws and regulations help us to investigate the problems and punish crimes. We also need better technology, new solutions, new approaches, trained people, more cooperation and establishing trust. [6]

There are also some differences how our societies operate in both spaces. As already mentioned, for the cars we developed special standards, homologation (certification) systems, regulation. Still we can have some issues like “Diesel Gate” or forgery of documents. But we have the legal environment to be able to analyze, take evidence, properly enforce the law, prosecute and punish.

In cyber space, the majority of applications (software) are sold with disclaimers “As-it-is”. If we buy them and install them, we (users) are responsible for possible data loss, data or hardware damage, even to third parties. Therefore we have a lot of software, which has to be patched often, which was not properly tested, which was developed without any standards, etc. Why do we accept such a different approach?

As a minimum for our critical information systems we have to take the right approach and to avoid challenging our societies with new threats and vulnerabilities.

HUMAN FACTOR AND ITS IMPORTANCE

Humans are a part of the cyber space. Car drivers are a part of the traffic eco-system.

The roads are very important for us. The roads connect our homes, offices, places of entertainment. We need them every day. Without secure roads, our societies will not be working effectively. The drivers using the roads have to be trained. The drivers need a proper license to drive a car on the public roads. The certification system is quite developed. We trust the system and we “trust” the certified drivers. We expect that drivers are well trained and will behave properly on the roads.

The critical information infrastructure is well developed. We need it. Our societies are dependent on it. Nevertheless, almost anyone can drive on the “road”. No certificates are mandatory. The regulations and standards are still under development. Why are we taking such a different approach?

Humans have to be trained to do their work properly, effectively and safely. That’s a fact!

Another aspect: Often people blame “users” to be the “weak link” in an IT security eco-system. Is this correct? Just imagine an example: a customer buys a chocolate in a shopping center. The chocolate is poisoned. The customer offers the chocolate to his or her friends and poisons them. Do you expect that a customer is an expert to recognize that the chocolate was poisoned? Is the customer responsible for the poisoning of other people? Who is responsible? Where is the fault? Is the customer (“the user”) the “weak link”?

Of course, you can look at the proposed example from many angles and say, in brief, yes, the customer was the “weak link”. But most probably it was not the customer, but another human who made the mistake or it was technology or a human who set up the technology or the system, and so on.

Let’s take a similar example in IT eco-system: The user receives an email and opens it. The email includes a malware. The user unwittingly distributes the malware in the entire organization and creates a chain of accidents. Why did it happen? Why the IT eco-system didn’t help to recognize the threat? Why did the user have so many administrative rights to spread the malware in the entire organization? Et cetera.

Shortly, it is not the user who is the “weak link”, maybe it is a human, but in the majority of cases it is a system (set of the procedures), which is not well developed and leaves too much independence or not the appropriate level of responsibility to a single link in the eco-system. Let us think about it. [7]

Of course, everything starts with a human. Therefore we educate ourselves. We are well trained how to behave as pedestrians, bicyclists or drivers. We know what to do before crossing a street or what speed is safe and what is already a risk. Sometimes we take a risk but usually we are aware of the possible consequences. Do we behave in the same way in the cyber space? Do we know how to behave as a “simple user”, a user of e-government systems or an employee of critical information system?

We need to improve our education system and start to learn all the cyber security basics as soon as possible. We will be very dependent on ICT systems. We are already dependent on them.

TRUST AND COOPERATION

As mentioned above several times, we need to establish proper trust and cooperation. Nobody in ICT environment can have all the information, sometimes due to lack of technology

resources, often because they are owned by different states or authorities you don't have direct access to. The electronic world is moving from “*need-to-know*” to “*need-to-share*”¹. Therefore, cooperation based on trust is necessary.

On the other hand, too much trust is also not welcome. It can create too strong a dependence and lack of responsibility. It is necessary to establish proper eco-system for sharing information, what information can be shared, with whom, etc. This again brings forth the importance of legal environment and standardization.

In the IT security environment there already exist some standards (e.g. ISO 27001) and several organizations dealing with security threats and cooperating with each other against cybercrime and other cyber issues. Still, we have to develop this eco-system as the major standards are not yet enforced for use, membership in the mentioned organizations is usually only on a voluntary basis, etc.

In the road space we have many bilateral and multilateral agreements between the national authorities to cooperate and support each other. For example: if a suspicious driver is crossing a national border, the police of the first country can cross the borders and chase the car in the other country (if there is the proper bilateral agreement between both countries, which is usually the case in Europe). Can we do this in the cyber space, to cross the boundaries and to take some offensive actions on the territory of another state?

FINANCIAL ASPECTS OF CYBER SECURITY ENVIRONMENT

There are also some differences between the road and cyber space. One of them is that road traffic is mostly symmetric, which is not the case of cyber space. One driver can cause only a limited damage. One computer user can cause an almost unlimited damage. To buy a car costs usually much more than to buy a cyber-attack. And so on.

There is also another financial point of view. Both spaces (road and cyber) need investment to protect the eco-system. By using some statistical data and project them world-wide, during the last 50 years we spent more than 100 t\$ in the automotive industry and road traffic development and approximately 3 t\$ on road traffic regulation². During the past year we spent almost 4 t\$

1 Mentioned on several occasions, taken from a public discussion on AFCEA Intelligence Symposium, 2014, Brussels, Belgium.

2 Several sources, including statistical data of the Czech Republic, European Union and public studies.

worldwide ion ICT development [8] and almost 75 b\$ protecting the cyber space [9]. It means we are spending 3% to regulate and protect the road space but only 0.6% to protect cyber space.

How important is the cyber space for our societies? How much are we dependent on it? What kind of damage can happen if the road space is not well regulated and what damage can happen in a single cyber-attack?

CONCLUSION

The cyber space is growing. Soon, we can expect other challenges, like e-cars, Internet of Things (IoT) and many other. In these areas the cyber and road spaces will be somehow connected. Just imagine a self-drive car has to take a decision before an accident happens: to injure its passengers by hitting a concrete wall or to hit an elderly pedestrian.³ What will the car's decision be? Who is responsible for this accident? The car developer, the software developer, the car service provider, or you?

There will be many threats and new challenges...

³ Several sources including internet and public discussions.

USED SHORTCUTS

AFCEA	Armed Forces Communication and Electronics Association
CI	Critical infrastructure
CII	Critical information infrastructure
e-	Electronic
ICT	Information and communication technology
IoT	Internet of Things
IT	Information technology

REFERENCES

- [1] Group of Authors, Strategy of the Czech Republic in the field of Cyber Security for 2012 - 2015, Praha: National Security Authority, Czech Republic, 2012.
- [2] P. Jirásek, L. Novák and J. Požár, Czech Cyber Security Glossary, 3rd issue ed., Praha, Czech Republic: AFCEA Czech Chapter, Police Academy of the Czech Republic, 2015.
- [3] Cambridge University Press, "Highways Act 1555," Wikipedia.org, 19 9 2013. [Online]. Available: https://en.wikipedia.org/wiki/Highways_Act_1555.
- [4] Unknown, "Traffic sign," Wikipedia.org, 2 11 2016. [Online]. Available: https://en.wikipedia.org/wiki/Traffic_sign.
- [5] United Nations, "UN Treaties," 1 10 2016. [Online]. Available: treaties.un.org/doc/Publication/UNTS/Volume%20125/v125.pdf.
- [6] P. Jirásek, "Cyber security and legal environment," in *KIT 2013 Proceedings*, Tatranské Zruby, 2013.
- [7] P. Jirásek, "Human factor and Cyber Security," in *Cyber Security III*, Praha, 2015.
- [8] Unknown, "Gartner Worldwide IT Spending Forecast," Garner, 2016. [Online]. Available: <http://www.gartner.com/technology/research/it-spending-forecast/>.

[9] S. Morgan, "Worldwide Cybersecurity Spending Increasing To \$170 Billion By 2020," Forbes, 9 3 2016. [Online]. Available: <http://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#50f676fc76f8>.

CYBERLAW

by CIJIC



***LOS NUEVOS INSTRUMENTOS DE PREVENCIÓN Y LUCHA CONTRA
EL NUEVO TERRORISMO: MALAS NOTICIAS PARA LOS DERECHOS
FUNDAMENTALES DE LOS CIUDADANOS
– ALFONSO GALÁN MUÑOZ***

LOS NUEVOS INSTRUMENTOS DE PREVENCIÓN Y LUCHA CONTRA EL NUEVO TERRORISMO: MALAS NOTICIAS PARA LOS DERECHOS FUNDAMENTALES DE LOS CIUDADANOS *

RESUMEN:

El presente trabajo analiza como la lucha contra las nuevas manifestaciones de terrorismo, dadas por el denominado terrorismo yihadista, ha llevado tanto a los legisladores nacionales, como al regulador europeo a crear amplios y controvertidos mecanismos represivos y de investigación penales que ponen en tela de juicio la vigencia de algunos de los derechos fundamentales de los ciudadanos. Así, se pone de manifiesto como se han creado figuras penales que ponen en cuestión la vigencia del derecho fundamental a la libertad de expresión, mientras que, por otra parte y paralelamente, se han establecido sistemas de captación y tratamiento de datos personales, (como los referidos a los datos de pasajeros PNR), que además de poner en tela de juicio derechos como los relativos a la protección de datos personales de los ciudadanos, extienden su ámbito de aplicación mucho más allá de aquel que se refiere a la prevención e investigación de delitos terroristas, lo que generaliza el régimen supuestamente excepcional previsto para tales delitos y, por tanto, cuestiona la propia consideración de los países que emplean tales sistemas como verdaderos Estados democráticos de Derecho.

* Este trabajo es una versión ampliada y revisa de la conferencia que bajo el título de «*Constituição, Legalidade Penal e Ciberespaço*» impartió el autor el 17 de noviembre de 2016, en el seno de la *I Conferência Internacional De Lisboa Sobre Segurança Da Informação E Direito Constitucional Do Ciberespaço*, celebrada en la Universidad de Lisboa (Portugal). Prof. Dr. Alfonso Galán Muñoz, Profesor Titular de Derecho penal, Universidad Pablo de Olavide, Sevilla, España.

1. ¿NUEVO TERRORISMO? ¿NUEVA POLÍTICA CRIMINAL?

El denominado terrorismo *yihadista* no es en realidad un fenómeno tan novedoso o reciente como se pudiera en un primer momento pensar.

Es indudable que existe y ha generado víctimas en muchos países del mundo desde hace muchos años¹. Sin embargo, fueron los atentados del 11 de septiembre de 2001 en Nueva York o los cometidos en Madrid en 2004 o en Londres en 2005 los que hicieron a las sociedades occidentales tomar conciencia de la magnitud y, sobretudo, de la cercanía del riesgo que su existencia representaba para sus ciudadanos².

Nos encontramos, por tanto, ante una forma de terrorismo que no es nueva, pero también ante una que presenta una serie de notas diferenciales con respecto a la tradicional que deben ser muy tenidas en cuenta a la hora de darle adecuada respuesta penal.

Así y en primer lugar, el terrorismo *yihadista* es un terrorismo que responde a la supuesta existencia de una guerra asimétrica y global que sus integrantes y partidarios han emprendido contra los países a los que consideran contrarios o enemigos de su “pueblo” o comunidad religiosa y de los valores que los caracterizan. Es, por tanto, un terrorismo que no trata de subvertir el orden constitucional del concreto país al que golpea. En ocasiones, ni tan siquiera pretende lograr una finalidad propiamente política referida al mismo, como la de doblegar la voluntad de su opinión pública o políticos para que desistan, por ejemplo, de tomar parte en una determinada campaña militar, sino que lo que intenta es, simple y llanamente, de ocasionar dolor y terror a los habitantes de dicho país y a los de su entorno, como represalia y venganza por los agravios o daños que

¹ Sobre los orígenes y ataques por todo el mundo que realizaron los diferentes movimientos terroristas yihadistas contemporáneos antes del 11 de septiembre, entre los que se encuentra el parece que ya olvidado primer atentado contra el World Trade Center de Nueva York de 1993, véase lo comentado, por ejemplo, por FUENTE COBO, I. “El yihadismo en su contexto histórico”, en Cuadernos de estrategia, 173. Ed. Ministerio de Defensa, Madrid, 2015, p. 54 y ss, disponible en http://www.ieee.es/Galerias/fichero/cuadernos/CE_173.pdf (últ vis. 10-12-2016).

² Así, señala GONZÁLEZ CUSSAC J. L. que, de hecho, tras los atentados del 11 de septiembre, el terrorismo dejó de ser considerado como una cuestión puramente criminal, pasando de ser un simple “riesgo” para la seguridad nacional a alcanzar la máxima categoría de “amenaza para la misma”, en “Nuevas amenazas a la seguridad nacional: los desafíos del nuevo terrorismo”, *Retos de la política criminal* actual. Revista Galega de Seguridad Pública, 9, 2007 p. 233 y ss. LARRIBA HINOJAR, B., por su parte, consideraba que han sido precisamente dichos atentados los han obligado a que se realice un replanteamiento de los parámetros que configuran los conflictos terroristas al plantear uno de los mayores desafíos a las democracias modernas, en “Globalización, terrorismo y libertad de expresión: Conminación penal de actividad terrorista en el entorno virtual”, en *Constitución, derechos fundamentales y sistema penal. T. II*. Ed. Tirant lo Blanch, Valencia, 2009. p. 1089.

supuestamente éstos habrían contribuido previamente a ocasionar a las personas o países con los que el terrorista se identifica por razones presuntamente religiosas, aunque ni siquiera los conozcan y se encuentren a miles de kilómetros de distancia de donde vive y atenta.

Es entonces un terrorismo que tiene ya en su código genético un marcado carácter supra- o transnacional, muy conectado, por otra parte, con una visión completamente maniquea del mundo, que clasifica a todas las personas en amigos (fieles, a los que hay que proteger y en su caso vengar) y enemigos (infieles, a los que simplemente hay que exterminar); visión que se ha expandido rápidamente a lo largo y ancho del globo, gracias, entre otras cosas, a la difusión de un discurso marcadamente adoctrinador y basado en una concepción completamente manipulada y tergiversada de las tendencias más radicales del Islam en los modernos medios de información y comunicación (principalmente Internet) y que trata, precisamente, de fomentar y de avivar el odio hacia aquellos a los que califica como infieles o enemigos.

Es, por tanto, un terrorismo no estrictamente político, pero sí uno dotado de un fuerte fundamento y discurso ideológico-religioso que se ha demostrado como tremendamente atractivo para determinadas capas de las sociedades actuales. Especialmente, aunque no de forma exclusiva, para aquellas que se conforman por los grupos de jóvenes de origen humilde, escasa formación y que viven sin demasiadas esperanzas de un futuro mejor, en muchas ocasiones, en verdaderos guetos incluidos dentro de las grandes ciudades occidentales y reservados aparentemente para los de su etnia o religión; sujetos a los que se trasmite el tal vez simplista, pero también muy seductor mensaje de que, en realidad, todo lo que padecen no es por culpa suya o del injusto sistema social en que les ha tocado vivir, sino que es un producto intencionadamente impuesto por los enemigos de su “gente” y de su religión. Enemigos contra los que evidentemente tienen que luchar.

Precisamente, este marcado carácter adoctrinador del terrorismo yihadista es el que puede llevar y, de hecho, ha llevado a que algunas personas individuales, que no contaban con apoyo ni contacto alguno con ninguna organización terrorista (los conocidos como “lobos solitarios”), hayan efectuado, de forma autónoma y por su cuenta y riesgo, ataques contra los “enemigos” de su pueblo o religión y en apoyo de la “guerra santa” que creen se está librando contra los mismos, incluso aunque ello les haya supuesto tener que sacrificar su propia vida para poder llegar a hacerlo, algo que, indudablemente, plantea serios y evidentes problemas a los tradicionales instrumentos penales de lucha contra el terrorismo.

Así, por ejemplo, ¿realmente los especiales y variados instrumentos jurídicos creados para luchar contra las estructuras criminales complejas, permanentes y altamente jerarquizadas propias del terrorismo tradicional y los sujetos que las integran, respaldan o ayudan pueden ser utilizados para responder adecuada y eficazmente a esta nueva forma de terrorismo incluso individual? Y en el mismo sentido, ¿la estrategia político criminal empleada contra el terrorismo tradicional, claramente volcada a la prevención general negativa mediante la amenaza de penas, en ocasiones, draconianas para la realización de las actividades que les eran propias, pueden tener alguna eficacia preventiva a la hora de hacer frente a unos sujetos que están dispuestos incluso a perder la vida para apoyar y respaldar las ideas por las que dicen luchar? ¿Cómo puede intimidar a un posible terrorista, para que no cometa un delito, la amenaza de una pena de larga duración cuando está dispuesto a morir para ejecutarlo?³

Ninguna de estas preguntas parecía encontrar una respuesta afirmativa y plenamente satisfactoria y esto es lo que llevó tanto el legislador español, como a los del resto de países occidentales y muchos organismo supra- e internacionales, -entre los que destaca la UE,- a tratar de crear nuevos mecanismos e instrumentos jurídicos que sirvan para responder de una forma más adecuada al reto que esta nueva forma de terrorismo les viene a plantear.

Para ello, y en primer lugar, se ha procedido a incrementar el número de posibles finalidades cuya persecución convertirá un delito en terrorista, para permitir así que estas figuras no dejen escapar del excepcional régimen previsto para su investigación, persecución y castigo a ninguno de los que se comenten para respaldar los objetivos buscados por esta nueva forma de terrorismo. Así, precisamente, una de las más destacadas y controvertidas novedades introducidas en el Código penal español por la reciente reforma realizada sobre el mismo por la LO 2/2015 ha sido aquella ha venido a añadir a las tradicionales finalidades delimitadoras de las actividades terroristas, (las de subvertir el orden constitucional o alterar gravemente la paz pública)⁴, otras como las de provocar terror en todo o en parte de la población, obligar a los poderes públicos a realizar u omitir actos que no tengan por qué hacer o dejar de hacer o, simplemente, la de alterar el funcionamiento de las instituciones estatales o de organizaciones internacionales; finalidades todas ellas que, si bien puede ser que sirvan para perseguir y castigar anticipada y severamente las muy variadas

³ También cuestiona dicho pretendido efecto motivador CANO PAÑOS. M. A. "La Reforma penal de los delitos de terrorismo en el año 2015. Cinco cuestiones fundamentales", RGDP 23 (2015), disponible en <http://www.iustel.com> (últ. vis. 13-11-2016) p. 14.

⁴ Respecto a dichas finalidades y su significado y papel véase, por ejemplo, lo comentado por NÚÑEZ CASTAÑO, E. *Los delitos de colaboración con organizaciones y grupos terroristas*. Ed. Tirant lo Blanch, Valencia, 2013, p. 119 y ss o GÓMEZ MARTÍN, V. "Notas para un concepto funcional de terrorismo", en *Terrorismo y Estado de Derecho*, Iustel, 2010 p. 45 y ss, entre otros.

actuaciones que pueden realizar estos nuevos terroristas, lo harán indudablemente a costas de ampliar y desdibujar hasta tal punto la tradicional delimitación del terrorismo que permitirán que puedan llegar a tenerse como tales a actuaciones que nada tienen que ver con dicho fenómeno lo que, sin duda, planteará enormes y difícilmente resolubles problemas de proporcionalidad y constitucionalidad⁵.

Otra medida claramente tendente a extender el posible campo de actuación de los excepcionales instrumentos jurídicos de lucha antiterrorista a las nuevas manifestaciones de las que venimos hablando ha consistido en permitir que el uso de tales instrumentos no queden ya exclusivamente limitados a las actividades desarrolladas por o en torno a organizaciones terroristas. Para conseguirlo, en un primer momento, se creó la controvertida figura del terrorista individual (art. 577 ACP)⁶, abriéndose posteriormente la utilización de los referidos instrumentos jurídicos especiales a los denominados grupos terroristas, concepto este mucho más amplio que el de organización y por ello, se entendía que más adecuado para luchar frente a las células autónomas

⁵ Esta adicción que encuentra su origen en el art. 1.1. de la Decisión Marco 2002/475/JAI, de 13 de junio, que delimita de forma tan amplia y difusa los fines que darán lugar a que la apreciación de delitos terroristas, que podría llevar a que se pudiesen considerar también como tales conductas como, por ejemplo, las lesiones graves que se realicen con finalidad de atemorizar a una parte de la población (p. ej. homosexuales, emigrantes, etc...) o los incendios o daños que se puedan realizar durante una manifestación con la intención de interferir en el funcionamiento de una cámara parlamentaria; conductas éstas que, si bien resultan graves y pueden y deben ser penalmente perseguidas, no parece que hayan de mezclarse ni asimilarse a las verdaderamente terroristas, si no se quiere desdibujar los contornos que realmente diferencian y hacen más grave a esta forma de criminalidad frente a otras. En tal sentido, ya se manifestaba, por ejemplo, NÚÑEZ CASTAÑO, E. quien consideraba que la ampliación de fines incluida en el Decisión Marco permitiría considerar como terrorista actuaciones que en modo alguno pretenderían atemorizar a la sociedad, con lo que se desdota al terrorismo de su tradicional elemento definidor. Op. cit. ant. p. 79; lo que se corresponde con lo más recientemente manifestado por MUÑOZ CONDE, F., quien ha señalado que la ampliación de posibles finalidades terroristas realizada por la LO 2/2015, puede llevar a que se incluyan en el concepto de terrorismo a numerosos movimientos sociales de protesta, incluso cometidos individualmente, en Derecho penal. Parte Especial. Ed. Tirant lo Blanch, Valencia, 2015 p. 790. Sin embargo y en claro contraste con lo anterior, otros autores, como CANO PAÑOS, M. A. critican la inclusión de los comentados nuevos fines, precisamente, por considerarla como innecesaria, al resultar perfectamente subsumibles, a su modo de ver, en los que tradicionalmente han delimitado el terrorismo, esto es la de subvertir el orden constitucional y alterar la paz pública, en “La reforma de los delitos de terrorismo” cit. ant. p. 917.

⁶ Sobre esta polémica figura y su controvertida inclusión en el concepto de terrorismo, véase, lo comentado, por ejemplo, por CANCIO MELIÁ, M. *Los delitos de terrorismo: Estructura típica e injusto*. Ed. Reus, 2010. p. 260 y ss; NÚÑEZ CASTAÑO, E. Op. cit. p. 108 y ss; GÓMEZ MARTÍN, V. quien de hecho afirma que la existencia de dicha figura y su calificación como terrorista solo tiene un fundamento procesal, ya que permitía incrementar la pena de quienes cometen delitos con finalidades terroristas, sin tener que demostrar o acreditar su pertenencia a organización criminal. “Notas para un concepto funcional de terrorismo” cit. ant. p. 40 o GONZÁLEZ CUSSAC, J. L. quien sí se manifestaba favorable a considerar dicho delito como verdaderamente terrorista, en “El Derecho penal frente al terrorismo. Cuestiones y perspectivas”, en *Terrorismo y proceso penal acusatorio*, Ed. Tirant lo Blanch, Valencia, 2006. p. 73.

propias del moderno terrorismo⁷, llegándose, finalmente y tras la entrada en vigor del nuevo art. 573 CP, introducido por la LO 2/2015, a desdotar con carácter general a los delitos terroristas de la tradicional exigencia de la concurrencia en su realización del requisito estructural referido a su conexión con alguna de las citadas organizaciones o grupos, lo que, evidentemente, determinará que todo el peso de la mayor gravedad propia que se supone caracteriza a estos delitos pase ahora, precisamente, a recaer de forma exclusiva en las finalidades con que se realizan, agravándose aún más los problemas que su ya comentada y controvertida definición ampliada va a generar⁸.

Sorprende, sin embargo, que las peculiaridades que presenta la nueva forma de terrorismo de la que nos venimos ocupando no hayan movido ni un ápice al legislador de su afán punitivista frente a esta clase de delincuencia, viniendo, de hecho, la última reforma del Código penal realizada con respecto a esta materia a dar una vuelta de tuerca más en la aparente imparable espiral

⁷ En este sentido, ya destacaba CANCIO MELIÁ, M. que la reforma de estos conceptos realizada por la LO 5/2010 afirmaba en su propio preámbulo que la inclusión del vaporoso concepto de grupo terrorista quería atender a las peculiaridades de *“determinados grupos o células terroristas de relativamente reciente desarrollo en el plano internacional”*, lo que era criticado por dicho autor, por entender que en realidad, la propia jurisprudencia había demostrado que no existía problema alguno para perseguir y castiga estas nuevas formas de organización en red, mediante la utilización del concepto clásico de organización terrorista, En *“Delitos de organización”*, cit. ant. p. 660.

⁸ De este modo, señala el propio Preámbulo de la LO 2/2015 que el tratamiento jurídico penal tradicionalmente establecido para bandas armadas como los GRAPO o ETA se había articulado sobre el eje de la definición de organización o grupo terrorista, castigando a quienes se integraban en ellas o les prestaban algún tipo de colaboración, afirmando, sin embargo, que si bien *“El Código Penal no debe, en ningún caso, perder esa perspectiva de tipificación de las conductas articuladas en torno a organizaciones o grupos terroristas, (...) es evidente que las nuevas amenazas exigen la actualización de la normativa para dar cabida al fenómeno del terrorismo individual y a las conductas que constituyen la principal preocupación de la comunidad internacional, en línea con la Resolución 2178 del Consejo de Seguridad de Naciones Unidas anteriormente citada”*, lo que ha llevado a que la nueva definición de los delitos de terrorismo, contenida en el nuevo art. 573 CP, los delimite estableciendo que se tendrán por tales cualquier delito grave contra bienes tan esenciales, como la salud o la vida, entre otros, si se realiza con alguna de las finalidades que se mencionan en dicho artículo, sin exigir, por tanto que hubiesen de ser cometidos alguien que lo hiciese *“perteneciendo, actuando al servicio colaborando con organizaciones o grupos terroristas...”*, tal y como hacía la anterior definición de dichos delitos, contemplada en el art. 572 ACP. Es precisamente, por ello, por lo que autores como MUÑOZ CONDE, F. han pasado a afirmar de forma rotunda que, tras la reforma de 2015, el núcleo de la definición del terrorismo lo constituye el tipo subjetivo, es decir, que los delitos de los que se trate se realicen con los fines de los que habla el art. 573.1 CP. En *Derecho penal. Parte Especial*, (2015) cit. ant. p. 789. En la misma línea se manifiestan, por ejemplo, CANO PAÑOS., M. A. *“La reforma de los delitos de terrorismo”* cit. ant. p. 913 o CAMPO MORENO, J. C. quien señalaba que, si bien la innecesidad del elemento estructural u organizativo del terrorismo se ha asumido ahora por cuestiones puramente prácticas y utilitaristas, quedando incluso reflejada en el propio tenor literal del Pacto de Estado que dio lugar a la citada reforma, en realidad, no podía erigirse en elemento esencial de su definición, *Comentarios a la reforma del Código penal en materia de terrorismo: L.O. 2/2015*, Ed. Tirant lo Blanch, Valencia 2015, p. 14. Partidario, ya antes de la reforma, de la eliminación de la exigencia del denominado elemento estructural del terrorismo, se mostraba GONZÁLEZ CUSSAC, J. L. quien además destacaba como el propio art. 55 CE, que da pie a la especial regulación antiterrorista, habla tanto de bandas como de elementos terroristas, lo que se refiere claramente a personas individuales. *“Nuevas amenazas a la seguridad nacional: los desafíos del nuevo terrorismo”*, *Retos de la política criminal* actual. Revista Galega de Seguridad Pública, 9, 2007 p. 250.

intensificadora que tradicionalmente ha caracterizado a la política criminal seguida con la misma. Así, se ha procedido de nuevo a incrementar de forma general y, en ocasiones, manifiestamente desproporcionada las penas previstas para las actuaciones terroristas, -previendo incluso la aplicación de la muy cacareada y controvertida pena permanente revisable para los delitos de terrorismo que ocasionen una muerte en el nuevo art. 573 bis.1.1ª CP-⁹, mientras que, por otra parte, se ha vuelto a endurecer su régimen de ejecución¹⁰, pese a que, como ya hemos señalado, resulta evidente que ambas medidas no solo son preventivamente ineficaces frente a esta nueva hornada de terroristas, sino que pueden resultar incluso contraproducentes frente a los mismos, ya que, al permitir que se sancione a los autores de conductas realmente leves con penas severísimas y completamente desproporcionadas a su gravedad objetiva por el mero hecho de haberlas realizado para respaldar los fines que las caracterizan como terroristas, se puede llegar a que se haga aparecer a quienes las padezcan como verdaderas víctimas de un sistema injusto y draconiano que les castiga tan severamente, no por la gravedad de lo que hacen, sino por haberlo hecho para defender sus ideales, convirtiéndolos así en verdaderos “mártires” y ejemplos vivientes a seguir para aquellos que comparten sus ideas y su visión maniquea del mundo¹¹.

Esto carece de cualquier sentido desde un punto de vista preventivo y nos hace pensar que tras esta nueva vuelta de tuerca punitiva no se encuentra, en realidad, una verdadera pretensión preventivo general negativa, sino una puramente preventivo general positiva que trata de dar una “falsa sensación de seguridad” a la ciudadanía, o lo que es incluso peor una simple y burda manifestación del más puro y duro populismo punitivo que, como señala CANO PAÑOS, es el que posiblemente haya llevado al legislador a querer curarse en salud frente a las críticas que se le podrían dirigir si se producen atentados, para que nadie le pueda reprochar entonces que no hubiese

⁹ Véase, a este respecto, lo comentado, por ejemplo, por CANO PAÑOS., M. A. “La reforma de los delitos de terrorismo” cit. ant. p. 918 y ss o el mismo autor en “La Reforma penal de los delitos de terrorismo en el año 2015. Cinco cuestiones fundamentales” cit. ant. p. 12

¹⁰ Llamativo, a este respecto, es el especialmente severo régimen de acceso a la libertad condicional establecido para los terroristas en los art. 90. 8 y 92.2 CP, sobretodo si se pone en relación con lo establecido en los art. 78.2 y 78 bis. 3 CP, como señalan, por ejemplo, por MUÑOZ CONDE, F./ GARCÍA ARÁN, M. *Derecho penal. Parte General*. Ed. Tirant lo Blanch, Valencia, 2015. p. 627. Sobre el régimen general de acceso a la libertad condicional, véase, por ejemplo, lo comentado por BARQUÍN SANZ, J. “De las formas sustitutivas de la pena de prisión y de la libertad condicional”, en *Estudios sobre el Código penal reformado (Leyes Orgánicas 1/2015 y 2/2015)* Ed. Dykinson, Madrid, 2015. p. 255 y ss.

¹¹ En este sentido, señala CANCIO MELIÁ, M. que una de las estrategias del terrorismo es provocar las reacciones del Estado que le lleven a una escalada punitiva que dé pie a la rebelión popular, al tiempo que dé a los terroristas la condición de beligerante que le permita ampliar su influencia social, con lo que la escalada de dura represión ejercida por el poder contra los terroristas, termina convirtiéndolo en cómplice funcional de las pretensiones perseguidas por los terroristas. En “Terrorismo y Derecho penal: Sueño de la prevención, pesadilla del Estado de Derecho”, en *Política Criminal en vanguardia. Inmigración clandestina, terrorismo, criminalidad organizada*. Ed. Thomson-Civitas, Cizur Menor (Navarra), 2008, p. 316 y ss.

sido previamente lo suficientemente duro o no hubiese hecho todo lo que estaba en su mano para tratar de evitar que se llegasen a cometer¹².

Ahora bien, todo lo anterior no supone que el legislador no haya sido plenamente consciente de que las amenazas de penas de larga duración, por muy elevadas que sean, y el endurecimiento de su posible ejecución no resultan en modo alguno eficaces a la hora de prevenir y evitar los ataques que pueden realizar quienes constituyen el último eslabón del mecanismo terrorista *yihadista*, el que nos viene dado por quienes materialmente ejecutan los ataques terroristas incluso a costa de su propia vida.

De hecho, ha sido dicha consciencia legislativa la que ha llevado a que, por ejemplo, la reforma realizada por la LO 2/2015 en España, haya adelantado una vez más la posible intervención penal frente a las actuaciones que lo caracterizan, creando una serie de figuras de nuevo cuño, que tratan de neutralizar el fenómeno terrorista en sus más primigenias manifestaciones, para lo cual persiguen y reprimen las iniciales actuaciones de captación, adiestramiento y adoctrinamiento, tanto pasivo como activo, de futuros terroristas, en lo que supone un claro intento de prevenir los actos lesivos que dichos sujetos podrían llegar a realizar, una vez preparados y entrenados, antes siquiera de que comiencen a darles ejecución.

Ahora bien, para hacerlo, no basta con crear nuevas figuras delictivas que prevean el castigo de dichas conductas iniciales de terrorismo. También se requiere que se creen instrumentos de investigación y prevención que atiendan a las particularidades que presentan dichos comportamientos tan alejados del efectivo comienzo de la ejecución de ataques a los bienes jurídicos concretos y que además, atiendan al hecho de que muchas de tales conductas se realizan, a día de hoy, através de Internet. Unos instrumentos de investigación criminal que se han ido desarrollando en paralelo a la aparición de estas figuras, en muchas ocasiones, desde organismos inter- o supranacionales¹³, y que, como sucede con dichas figuras, pueden poner en cuestión muchos de los derechos más fundamentales de los ciudadanos en la red y fuera de ella.

¹² CANO PAÑOS., M. A. "La reforma de los delitos de terrorismo" cit. ant. p. 951.

¹³ Llama la atención en tal sentido, la imparable aprobación de instrumentos de cooperación policial y judicial desarrollados a lo largo de los años en la UE, precisamente como consecuencia y en muchos casos a resultas de la realización de atentados terroristas. Sobre este proceso, véase, por ejemplo, lo comentado por FERNÁNDEZ OGALLAR, B., *El Derecho penal armonizado de la Unión Europea*, Ed. Dykinson, Madrid, 2014, p. 338; AIXALA, A. quien diferencia dos etapas distintas. Una primera que iría desde el atentado del 11 de septiembre en Nueva York hasta el del 11 de marzo en Madrid, donde, a su modo de ver, se adoptó un impulso primordialmente político a las medidas de cooperación judicial y policial en la UE, y otro que comenzaría con este último atentado, en el que se produjo un desarrollo mucho más técnico y, a su modo ver, también eficaz.

Veamos a continuación cómo se han desarrollado estos instrumentos normativos, centrando nuestra atención en dos de los aspectos que, a nuestro juicio, más ponen en cuestión el respecto y las garantías de los ciudadanos. En concreto, en la concreta y compleja regulación de la captación y adoctrinamiento activo de terroristas y la referida a la utilización de datos como instrumento de investigación y prevención de delitos terroristas.

2.LA REPRESIÓN PENAL DE LA CAPTACIÓN Y EL ADOCTRINAMIENTO TERRORISTA Y SU COMPLEJO EQUILIBRIO CON EL RESPETO AL DERECHO A LA LIBERTAD DE EXPRESIÓN

Sin duda, la forma general de castigar a aquella persona que comunica a un tercero un mensaje dirigido a conseguir que éste se decida a cometer un delito terrorista, sea el que sea, será considerarle bien como inductor, bien como cómplice psíquico de dicho delito¹⁴, calificación que, sin embargo, requerirá que el autor al que se induce a cometer un delito, comience, cuando menos, a ejecutarlo.

Precisamente por ello y dado que uno de los objetivos primordiales de la política criminal en materia de terrorismo es, y siempre ha sido, el de hacer factible que el Derecho penal pueda prevenir la comisión de los gravísimos atentados propios de esta forma de criminalidad, interviniendo incluso antes que el tercero al que se incite o se instruya para cometerlos llegue siquiera a decidirse a dar comienzo a su ejecución, no puede sorprender que el legislador optase hace ya tiempo por castigar en relación a estos delitos las formas de participación intentada descritas en los artículos 17 y 18 CP; previsión que continúa manteniendo la última reforma y que se contiene en el actual artículo 579.3 CP, donde expresamente se prevé el castigo de la

En “La estrategia de la UE ante el terrorismo internacional y la defensa de los derechos y libertades”, pág. 51, en <http://www.recercat.cat/bitstream/handle/2072/204360/6%20cap%204.pdf?sequence=6>. (últ. vis., 10-12-2016). En relación con esta evolución y, en especial con los cada vez más variados y utilizados mecanismos supranacionales de intercambio de información, véase, por ejemplo, GALÁN MUÑOZ, A. “La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea”. LA LEY 4619/2014, p. 3 y ss, entre otros.

¹⁴ Sobre la concreta delimitación de ambas formas de participación intelectual en el delito ajeno, véase, por ejemplo, lo comentado por GÓMEZ RIVERO, M. C. *La inducción a cometer el delito*. Ed. Tirant lo Blanch, Valencia, 1995. p. 172 y ss.

provocación, la proposición y la conspiración de *“alguno de los delitos regulados en este capítulo”*.

Será, precisamente, este precepto el que permitirá, por ejemplo y atendiendo a lo establecido en el art. 18 CP, que el Derecho penal pueda sancionar como provocadores a quienes se dedican a utilizar Internet o cualquier medio de comunicación de masas para difundir contenidos que están directa y manifiestamente dirigidos a incitar a sus posibles receptores a cometer un delito terrorista aún cuando estos últimos sujetos, por los motivos que fuesen, no solo no comenzasen a ejecutarlo, sino que ni siquiera hubiesen llegado conocer o ser convencidos por el mensaje que trataba de motivarles para que lo realizasen¹⁵. Lo mismo sucederá con quienes simplemente realicen actuaciones incitadoras de forma pública o ante una concurrencia de personas conforme a lo establecido en el art. 18 CP, lo que nos hace pensar que carece de todo sentido que el nuevo apartado 2 del artículo 579 del Código penal haya venido expresamente a castigar de forma separada y con la misma pena prevista para la provocación, precisamente, a quien *“públicamente o ante una concurrencia de personas, incite a otros a la comisión de alguno de los delitos de este Capítulo”*, ya que al poder incardinarse tal conducta, por definición, en el concepto general de provocación resulta del todo innecesaria esta segunda y separada tipificación.

Ahora bien, algo diferente sucede, sin embargo y tras la última reforma realizada en España, con la otra conducta que el nuevo art. 579.2 CP contempla al final de su descripción. Esto es, con los casos en los que el sujeto solicite directamente a otro, esto es, a un destinatario individual y definido, que cometa un determinado delito terrorista.

Estos supuestos, a juicio de un importante sector doctrinal, podían ser castigados, antes de la reforma operada por la LO 1/2015, mediante la apreciación de la figura de la proposición que, como hemos visto, también sanciona el vigente art. 579 CP en su tercer apartado, ya que consideraban que dicha forma de codelincuencia intentada, definida en el entonces vigente art. 17 ACP, castigaba precisamente a quien realizase una conducta dolosa de inducción idónea dirigida a convencer a su destinatario individual para que cometiese un concreto delito que, sin embargo,

¹⁵ En este sentido, señalaba BERNAL DEL CASTILLO, J. que la previsión de la provocación respecto a delitos terroristas determinaba que *“...cualquier mensaje o consigna que implique una incitación directa a un delito de terrorismo no seguido de su comisión ya está contemplado en el definición de la provocación”*, en *“Una visión crítica del nuevo delito de provocación al terrorismo del art. 579.1”* RDP nº 33, 2011, p. 70. Sobre los requisitos y límites de la provocación como forma de participación intentada, véase, lo comentado, por ejemplo, por REBOLLO VARGAS, R. *La provocación y la apología en el nuevo Código penal*. Ed. Tirant lo Blanch, Valencia, 1997, p. 78 y ss o BARBER BURRUSCO, S. *Los actos preparatorios del delito*. Ed. Comares, Granada, 2004, p. 238 y ss, entre otros.

no comenzase a ejecutar por parte de dicho sujeto¹⁶; postura que, no obstante, contrastaba con la sostenida por quienes señalaban que la comentada descripción general de la proposición, en realidad, solo permitiría castigar a quien estando decidido a cometer un delito por sí mismo, -lo que lo convertiría en su verdadero dominador o autor cuando lo comenzase a realizar-, incitaba a otro a ejecutarlo junto a él, actuando, por tanto, este último sujeto, en caso de aceptar la propuesta, como mero partícipe o, todo lo más, como coautor del delito en cuestión cuando se llevase a cabo¹⁷, algo que evidentemente dejaría al margen de esta forma de codelincuencia intentada a las actuaciones meramente preparatorias de la inducción individual de las que habla el nuevo art. 579.2 CP in fine.

Precisamente esta última y más restrictiva interpretación es la que, a nuestro modo de ver, ha encontrado definitivo respaldo por parte del legislador tras la reforma del artículo 17 CP realizada por la LO 1/2015, ya que, al establecer la misma que habrá proposición “...*cuando el que ha resuelto cometer un delito invita a otra u otras persona **a participar en él***” y no, como hacía su anterior versión, cuando quien estando “...*resuelto cometer un delito invita a otra u otras personas **a ejecutarlo***”, se deja definitivamente claro que solo podrá considerarse y castigarse como propositor a quien, estando decidido a cometer por sí mismo un delito invita (no incita) a otros, no a que lo ejecuten, sino a que simplemente se unan o “participen” en su realización, esto es, a que le ayuden a cometer el delito que él pretendía efectuar directamente, actuando, por tanto, como su verdadero dominador y autor¹⁸.

¹⁶ BARBER BURRUSCO, S. Op. cit. ant. p. 206.

¹⁷ Así, por ejemplo, REBOLLO VARGAS, R. quien consideraba que “*al admitir que el proponente está resuelto a intervenir con actos ejecutivos descartamos implícitamente la opción de que en el seno de la proposición tenga cabida la inducción intentada, ya que es inherente a la condición de inductor que éste no sea autor, es decir, que no tome parte directa en la ejecución del hecho*”, lo que le llevaba a considerar que la proposición en realidad no era sino una suerte de invitación a la conspiración, luego una propuesta de coautoría, que a diferencia de la conspiración no es aceptada por sus destinatarios. En Op. cit. ant. p. 51 y ss. También se decanta por esta visión restrictiva, por ejemplo, CAMPO MORENO, J. C. *Los actos preparatorios punibles*. Ed. Tirant lo Blanch., Valencia, 2000, p. 51 y ss.

¹⁸ De otra opinión, sin embargo, MIR PUIG, S. quien, pese al cambio legislativo producido, sigue manteniendo que la proposición continúa castigando “*la inducción no seguida de ejecución*”, ya que considera que al castigar el vigente art. 28 CP como autor de un delito no solo a quienes lo ejecutan o realizan, sino también a quienes ayudan necesariamente o inducen a otros a ejecutarlo, habrá que continuar entendiendo que haber resuelto cometer un delito, tal y como exige el art. 17.2 CP al propositor, no supone tener que querer ejecutarlo como autor, dado que cometer el delito significa algo más amplio que ejecutarlo. *Derecho penal. Parte General*. Ed. Reppertor, Barcelona, 2015. p. 353. Esto supone, a nuestro modo de ver, olvidar que, en realidad, lo que ha cambiado en la nueva redacción del art. 17.2 CP no es la exigencia de que el propositor quiera tomar parte en la comisión delictiva, sino el hecho de que exija que dicho sujeto tenga que invitar a terceras personas a “participar” en el delito que va a cometer y no que les invite “a ejecutarlo” como hacía antes. Con ello, se reduce la proposición a aquellos actos en los que la contribución que se pretende obtener de su destinatario sea siempre accesoria o, todo lo más, coadyuvante de aquella que pretendía efectuar directamente quien

Ello supone que el expreso castigo de la proposición contenido en el art. 579.3 CP no pueda ser ya utilizado, bajo ningún concepto, para perseguir y sancionar penalmente a quienes realicen actos no exitosos de mera inducción individual o personal de los delitos de terrorismo, sin intención alguna de convertirse en autores o coautores de los mismos, con lo que cobra pleno sentido que el legislador haya decidido castigar de forma expresa la ejecución de las actuaciones meramente incitadoras personales o individuales e intentadas en el apartado 2 del referido artículo, para evitar así que dicho tipo de peligrosas actuaciones se mantengan en el ámbito de lo penalmente irrelevante, por lo menos, mientras aquel al que se dirijan, (el solicitado), no comience a efectuar el delito que se le pidió que cometiese.

Ahora bien, el empeño del legislador en castigar los meros intentos de incitar a terceros para que cometan delitos terroristas no terminó aquí, sino que también le llevó a incluir en el primer apartado del artículo que venimos comentando la posibilidad de que se pueda llegar a castigar con las mismas penas que a los propositores, a los provocadores o a los meros inductores individuales intentados de los que habla el art. 579.2 *in fine* CP, a quien “...por cualquier medio, difunda públicamente mensajes o consignas que tengan como finalidad o que, por su contenido, sean idóneos para incitar a otros a la comisión de alguno de los delitos de este Capítulo”.

Nos encontramos ante un precepto que castigará tanto la difusión pública de mensajes o contenidos que tengan por “finalidad”, la de incitar a sus destinatarios a cometer algún delito de terrorismo, esto es, que estén orientados o dirigidos por quien los publica a producir dicho resultado en tales sujetos y se hayan difundido, por tanto, con un dolo que abarcará la comisión por su parte del delito que pretendían incitar, como la de aquellos otros que simplemente se manifiesten como idóneos para que sus receptores se decidan a efectuarlo, expresión esta última que indudablemente abrirá las puertas a que esta figura pueda también castigar a quien difunda cualquier mensaje que resulte objetivamente adecuado, desde un punto de vista *ex ante*, para generar la idea en quienes lo reciban de cometer algún delito terrorista y lo haga teniendo conocimiento de tal cualidad del contenido, aunque no pretendan dar lugar con su publicación a la comisión del delito en cuestión por parte de sus posibles destinatarios. Esto es, aunque lo haya publicado sin actuar con la finalidad o dolo directo de inducir a un tercero a cometer un delito

proponía realizar el delito, con lo que se obliga a éste (al propositor) a tener que actuar con intención de cometer el delito actuando como su autor o, cuando menos, como coautor y no como un simple inductor, produciéndose así precisamente aquella restricción referida al papel del destinatario de la proposición que el propio MIR PUIG decía que faltaba en la versión anterior a la reforma de esta forma de participación intentada, para excluir de su posible ámbito de aplicación a las meras inducciones intentadas (que castigase al que invitase a “tomar parte en la ejecución”, esto es, a participar y no a ejecutar como hacía el anterior texto del art. 17 CP), en *Derecho penal. Parte General*. Ed. Reppertor, Barcelona, 2002. p. 337.

terrorista, pero sí con un dolo que abarcase la idoneidad del contenido para poder llegar a hacerlo¹⁹.

La ampliación típica que la redacción de esta figura conlleva con respecto a la tradicional delimitación de la provocación, es tan evidente como cuestionable.

Lo es, a primera vista, porque, al no exigir el nuevo art. 579.1 CP que los mensajes o consignas publicados tengan que incitar directamente, esto es, de forma clara y manifiesta, a cometer algún delito, como exigiría la inducción o la provocación²⁰, sino castigar la publicación de cualquier contenido que tenga por finalidad o resulte idóneo para incitar a sus receptores a cometerlos, se permite que esta figura pueda sancionar la distribución de contenidos que busquen tal resultado o presenten dicha peligrosidad, aún cuando lo hagan de forma indirecta o implícita, lo que, sin duda, difuminará de forma notable los caracteres que tradicionalmente habían delimitado a los mensajes incitadores penalmente relevantes. En tal sentido, resulta evidente que

¹⁹ Esto último contrasta con el dolo exigido por la inducción, como forma de participación delictiva general que, tal y como señalan GÓMEZ RIVERO, C., aunque sea eventual, tendrá que abarcar y tener un doble objeto de referencia. Por una parte, el nacimiento de la resolución delictiva en el autor inducido y por otra, no solo la realización por parte de este último sujeto del delito que se le quería incitar a realizar, sino la consumación de dicho delito, en *La inducción a cometer el delito*. Ed. Tirant lo Blanch, Valencia, 1995, p. 402 y ss; dolo que a nuestro modo de ver, también habrá de darse en la provocación del art. 18 CP, para poder apreciarla, ya que, entre otras cosas, solo así se entenderá, a nuestro juicio, que el segundo apartado *in fine* del comentado precepto afirme que la provocación de un delito seguida de su perpetración se castigará como inducción, lo que evidentemente requeriría que dicho resultado haya sido abarcado por el dolo del provocador que vaya a responder de él.

²⁰ De hecho, y como señala BERNAL DEL CASTILLO, J. la Exposición de Motivos de la LO 5/2010 que vino a introducir la figura predecesora de la que venimos comentando, precisamente afirmaba que la misma estaría referida a mensajes o consignas que no necesariamente consistiesen en “resoluciones manifestadas de delito” Op. cit. ant. p.70, lo que se corresponde perfectamente con que este precepto no aluda a mensajes “directamente” incitadores, sino que tengan la finalidad o sean idóneos para incitar a cometer algún delito terrorista. Sobre la concreta interpretación de lo que debería entenderse por la expresión “directamente” utilizada tanto por la definición general de la inducción del art. 28 CP, como por la de la provocación del art. 18 CP, existe una viva polémica doctrinal, considerando algunos autores que la inclusión del comentado adverbio en el primero de los referidos preceptos supone la exigencia de que el contenido o mensaje incitador del inductor se dirija de forma personal del mismo al autor, como hacía GÓMEZ RIVERO, C. en relación a la regulación de la inducción y la provocación previa al CP de 1995, en Op. cit. ant. p. 114 o hace con respecto al actual MUÑOZ CONDE, F./ GARCÍA ARÁN, M. *Derecho penal. Parte General*. cit. ant. p. 472, mientras que otros, como REBOLLO VARGAS, R. Op. cit. ant. p. 90; BARBER BURUSCO, S. Op. cit. ant. p. 252. entendían en relación con los actos de provocación del art. 18 CP que por definición se realizarán a través de medios de comunicación masivos y, por tanto, no de forma personal o privada, que dicha expresión excluirá de dichos comportamientos penalmente relevantes a las incitaciones vagas, imprecisas o indefinidas; postura está que consideramos la más acertada y que también debe predicarse con respecto a la inducción, lo que dotará de coherencia a la utilización del referido adverbio en ambos preceptos, pero además y por lo que a nosotros concierne, hará que cobre pleno sentido la introducción de un precepto como el que venimos analizado, el contenido en el art. 579.1 CP, que vendría a castigar precisamente la difusión de contenidos idóneos para incitar a sus destinatarios a cometer delitos, pero que, como ya hemos señalado, y a diferencia de los que castiga la provocación propiamente dicha, no tendrán que ser clara y expresamente incitadores a la comisión de delitos.

un mismo mensaje que no promueva de forma directa, manifiesta o explícita a cometer delitos de terrorismo, podrá, sin embargo, considerarse idóneo para alcanzar dicho fin y podrá incluso utilizarse con la intención de inducir a cometerlos dependiendo de factores tales como el momento en que se produzca su publicación o cuáles pudiesen ser, en concreto, sus destinatarios, dado que, sin duda, no es indiferente para valorar la peligrosidad o idoneidad inductora que, por ejemplo, podría tener un mensaje radicalmente crítico con el Estado o con sus cuerpos y fuerzas de seguridad si se difunde cuando dichas instituciones acaban de realizar o se encuentran insertas en una controvertida operación militar y se dirige a quien comparte y apoya los ideales sostenidos o medios utilizados por los que promueven la “guerra santa” contra las mismas, que si se difunde en un contexto histórico diferente y se destina a quien no solo no los comparte, sino que los rechaza de forma tajante.

La indeterminación típica que ello genera cuando hablamos de mensajes difundidos de forma pública, como son todos aquellos de los que se ocupa el art. 579.1 CP, es indudable.²¹ Así, por ejemplo, ¿cuál de los posibles destinatarios del mensaje habrá de servir para fijar la peligrosidad o idoneidad inductora que lo convertiría en típicamente relevante? ¿Habrá que tomar como parámetro al “hombre medio”? ¿O, por contrario, habrá que entender que, precisamente, por encontrarnos ante actos de distribución o difusión pública, tendrá que partirse de que siempre podrá haber entre sus posibles destinatarios alguno de los que resultan especialmente sensibles a su mensaje incitador?

Podría pensarse que, en realidad y tal y como afirmaba algún autor en nuestra doctrina con relación a la versión previa del precepto del que nos venimos ocupando²², la amplia redacción dada al mismo por nuestro legislador solo trataría de dar respuesta a la exigencia comunitaria introducida en el artículo 3 de la Decisión Marco 2002/475/JAI por la modificación que del mismo hizo la posterior Decisión Marco 2008/919/JAI, que obligaba a todos los Estados miembros de la Unión Europea a castigar la provocación como delito ligado a actividades terroristas, entendiendo como tal “...la distribución o difusión pública, por cualquier medio, de mensajes destinados a inducir a la comisión de cualesquiera de los delitos enumerados en el artículo 1, apartado 1, letras a) a h), cuando dicha conducta, **independientemente de que promueva o no directamente la**

²¹ En similares términos CANO PAÑOS., M. A. “La reforma de los delitos de terrorismo” cit. ant. p. 945. Críticos con la anterior redacción de este precepto también se mostraban CANCIO MELIÁ, M. calificando la tipificación de lo que denominaba como “delito de propaganda” de “vaporosa y lesiva con el principio de legalidad”, En “Delitos de organización”, cit. ant. p. 665 y BERNAL DEL CASTILLO, J. quien la tildaba de inconstitucional por entender que su indeterminación típica era incompatible con los principios de seguridad jurídica y el principio de legalidad penal. Op. cit. ant. p. 72.

²² BERNAL DEL CASTILLO, J. Op. cit. ant. p.68.

comisión de delitos de terrorismo, **conlleve el riesgo de comisión de uno o algunos de dichos delitos**”, lo que, como bien señaló en su día BERNAL DEL CASTILLO dejaba muy claro que la provocación que todos los Estados debían castigar “...se trata de una conducta dolosa, destinada a inducir a uno de los delitos de terrorismo, independientemente de que promueva o no directamente la comisión de delitos concretos, siempre y cuando conlleve el riesgo de comisión de uno o de algunos de dichos delitos”²³.

Sin embargo esta posible interpretación todavía ampliaría más el número de preguntas referidas a este precepto dotadas de una difícil respuesta.

Así, por ejemplo, si la idoneidad inductora del mensaje típico del art. 579.1 CP puede estar referida, tal y como parece exigir la recoger la comentada Decisión Marco, a la incitación general a cometer delitos terroristas y no necesariamente a uno de ellos concreto y determinado, ¿cómo podremos valorar su existencia teniendo un referente tan amplio y variado como el que nos fijan los muy variopintos delitos de terrorismo? Y por otra parte ¿qué pasará entonces cuando el contenido pueda ser idóneo desde un punto de vista *ex ante* para incitar a cometer un grupo determinado de delitos terroristas (p. ej. unos daños y unas lesiones) y quien lo difunda abarque en su dolo dicho riesgo? ¿Tendremos que considerar que ha efectuado un único delito de difusión pública de mensajes terroristas del art. 579.1 CP, como parecía indicar la redacción del precepto comunitario en el que parece tener origen, o habrá de entenderse, por el contrario, que se debería condenar a su difusor de forma separada por cada una de las incitaciones a cada uno de los concretos actos delictivos que podría llegar a generar?

Hay que señalar frente a todas estas cuestiones que, si bien es perfectamente posible que al introducir el precepto que precedió al ahora comentado en la reforma penal realizada en el año 2010 (el contenido en el anterior art. 579.1. segundo párrafo CP), el legislador buscase, precisamente, atender a lo exigido por la referida Decisión Marco, abriendo así las puertas a que nuestro sistema penal pudiese castigar los actos públicos de incitación indirecta, (es decir, no expresa o clara, sino implícita o no manifiesta), y genérica, (esto es, orientados o adecuados para fomentar la comisión de cualquiera delito terrorista en general), resulta incuestionable que tras la modificación realizada sobre la comentada figura por la LO 2/2015, su previsión solo podrá cumplir ya parcialmente con tal cometido, dado que, si bien podrá continuar castigando los actos de incitación pública no manifiesta o directamente dirigidos a incitar a cometer un delito terrorista, pero que se difundan con la finalidad o resulten idóneos para incitarlo, no podrá hacerlo, sin

²³ BERNAL DEL CASTILLO, J. Op. cit. ant. p. 67.

embargo, con los que tiendan a provocar la comisión de delitos terroristas en general, puesto que, al determinar la nueva redacción del art. 579.1 CP que el mensaje difundido tiene que tender o ser idóneo “*para incitar a terceros a la comisión alguno de los delitos terroristas*” y no de “*cualquiera*” de ellos, como hacía su predecesor y establecer, además, la pena que le habría de imponer a quien lo difundiese, atendiendo a la que le habría de corresponder al concreto delito terrorista que su actuación tendiese o pudiese llegar a incitar y no de forma completamente independiente a dichas figuras, como hacía aquél, se deja completamente claro que nos encontramos ante un precepto que solo castigará actuaciones accesorias, dependientes y, por tanto, claramente preparatorias de un concreto y determinado delito terrorista.

No bastará, por tanto, con que se publiquen mensajes que creen una abstracta situación o clima que podría llevar a sus receptores a decidirse a cometer uno o varios delitos terroristas todavía no determinados, para poder apreciar este delito²⁴. Para hacerlo será necesario además que el mensaje difundido, por más que no suponga la directa y expresa propuesta de cometer un delito concreto, sí incremente el riesgo, desde un punto de vista *ex ante*, de que alguno de sus posibles destinatarios pueda decidirse a realizar un determinado y predecible delito terrorista, lo que tendrá dos importantes efectos con respecto a los problemas anteriormente planteados

Por una parte, y en primer lugar, delimitará los mensajes o contenidos cuya difusión o publicación podrá ser castigada por esta figura, ya que, al exigirse que éstos tengan que estar dirigidos o ser idóneos para dar lugar a la realización de un concreto y definido delito terrorista, excluirá de su ámbito típico a todos aquellos mensajes que, por muy radicales, rechazables o incendiarios que puedan resultar no resulten previsiblemente adecuados para poder generar la comisión de un delito terrorista concreto y determinable en el mismo momento en que se publicaron. No bastará, por tanto, con las incitaciones genéricas a “luchar contra el Estado” o a “combatir a los opresores”; mensajes que, si bien pueden generar un riesgo genérico de producción de delitos terroristas, en la mayoría de los casos no permitirán pronosticar, desde un punto de vista *ex ante*, qué concreto delito podrían llegar a provocar.

²⁴ En esto se diferencia claramente la nueva configuración típica de esta figura de su anterior delimitación, ya que, al exigir el art. 579.1 CP que el mensaje o consigna difundido tenga por finalidad o sea objetivamente idóneo para inducir a cometer aquel delito terrorista que establecerá el marco punitivo desde el que se determinará la pena aplicable a quien realice su publicación, ya no bastará para poder apreciar su comisión con que el mensaje en cuestión conlleve el riesgo de generar un caldo de cultivo adecuado para dar lugar a la comisión de delitos de terrorismo en general, como señalaba BERNAL DEL CASTILLO, J. con respecto a la anterior redacción de este precepto Op. cit. ant. p. 70, sino que será necesario que se produzca una publicación que esté conectada objetiva y subjetivamente con la realización de un acto terrorista futuro, concreto y determinado.

Para apreciar el art. 579.1 CP la publicación realizada tendrá que recaer sobre un mensaje que, por ejemplo, tras una intervención policial con víctimas mortales entre los terroristas, dijese que habría que *“hacer sentir a quien la realizó el mismo dolor que habían ocasionado con su ataque”*; mensaje éste que, por más que no contenga una propuesta directa, manifiesta o expresa de cometer un delito de homicidio terroristas contra el policía en cuestión, como exigiría la provocación, sí que incrementará de forma pronosticable y previsible el riesgo de comisión de tal delito y no de cualquier otro posible delito terrorista, lo que permitirá que la figura ahora analizada pueda castigar a quien lo publique tanto si lo hace con intención de incitar a cometer dicho homicidio, como si lo hubiese hecho sin tal finalidad o no se pudiese demostrar que lo había hecho con la misma, pero sí que había sido plenamente consciente de que su mensaje podría llegar a incitar a sus destinatarios a cometerlo.

Pero además y en segundo lugar, el hecho de que el injusto propio de la figura actualmente analizada solo contemple y castigue las conductas comunicativas generadoras del peligro de comisión de un único, pronosticable y concreto delito terrorista y no de un grupo indeterminado o numeroso de ellos, también llevará a que si el mensaje publicado tendiese o fuese idóneo para dar lugar a la realización acumulada y no alternativa por parte de sus destinatarios de varios de dichos delitos perfectamente predecibles y definidos y fuese, además, publicado por alguien que abarcase en su dolo dicha circunstancia²⁵, se le tenga que responsabilizar por tantas incitaciones delictivas del art. 579.1 CP como delitos terroristas concretos podría y sabría o querría llegar a generar con su actuación, mediante la apreciación del correspondiente concurso ideal de delitos entre las incitaciones de cada uno de dichos delitos terroristas.

Habrà que considerar, por tanto, que, si bien el comentado precepto del Código penal puede servir para castigar las incitaciones indirectas, implícitas o no manifiestas de las que hablaba el art. 3 la modificada Decisión Marco 2002/475/JAI, tanto si se realizan con el fin de incitar a cometer un delito terrorista, como si se hacen simplemente teniendo conocimiento de que la conducta efectuada era adecuada para producirlo, no podrá, sin embargo, hacerlo con los actos de incitación genérica que dicha disposición comunitaria también obligaba a sancionar.

²⁵ Respecto a la diferencia entre este dolo que podríamos denominar como “dolo acumulativo” y el “dolo alternativo” y las implicaciones concursales de la apreciación de uno u otro en la realización de un hecho delictivo, véase, lo comentado por GALÁN MUÑOZ, A. *“El Denominado “Dolo Alternativo”: Un caso entre el concurso de leyes y el de Delitos*. En Problemas actuales del Derecho penal y la criminología. Estudios penales en memoria de la Profesora Dra. Maria del Mar Díaz Pita. Ed. Tirant lo Blanch. Valencia, 2008, p. 279 y ss.

Podría pensarse, sin embargo, que esto se debe a que, en realidad, el Código penal español contempla desde hace tiempo una figura que podría castigar algunos de las más graves manifestaciones de incitación genérica indirecta a cometer delitos de terrorismo. Se trata, en concreto, del delito de enaltecimiento o justificación públicos de los delitos de terrorismo contenido en el art. 578 CP; una figura que, a juicio de algunos autores, no describe ni sanciona una simple modalidad específica de la apología del art. 18 CP, -lo que llevaría a que solo castigase actos constitutivos de una provocación, esto es, de incitaciones públicas directas e intentadas a cometer delitos concretos²⁶-, sino que habría introducido en nuestro ordenamiento un verdadero “delito de clima” que sancionaría la difusión de las ideas que generen un entorno social de hostilidad hacia determinados colectivos, instituciones o personas, que podría llevar a que quienes reciban dichos mensajes de odio y vivan en dicho entorno se decidiesen a realizar cualquier clase de delito terrorista contra las mismas, por más que no les induzca expresamente a ejecutarlos ni se pueda siquiera predecir, cuando se realiza su difusión, cuál de dichas figuras en concreto podría llegar a provocar²⁷.

Sin embargo, pese a que esta controvertida opción interpretativa sigue abierta y parece haberse visto incluso respaldada por la aceptación por parte de nuestro Tribunal Constitucional de la existencia y constitucionalidad de los denominados “delitos de clima” en alguna no muy lejana sentencia referida a otras figuras de expresión²⁸, no parece que ello haya satisfecho plenamente al legislador en su empeño por sancionar los actos de incitación terrorista generales e indirectos.

²⁶ A favor de esta restrictiva interpretación, se manifiesta, sin embargo, por ejemplo, NÚÑEZ CASTAÑO, E. Op. cit. ant. p.170.

²⁷ En este sentido, señala CAMPO MORENO, J. C., citando la STS nº 481/2014 de 3 de junio, que, mientras la apología del art. 18 CP exige la invitación directa a cometer un delito concreto, el enaltecimiento o justificación del terrorismo del art. 578 CP “*constituye una forma autónoma de apología caracterizada por su naturaleza genérica, sin integrar una provocación ni directa ni indirecta a la comisión de un delito concreto*”, en *Comentarios a la reforma del Código penal* cit. ant. p. 71; postura coincidente con la sostenida por MANJÓN CABEZA, A. cuando señalaba que el comentado delito “*tipifica un comportamiento apologético, que no requiere incitación directa ni indirecta, que no es un acto preparatorio, que no es provocación, que no se castiga por el peligro ni siquiera abstracto para un bien jurídico siquiera de referencia de los delitos de terrorismo, que tiene naturaleza de delito autónomo (...) y que tiene una pena propia*”, en “*Apología del terrorismo*”, en *Estudios penales en recuerdo del profesor Ruiz Antón*, Ed. Tirant lo Blanch, 2004, p. 580; afirmando también RAMOS VÁZQUEZ, J. A. que no se podría considerar que dicho delito requiera realmente de una provocación directa al delito tal y como exige el art. 18 CP, ya que ello contrariaría el propio tenor del comentado precepto así como la finalidad con la que se creó. En “*Presente y futuro del delito de enaltecimiento y justificación del terrorismo*”, en *AFCUC*, 12, 2008. 784. En términos similares, se manifiesta MUÑOZ CONDE, F. quien precisamente entiende que, al no atenerse el comentado precepto, en su modalidad de enaltecimiento o justificación del terrorismo, a los límites del art. 18 CP, su existencia plantearía serias dudas de constitucionalidad. En Op. cit. ant. p. 789.

²⁸ En concreto, se trata de la Sentencia del Tribunal Constitucional de 7 de noviembre de 2007, relativa a la constitucionalidad del delito de negacionismo y justificación del genocidio del, en aquel entonces vigente, art. 607 CP; sentencia en la que, si bien se declaró la inconstitucionalidad del castigo del negacionismo como tal, sí

Así lo demuestra, a nuestro modo de ver, el hecho de que el delito de colaboración terrorista además de castigar la mera organización de prácticas de entrenamiento terrorista (art. 577.1 CP) o la captación de futuros terroristas o su adiestramiento (art. 577.2 CP), haya pasado, tras la reforma realizada por la LO 2/2015, también a sancionar tanto las conductas de adoctrinamiento que estén “dirigidas” a incitar a cometer cualquier delito terrorista, que ya castigaba la versión anterior de este delito, como la que **“... por su contenido, resulte idónea para incitar a incorporarse a una organización o grupo terrorista, o para cometer cualquiera de los delitos comprendidos en este Capítulo”**, lo que, a nuestro entender, determinará que nos encontremos, ahora sí, ante una figura especialmente adecuada para poder llegar a sancionar los actos de incitación implícita o indirecta y meramente genérica a cometer delitos terroristas de los que hablaba la Decisión Marco anteriormente citada.

Así lo indica, a nuestro juicio, no solo el hecho de que el comentado precepto castigue tras la reforma los actos adoctrinadores que se dirijan o que simplemente resulten idóneos para incitar a efectuar “cualquier” delito terrorista y no “alguno” de ellos, como, por ejemplo, hacían las anteriormente comentadas conductas incitadoras indirectas o implícitas de delitos concretos castigadas en el ya comentado art. 579.1. CP, sino también y especialmente, el que el delito de colaboración terrorista en general sea una figura que castiga el suministro, por parte de personas no integradas en una organización o grupo terrorista²⁹, de ayudas o contribuciones genéricas a

que se admitió la compatibilidad con la Carta magna de aquella parte del comentado delito que castigaba la justificación del delito de genocidio, precisamente porque la manifestación acorde o la valoración positiva de su realización presenta un elemento tendencial de creación de un clima social de hostilidad que podría incitar indirectamente a la comisión de tan odioso delito; delimitación que, por ejemplo, a juicio de RAMOS VÁZQUEZ, J. A. podría transponerse al delito de enaltecimiento y justificación del terrorismo, convirtiéndolo en un delito de clima que indirectamente incitaría a cometer delitos de dicha naturaleza, en Op. cit. ant. p. 788 y ss y 799 y ss. Sobre el origen y desarrollo de esta corriente jurisprudencial que hunde sus raíces en la evolución de la jurisprudencia emanada del Tribunal Europeo de Derechos Humanos y, en concreto de la interpretación que dicho Tribunal ha realizado del art. 10 del CEDH en relación con el art. 17 de dicho convenio, para permitir la prohibición de los discursos de odio, véase, RODRÍGUEZ MONTAÑÉS, T. *Libertad de expresión, discurso extremo y Delito. Una aproximación desde la constitución a las fronteras del derecho penal*. Ed. Tirant lo Blanch, Valencia, 2011, p. 221 y ss. Sobre el origen dogmático de esta categoría de delitos y su posible aplicación a otros delitos de nuestro Código penal, como el contenido en el art. 510 CP, véase, lo comentado por GÓMEZ MARTÍN, V. “Discurso del odio y principio del hecho” en *Protección penal de la libertad de expresión e información. Una interpretación constitucional*. Ed. Tirant lo Blanch, Valencia, 2012, p. 89 y ss.

²⁹ De hecho, CANCIO MELIÁ, M. señalaba con relación a la anterior redacción de este precepto que el mismo parecía olvidar que, generalmente, las labores de adoctrinamiento y captación se suelen realizar por miembros de la organización y, por tanto, están ya perfectamente tipificadas y castigadas por los delitos de pertenencia a los mismos que tiene preferente aplicación, con lo que su expresa calificación como colaboración terroristas tiene escasa utilidad. En “Delitos de organización”, cit. ant. p. 661. De hecho, el referido autor señalaba que la práctica judicial relativa al delito de pertenencia a organización terrorista había precisamente considerado como una de las actividades que permitían apreciar su realización la de “...convencer a otros para realizar la yihad, esto es, el adoctrinamiento en el fundamentalismo islámico”, en “El delito de pertenencia a una

cometer delitos de dicha naturaleza y no las ayudas puntuales que simplemente tiendan a facilitar la comisión de uno o varios de ellos en concreto³⁰.

Este hecho convertiría al delito de colaboración terrorista en un delito de peligro abstracto completamente autónomo del resto de figuras de terrorismo, como lo demuestra el hecho de que castigue a quien cometa cualquiera de sus muy variopintas modalidades comisivas con una pena propia (de 5 a 10 años de prisión) completamente independiente de la establecida para la autoría o participación en el resto de dichos delitos. Un delito que, al contemplar expresamente entre sus posibles modalidades comisivas a los actos adoctrinadores que implícita o indirectamente puedan incitar a cometer delitos terroristas en general, permitirá que el ordenamiento penal español pueda finalmente responder a las exigencias incriminadoras europeas de las nuevas formas de provocación terrorista, haciendo factible que pueda castigar la difusión o transmisión del discurso del odio que caracteriza y tan buenos resultados está dando al terrorismo yihadista y que, además de no contener siempre una incitación manifiesta o clara a cometer delitos, en muchas ocasiones, ni siquiera se realiza de una forma que pueda considerarse como dirigida ni idónea, desde un punto de vista *ex ante*, para incitar a la comisión de delitos terroristas concretos y determinados, sino para fomentar la genérica e indeterminada realización de cualquiera de ellos en el futuro.

Ahora bien, no todo son luces en este precepto. De hecho, los problemas y cuestiones que su amplia redacción viene a plantear proyectan una larga y oscura sombra de duda sobre la posible legitimidad de su existencia y especialmente sobre su posible compatibilidad con el debido

organización terrorista en el Código penal español”, en *Derecho penal* del Estado social y democrático de Derecho. Ed. La Ley. Madrid, 2010. p. 1004. En la misma línea, señalaba GARCÍA ALBERO, R. que incluso “...en el improbable supuesto de que la organización decidiese “externalizar” sus servicios de captación adiestramiento y formación “*tertium no datur*”, tanto si la prestación de tales servicios se encomienda a un grupo de personas como a una sola, entonces o el grupo resultaría ser en sí mismo “organización o terrorista” (...) o bien la persona –el captador o adiestrador- individual habría de considerarla necesariamente como integrante, directamente de aquel grupo. Sólo queda entonces como hipótesis, una intervención puntual o episódica en tareas de captación, adiestramiento o formación”. En *Comentarios a la Parte Especial del Derecho penal*. Aranzadi. Cizur Menor (Navarra), 2011, p. 2260. El carácter completamente residual y excepcional de la aplicación de este precepto respecto a los actos de captación y adoctrinamiento frente a los delitos de integración en grupo u organización terrorista queda de manifiesto en las todavía escasas sentencias que han recaído sobre conductas de captación y adoctrinamiento de yihadista, como sería, por ejemplo, la Sentencia num. 789/2014 de 2 diciembre del Tribunal Supremo, referida a la condena del conocido como “Bibliotecario de AlQaeda”, o la todavía más reciente Sentencia, 23/2015, de 30 de septiembre, de la Audiencia Nacional que condenó a una célula de captación y reclutamiento de combatientes yihadistas en Ceuta, para la guerra que se viene desarrollando en Iraq y Siria.

³⁰ En este sentido, ya señalaba NÚÑEZ CASTAÑO, E. en relación a la anterior redacción de este delito, que la colaboración propia del mismo “*debe ser genérica, es decir no vinculada a una actividad concreta sino que conste en un apoyo genérico...*” mientras que “...si este apoyo material se concreta en una determinada conducta delictiva, la colaboración cede ante la coautoría o la complicidad”. En Op. cit. ant. p. 145; postura que también comparte, entre otros, GARCÍA ALBERO, R. Op. cit. ant. p. 2249.

respeto a alguno de los derechos fundamentales que todo verdadero Estado de Derecho debe respetar.

Así, por ejemplo y en primer lugar, parece evidente que el hecho de que esta figura convierta en autor de un delito completamente autónomo del resto de los terroristas a quien sería, todo lo más, un mero favorecedor o incitador ideológico genérico de los delitos que otro podría llegar a cometer en el futuro como consecuencia de su actuación, abre las puertas de par en par a que se pueda llegar a plantear si cabría considerar, a su vez, como inductor o incluso como provocador del delito de colaboración terrorista a quien induzca o simplemente intente inducir públicamente a un tercero para que adoctrine a otros incitándoles a cometer delitos de terrorismo en general³¹; posibilidad que, a nuestro juicio, hay que negar de forma tajante ya que supondría admitir la existencia y la relevancia penal en esta materia de una modalidad ciertamente particular de “inducción en cadena”, incluso meramente intentada, figura ésta que ha sido tradicionalmente rechazada por la doctrina³², incluso en su forma consumada, precisamente y entre otras cosas, por considerar, acertadamente a nuestro modo de ver, que su admisión supondría un adelantamiento excesivo e inadmisibles de las barreras de intervención penal³³.

Por otra parte, resulta llamativo que el artículo del Código penal español que venimos comentado castigue el “adoctrinamiento” y no la mera difusión pública de ideas o contenidos objetivamente peligrosos a los que aludía precisamente la propia Decisión Marco 2002/475/JAI en la que parecía tener origen³⁴, algo que, a nuestro modo de ver, no es en modo alguno consecuencia de una elección puramente casual del legislador español, sino de una muy meditada decisión por su parte, ya que, dicha expresión, si bien mantiene al margen de este tipo delictivo, por ejemplo, a todas aquellas actuaciones que podría realizar aquel periodista o cómico que difunda o comunique mensajes o viñetas que se mofen de las ideas y símbolos que defienden los seguidores

³¹ Este posible y cuestionable efecto ampliador, que permitiría castigar el mero acto preparatorio de lo que, todo lo más, sería a su vez, otro acto preparatorio ya fue puesto de manifiesto por CAMPO MORENO, J.C. *Comentarios a la reforma del Código penal* cit. ant. p. 75.

³² MIR PUIG, S. *Derecho penal. Parte General* (2015) cit. ant. p. 419 MUÑOZ CONDE, F./ GARCÍA ARÁN, M. *Derecho penal. Parte General* cit. ant. p.473, OLMEDO CARDENETE, M. *Comentarios al Código penal, Tomo III*, Ed. Edersa, Madrid, 2000, p. 308, entre otros.

³³ A este respecto véase lo comentado, por ejemplo, por GÓMEZ RIVERO, C. Op. cit. ant. p. 123 y ss y especialmente, p. 127.

³⁴ Así lo destacó en su día, CANCIO MELIÁ, M. quien además señalaba que ello contrastaba claramente con el hecho de que la citada Decisión Marco afirmase expresamente en su considerando 14 que “*la expresión pública de opiniones radicales, polémicas o controvertidas sobre cuestiones políticas sensibles, incluido el terrorismo, queda fuera del ámbito de la presente Decisión Marco y, en especial, de la definición de provocación a la comisión de delitos de terrorismo*”, lo que le llevaba a cuestionarse el posible encaje de esta modalidad con el propio Estado de Derecho, En “*Delitos de organización*”, cit. ant. p. 662 y 663. En idénticos términos se manifiesta también NÚÑEZ CASTAÑO, E. Op. cit. ant. p. 238.

de los radicales terroristas, por más que éstos puedan resultar absolutamente idóneos desde un punto de vista *ex ante* para determinar a alguno de sus destinatarios a cometer algún delito terrorista todavía por determinar y se pueda efectuar incluso sabiendo que pueden llegar a provocarlos, sí que permitirá castigar la instrucción, transmisión o enseñanza de ideas, creencias u opiniones que se correspondan con los postulados defendidos por los terroristas y se transmitan conociendo su peligrosidad incitadora. Esto es, la de las doctrinas que defienden y sustentan los diferentes movimientos terroristas³⁵.

Podría pensarse entonces que dicha decisión legislador patrio es acertada y positiva, ya que restringe significativamente el ámbito típico de esta concreta modalidad comisiva del delito de colaboración terrorista, limitándolo precisamente a los peligrosos discursos que utilizan los terroristas para captar apoyos. Sin embargo, la pregunta surge de forma inmediata. Si este delito solo permite castigar la transmisión de ideas defendidas desde el terrorismo (las adoctrinadoras) y no de las que pueden de forma general llevar a generar delitos de terrorismo, ¿no estaremos dejando de perseguir la transmisión de ideas por la peligrosidad lesiva que presentan para los bienes protegidos por los tradicionales delitos de terrorismo, para pasar a castigar directamente el simple mantenimiento o transmisión de los postulados defendidos por los terroristas? ¿No supone ello negar la posibilidad de defender dichas ideas y postulados y, por tanto, tratar imponer un pensamiento único sobre los temas que se cuestionan desde los movimientos terroristas, acabando de esa forma con la libertad de opinión, expresión e información sobre los mismos?³⁶

³⁵ Resulta significativo en tal sentido que mientras la conducta de adoctrinar aparece definida en el Diccionario de la Real academia de la Lengua española como la conducta consistente en *“Inculcar a alguien determinadas ideas o creencias”*, precisamente defina el vocablo doctrina en su tercera acepción como el *“Conjunto de ideas u opiniones religiosas, filosóficas, políticas, etc., sustentadas por una persona o grupo”*, lo que sin duda, delimitará la posible aplicación de esta modalidad comisiva a las conductas de transmisión de ideas religiosas, políticas y filosóficas que se incluyen en el ideario general de los grupos u organizaciones terroristas (a las doctrinas) y no a las que, por muy peligrosas que pudiesen ser, se sustenten de forma puntual por un sujeto sin estar encuadradas dentro de un ideario previamente configurado.

³⁶ En este sentido, hay que recordar que, como señalaba VIVES ANTÓN, T. S. resultaría del todo incongruente con la afirmación de la existencia de la libertad ideológica y de expresión de los Estados democráticos que fuesen precisamente dichos Estados los que decidiesen por los ciudadanos, supuestamente libres y autónomos, qué clase de ideas podrían llegar a conocer y cuáles no, ya que al hacerlo se les estaría negando la racionalidad, autonomía y libertad que supuestamente el ordenamiento les reconoce. En *“Sistema democrático y concepciones del bien jurídico; el problema de la apología del terrorismo”*, en *Terrorismo y proceso penal acusatorio*. Ed. Tirant lo Blanch, Valencia, 2006. p. 41.

Frente a esto se podría señalar que, en realidad, el precepto ahora analizado no castiga simplemente la enseñanza o transmisión de ideas, postulados o doctrinas sostenidos por los terroristas por muy radicales que puedan ser, salvo si los mismos se dirigen o resultan idóneos, en el caso concreto, para poder incitar a cometer delitos terroristas a sus destinatarios³⁷, lo que permitiría defender y transmitir libremente dichos postulados en el resto de supuestos y, además, dotaría de antijuridicidad material a los actos comunicativos o instructores verdaderamente típicos del delito ahora analizado. Sin embargo y a nuestro modo de ver, esta posible interpretación se enfrentaría a un claro y grave problema, ya que, al castigar el vigente art. 577.2 CP como delito autónomo y consumado la mera realización de conductas de adoctrinamiento, esto es, de mera transmisión de determinadas ideas o doctrinas que ni tienen que contener una manifiesta y expresa incitación a cometer delitos terroristas en general (puede ser tácita o implícita), ni tienen que resultar adecuadas desde un punto de vista *ex ante* para incitar a sus posibles receptores a cometer uno o varios delitos concretos y previsibles de dicha naturaleza (pueden incitar a cometer cualquiera de forma genérica), se desdibujan hasta tal punto los referentes conforme a los que se debería valorar la idoneidad incitadora que las ideas o informaciones “adoctrinadoras” tendrán que tener para ser típicas de esta figura, que se hace realmente difícil de determinar cuáles de entre ellas tendrán encaje en la misma y cuáles, sin embargo, se mantendrán al margen de su tipicidad.

Así, por ejemplo, ¿criticar la política que estuviese llevando un determinado país con respecto al colectivo musulmán ante un sujeto que se supiese o se sospechase que era afín o proclive a defender las ideas y métodos empleados por el terrorismo yihadista contrario a dicha política, podría llegar a ser considerado como un acto de adoctrinamiento castigado por el delito ahora analizado, al poder entenderse que quien la realizó, efectuó una actuación adoctrinadora que sabía que podría objetivamente llevar a su destinatario a cometer algún acto terrorista, por más que no supiese ni se hubiese planteado siquiera cuál en concreto podría éste llegar a ser? ¿Afirmar en un debate televisado que el tratamiento que estaban recibiendo los musulmanes en un determinado conflicto bélico era injusto y delictivo internacionalmente, como había previamente afirmado un determinado grupo u organización terrorista que llamaba además a la “guerra santa contra los

³⁷ En tal sentido, señalaba, por ejemplo, en relación a la anterior versión de este precepto, GARCÍA ALBERO, R. que el hecho de que el castigo de la conducta de adoctrinamiento pudiese plantear problemas por poder suponer la punición de la simple opinión manifestada, lo que trataba precisamente de evitar la ya citada Decisión Marco 2002/475/JAI, fue lo que llevó al legislador patrio optase acertadamente por vincular la posible relevancia penal de los mensajes que contemplaba este delito con la posible incorporación de otros a organizaciones terroristas o a la realización de delitos de dicha naturaleza, provocando, sin embargo, el solapamiento de esta figura con las de proposición, provocación o, incluso con la inducción. En Op. cit. ant. p. 2261.

infieles” como represalia, transmitiría una idea adoctrinadora adecuada o idónea para que alguno de los posibles e indeterminados receptores de tal mensaje pudiese decidirse a incorporarse a dicha guerra cometiendo una agresión terrorista cualquiera o integrándose o colaborando con dicha organización?

La amplitud e indeterminación de la nueva regulación parece ciertamente muy difícil de aceptar por un Estado de Derecho, respetuoso con los derechos y libertades fundamentales de la persona, que realmente se quiera tener por tal.

Pero es que además, si a esto se le añade que tras la reforma efectuada por la LO 2/2015, el delito de colaboración terrorista no solo castigará los actos adoctrinadores que se cometan con dolo de incitar a la realización de delitos de dicha naturaleza por parte de terceros o teniendo, cuando menos, conciencia de que las ideas transmitidas podían previsiblemente llegar a producir tal resultado (con un dolo de peligro), sino también y atendiendo a lo establecido en el nuevo apartado 3 del art. 577 CP, los que transmitan o enseñen dichas peligrosas ideas simplemente con imprudencia grave, -lo que, como es sabido, si bien obliga a tener que constatar que se había difundido o comunicado con infracción del deber de cuidado exigible a aquel que lo transmitió, no requerirá que la haya realizado siendo siquiera consciente de su peligrosidad-, el panorama normativo que se nos presenta resulta ya del todo desolador.

No solo nos encontramos ante un delito que no da unos referentes claros a la hora de determinar las ideas o doctrinas cuya enseñanza o transmisión quiere castigar. Además, estamos ante uno que transmite directa y expresamente a los ciudadanos el mensaje de que, por más que no se representen ni siquiera como posible que la idea o postulado acorde con los defendidos por los terroristas que quieran transmitir o enseñar pueda resultar idóneo o adecuado, en el caso concreto, para llevar a alguno de sus destinatarios a decidirse a cometer algún delito de terrorismo, dicho hecho no tendrá por que suponer que se mantengan exentos de responsabilidad penal por haberlos exteriorizado, transmitido o enseñado. Un mensaje, sin duda, que llevará a que más de uno de dichos ciudadanos se abstenga de defender o expresar tales ideas y doctrinas ante terceros, por más que estuviesen perfectamente amparadas por los derechos fundamentales a las libertades de expresión y de información en el caso y de la forma que pretendían hacerlo, ante el temor de que su posible equivocación a la hora de valorar su peligrosidad pudiese llegar a ser, precisamente, la que fundamentase su responsabilidad penal por imprudencia, generándose así un evidente efecto de desaliento sobre el posible ejercicio legítimo de tales libertades fundamentales por parte de tales personas; efecto que resulta a todas luces desproporcionado y obliga, en consecuencia, a considerar que la existencia de este delito es absolutamente incompatible con el reconocimiento y protección

que nuestra constitución otorga a las citadas libertades fundamentales, convirtiéndolo así en manifiestamente inconstitucional³⁸.

Se produce así una inadmisibles restricción de los derechos fundamentales de los ciudadanos con la supuesta finalidad de prevenir delitos que ni se habían empezado a cometer, ni tal vez nunca llegasen a cometerse; restricción que tendrá una especial fuerza en el ámbito de Internet, pero que no será la única realizada con la comentada finalidad que tendrá efectos sobre este especial ámbito de la vida cotidiana.

Veamos ahora que sucede con los instrumentos penales creados para investigar los comentados delitos.

3. LA INVESTIGACIÓN DE DELITOS TERRORISTAS COMO EXCUSA PARA LA RESTRICCIÓN DEL DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE TODOS LOS CIUDADANOS.

Como acabamos de ver, la nueva orientación político criminal adoptada frente al terrorismo yihadista persigue especialmente las conductas de difusión de determinadas doctrinas o mensajes susceptibles de generar *ex Novo* o, simplemente, de reafirmar o respaldar las ideas o tendencias que ya tuviesen sus posibles destinatarios de cometer delitos terroristas. Unas ideas o doctrinas que, como tuvimos ocasión de señalar al comienzo de este trabajo, han conseguido ser rápida y eficazmente difundidas, gracias, entre otras cosas, a las facilidades que proporciona un medio tan rápido, barato y global de comunicación, como es Internet.

Evidentemente, de nada serviría tener la creación de los controvertidos instrumentos represores de las actuaciones de difusión de dichas ideas, dados por las figuras anteriormente comentadas, si en la red primase un completo anonimato que garantizase a quienes las difundiesen que nunca se les podría llegar a identificar, ni, por tanto a sancionar,

³⁸ En este sentido, señalaba, por ejemplo, PRIETO SANCHÍS, L. que, aunque haya un ejercicio ilícito de la libertad de expresión *“una reacción penal excesiva frente a este ejercicio ilícito puede producir efectos disuasorios de desaliento sobre el ejercicio legítimo de los referidos derechos, ya que sus titulares, sobretudo si los límites penales están imprecisamente establecidos, pueden no ejercerlos libremente ante el temor de que cualquier extralimitación sea severamente sancionada”*, en *“La limitación constitucional al legislador penal”*, en *Justicia constitucional y Derechos fundamentales*, Ed. Trotta, Madrid, 2003. p. 296; efecto éste que determinará que la medida penal que lo provoque, como sucede con la ahora comentada, tenga que ser considerada como desproporcionada y resulte, por tanto, inconstitucional.

Precisamente para evitarlo, hace ya algún tiempo la UE creó mediante la aprobación de la Directiva 2006/24/CE, un ciertamente controvertido sistema de captación y almacenamiento generalizado de datos de telecomunicaciones, que obligaba a que todos sus Estados miembros adaptasen sus legislaciones nacionales para exigir a todos los proveedores de dicha clase de servicios a retener determinados datos externos, relativos a las comunicaciones que realizasen sus clientes, para garantizar que su realización se pudiese “trazar” o analizar posteriormente, en caso de que ello fuese requerido para investigar un delito grave (no solo uno terrorista). El sistema recibió críticas fundadas desde el mismo momento de su aprobación; críticas que incluso se vieron judicialmente respaldadas por el hecho de que algún Tribunal Constitucional, como el alemán, llegase a declarar que parte de la ley que traspuso dicha normativa europea al ordenamiento jurídico de aquel país era incompatible con los derechos garantizados por su Carta Magna³⁹.

Precisamente en dicha línea, la Corte Suprema de Irlanda y el Tribunal Constitucional de Austria plantearon sendas peticiones de Decisión prejudicial ante el Tribunal Europeo de Justicia, (asuntos C-293/12 y C-594/12 respectivamente), en las que solicitaban a dicho Tribunal que aclarase si ya el propio texto de la Directiva de conservación de datos era compatible o no con los derechos a la vida privada y a la protección de datos de carácter personal contemplados en los artículos 7 y 8 de la CDFUE, cuyo respeto, como ya vimos, resulta directamente vinculante para la propia Unión y judicialmente exigible ante dicho Tribunal, tras la entrada en vigor del Tratado de Lisboa⁴⁰.

Ambas peticiones fueron acumuladas por el Tribunal europeo y se resolvieron finalmente en ya celebre sentencia de 8 de abril de 2014; una Sentencia en la que el citado Tribunal afirmó que, dado que las captaciones y almacenamientos de datos que se efectúan conforme a lo establecido

³⁹ Véase a este respecto lo establecido en la Sentencia del BverG, de 2 de marzo de 2010, en la que se declara inconstitucional la normativa alemana que transponía esta Directiva por violar los principio de proporcionalidad y de determinación jurídica o claridad legal, comentada, entre otros, por ORTIZ PRADILLO, J. C. “Tecnología *versus* Proporcionalidad en la investigación Penal: La nulidad de la ley Alemana de conservación de datos de tráfico de las comunicaciones electrónicas”, en La Ley Penal nº 75, 2010, en www.laley.es (últ. vis. 2-5-2012). No faltaron tampoco las voces en España que desde un primero momento pusieron en tela de juicio la legitimidad del sistema establecido por esta Directiva por considerarlo incompatible con el principio de proporcionalidad. Véase a este respecto, por ejemplo, lo comentado por GONZÁLEZ LÓPEZ, J. J. “La retención de datos de tráfico de las comunicaciones en la Unión europea: Una aproximación Crítica”, en La LEY nº 6456, 2006, en www.laley.es (últ. vis. 10-5-2012), entre otros.

⁴⁰ En concreto, la Corte Suprema Irlandesa presentó su petición el 11 de junio de 2012, como consecuencia de la demanda presentada la Sociedad Digital Rights, dedicada a la promoción y protección de los derechos civiles y ciudadanos contra la normativa de aquel país que transpuso dicha directiva; mientras que Tribunal Constitucional de Austria presentó la suya el 19 de diciembre del mismo año, como consecuencia de los recursos interpuestos contra la normativa de aquel país por el Estado de Kärntner, el Sr. Seitlinger y otros 11.130 demandantes más.

en la citada Directiva indudablemente limitan o interfieren en los derechos a la vida privada y a la protección de datos personales protegidos por los mencionados preceptos de la CDFUE, se hacía necesario analizar si tal interferencia o limitación podía quedar, sin embargo, justificada atendiendo a lo establecido en el artículo 52 la propia Carta, donde se afirma que “...*cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades*”, para afirmar a continuación que “...*sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás*”.

Partiendo de esta base, el Tribunal europeo señaló que la cuestión fundamental a dilucidar en los asuntos que ante él se habían planteado, sería la relativa a si las concretas limitaciones de derechos establecidas por el sistema contenido en la cuestionada Directiva respondían o no a las exigencias derivadas del principio de proporcionalidad en sentido estricto; cuestión que obligaba a analizar, en primer lugar, si su imposición resultaría adecuada o no para conseguir la finalidad supuestamente justificaba su existencia, para después estudiar, si las concretas restricciones de derechos que iba a imponer para alcanzarla habrían quedado realmente limitadas a aquellas que resultaban estrictamente necesario imponer para hacerlo.

La primera de las cuestiones fue rápidamente resuelta por el Tribunal, ya que entendió como innegable que la captación de los datos relativos a las comunicaciones resultaba perfectamente adecuada e idónea para facilitar la investigación y persecución de delitos, sobretodo, teniendo en cuenta el papel fundamental que dichas comunicaciones han adquirido en la sociedad de la información en la que vivimos

Mucho más cuestionable resultaba, sin embargo, la segunda. Esto es, que se pueda realmente afirmar que el uso previsto para esta herramienta limitadora de derechos fundamentales hubiese quedado verdaderamente limitado a aquel que resultaba estrictamente necesario efectuar para perseguir tan legítimo fin.

En concreto, el TEJ consideró que la comentada Directiva vulneraría dicho límite con respecto al derecho a la protección de datos establecido en el art. 8 CDFU, al permitir, por ejemplo, que el nivel de las medidas de seguridad que los proveedores tendrían que imponer, para evitar posibles abusos con respecto a dichos datos, pudiese depender de una valoración de los costes que su implantación podría llegar a generarles a dichos sujetos y también al autorizar que los datos que

los mismos captasen y almacenasen pudiesen ser transferidos a terceros países, ajenos a la UE, donde su uso o posible abuso escaparía por completo al control de las autoridades independientes que, conforme a lo establecido en el apartado 3 del citado artículo de la CDFUE, deben garantizar el respeto a dicho derecho.

Tampoco respondía a las exigencias derivadas del principio de proporcionalidad el hecho de que la comentada Directiva implante un sistema de captación y almacenamiento general de los datos externos referidos a todas las comunicaciones, que lleve a que tales datos se puedan e incluso se tengan que recopilar y almacenar, aun cuando no exista indicio alguno, ni siquiera remoto, de que estuviesen relacionados con la comisión de un delito grave, o cuando se sepa incluso que estaban referidos a comunicaciones efectuadas por personas que estaban amparadas y obligadas a mantener el secreto profesional. Esto resultaba, a juicio del Alto Tribunal, absolutamente desmedido y, por tanto, desproporcionado, como también lo era que la citada norma comunitaria ordenase que los datos captados se almacenasen por un periodo mínimo de 6 meses, olvidando así que no todos los datos captados son igualmente útiles para perseguir e investigar delitos, con lo que la prolongación del almacenamiento de algunos de ellos carecerá de sentido a tales efectos y resultará, por tanto, también manifiestamente innecesaria y desproporcionada.

Pero es que además, tampoco resultaba posible mantener que las restricciones de derechos establecidas por esta Directiva hubiesen quedado realmente limitadas a las que resulta estrictamente necesario imponer para perseguir delitos graves, cuando su articulado ni determinaba que comportamientos debían considerarse como tales⁴¹, ni establecía ninguna limitación o control

⁴¹ De hecho, sobre la interpretación y delimitación de este concepto, del de delito grave, existe todavía una viva polémica doctrinal y jurisprudencial, ya que mientras algunos autores y tribunales parten de el mismo debe ser interpretado conforme a la clasificación de los delitos que realiza nuestro Código penal en su artículo 33 CP; otros, como, por ejemplo, RODRÍGUEZ LAINZ, J. L. en “Hacia un nuevo entendimiento de gravedad del delito en la Ley de conservación de Datos relativos a las Comunicaciones Electrónicas”, LA LEY nº 7789, 2012 www.laley.es (últ. vis. 4-2-2014) o en “El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones” cit. ant., propugnan una interpretación mucho más flexible y que no atienda tan solo a la concreta pena con la que el legislador sancione las conductas en cuestión, sino también otros factores, como la “relevancia social del hecho” o su repercusión; conceptos todos ellos altamente indeterminados y difusos, cuya concreción puede depender de criterios puramente subjetivos o incluso de factores tales como la importancia que los medios de comunicación decidan darle al hecho en cuestión, lo que nos lleva a rechazar su posible aplicación en este contexto, tal y como hace, por ejemplo, CORTES BECHIARELLI, E. por entender, como este autor, que el uso de tales conceptos no solo puede llevar a que los jueces se arroguen funciones casi legislativas en esta materia, sino también a que se olvide que cuando el legislador impone una pena de forma abstracta para un delito, es porque ha valorado y determinado la gravedad de su realización en la propia ley que lo castiga. En *El delito de corrupción deportiva*. Ed. Tirant lo Blanch, Valencia 2012 .p. 217.

que garantizase que sus restricciones no se podrían emplear para perseguir otro tipo de conductas diferentes de las finalmente se llegasen a tener como verdaderos delitos graves⁴².

Todo ello llevó al TEJ a considerar, finalmente, que la comentada Directiva resultaba incompatible con lo establecido en la Carta de Derechos Fundamentales de la Unión Europea, por lo que debía considerarse inválida y carente de todo efecto, pero también y paralelamente le hizo establecer una serie de criterios o referentes que habrán de ser tenidos muy en cuenta a la hora de valorar la posible compatibilidad de cualquier normativa que se haya creado o se vaya a crear con el fin de regular los sistemas de tratamientos de datos personales destinados a perseguir o investigar delitos, como los terroristas de los que venimos hablando, con las prescripciones y exigencias derivadas de la citada carta protectora de los derechos fundamentales.

Paralelamente al desarrollo de este proceso relativo a la regulación referida a las herramientas utilizables para la posible persecución e investigación de delitos graves en Internet y que, como ya señalamos, ha de tener una enorme repercusión en la posible investigación de los delitos de captación y adoctrinamiento terrorista, se vino desarrollando otro que resultaba espacialmente relevante para la investigación de otros de los nuevos delitos de terrorismo. Se trató de la regulación referida a la captación y tratamiento de los denominados Registros de Nombres de Pasajeros, más conocidos como PNR, en razón de la abreviatura de su denominación en inglés (Passenger Name Records).

La transcendencia de estos registros para la investigación y prevención de delitos terroristas fue pronto puesta de relieve tras los atentados del 11 de Septiembre en Nueva York. De hecho, fue

⁴² Ha de señalarse en este sentido, que aún a día de hoy, continúa habiendo una viva polémica doctrinal y jurisprudencial en nuestro país sobre las condiciones y requisitos procesales que han de cumplirse para poder acceder a dichos datos, ya que mientras algunas sentencias, como la STS 236/2008, de 9 de mayo, mantienen que dichos datos están disponibles para cualquiera de las autoridades responsables de la persecución e investigación de delitos de las que habla la Ley 25/2007, de 18 de octubre de 2007, de conservación de datos de comunicaciones electrónicas y redes públicas de comunicación, algunos autores, entre los que me incluyo, consideramos que el art. 7 de dicha ley obliga expresamente a contar con una autorización judicial para acceder a los mismos, ya que su acceso afecta también al derecho fundamental al secreto de las comunicaciones, tal y como ha afirmado el TEDH en reiterada jurisprudencia, desde su celebre Sentencia de 2 agosto 1984, referida al denominado “caso *Malone vs Reino Unido*”. Sobre esta polémica véase lo comentando, por ejemplo, por FRIGOLS I BRINES, E. “La protección constitucional de los datos de comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a intimidad a la luz del uso de las nuevas tecnologías”, en *La protección jurídica de la Intimidad*. Ed.. Madrid, 2010 p. 45 y ss o por mi mismo, en GALÁN MUÑOZ, A. “¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación”, En RGPD, nº 19, 2013, p. 46.

precisamente en dicho país donde primero se estableció la obligación de las compañías aéreas de recopilar y transmitir a las autoridades toda una serie de datos referidos a sus clientes con el fin de prevenir que atentados como el de las torres gemelas se pudiese volver a repetir⁴³.

No tardó mucho el gobierno americano en tratar de extender dicho sistema al resto de países, ya que resultaba evidente que, dada la enorme movilidad internacional que existe en nuestro días, el comentado sistema no sería efectivo de no contar con las informaciones referidas a los pasajeros que procediesen del extranjero. Precisamente por ello, el gigante americano comenzó a utilizar su arsenal político para conseguir que la Unión Europea y sus Estados miembros implantasen un sistema similar al americano y le transmitiesen los datos que captasen mediante su uso.

La presión ejercida y, sobretodo, la amenaza que pesaba sobre las compañías aéreas europeas que no participasen en el sistema de perder su licencia para volar en territorio norteamericano, llevó a que la Comisión adoptase varios acuerdos con el gobierno norteamericano que incluso fueron, en algún caso, anulados por el Tribunal Europeo de Justicia de las Comunidades Europeas⁴⁴. Ahora bien, paralelamente, la Unión Europea trató de establecer una regulación armonizada referida a dicha cuestión mediante la creación de diferentes propuestas de normativa.

Así, y en primer lugar, se realizó una propuesta de Decisión Marco en el año 2007, a la que siguió una controvertida propuesta de Directiva ya en el año 2011 que se vio paralizada precisamente por encontrar la expresa oposición tanto del Supervisor Europeo de protección de datos⁴⁵, como del Parlamento Europeo que rechazó el 29 de abril de 2013, en una celebre y ajustada votación realizada el día 24 del mismo mes, la comentada propuesta de Directiva, precisamente, por entender que la misma no respondía al principio de proporcionalidad y violaba, por tanto, lo exigido por el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.⁴⁶

⁴³ CATALINA BENAVENTE, M. A. "La transmisión de datos PNR entre la Unión Europea y Estados Unidos, Canadá y Australia", en *La transmisión de datos personales en el seno de la Cooperación judicial penal policial en la Unión europea*. Ed. Aranzadi, Cizur Menor, 2015, p. 301.

⁴⁴ Véase, en tal sentido, la sentencia del referido tribunal (TEJCE) de 30 de mayo de 2006, referida al primer acuerdo adoptado entre la UE y los Estados Unidos en el año 2005; comentada por CATALINA BENAVENTE, M. A. "La transmisión de datos PNR entre la Unión Europea y Estados Unidos, Canadá y Australia", cit. ant. p. 313 y ss

⁴⁵ Véase en tal sentido el Dictamen emitido por el Supervisor europeo de protección de datos, el 25 de marzo de 2011, con referencia a la propuesta de Directiva presentada por la Comisión el 2 de febrero de 2011, consultable, por ejemplo, en <http://www.asesoriayempresas.es/doctrinaadministrativa/JURIDICO/71730/dictamen-de-25-de-marzo-de-2011-utilizacion-de-datos-del-registro-de-nombres-de-los-pasajeros-para> (últ. vis. 26-12-2016)

⁴⁶ CATALINA BENAVENTE, M. A. "La transmisión de datos PNR en la lucha contra el terrorismo y otras formas de delincuencia grave", en *La transmisión de datos personales en el seno de la Cooperación judicial penal policial en la Unión europea*. Ed. Aranzadi, Cizur Menor, 2015, p. 450.

Parecía que, por una vez, el respeto y la salvaguarda de los derechos fundamentales de los ciudadanos habían conseguido frenar las ansias preventivas de los reguladores. Sin embargo, bien pronto una nueva sucesión de atentados terroristas realizados en el corazón de Europa volvió a poner la posible aprobación de la normativa referida registro de nombres de pasajeros en la agenda comunitaria.

Se trató, en concreto, de los atentados realizados en París entre otros contra el semanario cómico Charlie Hebdo el 7 de enero de 2015; unos atentados que conmocionaron a la opinión pública europea y cuya realización encontró rápida respuesta en el Parlamento comunitario que ya el 11 de febrero de 2015 aprobó una resolución en la que se comprometía a trabajar para aprobar una directiva sobre PNR que, sin embargo, según afirmaba el referido órgano, debería necesariamente respetar la sentencia del TEJ de 8 de abril de 2014 que, como vimos anuló la Directiva de captación de datos de tráfico.

La posterior repetición de ataques terroristas en Europa (atentados en la sala Bataclán en París, en Bruselas, etc...) no hizo sino acelerar los trabajos que finalmente culminaron en la todavía reciente aprobación de la Directiva 2016/681, del Parlamento y el consejo, de 27 de abril, relativa a la utilización de datos del registro de nombres de pasajeros (PNR) para la prevención, detección y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

Resulta imposible en este momento analizar con el detenimiento que merece tan compleja y completa norma. Por ello, centraremos nuestra atención en este momento, tan solo en aquellos aspectos que fueron precisamente los que llevaron a la derogación de la Directiva de conservación de datos en el año 2014; aspectos respecto a los cuales el TEJ estableció unos límites que, como ya hemos señalado, el propio Parlamento europeo utilizó expresamente como referente a la hora de establecer los límites que la captación y tratamiento de datos de pasajeros nunca debería superar para ser legítima.

Así, y en primer lugar, la comentada Directiva ha tratado de responder a las mencionadas exigencias jurisprudenciales, regulando en su artículo 13 el nivel de protección del que los datos captados gozarán de forma expresa; nivel que de forma general remite al que reconoce la Decisión Marco 2008/977/JAI, de 27 de noviembre, en relación al tratamiento de datos personales realizados en el marco de las actividades propias de la cooperación judicial y policial en materia penal. Se le otorgan así una serie de derechos y unas garantías que, evidentemente, y en razón de la materia y de la finalidad con la que se tratan, serán menores que los que se reconocen al ciudadano en relación con cualquier otra clase de tratamientos, lo que resulta cuando menos cuestionable en el

caso que nos ocupa, ya que, al recopilarse y tratarse en los sistemas de PNR los datos de todos los pasajeros de forma general y no solo los de aquellos sobre los que se tenga, cuando menos, indicios o sospechas de que representaban una amenaza delictiva, parece razonable pensar que dichos datos y sus titulares debería gozar un nivel de protección mucho más cercano a aquel que la todavía vigente Directiva 95/46/CE establece de forma general para cualquier tratamiento de datos que al que excepcionalmente establece la referida Decisión Marco para los datos trascendencia penal⁴⁷.

Precisamente, y en relación con esto último, llama la atención que la Directiva no diferencie el tratamiento que se ha de dar a los datos referidos a sospechosos o personas sobre las que existen indicios de ser responsables o de que van a cometer algún hecho delictivo de aquellos otros que están referidos a cualquier persona, lo que no parece respetar la exigencia jurisprudencial de que se otorgue un régimen jurídico diferente a los datos de unos y otros sujetos para considerar que el sistema que los capte y procese de forma general pueda ser considerado como proporcionado y, por tanto, como compatible con el respeto a los derechos fundamentales de los ciudadanos.

Lo que sí que parece haber tenido muy en cuenta el regulador comunitario es la exigencia jurisprudencial de que los datos captados de forma general para realizar investigaciones criminales hayan de tener una duración limitada y tengan que ser realizados para investigar unos delitos definidos, determinados y que se puedan considerar realmente como graves; cuestiones ambas que, sin embargo, la Directiva trata de resolver de forma cuando menos cuestionable.

Así, y por lo que se refiere al periodo de mantenimiento de los datos PNR, el art. 12 de la Directiva 2016/681 establece que los datos captados por las compañías aéreas permanecerán almacenados durante un periodo de 5 años desde que se transmitan a la Unidad única de información de pasajeros (UIP) que designe cada Estado miembro; plazo que, evidentemente, supera con creces al que el TEJ consideró como máximo aceptable y necesario para las labores investigadoras y preventivas que supuestamente venía también a cumplir el registro creado por la Directiva de

⁴⁷ Así lo entendió, de hecho, la Comisión de Transporte y Turismo en la opinión que emitió con respecto al proyecto de Directiva del año 2011, como señala, CATALINA BENAVENTE, M. A. en “La transmisión de datos PNR en la lucha contra el terrorismo y otras formas de delincuencia grave”, cit. ant. p. 458. Señalar que la citada Directiva 95/46/CE ha encontrado ya una norma que la deroga, la actualiza a la realidad digital actual y que pronto resultará aplicable. Se trata en concreto, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que está en vigor desde el 5 de mayo de 2016 y resultará de aplicación a partir del 25 de mayo de 2018.

conservación de datos del año 2006. Esta evidente contradicción llevó a que el regulador europeo tratase de satisfacer dichas exigencias jurisprudenciales estableciendo, a renglón seguido, en el apartado 2 del referido art. 12, que, si bien los datos PNR se tendrán que conservar por el referido periodo de 5 años, pasados seis meses desde su transmisión a la UIP tendrán que ser sometidos a un proceso de despersonalización que enmascaré aquellos datos que servirían para unirlos con el sujeto al que estaban referidos; proceso que, sin embargo, será reversible y, por tanto, permitirá volver a vincular los datos en cuestión a su titular, con lo que, en realidad y a nuestro modo de ver, la exigencia de su enmascaramiento solo supone un burdo intento normativo de eludir los límites temporales de conservación fijados por el TEJ, para volver a implantar periodos absolutamente desproporcionados e inaceptables de conservación de los datos de todos los ciudadanos.

Algo parecido sucede con la segunda de las cuestiones planteadas. La referida la delimitación de los delitos cuya prevención e investigación, justifican y permiten crear y utilizar unos mecanismos preventivos tan sumamente restrictivos de los derechos de los ciudadanos con son los sistema de tratamiento de PNR.

En concreto, el art. 1 de la Directiva 2016/681, establece que los datos PNR solo podrán tratarse con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de delitos graves; delitos estos últimos que el art. 3. 9) de la referida norma europea delimita estableciendo que se tendrá por tales a aquellos que cumplan dos requisitos de forma acumulativa.

En primer lugar, que sean punibles con una pena privativa de libertad que no sea inferior a los 3 años, límite este que atendiendo a la espiral punitivista que viven los ordenamientos jurídico actuales, no parece que represente restricción alguna a la hora de delimitar los delitos que por su gravedad podrán legitimar que se utilicen los sistemas de PNR en su prevención e investigación, ya que no parece que tan escasa pena haga realmente que las conductas para las que se prevea representen realmente la gravedad social que permitiría considerar justificada y proporcionada la general y preventiva restricción de derechos fundamentales que el uso de dichos sistemas representará.

Pero, además y en segundo lugar, se exige que los referidos delitos sean alguno de los incluidos en el Anexo II que se incorpora al final de la referida Directiva; un anexo en el que se contemplan delitos de lo más variopinto y de muy diversa gravedad, con lo que tampoco es que su expresa enumeración sirva para limitar el ámbito de utilización de los comentados sistemas a conductas realmente graves, ya que junto a delitos realmente graves, como puede ser la trata de

seres humanos o el tráfico ilícito de armas, se contienen otros de muy escasa gravedad, (como, por ejemplo, el tráfico de vehículos robados, la corrupción, el espionaje industrial o los delitos contra la propiedad industrial), o delimitados de forma tan amplia que cabe incluir en su seno conductas que, en modo alguno, deberían de ser consideradas como susceptibles de legitimar el uso de dichos sistemas (como, por ejemplo sucede cuando se permite utilizarlos para prevenir e investigar delitos informáticos, lo que abre las puertas a que se puedan emplear incluso en relación con pequeños daños informáticos o pequeñas estafas informáticas, sin demasiada trascendencia patrimonial ni social).

Como se puede comprobar, nada en la Directiva cumple de forma clara y tajante con las exigencias jurisprudenciales consideradas como necesarias para poder tener por legítima y proporcionada la restricción de los derechos a la protección de datos personales y de la vida privada y la intimidad que representa la implantación de sistemas de tratamiento y captación generalizada de datos personales, con finalidades preventivas e investigadoras. Habría que pensar, en consecuencia, que ello debería llevar a una pronta y firme reafirmación judicial de la vigencia de dichos derechos fundamentales, mediante la declaración de nulidad de este nuevo intento normativo de restringirlos de forma desproporcionada e ilegítima, realizado en el supuesto empeño de garantizar la seguridad.

Sin embargo, una enorme nube negra cubre en la actualidad la defensa de dichos derechos, ya que, en una situación como la actual, en la que los ciudadanos sienten verdadero terror ante los reiterados, graves y, en muchas ocasiones, impredecibles y casi imposibles de prevenir y evitar ataques terroristas que venimos sufriendo las sociedades occidentales desde hace ya más de una década (piénsese, por ejemplo, en los todavía recientes atentados realizados mediante la utilización de camiones en Niza o Berlín), resulta difícil que nadie, ni los políticos, ni los ciudadanos estén muy por la labor de preocuparse por defender la vigencia de dichos derechos si ello se hace, cuando menos aparentemente, a costa de disminuir en alguna medida la expectativa de tener seguridad y poder prevenir la realización de nuevos ataques.

Solo queda la esperanza de que los tribunales, y especialmente el TEJ, sigan defendiendo la vigencia de dichos derechos y garantías del ciudadano, algo que resulta especialmente alarmante, ya que viene a reconocer que ellos y solo ellos se han convertido ya en el último dique de contención de la ola de sacrificio de libertades y derechos que recorre las sociedades occidentales y también las de aquellos países que integran el autodenominado Espacio de seguridad, pero también de libertades y justicia que es la Unión Europea, en aras a conseguir una supuesta y harto cuestionable seguridad frente a los atentados terroristas.

4. RECAPITULACIÓN: LA UTILIZACIÓN DEL TERROR COMO FACTOR LIMITADOR DE DERECHOS FUNDAMENTALES. MALOS TIEMPOS PARA LOS DERECHOS FUNDAMENTALES

Si algo se ha puesto de manifiesto a lo largo de estas páginas es el hecho de que los derechos fundamentales de los ciudadanos están siendo sometidos a enormes tensiones y restricciones en los últimos tiempos como consecuencia de la aparición de un fenómeno criminal muy concreto: El denominado terrorismo yihadista.

Ha sido dicho terrorismo el que ha llevado al legislador a adoptar medidas penales y procesales verdaderamente excepcionales para combatirlo; medidas que, además, se pueden combinar de una forma ciertamente perversa.

Imagínese, en tal sentido, el efecto que podrá tener la combinación del castigo penal de las conductas de adiestramiento o adoctrinamiento pasivo que sancionan, por ejemplo, el mero hecho de visitar de forma reiterada webs con contenidos yihadistas o el viajar al extranjero con la finalidad de adiestrarse con la implantación de sistemas de captación generalizada de datos referidos precisamente a nuestra navegación por Internet o a los viajes aéreos que podemos realizar; una combinación que permitirá que se identifique y se tenga, cuando menos, por sospechoso a cualquier persona que realice una conducta tan, en principio inocua como visitar una web con contenidos religiosos radicales o viajar a un país considerado como peligroso incluso por motivos profesionales.

Pero, como hemos tenido ocasión de comprobar, no es este el único ni el principal peligro que se ha generado con la creación e implantación de dichas medidas. En realidad, y como hemos visto, el mayor problema que plantean se deriva del hecho de que su creación y utilización podría llegar y, de hecho, llega en ocasiones a restringir de forma absolutamente desproporcionada derechos tan fundamentales para los ciudadanos como su libertad de expresión, el derecho a su vida privada, a su intimidad o a la protección de sus datos de carácter personal. Esto, evidentemente, resulta absolutamente inadmisibles en sociedades que realmente quieran tenerse por democráticas

Pero es que además y como también hemos visto, el escaso rechazo social que han suscitado la implantación de dichas medidas ha sido utilizado por el legislador para tratar de extender su utilización a la prevención e investigación de otros hechos criminales mucho menos graves que los terroristas, lo que, de hecho, puede llevar a que el Derecho penal de los países occidentales

deje realmente de servir de forma general para garantizar los derechos fundamentales de sus ciudadanos y pase, en realidad, a ser precisamente uno de los más claros y generales instrumentos lesivos de dichos derechos.

El riesgo de que ello suceda existe y para evitarlo, como ya hemos visto, parece que ya solo nos queda la barrera que establecen los tribunales; unos tribunales que, por otra parte, no se sabe cuánto tiempo más aguantarán la presión a la que los someten unos medios de comunicación y unos políticos que de forma reiterada los ponen en la picota ante la opinión pública, calificándolos de obstáculos que impiden luchar eficazmente a los Estados contra los grandes peligros que acechan al ciudadano.

Es una barrera débil que ha de ser apuntalada recordando a la opinión pública que el principal objetivo de los terroristas es, precisamente, el acabar el régimen de libertades en el que vivimos y también que el discurso de que la cesión y restricción de sus derechos fundamentales les llevará a vivir más seguros y protegidos puede ser atractivo, pero también es completamente falso, por cuanto, mientras que resulta ciertamente cuestionable que, por ejemplo, almacenar todos los datos de quienes viajamos en avión vaya a servir realmente para prevenir o evitar delitos como los realizados en los últimos tiempos, (como lo demuestra el hecho de que muchos de sus autores estuviesen ya bajo vigilancia y observación policial, lo que no les impidió cometerlos), lo que sí que es completamente cierto y seguro es que la captación y procesamiento de dichos datos supondrá una efectiva y peligrosísima lesión de sus derechos, como también lo será que el que se les pueda llegar a sancionar penalmente por expresar ideas que, por muy coincidentes que sean con las de los terroristas, han de poder ser defendidas en una sociedad que quiera mantener el pluralismo ideológico que requiere para poder ser verdaderamente democrática.

Existe, por tanto, el peligro real de que la excusa de la lucha contra el terrorismo permita implantar un verdadero Estado de emergencia permanente y general en el que la restricción de los derechos de los ciudadanos deje de ser una triste excepción y pase a convertirse en la regla general, haciendo así que sea el propio Derecho estatal y no los terroristas los que consigan su objetivo final: Acabar con el Estado de Derecho y libertades que disfrutamos y tanto nos ha costado conquistar.

La conclusión es desalentadora, pero no puede ser otra. Corren malos tiempos para los derechos fundamentales y es por ello, por lo que, hoy más que nunca, hay que recordar que la política criminal de los países democráticos no puede estar exclusivamente orientada a la efectividad en la prevención y castigo de delitos, sino que también ha de tender a garantizar los

derechos y garantías que los convierten en tales; una garantía que lejos de ser considerada como un obstáculo a salvar, debe ser considerada como un objetivo primordial y preferente que deben perseguir las legislaciones penales de los referidos países, por lo que su consecución y tutela nunca debería quedar, como ahora sucede, exclusivamente en manos de los tribunales.

CYBERLAW

by CIJIC



***THE RIGHT TO BE FORGOTTEN: A NEW DIGITAL RIGHT FOR
CYBERSPACE
- IOANNIS IGLEZAKIS***

THE RIGHT TO BE FORGOTTEN: A NEW DIGITAL RIGHT FOR CYBERSPACE *

ABSTRACT:

The right to be forgotten is a new digital right which is included in the General Data Protection Regulation (Regulation 2016/679), entering into force in 2018. It has also been recognized by the decision of the Court of Justice of the EU with its decision of 13 May 2014 in case C-131/12, which interpreted the provisions of Directive 95/46/EEC as to include a right ‘to be forgotten’ on the Net. This case dealt with search engines and their obligation to remove links to web pages from their lists of results, following requests of data subjects on the grounds that information should no longer be linked to their name by means of such a list and taking into account that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. The digital right to be forgotten, however, is more than an obligation of search engine providers to remove links to personal data. It, moreover, embodies the claim of individuals to have personal data relating to them deleted, particularly those posted in social media, unless there is a compelling ground for keeping it. It, effectively, deals with the consequences of an Internet that ‘never forgets’, ensuring personal autonomy and privacy.

Keywords: Data protection, freedom of expression, right to be forgotten, right to oblivion, search engines

* Associate Professor, Faculty of Law, Aristotle University of Thessaloniki, Greece.

Paper presented at: Segurança da informação e Direito Constitucional do ciberespaço, 17-18 November 2016, Lisbon

I. INTRODUCTION

In 2012, the EU Commission presented the proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('General Data Protection Regulation', GDPR), repealing Directive 95/46/EEC, with the aim to modernize the legal framework for data protection in the EU (Hornung, 2012; De Hert/Papakonstantinou, 2012; Danagher, 2012; Kuschewsky, 2012; Traung, 2012). A central provision in the proposed Regulation was Article 17 introducing the 'right to be forgotten' in the digital environment, which drew its origins from the 'right of oblivion' – or *le droit à l'oubli*, recognized by case-law in France, Italy and other countries (Mantelero, 2012). In the final text of the Regulation that was recently adopted, i.e. Regulation 2016/679, some changes took place, but the essence of the right to be forgotten remained unaffected, while its title changed to 'Right to erasure'.

The intended effect of the right to be forgotten is to enhance users' rights on the Internet and remedy the lack of control over their personal data (Ausloos, 2012). It also presents an attempt to deal with the issue of digital forgetting, in other words, with the privacy issues arising in a Web that never forgets (Rosen, 2011). In more particular, in the digital age the 'default of forgetting' has gradually shifted towards a 'default of remembering' as pointed out by Mayer-Schönberger (Mayer-Schönberger, 2009), and this causes major privacy risks in a world of big data (Koops, 2011). This is a world in which it is almost impossible to escape the past, since every status update or photograph, and every tweet may be copied and/or reposted by other users or saved in Internet archives, such as the wayback machine¹, and in cached pages²; as a result that information may be available online, even if it has been deleted in its initial place (Mitrou/Karyda, 2012). Moreover, search engines provide a great number of personal information for any particular person in case a search with a name and/or surname is carried out.

In this context, the introduction of a right to be forgotten is the recognition of the enhanced capacity of cyberspace to disseminate and distribute huge amounts of data, including personal data, hence making it impossible to control the flow of personal information (Ausloos, op. cit.).

1 <https://archive.org/web/>

2 http://www.googleguide.com/cached_pages.html;

<http://www.cachedpages.com/>

<http://www.viewcached.com/>

It should be noted that there are different conceptual approaches as regards this new right in the literature. While it is conceived primarily as a right (e.g., Conley, 2010), other authors speak of an ethical or social value (Blanchete/Johnson, 2002) or of a policy aim (Mayer-Schönberger, op. cit.) and of a 'legitimate interest to forget and to be forgotten' (Rouvroy, 2008). In addition, it is connected with the right to personal identity, in so far as it expresses 'the ability to reinvent oneself, to have second chance to start-over and present a renewed identity to the world' (Andrade, 2011, p. 91).

What is common in these conceptualizations is the recognition that an individual has a significant interest possibly protected by a legal right in not being confronted by others with data from the past, which are not relevant for current decisions or views about him or her (Koops, 2001, at 232). In the digital world, this right takes a more pragmatic form; it is conceived as an individual's claim to erasure of data relating to him and it may as well be rephrased as a right to 'cyber oblivion' (Xanthoulis, 2012).

II. THE RIGHT TO BE FORGOTTEN AS A CONSTITUENT OF INTERNET PRIVATE RIGHTS

As the Internet is an inherent part of our lives today, privacy on the Internet has become a very important issue. In our understanding, privacy is not the right to 'be let alone', which amounts to an outdated conception (Warren/Brandeis, 1890), but more or less stands for the autonomy of the individual to decide which information and where he or she wishes to disclose.

To deal with threats to privacy and autonomy, it is suggested to embrace a set of internet privacy rights, which will deal efficiently with those threats (Bernal, 2014). Such a rights-based approach differentiates from a purely statutory approach and it refers to the concept of expectations in the theory of Luhmann (Luhmann, 1995), as they reflect what individuals consider to be their rights. In particular, the digital rights are the following:

- a) The right to browse the internet with privacy: it means that internet users when searching for and accessing to information, when buying or making another transaction have a legitimate expectation of privacy
- b) The right to monitor those who monitor us: this right is understood as the right to be informed in case of lawful data monitoring

c) the right to delete personal data: this represents the claim of the individual to have its personal data deleted, so this constitutes the right to be forgotten

d) the right to an online identity: this is the right to create an online identity, to assert that online identity and to protect it. This includes the right to keep identity data confidential and not revealing those data, unless it is absolutely necessary.

As it is evident, the right to be forgotten which the subject of this presentation has a pivotal position in the above set of digital rights. In our view, it is important to comprehend the above right as part of our fundamental digital rights, since it is, in a sense, distinct from privacy. More particularly, the right to privacy extends to information that it is not publicly known, while the right to be forgotten refers to information to be deleted that were made previously public (Weber, 2011).

III. THE REGULATION OF ARTICLE 17 GDPR AND THE CJEU DECISION IN THE GOOGLE SPAIN CASE

The provision of Article 17 GDPR basically includes a right to erasure of data that requires the controller to delete personal data and preclude any further dissemination of this data, but also to oblige third parties, e.g. search engines, etc., to delete any links to, or copies or replication of that data.

This applies in six instances, which derive from data protection principles (Costa, Pouillet, 2012): (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing; (c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing; (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services to children.

The right to be forgotten which is enshrined in the GDPR is not conceived as an absolute right; thus, a number of exceptions restrict its ambit, the most important being the freedom of expression and information. There is consensus that such a right cannot amount to a right of erasure

of history and turn our modern society into a society of ‘lotus eaters’ (Iglezakis, 2014), which would be the case if the Internet was programmed to forget, e.g. if Internet content was programmed to auto-expire (Fleischer, 2011).

However, there are concerns expressed by US authors, mainly, that this right will have chilling effects on free expression, as it might force Internet intermediaries to censor the contents that they publish or to which they link, and hence, lose their neutral status (see, e.g., Rosen, 2012, Fleischer, 2011). IN U.S. there is a legal tradition which denies protection of the right to be forgotten, at least as far as media and the press are concerned, which enjoy the right to publicize information that is legally available and not countervailing argument could be invoked to restrict this right with regard to the past of criminals and other detestable persons (Werro, 2009).

Search engines are also affected by a right to be forgotten. In more particular, search engines facilitate the finding of data through the myriad of pages published in the World Wide Web and in consequence, they enhance the ability of individuals to receive and impart information. Any restriction of search engines' functioning, therefore, might be seen as a restriction of freedom of expression (Alsenoy et al., 2013).

Viviane Reding, the former EU Justice Commissioner and former Vice-President of the EU Commission, pointed out that this right builds on already existing rules, and is not an *ex novo* right (Redding, 2012). Indeed, the European Union Court of Justice issued a decision on May 13 2014, in case C-131/12 (Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez), in which it confirmed that view, as it found that the ‘right to be forgotten’ is rooted in the provisions of Directive 95/46/EEC. Consequently, Vivian Reding referred to this decision in a post on Facebook as a ‘clear victory for the protection of personal data of Europeans’³.

Thus, the decision of the CJEU reinforced digital forgetting despite the hesitating stance of EU governments that decided to delay the data protection reform initiated by the Proposal for a Data Protection regulation until 2015, though it was expected to have the data protection reform finalized before the European Parliamentary election of May 2014⁴. It should be underlined that this decision comes one month after the decision of the Court in case C-293/12 and C0594/12 (Digital Rights Ireland and Seitlinger and Others), which declared the Data Retention Directive to be invalid. This does not suggest that the Court is carrying out judicial activism in favor of

³ See <http://www.bbc.com/news/world-europe-27388289>

⁴ In the conclusions agreed on at the European Council Meeting in Brussels it is mentioned that new EU data protection rules and a new cyber security framework are to be adopted "by 2015", see: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

informational privacy, since the rulings in both cases are justified. It represented a clear message, nevertheless; particularly as far as the Google case is concerned, it is evident that it supported the reform of the EU legal framework on data protection and the introduction of a control right, such as the ‘right to be forgotten’. It makes no surprise, thus, that this right was actually included in the Regulation 2016/679.

Moreover, it is evident that the ruling of the CJEU in this case, which recognized a right to have Google delete links to data that are irrelevant and/or outdated, will have significant repercussions, particularly to Internet companies, such as search engines. Google, shortly after the decision was issued, received certain removal requests; more specifically, an ex-politician seeking re-election demanded to have links to an article about his behavior in office removed, a man convicted of possessing child abuse images also requested links to pages about his convictions to be erased and, a doctor asked for the removal of negative reviews from patients from the results on searches⁵.

From Google’s perspective this represents a very negative situation, as it received an overflow of removal requests, on the basis of the CJEU decision. In order to cope with it, it created a new process for the erasure of data, namely, a web form through which people can submit their requests for the erasure of links to information regarding them⁶. Google reported to have received more than 91,000 requests by July, 2014, which covered a total of 328,000 links, and it approved more than 50% of them, it asked for more information in about 15% of the cases and rejected more than 30% of the applications⁷. The way Google handled the removal requests, however, was criticized by EU regulators, since it restricted the removal of Internet links to European sites only and it notified the owners of websites that have been removed from search results when it proceeds to such removal⁸.

5 See J. Wakefield, *Politician and paedophile ask Google to ‘be forgotten’*, bbc.com, 15 May 2014, <http://www.bbc.com/news/technology-27423527>

6 ”Google launches ‘right to be forgotten’ webform for removal requests”, theguardian, Friday 30 May, 2014, www.theguardian.com

7 See Dave Lee, *Google faces data watchdogs over ‘right to be forgotten’*, <http://www.bbc.com/news/technology-28458194>

8 See J. Fioretti, *Google under fire from regulators on Eu privacy ruling*, Reuters, July 24, 2014.

IV. THE ECJ DECISION IN THE GOOGLE SPAIN CASE, IN PARTICULAR

The main issue at stake in the Google Spain case was whether the relevant provisions of the Directive might serve as a legal basis for claims of removal of personal data from the list of search names displayed after a search is made on the basis of the name of an individual.

The CJEU considered first the provision of Article 12 (b) of the Directive, which states that ‘Member States shall guarantee every data subject the right to obtain from the controller as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the Directive, in particular because of the incomplete or inaccurate nature of the data’. The list of the reasons that justify such a claim is not an exhausting one, so the Court held that the incompatibility of the processing with the provisions of the Directive may also result from the fact that such data are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary, unless they are required to be kept for historical, statistical or scientific purposes. This is a particular reference to the data quality principle as enshrined in the provisions of Article 6 (1) (c) to (e) of the Directive⁹.

The Court further made the argument that even initially lawful processing of accurate data may, in the course of time, become incompatible with the Directive where those data are no longer necessary in the light of the purposes for which they were collected or processed¹⁰. It is evident that this line of argumentation is influenced by the provisions of the Draft Regulation establishing the right to be forgotten and shows the commitment of the Court to the data protection reform process.

Subsequently, the Court applied this maxim to the circumstances of the case; it stated in particular that if a request by the data subject is made, in accordance with Article 12 (b) of the Directive, clarifying that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the Directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, then the information and links in the list of results must be erased¹¹.

⁹ Case C-131/12, nr. 92-95.

¹⁰ Op. cit., nr. 93.

¹¹ Op. cit., nr. 94.

Further, in case the data subject exercises his/her right to object on compelling legal grounds relating to his/her particular situation to the processing of personal data relating to him/her, according to Article 14 (a) of the Directive, the Court supported the view that where such requests are based on alleged non-compliance with the conditions laid down in Article 7(f) of the Directive, the processing must be authorized under Article 7 for the entire period during which it is carried out¹².

The time factor appears to play a role in this case, and thus, the Court found that in such requests it should be examined whether the data subject has a right that the information relating to him/her personally should, at this point in time, no longer be linked to his/her name by a list of results displayed following a search made on the basis of his name¹³.

The CJEU went even further; it emphasized that the right of the data subject to request the removal of information from the search results of search engines is based on Articles 7 and 8 of the Charter of Fundamental Rights of the EU and these rights override not only the economic interest of the operator of the search engine, but also the interest of the general public in finding information concerning a data subject.

An exception from this rule is made in case the data subject is a public figure, because then the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question¹⁴.

Finally, the Court made particular reference to the issue in the main proceedings concerning the display, in the list of results that the internet user obtains by making a search by means of Google Search on the basis of the data subject's name, of links to pages of the on-line archives of a daily newspaper that contain announcements mentioning the data subject's name and relating to a real-estate auction connected with attachment proceedings for the recovery of social security debts. The Court's decision is that, taking into account the sensitivity of this information and the fact that this information had taken place 16 years earlier, the data subject substantiated a right not to have this information linked to his name by means of a list of search results.

12 Op. cit., nr. 95.

13 Op. cit., nr. 96.

14 Op. cit., nr. 97.

V. CONCLUSION

The new digital right to digital forgetting has already had quite a success, although its statutory implementation is yet to happen. Search engines have complied with the decision of the CJEU in the Google Spain case and respond to requests for deleting search results. The first company that published a form for deletion requests was Google, but also Bing and Yahoo followed suit¹⁵. Although, in the beginning the removals only took place as regards European versions of Google, it has been extended to all of its domains, as the French data protection authority threatened to impose sanctions on Google if it did not remove search results globally across all versions of its service and not just European domains¹⁶. Naturally, once the GDPR enters into force, the right to be forgotten will acquire a wider dimension, covering a multitude of internet services.

15 See 'Microsoft and yahoo respond to European 'right to be forgotten' requests', theguardian, 1 Dec. 2014, <https://www.theguardian.com/technology/2014/dec/01/microsoft-yahoo-right-to-be-forgotten>

16 See 'Google to extend 'right to be forgotten' to all its domains accessed in EU', the guardian 11 Febr. 2016, <https://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom>

REFERENCES:

- Alsenoy, B., Van/Kuczerawy, A./Ausloos, J., *Search engines after Google Spain: internet@liberty or privacy@peril?*, ICRI working paper 15/2013, online available at: <https://www.law.kuleuven.be/icri/> and <http://ssrn.com/link/ICRI-RES.html>.
- Ausloos, J., *The 'Right to be Forgotten' Worth remembering?*, (2012) *Computer Law & Security Review* 28, pp. 143-152.
- Bernal, P., *Internet Privacy Rights. Rights to Protect Autonomy* (2014) Cambridge University Press.
- Blanchette, J. -F./Johnson, D.G., *Data Retention and the panoptic society: The social benefits of forgetfulness*, (2002) *The Information Society: An International Journal*, vol. 18, issue 1.
- Conley, C., *The Right to Delete*, AAAI Spring Symposium Series, North America, (2010), online available at: <http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482>
- Costa, L./Poullet, Y., *Privacy and the regulation of 2012*, (2012) *Computer Law & Security Review* 28, pp. 254-262.
- Danagher, L., *An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?*, (2012) *European Journal of Law and Technology* vol. 3, No. 3, online available at: <http://ejlt.org//article/view/171/260>.
- Fleischer, P., *Foggy Thinking About the Right to Oblivion, Privacy...?* (Mar. 9, 2011), online available at: <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html>.
- Hert, P. De/Papakonstantinou, V., 'The proposed data protection regulation replacing Directive 95/46/EC: a sound system for the protection of individuals', (2012), *Computer Law & Security Review*, issue 2, vol.28, pp.130 – 142.
- Hornung, G., *A General Data Protection Regulation for Europe? Light and Shade in the Commission's draft of 25 January 2012*, (2012) *scripted* vol. 9, issue 1, 2012.
- Iglezakis, I., *The right to digital oblivion and its restrictions* (2014), Sakkoulas ed. (in Greek).
- Koops, B.-J., *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to Forgotten" in Big Data Practice*, (2011) *scripted* vol. 8, Issue 3, Dec. 2011.

Kuschewsky, M., *Sweeping Reform for EU Data Protection*, (2012) *European Lawyer*, 112, pp. 12 et seq.

Luhmann, N. *Social Systems* (1995), Stanford University Press.

Mayer-Schönberger, V., *Delete: The Virtue of Forgetting in the Digital Age* (2009), Princeton University Press.

Mandeler, A., *U.S. Concern about the European Right to Be Forgotten and Free Speech: Much Ado about Nothing?* (2012), *Contratto e impresa*, pp. 727-740, online available at: <http://porto.polito.it/2503514/>

Mitrou, L./Karyda, M., *EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge?* (February 5, 2012). 5th International Conference of Information Law and Ethics 2012, Corfu-Greece, June 29-30, 2012, online available at SSRN: <http://ssrn.com/abstract=2165245>

Reding, V., *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, Munich 22 January 2012, Speech/12/26.

Rosen, J., *Free Speech, Privacy, and the Web that Never Forgets*, (2011) 9 J. on Telecomm. and High Tech. L. 345.

Rosen, J., *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88, February 13, 2012, online available at: <http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf>

Rouvroy, A., *Reinventer l'art d'oublier et de se faire oublier dans la de l'information? version augmentée*, (2008) online available at: http://works.bepress.com/antoINETTE_rouvroy/5/

Traung, P., *The Proposed New EU General Data Protection Regulation*, (2012) *CRi*, issue 4, pp. 33-49.

Werro, F., 'The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash', in: Aurelia Colombi Ciacchi, Christine Godt, Peter Rott, Leslie Jane Smith, (eds.), *Liability in the Third Millennium*, F.R.G., 2009, online available at: SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357

Xanthoulis, N., *Conceptualising a Right to Oblivion in the Digital World: A Human Rights-Based Approach* (2012), online available at SSRN: <http://ssrn.com/abstract=2064503>

ADDITIONAL READING:

Ambrose, M.L./Friess, N./Matre,J.V., *Seeking Digital Redemption: the Future of Forgiveness in the Internet Age*, Santa Clara Computer and High Technology Law Journal, Vol. 29 (2012).

Andrade, N. G. de, *Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization*, in: S. Gutwirth et al (eds), *Privacy and Data Protection. An Element of Choice* (2011), pp. 65-97.

Blanchette, J.-F., *The Noise in the Archive: Oblivion in the Age of Total Recall*, in Gutwirth S. et al.(ed.), *Computers, Privacy and Data Protection: an Element of Choice* (2011), p. 25 ff.

Castellano, P, S., *The right to be forgotten under European Law: A Constitutional debate*, Lex Electronica, vol. 16.1 (Winter 2012).

Giannakaki, M., *The right to be forgotten in the era of social media and cloud computing*, in: Akrivopoulou C. and Garipidis N. (ed.), *Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies*, 2012, p. 11 ff.

Mayer-Schönberger, V., *Usefull Void: The Art of Forgetting in the Age of Ubiquitous Computing*, Working paper RWP07, John F. Kennedy, School of Government, Harvard University, April 2007, online available at: http://www.vmsweb.net/attachments/pdf/Useful_Void.pdf

Szekely, I., *The Right to Forget, the Right to be Forgotten. Personal Reflections on the Fate of Personal Data in the Information Society*, in: S. Gurwith et al (eds.), *European Data Protection: In Good Health?*, 2012.

Terwangne, C. de, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*, (2012) IDP Numero 13, pp. 109-121.

Walker, R., K., *The Right to Be Forgotten*, (2012) Hastings Law Journal, Vol. 64:101, pp. 257-286.

Warren, S & Brandeis, L., ‘The Right to Privacy’, (1890) Harvard Law Review, Vol. IV, December 15, 1890, No. 5.

Weber, R.H., *The Right to Be Forgotten More Than a Pandora’s Box?*, (2011) Jipitec 2, no. 2 (July 26), online available at: <http://www.jipitec.eu/issues/jipitec-2-2-2011/3084>

Zittrain, J. L., *The Future of the internet, And How to stop it*, Virginia, Yale University Press 2008.

CYBERLAW

by CIJIC



AS PLATAFORMAS CIBERNÉTICAS PARA A EXPONENCIAÇÃO DO TERRORISMO TRANSNACIONAL - NUNO LEMOS PIRES

AS PLATAFORMAS CIBERNÉTICAS PARA A EXPONENCIAÇÃO DO TERRORISMO TRANSNACIONAL *

1. AS DESFRONTEIRAS DO TERRORISMO

Hoje e no futuro será cada vez mais difícil limitar causas, motivações e efeitos no uso do terrorismo. O terrorismo é simplesmente uma técnica, uma tática, uma ferramenta, que qualquer um pode utilizar, que qualquer grupo pode escolher, para afirmar uma determinada ideologia ou conseguir obter um determinado objetivo¹.

Sabemos que temos, para lá das tradicionais ameaças e riscos que sempre condicionaram as vidas das sociedades, dos cidadãos e dos Estados onde se inserem, novas dimensões, que potenciam e exponenciam enormemente todas as anteriores e para as quais não estamos preparados¹. São a grande novidade estratégica do Século XXI e que formam uma mistura assustadora entre as alterações climáticas, a demografia crescente e desregulada, um desequilíbrio agravado na distribuição de recursos e uma decadência maior na gestão do poder global, regional e local.

Terrorismo não existe de forma isolada e, provavelmente, o adjetivo de terrorista a determinado grupo ou pessoa, é um atributo bastante complicado de escolher e, conforme os contextos, profundamente divergente. Classificar um ato, um grupo, uma pessoa, mesmo um Estado ou uma entidade supranacional, como terrorista, depende do contexto, de quem classifica, de quem interpreta e da época histórica (os *terroristas* de uns podem ser os *combatentes da liberdade* para outros). Sobre definições e interpretações sobre o que é ou não o terrorismo, já tivemos oportunidade de publicar várias vezes sobre o mesmo, pelo que não nos queríamos repetir (deixamos na bibliografia as referências). O que é relevante não é a tentativa de classificar grupos, pessoas, atos ou entidades como terroristas, mas sim, conseguir determinar as motivações valorativas antes das ambições políticas que perseguem, as plataformas que usam para espalhar as

* Nuno Lemos Pires: <https://academiamilitar.academia.edu/NunoPires>

1 Lemos Pires, 2012a.

1 Lemos Pires, 2016a.

suas mensagens, para manterem um apoio significativo e para conseguirem uma atividade consistente, clandestina e consequente, entre as sociedades que pretendem atacar.

Hoje, talvez mais do que em décadas passadas, temos de fugir das simplificações explicativas assentes, apenas, em racionais geopolíticos, em jogos de interesses entre os principais atores do Sistema Internacional ou em simples análises sociológicas sobre ambições de poder. Esta análise não chega e pode até ser contraproducente. O percurso de alguns movimentos, que normalmente classificamos de terroristas, pode ter raízes muito profundas ou mesmo muito antigas, que o contexto exponencia, positiva ou negativamente, que nos deve obrigar a uma reflexão sobre a origem da crença humana em sistemas de valores, em códigos de conduta social, em suma, em traços de união civilizacional.

Hoje, garantidamente mais do que em décadas passadas, porque quase nada aparece de forma isolada, porque há conflitos que surgem por consequência deste novo ambiente estratégico, como a relação entre clima e guerra, ou entre as vagas de refugiados e o crescimento de estados fragilizados¹, temos de ler, analisar e entender os fenómenos de forma cruzada, abrangente e complementar. O terrorismo moderno apoia-se em redes de centenas de milhar de simpatizantes e não em poucas centenas ou milhares como acontecia em meados do século XX. As redes terroristas e os grupos que usam o terrorismo como técnica preferencial de atuação, como o Daesh, a al-Qaeda, o Boko-Haram ou o al-Shabab, usam todo o planeta como área de operações. Mesmo quando ambicionam agir localmente decidem atacar globalmente para quebrarem a vontade dos que se sentem seguros nos países de onde partem acusações sobre as suas ideologias, ou simplesmente para assustarem quem vem de fora ou, finalmente, para os isolarem dos que lhes estão mais próximos. O terrorismo transnacional, atual e futuro, é uma face de muitos problemas, não é um único problema.

1. RECRUTAMENTO E PROPAGANDA, DE FORMA PRESENCIAL E NO CIBERESPAÇO

Antes de referirmos as plataformas cibernéticas teremos de recordar que as atividades de recrutamento e propaganda podem ser feitas através de plataformas muito distintas, desde a organização de reuniões, encontros ou piqueniques, a ações nas Madraças, nas Igrejas, em Centros Sociais, em Bares Clandestinos, nas salas de leitura e livrarias, até ao uso, principalmente, dos

1 Do autor: <http://cei.iscte-iul.pt/blog/is-there-anybody-out-there-the-link-between-climate-change-and-war/> .

media e das redes sociais². Estas ações visam recrutar, fundamentalmente, três tipos de elementos, a que correspondem tipologias e abordagens distintas tanto nas mensagens como nos meios em que as mesmas são disseminadas:

Prioritariamente os *terroristas combatentes*, para o combate direto e a gestão nos territórios alvos de ataques: usam a imagem glorificada dos guerreiros, do uso do poder e da pertença a uma organização superior, que somam três efeitos – medo (imagens de dor, sofrimento e morte sobre adversários); poder (principalmente sobre minorias, mulheres, crianças e povos locais reduzidos à escravidão); certeza (dividindo o mundo em dois, os que apoiam a causa e os que são contra, nos casos de inspiração religiosa entre os crentes e os apóstatas, os que servem e os que devem morrer, *verdadeiros combatentes e cobardes*, ou *verdadeiros crentes (judeus, cristãos, muçulmanos) e pecadores (hereges, taqfires)*).

Em segundo lugar *dos adeptos*, para conduzir a política contra os restantes poderes: através do anúncio do combate à corrupção, aos governos *desviantes* e usurpadores de um poder ilegítimo, salientando a identidade superior da sua solução política (Soberania étnica, política ou religiosa).

Por último, de *simpatizantes* (entusiastas, apoiantes, fundamentalistas), para garantirem uma adesão, sem retorno, a uma ideologia afirmativa ou radical.

Toda esta ação de recrutamento necessita de instrumentos que garantam uma profunda difusão e apoio: *Operações de Propaganda* e ações em todos os media³, como são exemplo as revistas do jiadismo radical: da *Inspire* (al-Qaeda) ao *Dabiq / Dar-al-Islam/ Konstantiniyye/ Rumayyah* (do Daesh); ou de *sites* como Al-furan e Hayat⁴.

Além do recrutamento, as operações terroristas, materializam-se em táticas, técnicas e procedimentos bastante eficazes, simples de aprender e amplamente difundidas. Primeiro que tudo é preciso privilegiar as autoridades locais. Tal como *al-Suri* defende na sua obra do Jiadismo

2 Durante o processo de recrutamento usam entrevistas em que detalham completamente o perfil do candidato: “what’s your background? Are you good with media? With Weapons?”, Flynn, 2016: 28. Sobre o treino, de 6 a 8 semanas, bastante exigente, ver Nance, 2016: 344-352.

3 Fundamentalmente dirigida para o dentro das comunidades que se pretendem cooptar, no caso do radicalismo jiadista, a comunidade alvo é a muçulmana: “the overwhelming majority of official terror media over the past three decades from both ISIS and al-Qaeda is internal propaganda aimed at recruiting new members and bolstering the determination of already-indoctrinated members”, Nance, 2016: 383.

4 Al Hayat Media Center através de vídeos propagandísticos como o *Flames of War*, revistas como a *Dabiq* (por exemplo o número 15, de julho de 2016 está disponível em: <http://www.clarionproject.org/factsheets-files/islamic-state-magazine-dabiq-fifteen-breaking-the-cross.pdf>, consultado em 06 de Agosto de 2016), a *Dar-al-Islam* (dirigida fundamentalmente contra a França), a *Konstantiniyye* (dirigida contra a Turquia) além de relatórios de batalhas, quer em árabe, quer em inglês e outras línguas europeias. A revista *Inspire* da Al-Qaeda, também a número 15, de 15 de Maio de 2016, está disponível em: <http://jihadology.net/category/inspire-magazine/>. O uso de mensagens instantâneas no Twitter, as denominadas “Twitter bombs”, Nance, 2016: 38.

global⁵, primeiro é preciso cooptar as tribos locais, deixando-os manter o poder sobre o comércio e as populações, desde que, em troca, lhes sejam dadas algumas condições – a aplicação estrita da *Sharia*, o respeito pelo poder absoluto das chefias superiores e a implementação de uma organização política de um *Estado Islâmico*⁶. Ainda neste exemplo do Daesh, é importante ver a grande aposta no bem-estar social dando ênfase aos serviços prestados, como por exemplo, através da ajuda aos pobres, inválidos, órfãos, viúvas, familiares das vítimas de ataques aéreos, subsídios às escolas, restabelecendo serviços públicos, controlando e verificando os preços dos bens essenciais, apoiando os tribunais e forças de polícia local no seu território, cobrando impostos e assegurando a distribuição⁷. Faz e anuncia atos muito populares como, por exemplo, punindo exemplarmente a corrupção, atos considerados indecentes como a pedofilia, homossexualidade, adultério, consumo de droga ou outros vícios (publicamente de forma cruel e específica de acordo com o *crime* através de decapitações e crucificações)⁸. A ideia central a quem busca conseguir a aceitação para um projeto político alternativo é cooptar as populações locais porque, sem esse ingrediente, todas as ações terão um efeito limitado no tempo e na ação tomada. É preciso, além de um esforço em publicitar mensagens e ideais, o de manter a população informada das ações tomadas ao longo do tempo ou, em sinal contrário, de esconder os indícios de que a prática é diferente dos princípios anunciados, sendo assim, passando informações falsas, apostando na contrapropaganda ou bloqueando o acesso a órgãos de informação independentes.

Além desta dimensão local crescem as mensagens e ideias de dimensão regional e global. É, e sempre que as causas perseguidas ultrapassam a dimensão local, anunciado um determinado estado final (*end-state*), em que os princípios defendidos pelos grupos terroristas são passados e repetidos. No caso dos fundamentalistas islâmicos, será um mundo sob dominação neo-*salafista*

⁵<http://www.hurstpublishers.com/book/architect-of-global-jihad/> e <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub809.pdf> (consultado em 04 de agosto de 2016).

⁶ Nance (2015) identifica quatro medidas que o Daesh adota para que a população local o reconheça como governo legítimo: a proteção dos comerciantes, distribuição de comida e caridade aos pobres, a oferta de perdões aos antigos inimigos e o estabelecimento de tribunais de *Sharia*.

⁷ The tasks for this stage are (1) spread and preserve internal security, (2) provide food and medicine, (3) secure the region from external attack, (4) establish shari'a justice, (5) train the youths to create a fighting society, (6) work for the spread of shari'a science and worldly sciences, (7) construct an intelligence agency, (8) unite the people through money and shari'a governance, (9) force domestic hypocrites to hide their unbelief and comply with authority, (10) attack the enemies, (11) establish coalitions, and (12) advance managerial groups to participate as an emirate in the caliphate, Naji, pp. 17-19, em <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub809.pdf> - pg. 14)

⁸ São os grupos denominados de *Hisbah* (prestar contas), uma espécie de Comité da Virtude e para a prevenção dos Vícios, organizados em batalhões sob o comando de um Emir da Lei *Sharia* e geralmente atuam em veículos com um ou dois homens, vestidos de preto (*dishdashas*), Nance, 2016: 221-222.

radical – a *Umma* (comunidade dos crentes) estendida a todos⁹, no caso de um grupo terrorista político, é a obtenção de um sistema global (embora possa ser apenas regional ou local), como vitória da anarquia mundial, ou do comunismo, ou do nacional-socialismo ou qualquer outro tipo de “ismo”, identidade étnica ou regional.

2. DO USO DAS PLATAFORMAS DIGITAIS PARA DIFUNDIR, DEFENDER E COMBATER IDEIAS

Durante a Grande Guerra em África (1914-1918) afirmava-se que, para se saber quem iria vencer entre as potências coloniais, bastava ver as escolhas que faziam os povos nativos locais porque, escolhiam sempre, o lado dos vencedores. Quando os Macondes escolheram os Portugueses no norte de Moçambique, em vez dos alemães em 1917, esse facto foi logo entendido como um bom prenúncio dos combates futuros. Esta ideia mantém-se, não basta ter uma boa difusão de mensagens iniciais, é forçoso manter uma constância nas ideias e nas ações, na prática e na demonstração dos resultados obtidos.

Por isso, grande parte do que vemos em uso e difusão na internet, não visa simplesmente o recrutamento e a propaganda referido anteriormente mas, também, o da construção de modelos consequentes, afirmativos, bem estruturados e sustentados. Assim, entendemos dividir as ações do uso das plataformas cibernéticas consoante os efeitos que se desejam obter:

2.1 PARA VIGIAR INDIVÍDUOS E GRUPOS

O uso inteligente das plataformas cibernéticas permitem encontrar algoritmos para rapidamente determinar dimensões de pesquisa, buscas mais procuradas, áreas onde determinada mensagem passa com mais frequência, tipologia dos internautas e associações entre indivíduos. É passível de ser feito por Estados e por Organizações clandestinas, por quem se defende de ameaças diretas e indiretas e por quem busca obter apoios para os seus projetos clandestinos.

Os mecanismos de vigilância permitem agrupar indivíduos em diversas categorias. Desde a mais óbvia classificação, que é a da verdadeira associação “per se”, a sistemas muito mais diluídos como os indivíduos com tendência para a radicalização, para determinadas ideologias ou religiões,

⁹ “A grande sociedade Islâmica de Árabes, Persas, Sírios, Egípcios, Marroquinos, Turcos, Chineses, Indianos, Romanos, Gregos, Indonésios, Africanos (...) incluía pessoas de todas as nações e raças (...) Esta civilização maravilhosas não era Árabe (...) era uma civilização Islâmica. Nunca foi uma nacionalidade mas sempre uma *Comunidade de crentes*”, Qutb, 1964: 38.

mais suscetíveis de serem corrompidos economicamente, por áreas geográficas, por etnias, por famílias, clãs, grupos ou tribos, por diásporas, por conhecimentos culturais e académicos, pelas especificidades linguísticas. Por fim, todos (sim, todos, porque a tecnologia de *metadados* o permite) podem ser classificados e manter-se a vigilância, individual, sobre o que se fez, o que se disse e com quem se está.

2.2 ARMAZENAR, ORGANIZAR E PRODUZIR INFORMAÇÃO

A forma como se retira informação e/ ou do modo como se a comunica. Podem ser usados canais abertos ou encriptados, para produzir produtos, pacotes de propaganda ou edificar ideologias estruturadas. Da mesma forma que é possível fazer extensas bases de dados (*metadados*) para permitir detetar e analisar as intenções de supostos grupos terroristas e também, em sentido contrário, é possível construir projetos políticos, radicalizados, com uma estrutura bem edificada, com referências pensadas e projetadas numa ampla reflexão passada e com iterações lógicas num futuro alternativo. As plataformas cibernéticas possibilitam pesquisar, recolher, armazenar, processar, seleccionar, transferir e partilhar enormes quantidades de informação, tanto ao nível das pesquisas pessoais, individuais até, inclusivamente, à obtenção de matérias classificadas por empresas ou entidades estatais. Assim, além do esforço de construir projetos e idealizações alternativas, acresce o grave risco de se juntarem e de se apresentarem grandes informações classificadas que podem comprometer a ação das organizações governamentais e não-governamentais.

A partir de informações verdadeiras obtidas (veja-se o exemplo do *Wikileaks*) podem construir-se narrativas conspiratórias ou deliberadamente manipuladas para exacerbar opções radicais. Através de práticas de *Haktivismo* conseguem-se manipulações efetivas de informações e ideologias. Num cenário muito negativo conseguem-se obter informações classificadas que não deveriam ser divulgadas e usadas criteriosamente para exponenciar uma determinada visão. Mas também podem, simplesmente, ser usadas para se entender os modos de ação de determinado grupo ou organização governamental e construir, partilhar, difundir, alertar, milhares (milhões) de pessoas para questões que, de outra forma, nem seriam conhecidas (exemplo do uso das redes sociais durante as denominadas primaveras Árabes). À simples divulgação de material classificado, que em si mesmo pode não ser muito prejudicial, porque até, em determinadas causas, pode ser benéfico, acresce o risco real da manipulação, da escolha e exponenciação de conteúdos, por forma a materializar ideologias radicais e alternativas.

2.3 INTIMIDAÇÃO E MEDO

Receber mensagens, ver o seu nome, de seus familiares ou amigos, referido nas redes sociais, é profundamente intimidante. Por vezes basta a simples omissão para causar um efeito terrível. Se for publicada uma lista local com os nomes que são *uma boa referência* e, o respetivo nome não aparecer, pode equivaler a uma denúncia intimidatória. O que se diz, o que se escreve, o que se mostra e tudo o que não se diz, ou porque não se referencia, ou porque não se está identificado entre os que apoiam, são armas poderosíssimas nas plataformas cibernéticas.

São situações extremas porque, ou se participa e fica comprometido, ou não se participa e fica identificado como estando de fora. Ambas as situações são exploradas. A vulnerabilidade cresce sempre que o clima de denúncia ou de simples pressão se intensifica, se se alarga a vários membros da mesma família, a simples amigos, a organizações sociais ou a grupos. O modo varia, desde a simples sinalização, através de identificações nas redes sociais como a elas pertencendo (ou não), à pertença de determinado grupo, ideologia, religião ou simpatia política até às ameaças constantes através de mensagens, por telemóvel, por endereços *email*, ou por referências abertas nas redes sociais (Twitter, Face-Book, Instagram, etc.).

Basta por vezes associar um indivíduo a determinado vídeo ou imagem para o comprometer numa situação delicada. É que depois, quer se atue quer não, o efeito fica automaticamente criado e há uma imensa dificuldade em se sair da “armadilha”. Porque se não se reage é porque está comprometido, porque se reage positivamente é porque está associado à ideia ou apoia o grupo, porque se reage negativamente fica identificado com a ideia contrária. Pode ser uma situação “*loose-loose*” e que condiciona a atividade social, em redes cibernéticas, de muitas pessoas.

2.4 SEGURANÇA E VULNERABILIDADE

Vive-se com a ideia de um rede vigiada e insegura. Se não se compra e atualiza os instrumentos anti-virus, anti-*spam*, anti (...), fica a sensação de uma enorme vulnerabilidade. Uns exigem a segurança, outros desconfiam e deixam de utilizar as redes, muitos optam por voltar a sistemas antigos com reuniões privadas, cartas escritas à mão e mesmo o uso de códigos pré digitais (com o recurso ao lápis e papel).

A vulnerabilidade do sistema é conhecida com a agravante de se saber que a identidade cibernética pode ser “roubada” e usada por terceiros. Um endereço falso, uma entrada no sistema privado, um uso sobre o seu domínio tem implicações terríveis: denuncia as suas ideias e

mensagens, permite mandar mensagens falsas e, pior, pode revelar ou indiciar práticas criminais de quem nunca as cometeu.

O extremo desta vulnerabilidade é a criação de sistemas “*ultra-seguros*” que, se o forem verdadeiramente, provavelmente deixam de ser espaço, ou ciberespaço, livre e fluidos para troca de informações. É o paradoxo da intenção do que foi criado em face daquilo que se conseguiu atingir.

2.5 LOCALIZAÇÃO E REFERENCIAÇÃO

Desde o GPS dos aparelhos à referência disponível dos motores de busca. Estes sistemas, amplamente disponíveis até aos mais pequenos instrumentos do dia-a-dia (como os localizadores em chips), têm a grande vantagem para quem procura e a enorme incerteza para quem se quer esconder. Permitem encontrar alvos e atacantes, defender e expor defesas ou, simplesmente, identificar vidas, percursos, localizações, posições ou frases ditas e ações tomadas em contextos muito distintos.

Localização significa saber o que se faz, onde e com quem. Referenciar significa usar e utilizar todas as palavras proferidas, todas as iniciativas tomadas e as presenças comentadas em eventos. Que podem ser usados, de forma positiva, quando indicam coerência na assunção de posições ou, de expor contradições e de forma negativa, quando o discurso muda em momentos distintos ou conforme a audiência. *Uma vez na internet, sempre na internet.*

2.6 CIBERTERRORISMO PROPRIAMENTE DITO

Este é o campo privilegiado para a ação terrorista que visa, através das redes, conseguir o efeito do terror. Interromper sistemas, atacar infraestruturas cibernéticas, causar a disrupção de serviços, levar a destruições, provocar o colapso de cidades (interferindo no fornecimento de água, de eletricidade, de combustível, dos sistemas de navegação e controlo marítimo, aéreo, da circulação viária, (...), infelizmente as possibilidades são imensas) que pode levar a um estado de caos que redunde em violência generalizada, são passíveis e impossíveis de determinar porque partem da imaginação e do engenho humano.

Mas para além do ato deliberado está a exploração dos efeitos e, também neste campo, a ação terrorista pode ser terrível. Repetindo, mostrando, distorcendo e ampliando os efeitos dos seus ataques (cibernéticos mas todos em geral), pode ser obtido um resultado muito maior do que

a simples ação sobre os alvos em si. Causa alarme, causa efeitos reais e mantém um clima de insegurança para futuras e possíveis ações.

2.7 DO FINANCIAMENTO E DA COMUNICAÇÃO

Pode parecer a ação mais óbvia mas o uso das redes pode exponenciar a obtenção de financiamentos a apoios. A eficácia da ação abre o desejo dos adeptos radicais tentarem apoiar e, simultaneamente, a morbidez das imagens e mensagens violentas, criam dependências a quem, simplesmente, procura satisfazer desejos mórbidos e sádicos. Esta ação permite recolher fundos, alimentar grupos com pagamentos ou, através de ameaças mais ou menos veladas, extorquir “donativos voluntários”.

Na comunicações entre terroristas, entre redes e grupos terroristas, entre terroristas e simpatizantes mas, também, entre quem os combate. Manter as comunicações entre quem promove o terrorismo pode ser mais importante, por vezes, do que destruir ou mostrar estas ligações. É o que se denomina de “*Intelligence gain/loss*”. Podemos, como ação contrterrorista, ganhar mais em vigiar e seguir as comunicações do que em interromper ou tentar capturar quem usa o meio. Mantendo um operacional a comunicar, correndo o risco de não o capturar, ganha-se a oportunidade de saber procedimentos, descobrir mais membros das redes e evitar futuros atentados.

2.8 ENDOUTRINAMENTOS (CIBER-IDEALISMOS, RADICALISMOS, JIADISMOS)

Este será o ponto que une os primeiros pontos tratados no texto com as ações sobre as redes. Tudo o que se faz em termos de recrutamento e propaganda procura ser mantido, explicado e exacerbado, ao longo do tempo (*endoutrinado*). A preocupação de quem usa estes meios é o de tentar passar mensagens claras, simples, apelativas e, simultaneamente, ancorar o discurso numa narrativa consistente¹⁰, em ideias estruturadas, bem organizadas, com múltiplas referências e pontos de vista confluentes.

A postura destes radicalismos é a de procurar adesões emotivas com uma base teórica bem fundamentada. Isso implica uma presença permanente nas redes sociais, nos *Media*, em debates

¹⁰ Lemos Pires, 2016c.

públicos, em espaços de informação mediatizada. Implica ainda uma grande quantidade de *sites* com informação, apresentada de forma sugestiva, com profissionalismo e aparente profundidade. A maioria destes *sites* têm links para publicações, imagens, filmes e notícias. Além disso, tentam sempre manter um grupo alargado de especialistas que responde a comentários, induzem ou anulam opiniões desfavoráveis. São pessoas (ou grupos) bem preparadas que tentam manter o ritmo e a novidade da informação e reagem, rapidamente, sempre que um meio é fechado ou “atacado”.

3. UM ALERTA E UMA POSSÍVEL SÍNTESE SOBRE AS PLATAFORMAS CIBERNÉTICAS PARA A EXPONENCIAÇÃO DO TERRORISMO TRANSNACIONAL

O alerta reflete-se no cumprimento do Direito, das Leis e dos Princípios fundacionais dos Estados Democráticos. Esta é uma dimensão que deve fazer toda a diferença. Um grupo terrorista tem, ou não tem, a ética que entender usar. Geralmente abusa da sua impunidade para recorrer a todos os meios ao seu alcance sem qualquer respeito por leis, princípios ou valores daqueles que pretende visar. Quem os combate não pode, nem nunca o poderá permitir, que a reação ou a prevenção se faça sem a premência do primado da lei. Vencer estes grupos apenas terá efeitos no tempo se for feito no escrupuloso cumprimento das leis nacionais e internacionais e no respeito pelos princípios, direitos, liberdades e garantias que as sociedades democráticas defendem.

Os valores e princípios fundacionais dos Estados de direito democrático, nem na clandestinidade, nem na profundidade escondida da *deep web* (também referida como *dark net* ou *dark web*), podem ser considerados como manipuláveis ou ignorados. Essa dimensão, tão distinta entre adversários com estratégias opostas, tem de se manter e, mesmo sabendo das enormes dificuldades que causam a quem usa armas de forma diferente, não pode ser comprometida. Há formas de contrariar a ação terrorista nas plataformas cibernéticas sem prejudicar a ação essencial, basta que existam mecanismos de controlo, de supervisão e de fiscalização, que sejam garantes da justiça, da equidade e da dignidade na ação.

Como síntese diríamos que o terrorismo vive do efeito de terror que visa causar e manter. Uma explosão, a morte e a destruição, quando não divulgada e conhecida, apenas se limita aos danos e mortes causadas. O terrorismo precisa do oxigénio da mediatização e, naturalmente, da força das plataformas cibernéticas para exponenciar os seus efeitos. Este é o elemento fundamental e primário da relação entre ambos mas, como vimos, há bastantes mais níveis de aproveitamento e de análise que o cruzamento permite.

As plataformas cibernéticas permitem tanto a propaganda como o clandestino. As fontes abertas escondem mensagens e o uso da *deep web* permite o planeamento de operações secretas. Neste domínio, e como sempre quando tratamos de assuntos de conflitualidade, todos os meios e recursos podem ser pensados e usados para se atingirem os fins que se pretendem. Por isso, muito para além da exponenciação do fenómeno, tentámos demonstrar que estas plataformas servem para fazer, praticamente, o uso de todas as ações previstas pela estratégia, incluindo o combate e as ações diretas (de ciberguerra). Neste domínio fluem negociações diplomáticas, afirmações políticas, objetivos económicos, associações entre crime e terrorismo, entre o financiamento e o simples lucro, entre a vontade de agir, de publicitar e também de esconder e confundir. É um meio inesgotável, tanto para quem o usa para efeitos de terrorismo como para quem procura combater na dimensão do *contraterrorismo* ou da *contraradicalização*.

Como corolário do enunciado das afirmações anteriores ficamos com a firme convicção de que, quem quer combater o terrorismo, encontra nestas plataformas inúmeras formas para os contrariar. No escrupuloso cumprimento dos valores, dos princípios e das leis, internacionais e nacionais, há organização e saber muito superior ao do adversário para o conseguir vencer. Quem usa o terror raramente partilha dos mesmos argumentos de quem tem os valores do seu lado, da defesa da integridade da pessoa humana e na defesa da honra da sociedade que soubemos construir, queremos melhorar e juramos, mesmo com o sacrifício da própria vida, defender.

BIBLIOGRAFIA

AL SURI, Abu-Mus'ab (2004), *The Call to Global Islamic Resistance*, CENTRA Technology, Inc, trans., sponsored by the DCIA Counterterrorism Center, Office of Terrorism Analysis, EUA (disponível em www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_6093_989_0_43/http%3B/apps.opensource.gov%3B7011/opensource.gov/content/Display/6719634/pdf?file=2006.pdf) .

FLYNN, Michael T. (2016), *The Field of Fight: How we can win the Global War against Radical Islam and its Allies*, St. Martin's Press, New York.

LEMOS PIRES, Nuno:

- (2012a), "Terrorismo: uma tecnologia "off the shelf", Revista "Dragões d'Entre Douro e Minho" do Regimento de Cavalaria Nº6, Julho – Ano XII – nº 33, pp. 46-49.

- (2012b), "Terrorismo: Uma ameaça Perene", Revista Militar Vol 64 nº 6/7 (Junho-Julho), pp. 663-680 (disponível em: http://www.revistamilitar.pt/artigo.php?art_id=714).

- (2016a), "Das Ameaças e Riscos Intangíveis aos Estados Frágeis e às Guerras Civis", no livro *Ameaças e Riscos Transnacionais no novo Mundo Global*, Porto, Fronteira do Caos, pp. 153-174.

- (2016b), *Resposta ao Jihadismo Radical*, Nexo, Lisboa.

- (2016c), "Do Terrorismo Transnacional ao Choque de valores", Revista Nação e Defesa nº 143, Lisboa, pp. 79-87.

NANCE, Malcom (2015), *The Terrorists of Iraq*, CRC Press, Boca Raton.

NANCE, Malcom (2016), *Defeating ISIS: Who they are, how they fight, what they believe*, Skyhorse Publishing, New York.

NAJI, Abu Bakr (2006), *The Management of Savagery: The Most Critical Stage Through Which the Umma Will Pass*, Funding for this translation was provided by the John M. Olin Institute for Strategic Studies at Harvard University, and any use of this material must include a reference to the Institute. (Disponível em: <https://azelin.files.wordpress.com/2010/08/abu-bakr-naji-the-management-of-savagery-the-most-critical-stage-through-which-the-umma-will-pass.pdf>)

QUTB, Sayyid (1964), *Milestones*, disponível em: <http://holybooks.lichtenbergpress.netdna-cdn.com/wp-content/uploads/Milestones.pdf?5c9fb2>

CYBERLAW

by CIJIC



PODERES E ACTORES NO CIBERESPAÇO

- ARNAUT MOREIRA

PODERES E ACTORES NO CIBERESPAÇO *

RESUMO:

A Internet das Coisas começa a revolucionar a forma como nos relacionamos com os objectos que fazem parte do nosso quotidiano. Não apenas estes objectos incorporam módulos de inteligência artificial, mas também estão crescentemente interconectados entre si e com o utilizador. Este mundo do futuro, trazido até nós pela revolução digital e pelas tecnologias das telecomunicações e dos sistemas de informação, não está isento de riscos.

A competição entre empresas por disponibilizar novas funcionalidades nos seus equipamentos não tem vindo a ser acompanhada pelo robustecimento dos sistemas de segurança associados, deixando o utilizador exposto, nos seus dados pessoais e na sua vida privada, a práticas simples de hacking.

Este artigo procura contribuir para uma melhor percepção dos riscos que corremos e caracterizar o conjunto de actores que utilizam o ciberespaço para as suas actividades. É interessante verificar como num mesmo espaço de interconexão, se podem cruzar motivações e objectivos tão distintos, do mais vulgar dos internautas, ao mais perigoso dos cibercriminosos.

E porque informação sempre foi poder, também os Estados e os actores geopolíticos internacionais não deixam de observar atentamente e de interferir neste espaço criado e desenvolvido numa lógica inocente de plataforma de acesso universal à informação.

Palavras-chave: Ciberespaço, Cibersegurança, Internet das Coisas, Actores Geopolíticos

* Por Major-General Arnaut Moreira, no âmbito da I Conferência Internacional de Lisboa sobre Segurança da Informação e Direito Constitucional do Ciberespaço, 17 de Novembro 2016.

1. LUZES E SOMBRAS

Em plena Guerra Fria a agência norte-americana ARPA (Advanced Research and Projects Agency) foi mandatada para conceber um sistema com elevada capacidade de sobrevivência. Deveria ligar bases militares a centros de investigação e assentar numa rede com múltiplas conexões e sem um centro de controlo definido. É com base neste conceito que é criada para fins militares, em 1969, a ARPANET. Como estavam envolvidos também os mais reputados centros de investigação, o potencial deste conceito não passou despercebido a muitos investigadores levando a que, nos anos 80, se procedesse a uma separação entre a rede militar – a MILNET – e uma aplicação para fins civis – a INTERNET.

A este conceito devemos adicionar a facilidade de navegação introduzida por Tim Berners-Lee do CERN, com a invenção do hipertexto e do primeiro navegador, a que chamou de WorldWideWeb. Os utilizadores passaram também a poder digitar nomes de domínio em vez de incompreensíveis endereços numéricos para acederem aos servidores que continham a informação de que precisavam. A oportuna reunião de todos estes contributos explica o sucesso deste projecto gigantesco a que já aderiu quase metade da população mundial.

Enquanto decorria este enorme entusiasmo com as potencialidades de um acesso universal à informação através da net, outros desenvolvimentos mais sombrios mostravam também o enorme espaço de vulnerabilidades que se estava a abrir. Devo aqui referir John Von Neumann (1903-1957), especialista em sistema de modelação matemática e colaborador do projecto ultra-secreto Manhattan. Os seus contributos para a arquitectura dos computadores modernos são hoje plenamente reconhecidos, da mesma forma que a publicação da sua tese *Theory of Self-Reproducing Automata*, de 1949, constitui a base para o desenvolvimento dos primeiros vírus informáticos.

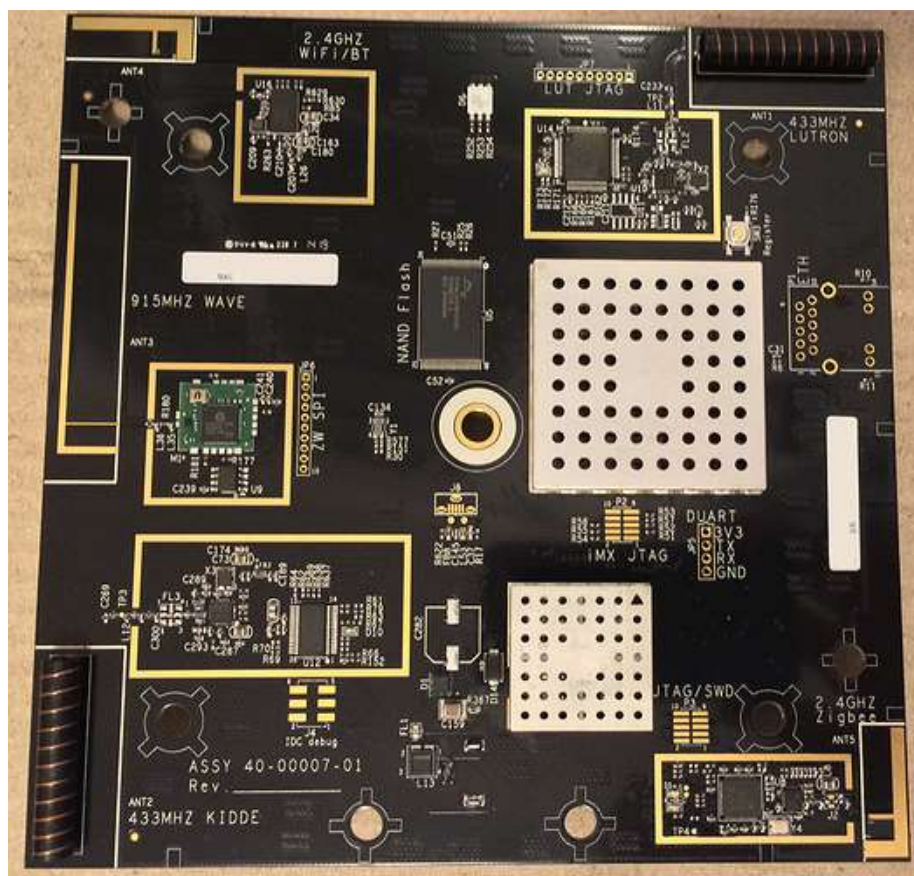


Figura 1: Motherboard de um controlador de dispositivos para casa

Fonte: <https://community.smarthings.com/t/wink-hub-teardown/3288>

2. VULNERABILIDADES E VÍCIOS

A esmagadora maioria dos utilizadores do Ciberespaço possui uma baixíssima literacia digital. As transacções de informação e respectivos fluxos, armazenamentos temporários, *backups* automáticos, protocolos ou técnicas de encriptação são tudo aspectos a que parecemos não dar excessiva importância. Também partilhámos o sentimento de que quantos maiores forem as preocupações de segurança sobre uma determinada actividade, menor é o seu grau de praticabilidade. Assim, a única coisa que parecemos desejar é que se possa carregar numa ligação em hipertexto e, sem complicações, o dispositivo nos leve onde queremos chegar.

Utilizamos apenas uma parcela ínfima das capacidades e aplicações que temos disponíveis nos nossos equipamentos e nem suspeitamos o que estes fazem para lá do que nós achamos que

fazem. Parecemos confiar infinitamente nos nossos interfaces com o Ciberespaço, como os nossos computadores, os tablets, os smartphones e toda a panóplia de novos equipamentos que a internet das coisas tornará inevitável nas nossas vidas com a entrada da inteligência artificial nos nossos automóveis, nas nossas casas, nas nossas roupas. A esta confiança quase absoluta adicionamos a disponibilização ao ciberespaço, algumas vezes de forma inconsciente e desnecessária, de um excesso de dados pessoais. Reunimos assim todos os ingredientes para uma experiência futura cheia de dissabores.

Acresce a esta vertigem pela praticabilidade, um outro factor perturbador não despiciendo: estamos viciados no ciberespaço. É um vício com características muito próprias, pois não depende da idade das pessoas, não depende do seu género ou religião, não depende do lugar do mundo ou da civilização com que se identifica. E não depende da hora do dia ou da noite. Parecemos estar disponíveis em permanência para nos conectarmos ao ciberespaço.

Como em todos os vícios, somos capazes de abdicar de muita coisa para nos conectarmos. Normalmente optamos por prescindir de dois bens essenciais: o nosso tempo de descanso e a nossa segurança.

3. ACTORES NO CIBERESPAÇO

Todos estamos de acordo quando se afirma que não existem dois utilizadores idênticos nos seus hábitos de navegação na internet. Parece-me no entanto possível agrupar os diferentes utilizadores em categorias de actores de acordo com as suas principais motivações para a utilização do Ciberespaço. Esta metodologia tem a vantagem de nos permitir uma análise sobre um mais reduzido número de situações. Ainda assim, para não simplificarmos demais o problema, vamos agrupar os nossos utilizadores em nove categorias de actores.

Informação é poder e, nesse sentido, é interessante olhar igualmente para o Ciberespaço como uma dimensão onde se estabelecem parcerias, competições, conflitos e combates entre os diferentes actores que o utilizam.

OS INTERNAUTAS

Estima-se que existam hoje mais de três mil milhões de utilizadores da Internet, um número impressionante que representa cerca de 40% da população total do planeta. Em pouco mais de dez anos, e de uma forma crescente e sustentada, adicionaram-se dois mil milhões de internautas.

Não obstante os custos de adesão ao serviço terem vindo a diminuir substancialmente, a disponibilidade de pontos de acesso está desigualmente repartida pelo planeta. Enquanto no mundo ocidental o acesso à internet é generalizado, a largura de banda disponibilizada é generosa e a oferta é até concorrencial, em muitos outros pontos do planeta o acesso continua a ser penoso. Nesses casos os pontos de acesso repartidos, como os cibercafés, continuam a ser a forma possível para aceder ao ciberespaço.

Os interesses do internauta no ciberespaço são certamente diversos, mas talvez os possamos sintetizar nos conceitos de lazer, de sociabilidade e de acesso à informação. Nem o lazer, nem a sociabilidade nem o acesso à informação são um exclusivo da internet. Pelo contrário, são actividades que acompanham a humanidade desde o seu dealbar. Então porque procuramos estas actividades no nosso telemóvel em vez de as encontrarmos na pausa de café do emprego, junto dos nossos colegas? Talvez porque a internet tenha permitido diversificar os nossos temas de interesse e alargar o nosso círculo de amigos para além daqueles com quem o contacto é imediato. Temos a sensação que o Mundo cabe melhor dentro do nosso smartphone do que dentro da sala de café.

Ainda em fase precoce, mas com perspectivas de desenvolvimento muito animadoras se encontram as soluções tecnológicas que nos permitirão trabalhar a partir de casa, um acontecimento que revolucionará as cidades e periferias bem como os sistemas que as mantêm em funcionamento permanente.

Cada internauta acede ao ciberespaço de forma muito livre, escolhendo a sua plataforma, o seu fornecedor de serviços, o seu navegador, a sua *firewall*, o seu antivírus, as suas aplicações e navega ao sabor das suas paixões e dos seus interesses. Torna-se assim virtualmente impossível encontrar soluções seguras universais que a todos sirvam. Às vulnerabilidades e vícios já enunciados há portanto que adicionar esta impossibilidade técnica de garantir a segurança absoluta do utilizador.

É toda esta combinação explosiva de fragilidades que tornam os internautas o principal alvo do interesse de todos os outros actores do Ciberespaço.

AS EMPRESAS

O segundo grupo de actores que nos interessa particularizar é o das empresas. As empresas procuram no ciberespaço uma forma de dar visibilidade aos seus produtos, de estabelecer um contacto mais próximo com os clientes e de fazer negócio. Crescentemente procuram acesso ao nosso *email* por forma a que nos possam inundar com as suas campanhas de *marketing*. De forma bastante mais sofisticada, através dos *cookies* que vão instalando nos nossos computadores, procuram conhecer o nosso perfil de gostos através das páginas que visitamos, de forma a serem mais objectivos nos anúncios que colocam nas páginas a que acedemos.

Muitas empresas, com quem já fizemos negócio por exemplo, dispõem de um conjunto muito relevante dos nossos dados pessoais, como o nosso nome, endereço electrónico, número fiscal, morada, cartão de crédito ou lista de compras efectuadas, para citar apenas os elementos mais comuns. Estão estes nossos dados suficientemente protegidos por estas empresas? São partilhados entre as empresas do mesmo grupo? São os nossos endereços electrónicos ou as informações dos nossos perfis cedidos, trocados ou vendidos a outras empresas ou a outros actores do ciberespaço? É crescente o número de internautas que se queixa de os seus dados estarem a ser utilizados fora do âmbito para que foram fornecidos.

No universo das empresas há que prestar uma particular atenção às que operam naquilo a que designamos por sectores críticos, pois desempenham funções ou prestam serviços indispensáveis para o nosso dia a dia. Ilustram este caso as que operam no sector da energia, no sector dos transportes, no sector bancário ou no sector das telecomunicações. Este conjunto de actividades, essencial à normalidade de funcionamento da sociedade, depende crescentemente das tecnologias de informação e de comunicações quer para o seu funcionamento interno quer para as relações comerciais estabelecidas com os clientes. Pela sua criticidade são alvos muito apetecíveis. Um ciberataque coordenado de grande escala a estes sectores pode paralisar um país inteiro.

Os ataques podem ter também impacto destrutivo: o ataque com o *worm* Stuxnet, em 2010, à capacidade industrial iraniana de enriquecimento de urânio, mostra que os ciberataques não se resumem aos sistemas de informação, mas podem ser dirigidos aos controladores de dispositivos que gerem equipamentos industriais, provocando-lhes falhas graves e eventualmente a sua destruição. Basta que sejam colocados a operar fora dos limites de funcionamento admissíveis.

AS INSTITUIÇÕES

Agrupamos neste conceito o conjunto muito diverso de organizações públicas ao serviço de um Estado, que, como seria de esperar num espaço de poder, se considera naturalmente um actor importante. É um conjunto muito heterogéneo de organizações em sectores tão diversos como a actividade política, as finanças, a saúde, a segurança ou a defesa, agregadas no ciberespaço através de dois objectivos centrais: por um lado dar a conhecer a acção do Estado, mantendo o cidadão informado da actividade desenvolvida e, por outro lado, facilitar o acesso dos cidadãos aos serviços institucionais. A concentração dos serviços disponíveis em portais especializados, estreita o relacionamento do cidadão com a máquina do Estado. Todos parecem lucrar com esta disponibilidade: o cidadão preenche as suas declarações através da internet, poupando tempo e evitando deslocamentos onerosos e as Instituições podem reduzir a dimensão dos postos de atendimento presenciais.

Os dados pessoais de maior qualidade que é possível obter situam-se exactamente na posse das instituições do Estado e contemplam todas as diferentes áreas da nossa vida pessoal como a nossa saúde, os nossos dados fiscais e financeiros e os dados familiares, para citar apenas alguns. A posse de todas as nossas facturas permite, também, reconstruir uma parte significativa dos passos que damos diariamente na nossa vida privada. Trata-se portanto de informação muito sensível que importa proteger de forma absolutamente segura.

Qualquer sucesso no acesso ilegal aos dados residentes nas Instituições constitui um desprestígio público do Estado, um objectivo que pode ser tentador para activismos políticos, para cibercriminosos ou para potências estrangeiras.

OS SERVIÇOS DE INFORMAÇÕES

Em face de tanta disponibilidade revelada por internautas, empresas, governos, activistas e outros actores para colocar todos os dados possíveis e imaginários na internet, os serviços de informações têm a sua actividade bastante facilitada.

Com efeito aquilo a que chamamos de Fontes Abertas (*Open Sources*) constituem um manancial inesgotável de informação para estes serviços. Tendo começado por se concentrar na leitura de notícias publicada por jornais, revistas e agências noticiosas, a crescente utilização das redes sociais pelos mais diversos e perigosos actores abriu um inesgotável campo de pesquisa para os especialistas na análise destas fontes.

Também com acesso à *Dark Web*, de que falaremos mais tarde, os serviços de informações estão naturalmente atentos às inúmeras actividades ilícitas que por lá se desenvolvem e negociam.

O grau de confiança da fonte e de verosimilhança da notícia não são normalmente muito elevados no caso das fontes abertas, mas da sua análise podem surgir alertas que constituem um primeiro passo para investigação adicional.

AS FORÇAS ARMADAS

A História ensina-nos que a Guerra sempre foi uma actividade de emprego de tecnologias emergentes, algumas criadas com intenção puramente militar e outras adaptadas às condições particulares de cada cenário.

O Ciberespaço tem todas as características para poder ser considerado uma nova dimensão do campo de batalha. Com efeito ele obedece a três condições essenciais para que se possa considerar uma nova dimensão. Por um lado possui uma estratégia própria de emprego, orientada para a neutralização ou degradação da capacidade de operação dos servidores críticos do adversário, quer ligados à defesa quer aos serviços essenciais do país. Por outro lado as hostilidades podem ser conduzidas independentemente das outras dimensões (da dimensão aérea por exemplo), tendo potencialidades para a condução de operações autónomas ou em conjugação com operações militares nas outras dimensões. Finalmente possui armas específicas para a condução desses ataques (vírus, malware, negação de serviços, etc).

Não estamos ainda suficientemente dependentes do ciberespaço para que uma guerra conduzida exclusivamente nesta dimensão tenha um sucesso que não seja apenas limitado temporalmente, mas todos os dias as sociedades caminham para uma maior dependência do ciberespaço, tornando a ciberguerra um evento cada vez mais provável.

No caso de uma guerra no ciberespaço não é expectável que ela se concretize exclusivamente contra sectores ligados à componente militar da Defesa Nacional. Muito provavelmente as instituições mais representativas do Estado, bem como os sectores críticos mais dependentes dos sistemas de informação, serão também seriamente afectados, pelo que importa treinar e afinar os processos que permitam a passagem da Cibersegurança para a Ciberdefesa e qualificar os recursos humanos que escassamente existem nestas áreas.

Releva-se aqui a importância do exercício anual do Exército, CIBERPERSEU, que num único cenário de transição de uma situação de Cibersegurança para uma situação de Ciberdefesa,

cria situações que permitem treinar os principais actores nacionais nestas áreas, incluindo os sectores críticos e outros sectores que podem vir a ser alvo de uma acção concertada por parte de entidades externas.

A grande dificuldade que se continua hoje a colocar, é a de se proceder a uma identificação inequívoca do atacante no ciberespaço como sendo um Estado, ou uma entidade oficial pertencente a um Estado. Sem esta identificação inquestionável ou sem a confissão declarada de autoria por parte de um Estado, um ciberataque dificilmente conduzirá a uma declaração de Guerra.

OS ACTIVISMOS

O objectivo dos activismos na Internet é o de difundir globalmente a sua mensagem de natureza política, o de denunciar práticas contrárias à sua doutrina, o de aliciar seguidores para as suas causas, o de congregar vontades, coordenar ou conduzir ataques às organizações que combatem.

Esta actividade pode ser desenvolvida quer de uma forma aberta e convencional, ao abrigo das disposições constitucionais consagradas para a liberdade de expressão, mas pode também ser desenvolvida com recurso a acções ilegais. A intrusão nas *homepages* das empresas e organizações que pretendem combater e a desfiguração das mesmas com a introdução de mensagens favoráveis às doutrinas dos activismos, constituem um método recorrente.

OS HACKERS

Com este novo actor entramos definitivamente no lado das actividades ilegais no ciberespaço. Normalmente associamos um *hacker* a um perfil muito particular de pessoa. É um jovem, normalmente um rapaz com uma idade rondando os vinte anos, com um baixo perfil de sociabilidade, com um talento especial para a programação e elevadíssimos conhecimentos de sistemas digitais, protocolos de comunicação, sistemas de computadores e linguagens de programação. Pode ter uma baixíssima propensão para o estudo académico, mas sobra-lhe especial intuição e método de trabalho científico. Experimenta e aprende com os próprios erros.

O ciberespaço oferece aos *hackers* quer um campo de actuação adequado às suas competências, quer um espaço de aprendizagem e de promoção da sua notoriedade. O que o distingue de um cibercriminoso tem a ver com o facto de o *hacker* não estar motivado pelo dinheiro que pode obter, mas com a adrenalina que resulta dos desafios em quebrar sistemas de protecção

que lhe permitam aceder com outro tipo de privilégios de controlo quer relativamente a sistemas de informação, quer relativamente a dispositivos electrónicos. O conhecimento, mas também a persistência, são duas qualidades que utiliza para superar estes desafios.

Ilustremos o que atrás dissemos recorrendo ao percurso conhecido de um famoso Hacker. George Hotz tinha apenas dezassete anos quando desbloqueou o primeiro iPhone. Aos vinte anos desbloqueou a consola Playstation 3 da Sony e aos vinte e quatro anos entrou na root do Samsung Galaxy S5.

Em nenhum destes casos se serviu da sua proeza para ganhar ou exigir dinheiro, se bem que algum tenha poupado por ter feito correr jogos na Playstation que não estavam autorizados. Com o acesso aos Iphone e ao Samsung George H. procurou descobrir que funcionalidades estavam contidas nos equipamentos e que não eram disponibilizadas, por bloqueio do fabricante, ao público.

Que consequências resultaram deste conjunto de ilegalidades? Praticamente nenhuma. A Sony colocou George Hotz em tribunal, chegando posteriormente a acordo extrajudicial com ele para garantir que o mesmo não tornaria a desbloquear equipamentos Sony. Apenas isso. Tal acordo parece revelar uma faceta interessante do sistema económico e judicial norte-americano: um jovem com as competências de George H. não pode estar preso. Ele tem conhecimentos muito relevantes que são fundamentais para a indústria. Não é de estranhar, nesse sentido, que, depois destas incursões pela arte do hacking, George H. tenha sido contratado pelo Facebook em 2011 e pela Google em 2014. Actualmente parece interessar-se pela programação de veículos autónomos.



Figura 2: A estrutura da Internet

Fonte: <http://www.adslzone.net/2016/03/02/deep-web-y-dark-web-curiosidades-contenidos-y-peligros-infografia/>

OS CIBERCRIMINOSOS

Agrupamos nesta definição o conjunto de actores do ciberespaço que, possuindo o mesmo perfil técnico dos Hackers, possui um diferente perfil ético. Com efeito este conjunto de actores não procura nem reconhecimento nem notoriedade, sendo neste capítulo o oposto do *hacker*. Através do anonimato executa, entre outras acções criminosas, vinganças pessoais e profissionais, acesso a dados de pessoas e a controlo de fluxos financeiros ou bloqueio de computadores e encriptação de dados para extorquir dinheiro.

O cibercriminoso move-se com facilidade numa zona muito especial da Internet, conhecida por Dark Web, onde tudo se compra e tudo se vende através de um sistema de múltiplas camadas de encriptação e de anonimização.

Com efeito podemos encontrar na Net três zonas claramente distintas. A mais conhecida é a *Surface Web*, a parte da Internet com acesso livre e a que acedemos com os nossos navegadores, aplicações sociais e motores de pesquisa. Ela representa no entanto uma parte ínfima da internet, pois cerca de 90% não está disponível através das ferramentas que diariamente utilizamos. Este espaço enorme não acessível pode subdividir-se em duas categorias: a *Deep Web*, onde se alojam bases de dados académicas, dados clínicos, registos financeiros, relatórios científicos e governamentais, informação para subscritores e outros dados, e a *Dark Web*, a que se acede com navegadores especiais como o TOR para encontrar produtos e outros materiais ou serviços ilícitos ou criminosos.

AS FORÇAS OCULTAS

A internet foi concebida no seu início como uma plataforma livre e aberta, utilizada por pessoas respeitáveis em busca de informação global e não como espaço para actividades ilícitas e criminosas. Tal arquitectura, traduzida na forma como os pacotes de dados codificados da internet são concebidos, origina imensas dificuldades em determinar verdadeiramente o autor de uma determinada acção no ciberespaço. O anonimato que a internet permite, abre campo para um conjunto muito grande de desagradáveis surpresas.

Em 13Set2016 o WikiLeaks disponibilizou 678 MB de novos documentos do DNC (Democratic National Committee) dos Estados Unidos da América, depois de em Julho desse ano ter disponibilizado vinte mil emails residentes nesses servidores. O autor deste acesso ilícito aos dados do Partido Democrata intitula-se Guccifer 2. Mas quem pode ser Guccifer 2? Um activista

movido pelo desejo de prejudicar um partido político ou uma campanha presidencial? Ou estamos perante algo muito mais sinistro, destinado a desacreditar todo o sistema democrático ocidental?

As investigações conduzidas aos servidores do DNC mostraram a existência de duas aplicações distintas, sofisticadas e não existentes no mercado, com arquitecturas que já foram encontradas anteriormente noutros ataques e a que os especialistas baptizaram de Fancy Bear e de Cozy Bear. A aplicação de Fancy Bear tinha entrado nos servidores em Abril de 2016, mas a aplicação Cozy Bear já estava instalada silenciosamente desde 2015, monitorizando *emails*.

Existe um conjunto de pontos de sintonia entre estes dois ursinhos. Estes actores não se interessam por proveitos económicos, atacam apenas figuras e instituições com elevado perfil político, diplomático ou militar, realizam apenas ataques personalizados – não enviam 1 milhão de *emails* como os cibercriminosos – e usam software muito sofisticado.

Enquanto o Cozy Bear demonstra excelente capacidade em ocultação das suas aplicações de infecção no interior de ficheiros normais, com uma propensão para os vídeos engraçados que circulam na net, o Fancy Bear parece escolher criteriosamente os seus alvos através das redes sociais, dirigindo depois o ataque através de *emails* pessoais contendo uma ferramenta chamada *Sourface* que permite vir a controlar o equipamento da vítima. Quando alguém, no seu LinkedIn afirma que trabalha no DNC, por exemplo, está a fornecer uma valiosíssima informação a quem pretenda infiltrar-se informaticamente naquela instituição.

De forma progressivamente mais contundente os Estados Unidos têm vindo nestes últimos meses a acusar a Rússia de estar por detrás dos ataques cibernéticos ao Partido Democrata. Cresce a convicção, até já verbalizada a nível presidencial, que a natureza e o âmbito destes ataques constituem uma ingerência inaceitável da Rússia na política norte-americana, alegações que a Rússia repudia também ao seu mais alto nível. Numa resposta sem precedentes a este tipo de actividade no ciberespaço, no final de Dezembro de 2016 os Estados Unidos expulsaram 35 cidadãos russos que desempenhavam funções em instalações diplomáticas em Washington e São Francisco.

Todos nos lembramos aqui da apresentação, feita pelos Estados Unidos em 25 de Outubro de 1962 nas Nações Unidas, de fotografias tiradas através dos aviões U2, demonstrando inequivocamente a preparação de bases de mísseis balísticos em Cuba. No Ciberespaço esta apresentação de provas é extraordinariamente mais complexa, o que claramente favorece o agressor.

Torna-se evidente que a capacidade de dissimulação no Ciberespaço facilita a condução de ataques contra o sistema político ocidental que está muito dependente das tecnologias da informação e das comunicações e que esta é uma área onde não deixaremos de continuar a ter más notícias.

4. ALGUMAS NOTAS FINAIS

Não adianta lutar contra a evolução tecnológica como resposta à crescente ameaça à nossa privacidade. Queremos sentir-nos modernos e isso significa ver através do nosso telemóvel o que está o nosso cão a fazer em nossa casa. É muito importante ter a nossa casa repleta de câmaras vídeo? Talvez não, mas faz-nos sentir modernos. Queremos estar felizes nas Caraíbas e partilhar os nossos vídeos com os amigos que estão a trabalhar no escritório. Não podia ser por carta? Podia, mas não faria a o mesmo furor. Queremos ligar o módulo de condução autónoma do veículo e viajar no banco de trás a ver um vídeo. Atropelamos um peão. Somos culpados? Não tenho resposta para isto, mas sei que a condução autónoma faz parte do mundo novo de que não queremos ser excluídos, mesmo com imensos riscos e insondáveis danos colaterais. Na verdade andamos à procura de um mundo novo que não existe como o imaginamos: aquele onde a inteligência artificial toma conta das tarefas que nos consomem tempo, paciência e esforço, mas onde é possível esconder a nossa identidade, as nossas preferências, hábitos e defeitos.

A Internet das Coisas está a explodir em frente dos nossos olhos e, do ponto de vista da protecção da vida privada, ela apresenta desafios imensos. Não apenas aumentará o perímetro de segurança que importará defender de intrusões, como exigirá conhecer muito mais de nós do que um mero computador. Teremos mais dados pessoais disponibilizados através de dispositivos pouquíssimo seguros. E quem nos garante que um dispositivo comprado no mercado não está a recolher muito mais dados do que aqueles que achamos que estamos a disponibilizar?

O Ciberespaço é tudo isto: para uns é lazer, sociabilidade e informação, enquanto para outros é a oportunidade de exercitar os desafios das insondáveis mentes criminosas. E para todos é um espaço onde se exercita poder entre actores desiguais nas suas capacidades e diferentes nas suas motivações.

CYBERLAW

by CIJIC



CIBERESPAÇO – ESPAÇO ESTRATÉGICO DE CONFLITO
- GONÇALO SOUSA

CIBERESPAÇO – ESPAÇO ESTRATÉGICO DE CONFLITO

A nossa sociedade está cada vez mais dependente das funcionalidades oferecidas pelo ciberespaço; os serviços dependem cada vez mais dele, principalmente as infraestruturas críticas¹, criando muitas vulnerabilidades que devem ser evitadas.

A Web² tem a capacidade de nos provocar as maiores alegrias, mas também as maiores angústias; promove a universalidade e, por isso, emerge como peça fulcral da Globalização. Criada pelo homem e para o homem, permite a troca e disponibilização de informação em tempo real de e para qualquer ponto do mundo, com um manancial imensurável de conhecimento, disponível e à espera que alguém a use. Esta razão é suficiente para ser dada atenção muito particular a esta realidade, devendo ser acautelados os riscos dela resultantes.

Com isto a importância da sua regulação, deve normalizar não só a respetiva utilização, mas e acima de tudo, prevenir que ela seja utilizada para prejudicar terceiros. Os ataques no ciberespaço podem ser efetuados pelos mais variados atores: cidadãos comuns, sociedades criminosas, organizações terroristas ou até mesmo Nações.

Tais ataques podem ser extremamente sofisticados e envolver muitos participantes, como os ataques realizados contra a Estónia em 2007, efetuados pelos chamados "*hackers patrióticos*"³; que consistiram no uso de *botnets*⁴ que, atuando em conjunto, assumiram características de operações militares.

1 Estruturas, cuja inoperacionalidade prolongada causa prejuízos graves à economia devido à paralisação das atividades estratégicas, podendo por em causa a capacidade de resposta de um Estado.

2 World Wide Web, abreviado para *web*, é um conjunto de ligações e ficheiros que se encontram interligados pela internet, permitindo a sua execução em tempo real.

3 Indivíduo ou grupo de indivíduos, que se dedicam, a conhecer e modificar os aspetos internos de dispositivos, programas e redes de computadores. Esses conhecimentos, permite-lhes obter soluções e efeitos extraordinários, que extrapolam os limites do funcionamento "normal" dos sistemas como previstos pelos seus criadores; incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controlo de certos sistemas e o acesso a certos dados. Neste caso, a motivação foi a alegada devoção à pátria e aos seus símbolos.

4 É uma coleção de agentes de *software* vulgarmente designados *bots* que se auto executam autonomamente e automaticamente. Permitem lançar a partir de milhares de computadores, simultaneamente, ataques informáticos em massa contra um *site*, colocando-o fora de serviço.

Já alguns anos a esta parte que o ambiente de segurança é descrito como estando em permanente mudança, de forma complexa, global e sujeita a uma evolução imprevisível. A evolução da segurança internacional tem um impacto crescente na vida do Homem.

Num mundo cada vez mais complexo a paz, a segurança e o desenvolvimento estão mais interligados do que nunca. Isto serve apenas para destacar a necessidade de estreita cooperação e coordenação entre as organizações internacionais e a exigência de que elas desempenhem seus respectivos papéis de forma complementar e interligada, na prevenção e gestão de crises.

No entanto esta segurança não deve ultrapassar determinados limites, nomeadamente os relacionados com a privacidade. O direito à proteção da vida privada, consagrado como direito fundamental na Declaração Universal dos Direitos Humanos, adotada pelas Nações Unidas em 10 de Dezembro de 1948, elege-o, no elenco dos direitos tidos por fundamentais, como um ideal comum de todos os povos e Nações, embora carecendo de força jurídica coativa:

*“o ideal comum a ser atingido por todos os povos e todas as nações... se esforce, pela adoção de medidas progressivas de carácter nacional e internacional, por assegurar o seu reconhecimento e sua observância universal e efetiva...”*⁵

Esta foi posteriormente retomada na Convenção Europeia dos Direitos do Homem⁶ de 1950 no âmbito do Conselho da Europa, onde são reafirmados os direitos e as liberdades do cidadão, consagrando os seus direitos políticos e sociais. Surge no contexto do pós-guerra, assegurando a dignidade humana frente ao avassalamento dos regimes tiranos e totalitários, espalhados nessa altura um pouco por todo o mundo.

No entanto alguns acontecimentos levaram a que a atenção do mundo se virasse para os atos de terrorismo, em detrimento da guerra simétrica, incluindo, sem a menor margem de dúvida, o uso ciberespaço, que vem abalar os pilares de segurança nacionais e internacionais, levando à dicotomia da segurança *versus* privacidade. Este terrorismo – que se assume de uma forma cada vez mais global e com alcances letais – está identificado como uma das principais ameaças a enfrentar durante os próximos anos e surge em inúmeros formatos.

O ciberterrorismo surge da convergência do terrorismo ao ciberespaço, geralmente entendido como ataques ilegais e ameaças de ataque contra os computadores, redes e as

⁵ Preâmbulo da Declaração Universal dos Direitos Humanos, 1948.

⁶ Convenção para a proteção dos Direitos do Homem e das liberdades fundamentais, tem por objetivo proteger os Direitos Humanos e as liberdades fundamentais, permitindo um controle judiciário do respeito desses direitos individuais. A Convenção faz referência à Declaração Universal dos Direitos Humanos, proclamada pelas Nações Unidas em 10 de dezembro de 1948.

informações neles armazenadas, com o intuito de intimidar ou coagir um governo ou o seu povo em prol de objetivos políticos ou sociais é sem dúvida um dos mais populares.

A necessidade de proteção contra este tipo de ataques, independentemente de quem tenha a responsabilidade da proteção dos sistemas e das infraestruturas - quer seja sector público, sector privado, ou ambos -, deve ser realizada dentro dos limites da lei, incluindo as regras do direito internacional, especialmente quando os ataques ultrapassam as fronteiras nacionais – o que acontece na grande maioria dos casos.

A dependência das sociedades nas redes informáticas é um facto, como são exemplo o banco direto, governo electrónico, telemedicina, redes energéticas, controlo de tráfego aéreo, só para referir alguns, mas esta correlação cria maior espectro de vulnerabilidade a incidentes. Na eventualidade de uma destas ocorrências, aplicar uma resposta que sirva todas as situações, torna-se extremamente difícil, quer se opte por encerrar a interação com o agente malicioso (desligar a ligação)⁷, ou respondendo sempre, o que pode ser totalmente ineficaz ou, pior ainda, ilegal.

Os desenvolvimentos no ciberespaço e a subsequente necessidade de o regular, levou o tema da cibersegurança às agendas de todas as organizações e consequentemente à necessidade de o regular. Assiste-se assim à concepção de um sem número de leis, quer implementadas à força por sanção, por normas sociais, ou mercados e arquiteturas de regulamentação do ciberespaço.

Os exemplos recentes de ciberacidentes têm minado a resiliência das infraestruturas e serviços nacionais em prol de determinados ideais.

Começa-se por constatar que seja qual for a abordagem a este problema, ela carece de desenvolvimento sistémico⁸ e endémico⁹, interpretação e aplicação de áreas e instrumentos jurídicos.

Os instrumentos legais aplicáveis à sociedade da informação e comunicação, cibercrime e segurança nacional diminuirão as lacunas existentes na regulação e reduzirão as inconsciências da interpretação legal.

Por isso torna-se essencial comparar e correlacionar as perspetivas dos juristas, políticos e

⁷ Quando se desliga a ligação, por exemplo, impossibilita a recolha de provas para o processo criminal, *counter-targeting*, ou a recolha de informação que possa ser utilizada numa operação de contraespionagem. Por outro lado, respondendo ou realizando qualquer tipo de vigilância, pode violar as leis nacionais.

⁸ De forma organizada e coordenado entre todas as entidades atinentes.

⁹ Visto de forma nativa às realidades da tecnologia, mas não esquecendo a superação do ser humano a outras revoluções.

tecnólogos, para dessa forma criar cibersegurança da forma mais efetiva possível.

As Nações necessitam de rever os seus objetivos, pois a sociedade da informação atingiu uma fase revolucionária em que a sua defesa requer a revisão de todos os princípios, estratégias, táticas e processos de tomada de decisão.

A segurança dos computadores tornou-se num assunto de segurança nacional; por isso urge combinar ameaça, reserva e resposta, com diferentes áreas de autoridade e responsabilidade, pois só assim se conseguirá eliminar os problemas da prevenção, detecção, resposta e recuperação.

A rede¹⁰ é privada e, por conseguinte, a resposta dada através desta, que se encontra projetada para situações normais em ambiente de paz e com cariz maioritariamente comercial, será sempre condicionada pelos fornecedores.

Quanto à aplicação da lei e às capacidades de defesa do país, a necessidade de uma autoridade capaz de tratar e responder a um acidente é a solução a seguir. Se no momento do ciberataque é impossível determinar se este foi iniciado por “script kiddie” (cracker inexperiente), alguém de dentro da organização, crime organizado ou por uma nação, essa determinação terá que surgir o mais rápido possível porque vai alterar determinantemente o tipo de resposta. Esta pode passar do sector privado para a ordem pública ou mesmo militar com muita rapidez, como tal carecendo da apropriada coordenação e habilitação legal pelas ações a serem tomadas.

Sem uma correta concertação jurídica será muito difícil colmatar as lacunas das leis e regulações existentes; tais lacunas enfraquecem o efeito dissuasor e têm como efeito o incentivo à prática do crime. A Lei deve ser ponderada respeitando as motivações sociais do desenvolvimento tecnológico.

É inadiável a publicação de uma *Lex informática* que evolua de um conjunto de regras sobre fluxos de informação imposta pela tecnologia e redes de comunicações. É ainda necessária uma análise legal multidisciplinar e funcional, assim como mais regulação que permita delinear os limites da moldura legal atual, reforçando a segurança Nacional, enfrentando o cibercrime e minimizando a utilização da internet pelos terroristas. Respondendo a uma grande variedade de riscos e ameaças, permitindo assim às autoridades competentes a proteção de um largo espectro de alvos, desde o individuo às infraestruturas críticas e acima de tudo legitimando a internet como espaço de livre expressão e agregação.

Conceitos legais como privacidade, liberdade de expressão, anonimato e não atribuição dos

¹⁰ Internet.

reconhecidos direitos na sociedade da informação, devem ser sujeitos a fortes restrições.

Neste contexto multidisciplinar que combina os conceitos legais existentes e as suas interpretações ao novo paradigma do ciberconflito, potenciará a discussão construtiva de uma mudança qualitativa e quantitativa.

Os modelos atuais que regem a cibersegurança, focam primariamente o mercado e o cibercrime, revelando-se incompletos e fragmentários.

A noção e o objetivo da cibersegurança mudaram radicalmente nos últimos 10 anos; os ataques não são apenas individuais e com fins económicos, passando a ser multialvos e, como tal, os planos de proteção existentes perderam a sua eficácia. Os acidentes deixaram de ser informáticos para passarem a ser sociais, negociais, criminosos e de segurança nacional.

É essencial a interação entre lei, tecnologia da informação e política pública e, como tal, conceitos, princípios e práticas baseadas nas recentes pesquisas, na experiência de países que lidam/ram concretamente com este problema e nas conclusões dos mais variados fóruns sobre este tópico. Tudo isto constitui um vasto espectro de instrumentos a estudar, de forma a melhorar os conceitos existentes e a agilizar a sua aplicação ao ciberespaço.

A discussão deve ser levada para além da identificação dos problemas e obstáculos: é necessário o estabelecimento de regras e comportamentos que conduza as nações a melhorar o nível de defesa.

É necessário equilibrar a tecnologia, com a política pública e a lei. Por outras palavras, estabelecer uma cibersegurança baseada na tecnologia e respetiva arquitetura - *security by design* - e, ao mesmo tempo, acautelando a política pública de cariz nacional e internacional, enquadrando-a com um quadro legal apropriado que suporte tal equilíbrio.

Como a criação de diferentes campos de especialidades legais envolvidas no manuseamento de um ciber evento (sociedade, telecomunicações, criminal, defesa nacional e conflitos armados).

Porque responder apropriadamente implica um entendimento subjacente da situação (terminologia, conceitos e as bases da tecnologia da informação).

É também necessária uma constante atualização, pois os conceitos das áreas legais envolvidas, necessitam de estar alinhados com a comunidade internacional.

Se existe a dependência das infraestruturas críticas e a dependência destas dos sistemas de informação, torna-se essencial regular a web, pois mesmo que os ciberataques pareçam

semelhantes em termos de alvos, métodos e contexto, a caracterização legal pode variar drasticamente. Essa regulação deve passar pela criação de uma plataforma centralizada e de uma política de segurança comum a todos os sistemas.

Esta responsabilidade começa numa política de estratégia de cibersegurança assente numa cultura de segurança da sociedade, cooperação entre as entidades envolvidas e resiliência dos sistemas, pois só eliminando os elos mais fracos, se consegue a segurança geral dos países, das empresas e do indivíduo.

REFERÊNCIAS

BENTLY, Lione, SUTHERSANEN, Uma, TORREMANS, Paul, *Global Copyright, Three Hundred Years since the Statute of Anne, from 1709 to Cyberspace*, Edward Elgar, Estados Unidos da América, 2010.

CCDCOE, “International Cyber Conflict,” presented at Legal & Policy Conference 2009, Tallinn, Estonia, 2009.

DENNING, D. E., “The Ethics of Cyber Conflict in Information and Computer Ethics,” faculty.nps.edu Versão online no site: <http://faculty.nps.edu/dedennin/publications/Ethics%20of%20Cyber%20Conflict.pdf>.

DIREITO, Faculdade de, Segurança Publica e Privada, 1.º Congresso de Segurança Publica e Privada, 6 a 7 de julho de 2011, Coimbra Editora 2012.

ECONOMIST, The, Versão online no site: www.economist.com/world/international/display_story.cfm?story_id=E1_JNNRSVS.

FEDERAL NEWS RADIO, “Federal Cyber Preparedness”, Versão online no site: <http://www.federalnewsradio.com/?sid=2065555&nid=293>.

REAGLE, J., “Why the Internet is Good,” cyber.law.harvard.edu, 1998. Versão online no site: http://cyber.law.harvard.edu/archived_content/people/reagle/regulation-19990326.html.

SUMIT, Ghosh, TURRINI, Eliot, *Cibercrimes: A Multidisciplinary Analysis*, Springer, Estados Unidos da América, 2011.

TIKK, Eneken, *Comprehensive Legal Approach to Cybersecurity*, Tartu University Press, Estonia.

TIKK, Eneken, *Frameworks for International Cyber Security, Legal and Policy Instruments*, Estonia 2010.

WINGFIELD, Thomas C., *The Law of Information Conflict, National Security Law in Cyberspace*, Aegis Research Corporation, Estados Unidos da América 2000.

WINGFIELD, T. C., MICHAEL, J. B., and WIJESKERA, D., “Optimizing Lawful Responses to Cyber Intrusions,” dodccrp.org Versão online no site: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/290.pdf.

WINGFIELD, T. C. and TIKK, E., “Frameworks for international cyber security, the cube the pyramid and the screen”, 2009.

CYBERLAW

by CIJIC



A EXPERIÊNCIA DE ACOMPANHAMENTO DA ICANN - PEDRO VEIGA

A EXPERIÊNCIA DE ACOMPANHAMENTO DA ICANN *

A criação da ICANN (*Internet Corporation for Assigned Names and Numbers*) ocorreu em 1998 e procurou ser a resposta, rápida, eficiente e baseada em critérios técnicos rigorosos e abertos ao crescimento da Internet que se estava a verificar desde 1995.

Desde a criação da ICANN e até 2013 fizemos um acompanhamento muito próximo das atividades e da evolução desta organização. Este acompanhamento foi feito, até 2008, no seio do GAC (*Government Advisory Committee*) como representante de Portugal na organização. Após 2008 e para realinhar a nossa intervenção face aos estatutos da ICANN, entretanto alterados, passamos a integrar o ccNSO (*Country-code Name Supporting Organization*) na medida em que julgamos ser mais adequado face à nossa responsabilidade como gestor do domínio .pt.

Cremos que o longo período de tempo em que acompanhamos o funcionamento da ICANN nos permitiu ter uma visão do funcionamento da organização que, de um modo genérico, avaliamos como positivo face à dinâmica que a evolução da Internet exige, aliada a uma consulta alargada a todos os parceiros e interesses envolvidos e diversos.

O FUNCIONAMENTO INICIAL DA ICANN

A ICANN foi concebida como uma estrutura assente num conjunto de linhas de orientação interessantes, a saber:

- Conselho de Diretores com uma representatividade geográfica mundial, em torno de 5 regiões: África, América no Norte, América do Sul e Caraíbas, Ásia e Pacífico e Europa; o número de diretores distribuía-se de igual modo por estas regiões;
- Mandato dos diretores obrigava a uma rotatividade, com mandatos de entre 1 a 3 anos, evitando a perpetuação de diretores nos cargos;
- Diretores representavam os diferentes grupos de interesses;

* Pedro Veiga -Centro Nacional de Cibersegurança, Coordenador. Faculdade de Ciências da Universidade de Lisboa, Professor Catedrático.

- Setor privado, com o argumento de que tinha sido este setor o responsável pelos investimentos que conduziram ao desenvolvimento comercial da Internet, devia ter um peso central no funcionamento da ICANN;
- Representação dos setores segundo as linhas mais relevantes do desenvolvimento da Internet global: Registos dos domínios globais (*registries*); agentes de registo (*registrars*); ISP (*Internet Service Providers*); comunidade científica e técnica, grupo de interesses comerciais; grupo de interesses não comerciais, o terceiro setor; grupo de interesses em propriedade intelectual; representantes da comunidade Internet mundial;
- Existência de um grupo de representação dos Governos, mas unicamente com papel de aconselhamento, o GAC.

Numa fase inicial foi dada grande importância aos aspetos relativos aos endereços dos protocolos da Internet, tendo sido criados RIRs (*Regional Internet Registries*) nas 5 regiões geográficas, mas muito à semelhança do que já existia na Europa, o RIPE (www.ripe.net) que tinha sido criado no início da década de 90 do sec. XX com um funcionamento considerado exemplar.

Também foi dada importância à criação de novos domínios de topo globais, para tentar fazer concorrência ao domínio .com. Vieram ser criados novos domínios de topo, tais como .biz, .name, .pro, .museum, .aero, .coop, .cat, ... mas cuja implementação sempre foi limitada, mesmo à data de hoje.

A FASE DE CONSOLIDAÇÃO

A experiência dos anos iniciais da ICANN levou a que tenha sido recolhida experiência do seu funcionamento, tendo vindo a ocorrer uma adaptação dos estatutos para aproximar a organização de um funcionamento mais operacional e globalizado.

Não sendo possível entrar em muito detalhe, veio a ser criado o ccNSO (*Country-code Name Supporting Organization*) que se devia construir com base nas 5 regiões geográficas, o que veio a acontecer com algum atraso em relação à previsão inicial, face à complexidade prevista nos estatutos para a sua criação efetiva.

À semelhança do que acontecia desde a criação da ICANN o funcionamento dos vários grupos realizava-se de um modo aberto e transparente, com uma vertente técnica muito forte, para assegurar o crescimento sustentado e aberto da Internet.

As movimentações organizativas e técnicas eram sempre suportadas em documentos elaborados por especialistas e eram alvo de discussões abertas e prolongadas, para analisar todos os aspetos relevantes, para um crescimento forte mas estável da Internet.

Foi neste contexto que foram feitos desenvolvimentos tão relevantes tais como: DNSSEC, IDNs (*Internationalized Domains Names*), processo de concurso de cerca de 2.000 novos gTLDs, incluindo introdução de IDNs nos *root-servers* (*raíz*).

De especial relevo foram os estudos para avaliar a capacidade da raíz suportar evoluções técnicas, tais como: DNSSEC, IPv6, novos 2.000 gTLDs, IDNs.

O GAC manteve-se como órgão de aconselhamento. Apesar de depois de 2008 termos deixado de integrar o GAC, tendo passado a intervir no seio do ccNSO, acompanhamos os desafios que se colocavam a este órgão, que eram de monta, pelo facto de ter vindo a aumentar o número de países participantes e, também, pelos desafios provenientes das evoluções técnicas e organizativas que descrevemos.

Recentemente verificou-se a autonomização da *IANA function*, uma atividade eminentemente técnica mas que historicamente mantinha supervisão do Governo dos EUA. Não tratamos aqui deste assunto que, por si só, justificaria uma abordagem mais aprofundada.

CONSIDERAÇÕES FINAIS

A ICANN veio a representar um novo modelo de colaboração a nível internacional na gestão de muitos aspetos técnicos de um novo recurso global, a Internet.

Há inúmeras críticas que, ao longo dos anos, tem vindo a ser feitas ao modelo e modo de funcionamento da ICANN. Têm sido discutidas outras alternativas, tais como a passagem das atividades para a ITU, ou a criação de um tratado internacional que contemple as atividades de gestão dos recursos globais da Internet. Infelizmente a realidade de funcionamento destas alternativas não é compaginável com a celeridade que a evolução da Internet impõe. Além disso a politização, que se nota um pouco no funcionamento da ICANN, que resultaria das abordagens mais “pesadas” da ITU ou de outra alternativa mais tradicional, tememos que fosse incompatível com a velocidade de evolução da Internet e poderia representar um retrocesso face ao que a ICANN vem fazendo.

Mas claro que há problemas no modo como a ICANN está a funcionar, nomeadamente aspetos jurisdicionais, cuja relevância tem que ser avaliada face às evoluções recentes.

CYBERLAW

by CIJIC



ICANN, O “*NOVO DEUS*” NA INTERNET

- MANUEL SILVA PEREIRA

RESUMO: “*Se a Internet tem um Deus, ele é provavelmente Jon Postel*”, escreveu o The Economist, em 1997, um ano antes da Administração Clinton-Gore privatizar os recursos críticos da “rede das redes”. Líder da *Internet Assigned Names Authority*, que viu nascer no “seu” Instituto de Ciências da Informação da Universidade do Sul da Califórnia, Postel recusou o apodo, favorecendo ao invés a cooperação global para operar uma Internet “segura e robusta”. Assumida pela ICANN, nos termos de um *no-cost-to-the-government-agreement*, a função vital de alocar e gerir os identificadores únicos do sistema de nomes de domínio permaneceu quase duas décadas sob a supervisão de um só país, os E.U.A. Ao adquirir carta de alforria, em 30 de Setembro de 2016, a organização passou a ser responsável perante a “comunidade empoderada de stakeholders”, mas manteve inalterada a sua jurisdição. Para os cidadãos do ciberespaço nenhuma alteração é visível, mas o “novo Deus na Internet” prega aos fiéis sem tratado ou convenção internacional que o legitime. Com a lente focada na IANA e no processo de globalização, a presente comunicação elabora sobre o que de substantivo se altera na governação da Internet e sobre os argumentos a favor e contra uma transição que a Administração Obama quis ver concluída antes das presidenciais de Novembro.

Palavras-chave: IANA, ICANN, Governação da Internet, E.U.A.

ABSTRACT: “*If the Net does have a God, he is probably Jon Postel*,” wrote The Economist in 1997, a year before the Clinton-Gore Administration decided to privatize the critical resources of the Internet. Director of the Internet Assigned Names Authority, born at USC Information Sciences Institute, Postel declined the nickname, instead favoring global cooperation to operate a “secure and robust” network. Inherited by ICANN, under a *no-cost-to-the-government-agreement*, the vital function of allocating and managing the unique identifiers of the domain name system remained almost two decades under the supervision of a single country, the US. On September 30, 2016, the organization became only responsible to the empowered community of stakeholders, with revised bylaws but an unchanged jurisdiction. For the citizens of cyberspace no change is visible, but the “*new God on the Internet*” preaches to the faithful without a treaty or international convention that legitimizes it. With the lens focused on the IANA and the globalization process, this paper elaborates on what substantive changes happened in Internet governance and on the arguments for and against a transition that the Obama Administration wanted to see completed before the November presidential elections.

Key words: IANA, ICANN, Internet Governance, U.S.A.

ACRÓNIMOS:

AC – Advisory Committee

ADN – Ácido Desoxirribonucleico

AS – Autonomous Systems

ASCII – American Standard Code for Information Interchange

ccTLD – Country Code Top-Level Domain

CSC – Customer Standing Committee

gTLD – Generic Top-Level Domain

DARPA – Defense Advanced Research Projects Agency

DNS – Domain Name System

DNSSEC – Domain Name System Security Extensions

DoC – U.S Department of Commerce

GAC – Governmental, Advisory Committee

GAO – U.S. Government Accountability Office

IANA – Internet Assigned Names Authority

ICANN – Internet Corporation for Assigned Names and Numbers

IDN – Internationalized Domain Names

IETF – Internet Engineering Task Force

IGO – Intergovernmental Organization

IP – Internet Protocol

ISI – Information Sciences Institute

ITU / UIT – União Internacional de Telecomunicações

GNSO – Generic Names Supporting Organization

NTIA – National Telecommunications and Information Administration

NU – Organização das Nações Unidas

PTI – Public Technical Identifier

RIR – Regional Internet Registry

RZERC – Root Zone Evolution Review Committee

RZF – Root Zone Files

RZMA – Root Zone Maintainer Service Agreement

SO – Supporting Organization

USC – University of Southern California

WIPO / OMPI – Organização Mundial da Propriedade Intelectual

WSIS – World Summit on the Information Society

ICANN, O “NOVO DEUS” NA INTERNET *

Ao adotar uma governação multissetorial, que coloca nas mãos de atores não-governamentais a gestão de recursos críticos para o funcionamento da rede, a ICANN inova no plano político e no das relações internacionais, não sem que vozes se tenham erguido para questionar a legitimidade e responsabilização da nova organização.

Wolfgang KLEINWACHTER, 2016

A data de 30 de Setembro de 2016 entra nas atas da governação para enaltecer o momento em que, liberta da supervisão dos E.U.A., a Corporação da Internet para a Atribuição de Nomes e Números, a.k.a. ICANN, adquire carta de alforria.

Entidade privada, sem fins-lucrativos, a organização nasce em 1998 para coordenar e gerir os identificadores únicos da Internet, recursos críticos para a estabilidade e segurança do sistema de comunicação global. O desempenho das funções IANA, como designado, encontra na herança tecnológica e nos contratos sucessivamente outorgados pela autoridade nacional para as telecomunicações e informação (NTIA) do Ministério do Comércio (DoC) dos E.U.A., o seu fundamento e legitimidade.

Quase duas décadas volvidas sobre o que foi prometido como transitório, o cordão umbilical com o governo estado-unidense é cortado, transitando para a comunidade de stakeholders, dotada de poderes reforçados, a missão de confrontar e, sendo o caso, invalidar as decisões da ICANN e as obrigações que impõe a quem com ela coopera ou presta serviço.

Para os utilizadores, “cidadãos do ciberespaço” desde o “Consenso de Marraquexe” (Março 2016), nenhuma alteração é visível. Representados por uma entidade supranacional, continuam a navegar, sem sobressalto de maior, pelo intangível universo de bits e bytes que globaliza a informação e as ideias.

A contrário, defensores e oponentes da transição operada, dela afirmam, a um tempo, que consagra o modelo de governação multiparticipada, o ideal de uma Internet universal, diversa e inclusiva, bem como a “persistência e coragem de muitos indivíduos e organizações na

* Comunicação à «1ª Conferência Internacional sobre Segurança da Informação e Direito Constitucional do Ciberespaço / Sessão V», Faculdade de Direito de Lisboa, 17 e 18 de Novembro de 2016

materialização do que é melhor para a Internet” (Brown, 2016); e a outro, que compromete a liberdade na rede, reforça o poder e influência dos governos, favorece a captura da ICANN por grupos de interesses e aliena um bem comum, propriedade do Estado, sem a requerida autorização do Congresso e em contravenção ao estatuído na Constituição.

Com a lente focada na IANA e no processo de privatização, a presente comunicação elabora sobre o que de substantivo se altera na governação da rede, e sobre os argumentos a favor e contra a transição que a Administração Obama quis ver concluída antes das presidenciais de Novembro.

I. FUNÇÕES IANA.

A Internet é uma “rede de redes”, governada de forma distribuída. O modo como opera, estável e seguro, não depende de nenhum governo ou autoridade central, antes resulta da adesão voluntária dos seus utilizadores a protocolos, com *standards* definidos por organizações técnicas. Sendo aqueles livres de abandonar o sistema a qualquer momento, já o mesmo não ocorre com os dispositivos de conexão que, a não serem conformes, ficam impossibilitados de comunicarem entre si.

Surgida na década de 70 do século passado, a Internet Assigned Names Authority (IANA) é uma das mais antigas entidades do ecossistema de governação. Responde pela alocação e manutenção dos identificadores únicos e sistemas numéricos dos protocolos da Internet, tendo em vista o “suave” funcionamento do sistema. As atividades que desenvolve agrupam-se em três categorias:

1. Função numérica, ou a alocação de blocos de endereços IP (Internet Protocol) aos Registadores Regionais da Internet (Regional Internet Registries, RIR) que, em seguida, os distribuem pelos agentes de registo nacionais e estes pelos provedores de acesso à rede e pelos utilizadores finais. O endereço IP de cada dispositivo de conexão – e são, hoje, milhares de milhões! – é único, localiza-o num servidor e autoriza o seu titular a enviar e receber mensagens, fazer pagamentos online e a aceder à informação em todos os outros dispositivos conectados, a qualquer hora e em qualquer lugar.

2. Função nominal, que inclui o sistema de nomes de domínio (DNS) e a zona-raiz de servidores. O DNS permite navegar na Internet, ao “resolver” em nomes as sequências alfanuméricas dos endereços IP. Espaço único, formado pelos mais de 1400 domínios de topo

existentes (genéricos e com código de país), tem na zona-raiz de servidores e no diretório-mestre de domínios de topo os seus recursos estruturais. Atualizados uma vez por dia, os ficheiros da zona-raiz – onde constam os endereços IP dos servidores-raiz e os dados dos operadores credenciados em cada domínio de topo – são públicos. As alterações aos ficheiros, que desde 1991 careciam da aprovação formal do DoC / NTIA, são agora autorizadas pela ICANN e tecnicamente validadas pela VeriSign, Inc., nos termos do “Root Zone Maintainer Service Agreement” (RZMA) celebrado em Setembro de 2016 e válido por oito anos .

3. Função de parâmetros dos protocolos. Os protocolos configuram a estrutura e o formato dos dados; graças a eles, a informação é gerada e recebida em modo *standard*, interoperável. Por seu turno, os parâmetros de protocolo são comandos ou identificadores que gerem a transmissão dos dados; compostos por sequências de letras, números ou símbolos, dão corpo a uma base de dados pública. Esta contém cerca de 2800 registos e sub-registos; sempre que um novo protocolo é definido e aprovado, vide pela Internet Engineering Task Force (IETF), a IANA adiciona os seus parâmetros à base de dados, para que os criadores de *software* os adotem nos seus programas e aplicações.

Uma nova organização privada, não-lucrativa, designada Public Technical Identifiers (PTI), assegura desde 1 de Outubro de 2016, por contrato com a ICANN, o desempenho das funções IANA. Com natureza técnica, a PTI não estabelece políticas, nem critérios para a alocação de nomes e números ou o clausulado contratual com os RIR. Cabe-lhe, porém, tudo fazer para “manter inalterada a confiança da comunidade nos serviços que presta de forma isenta, responsável e eficaz” (PTI Mission Statement).

II. FARDO GOVERNAMENTAL.

Ao abreviar, em post recente, os mais de 30 anos de história da IANA, Kleinwachter (2016) lembra que a organização nunca foi o “controller” da Internet, mas sim o “enabler”, o seu potenciador.

Jon Postel, a quem o The Economist apodou de “o Deus da Internet”, lidera a organização desde os primórdios, com o auxílio de um único colaborador e no âmbito de um contrato entre o “seu” Instituto de Ciências da Informação (ISI), na Universidade do Sul da Califórnia, e a DARPA, a agência de projetos de pesquisa avançada do Ministério da Defesa dos E.U.A.

A invenção da world wide web, no início da década de 90, acelera a expansão da rede e convida à criação de novos domínios genéricos de topo (gTLD), para lá dos existentes desde os anos 80 – .COM, .NET, .ORG, .GOV, .EDU e .MIL – o que Postel quer fazer em articulação com a União Internacional de Telecomunicações (ITU / UIT) e a Organização Mundial da Propriedade Intelectual (WIPO / OMPI).

Reticente, a Administração Clinton opta por outro caminho, o de incentivar o surgimento de um ente privado, com dimensão internacional, formatado segundo a lei do Estado da Califórnia para as organizações não-lucrativas (§501 (c) (3)), fiscalmente isentas, que “prosseguem interesses públicos e caritativos” (§3 do clausulado de incorporação, 1998). A ICANN nasce em 1998, com um ADN revelador, o “atenuar do fardo governamental e a promoção do interesse público global na estabilidade operativa da Internet” (idem).

O propósito é alcançável pela “manutenção da conectividade universal da Internet” (ibidem), sendo que “um misto de imperativos técnicos e ideais democráticos, de colaboração entre todas as partes e de empoderamento dos utilizadores – o modelo multistakeholder – tudo temperado pela crença nos mercados e na sua capacidade de fomentar um grau elevado de competitividade” (Bygrave and Bing, 2009) se destaca no clausulado estatutário, aprovado em 1998, revisto e emendado em Dezembro de 2001, Julho de 2014 e, por último, em 2016, para incorporar as alterações resultantes da privatização das funções IANA.

Desde a criação que a ICANN, e o modelo eleito para a governar, são alvo de crítica e controvérsia. Kaplan (1998) lembra o “formato inusual escolhido” e cita Post, para quem “uma organização apta a controlar o sistema de endereçamento da Internet tem o poder de “estrangular” o ciberespaço”. Fuller (2001), por sua vez, prefere sublinhar o “momento constitucional”, corporizado na passagem para mãos privadas do controlo governamental sobre a rede.

A autora, como outros, ecoa o sentimento de desconforto dos governos, “arrumados” numa comissão de aconselhamento (Governmental Advisory Committee, GAC), sem voto para impor as recomendações que consensualiza. São, todavia, questões de legitimidade e de responsabilização (accountability) as que mais contribuem para alimentar a polémica.

Diane Cabell, membro do Boston Working Group, estranha a ausência de acionistas ou de membros filiados na organização, bem como a ausência de concorrência e de supervisão regulatória, o que na prática equivale a um “board que não presta contas a ninguém”. A concentração de poder nas mãos de uns poucos, “running this thing for the whole world”, preocupa Karl Auerbach, que desde 1973 coopera no desenvolvimento e expansão da Internet. E, até, Becky

Burr, administradora da NTIA para os assuntos internacionais, na carta que em Outubro de 1998 dirige ao diretor executivo do ISI, faz notar os aspetos “substantivos e operacionais” que, a não serem superados, colocam em cheque a organização. Entre eles, a carta menciona a falta de transparência do processo decisório, os conflitos de interesses dos membros da direção, o papel que a ICANN a si própria se reserva na alocação de domínios com código de país (ccTLD) e a inexistência de mecanismos de responsabilização do board, quer no plano financeiro, como no da representatividade geográfica.

Por todos, vale a ironia de Zittrain (1998). Ao contextualizar o processo de criação e avaliar o perfil da organização nascente, o professor de Harvard constata que “ao mesmo tempo que o governo quer privatizar o DNS, faz o possível e o impossível para que a nova entidade se assemelhe em tudo... a um governo”.

III.COMPROMISSO DINÂMICO.

“Supervisão” ou “liderança”, como nuançado por Ira Magaziner, conselheiro de Clinton, o papel dos E.U.A. na governação da ICANN é pomo de discórdia entre governos durante a Cimeira Mundial da Sociedade da Informação (WSIS), convocada pelas Nações Unidas em duas fases, em 2003 e 2005.

De um lado, os próceres do controlo intergovernamental da ICANN, assente no princípio da igualdade soberana dos Estados, que a Carta da organização consagra; do outro, a defesa incondicional da natureza técnica da gestão dos recursos, onde o político não tem lugar, sob pena de frustrar o desenvolvimento de uma tecnologia promotora de “inovação sem permissão”.

A Agenda de Tunes (2005), documento final da cimeira, faz a ponte e avança com um “compromisso dinâmico” (Kleinwachter, 2016), que os 193 Estados-membros subscrevem. Com efeito, o parágrafo 68 prescreve um “papel e responsabilidades iguais” para os Estados na governação internacional da Internet e no garantir da “estabilidade, segurança e continuidade” da rede; porém, as expectativas quanto ao futuro divergem, confiando uns que o contrato IANA caducará no curto / médio prazo e, outros, que a sua execução será supervisionada por um conselho intergovernamental, sem que tal comprometa a relevância que o “cordão umbilical” estado-unidense assume no potenciar da Internet, fazendo dela a tecnologia estruturante das sociedades do século XXI.

Os anos que se seguem não invertem o *status quo*. Projetos conjuntos e “afirmação de compromissos” entre a NTIA e a ICANN são sucessivamente renovados, ao mesmo tempo que os protestos de países como a Rússia, China, Índia, Brasil e Arábia Saudita, ecoam, ruidosos, dentro e fora das cimeiras e reuniões internacionais, para expor o descontentamento e pugnar por um modelo de governação multilateral.

Ao tornar pública, em Março de 2014 – no rescaldo do caso Prism / Snowden (Junho 2013) e em antecipação à NETMundial – Encontro multissetorial global sobre o futuro da governação da Internet (Maio 2014), convocado pela então presidente do Brasil, Dilma Rousseff – a intenção de privatizar as funções IANA e responsabilizar a comunidade global da Internet pela supervisão do DNS, o modelo multistakeholder de governação apresenta-se consolidado e de boa saúde, recomendado e fortalecido como fora pelo G8 (Deauville, 2011), pela Comissão Europeia e pela própria UIT, que do insucesso do Dubai, em 2012, evoluiu, na plenária de Busan (2014), para o reconhecimento da ICANN como a “entidade adequada para gerir o sistema de nomes e números da Internet”.

Assim, para lá dos requisitos formais de segurança, estabilidade e resiliência, da abertura da rede e de resposta às “necessidades e expectativas dos utilizadores, clientes e parceiros dos serviços IANA”, a ninguém soou estranho que o DoC / NTIA exigisse, para proceder à transição, não apenas que o modelo multissetorial fosse preservado e aprofundado, como ainda que governo ou entidade intergovernamental alguma viessem reclamar a herança tecnológica a que não tinham direito.

Dois anos depois, 32 mil *e-mails* trocados, 800 horas despendidas em seis centenas de reuniões e mais de 1.100 eventos, nos cinco continentes, convocados para “apresentar, debater, organizar e planear as etapas” (ICANN, 2016), a proposta de transição entra na reta final. Dividida em duas partes, abarca quer o fim da supervisão dos E.U.A. e a “entrega” à ICANN das funções IANA, quer a revitalização dos anémicos mecanismos de responsabilização da organização perante a comunidade de stakeholders.

Como manter uma ICANN íntegra e responsável, ao abrigo de intenções hegemónicas ou de captura por grupos de interesses, bem como reforçar o papel dos Estados na governação sem todavia lhes conferir o direito de veto, foram questões dominantes na agenda e nas intervenções dos atores chamados a participar. Os compromissos alcançados estão longe de apaziguar os descontentamentos, mas só o tempo provará ter-se tratado, como proclama o board da ICANN, de uma “evidente demonstração da força e de afirmação do modelo multistakeholder”.

IV. PRÓS e CONTRAS.

Em carta endereçada à Câmara dos Representantes, em Abril de 2014, Karl Auerbach, que em tempos exerceu funções de direção na ICANN, questiona a urgência da transição. Para ele, não era a “estabilidade técnica” que estava em causa, pois a ICANN, e os 400 milhões de dólares faturados em 2013, apenas numa pequena parte serviram para a garantir. Pelo contrário, aquilo em que a organização se concentrava era em tirar partido do monopólio sobre a indústria de domínios “para negociar direitos territoriais”, para outorgar “privilégios de comércio”.

Assim sendo, o papel da NTIA não era o de supervisionar a ICANN, mas sim o de escudá-la de questões incómodas, como as que por norma “são formuladas às entidades privadas que agem no sentido de restringir a concorrência e a inovação”. Para o autor, o que a transição visou foi “atenuar a perceção externa de uma ICANN instrumento da hegemonia dos E.U.A. sobre a Internet” e, em simultâneo, responsabilizar a organização perante a comunidade de utilizadores, deixando de ser a arena privilegiada de concessão de interesses comerciais que foi no passado.

As objeções de Auerbach não foram ouvidas nos corredores do Congresso, nas candidaturas presidências e nos think-tank conservadores. Uns e outros lutaram até ao limite pela anulação e/ou adiamento da transição, com o argumento do novo modelo não estar suficientemente testado e da prudência recomendar gradualismo, sob pena da liberdade na Internet ficar comprometida, do vazio deixado pelos E.U.A. ser preenchido por governos autoritários, da ICANN “escapar” à jurisdição estado-unidense e da rede das redes se ver fragmentada em internets nacionais ou regionais, com perda do seu carácter global. Os tribunais a que recorreram em derradeira instância, para impedir o que o Congresso se mostrou incapaz de consensualizar, não reconheceriam mérito ou razão aos fundamentos invocados.

O novo modelo, em vigor desde 1 de Outubro, assenta na separação estrutural entre o técnico e o político, entre o desempenho das funções IANA e a definição das políticas públicas orientadoras, reservando o primeiro a uma nova entidade, subsidiária da ICANN, a Public Technical Identifiers ou PTI. Uma nova comissão, denominada Customer Standing Committee (CSC), supervisiona o desempenho operacional da PTI.

Com estatutos revistos e já aprovados, a ICANN substitui-se à NTIA na aprovação das alterações à zona-raiz. A serem conformes aos critérios estabelecidos, serão em seguida validadas pela VeriSign, Inc., que entretanto viu prorrogado até 2024 o unsponsored registry agreement, que lhe confia a gestão exclusiva do domínio de topo .COM e dos seus mais de 127 milhões de subdomínios ativos.

No capítulo da *accountability*, as decisões da direção da ICANN passam a ser escrutinadas pela comunidade Internet, composta pelos stakeholders identificados na Agenda de Tunes (#35) – utilizadores, setor privado, entidades técnicas e governos – e representados nas organizações de apoio (supporting organizations, SOs) e nas comissões consultivas (advisory committees, ACs) em que a ICANN se ancora. Reconhecidos como decisional participants, dispõem de poderes reforçados na supervisão do board, em especial no que toca à composição e modo de seleção dos seus membros, aos planos estratégicos, aos orçamentos anuais e à aprovação de propostas de alteração dos estatutos.

Com assento na comissão de aconselhamento governamental (GAC), os 160 Estados atuam a partir de agora com completa igualdade, mas nem por isso veem aumentar a sua influência, já que se manteve inalterado o papel consultivo que lhes foi originalmente atribuído. Em contrapartida, as recomendações que emitem por consenso, vide sobre as políticas públicas, em particular as que “interajam com as leis nacionais ou as convenções e tratados internacionais”, passam a requerer uma maioria de 60 por cento do board para serem rejeitadas.

Entretanto, sobre o argumentário usado para contestar ou legitimar o processo de transição e o modelo de gestão da “nova” ICANN, valerá a pena uma reflexão mais demorada, a que o tempo e a prática poderão emprestar pertinência e valor. Assim:

- A comunidade Internet não é uniforme; os grupos que a compõem prosseguem, em regra, os interesses que lhes são próprios e tendem a abster-se quando as decisões os não envolvem ou afetam. No decurso da transição, bateram-se pela existência de membros filiados, com direitos e obrigações a consignar pelos estatutos; acabaram por aceitar um regime muito mais fraco, chamado de “sole designator”, que lhes confere poder tão só quando estão em causa alterações aos “fundamental bylaws”. As demais, não-fundamentais, como a aprovação do orçamento, requerem o consenso prévio dos vários grupos, o que pode revelar-se espinhoso e difícil de alcançar;

- Nenhum governo toma assento no board, pelo que a “captura do DNS por um governo autoritário”, acompanhada do eventual condicionamento da liberdade de expressão e de filtragem dos conteúdos que navegam pela rede, afigurar-se-á improvável. Os testes de stress (work stream 1 and 2), feitos a uma ICANN sem a supervisão governamental, concluíram que a “abertura e natureza inclusiva do modelo, as decisões bottom-up por consenso, o processo de resolução de conflitos e os instrumentos de recurso existentes, bem

como a transparência das reuniões e encontros públicos, em que todos são convidados a participar”, mitigam os riscos e frustram as tentativas de controlo hegemónico. Será?

- Decisões por consenso são de louvar, mas nem sempre ocorrem. Uma semana sobre a transição e eis que os governos e organizações intergovernamentais (IGOs) se vêm acusados de desrespeitar o processo decisório estabelecido. A questão remonta a 2011 e é relativa à proteção especial que as IGOs clamam para si e para os acrónimos por que são conhecidas, isentando-os de concorrência ou disputa. Reunidas em small group com o staff da ICANN, o consenso a que chegaram conflitua com o parecer do Generic Names Supporting Organization (GNSO), para quem nada justifica conceder às IGOs um tratamento similar ao de uma marca registada. A divergência, porventura menor e de fácil superação, serve aos críticos para questionar a disponibilidade do GAC e das agências especializadas das N.U. em participarem, como os demais, em processos de elaboração de políticas sob a liderança do GNSO ou, ao invés, prosseguirem os interesses que lhes são caros em reuniões à porta fechada com o board;

- A nova ICANN permanece como organização privada, não-lucrativa, com sede na Califórnia e, enquanto tal, sujeita à lei do Estado. Nenhum preceito estatutário a imuniza das decisões dos tribunais, que sentenciam com respeito da lei e do interesse público dos E.U.A.. Confrontada com sentenças judiciais desfavoráveis, não pode a ICANN eximir-se ao seu cumprimento. Função global, a alocação de nomes de domínio e os critérios que a enformam não devem, por princípio, estar sujeitos às decisões de instâncias judiciais de um único país;

- Para modificar o clausulado de incorporação, bem como as disposições relativas à sede física da ICANN e / ou à sua natureza de entidade privada não-lucrativa, os novos estatutos obrigam a uma maioria qualificada de votos dos membros da direção. A dificuldade em reunir consenso sobre a questão, tem incentivado outros a refletir sobre os potenciais benefícios de uma ICANN intergovernamental ou, como avançado pelo Senado francês, em Julho último, de fazer evoluir a organização para uma entidade dotada de personalidade jurídica internacional, imune à lei dos E.U.A., à semelhança da organização das Nações Unidas e das suas agências especializadas;

- Ao contrário do invocado pelos congressistas Grassley, Goodlatte, Issa e Cruz, em carta endereçada ao Comptroller General, em Setembro de 2015, os ficheiros da zona-raiz (RZF) do DNS nunca foram propriedade federal. Como Mueller explicitou em 2015 – e no

ano seguinte o Government Accountability Office (GAO, 2016) reiterou – a RFZ não tem copyright, sendo uma lista dos domínios de topo existentes e dos servidores de nomes que os alojam. Na relação contratual estabelecida com a ICANN e a VeriSign, Inc., jamais o DoC / NTIA reivindicou a propriedade da RFZ ou das instalações físicas e programas de software que operam os 13 servidores-raiz. A única exceção é a dos servidores operados pela NASA, pelo U.S. Army Research Lab e pelo NIC do departamento de Defesa, que continuam, todavia, a ser operados por entidades federais, não tendo transitado para qualquer outra esfera.

V.CONCLUSÃO.

A privatização das funções IANA ocorre 18 anos após ter sido prometida. No ínterim, a ICANN progrediu, inovando com os nomes internacionalizados de domínios (IDNs) (carateres não-ASCII), o protocolo de segurança DNSSEC e, em 2005, com o programa de expansão de domínios genéricos de topo, que lhe tem facultado avultados dividendos – a título de exemplo, o gTLD .WEB foi recentemente leiloado por 135 milhões de dólares.

No plano interno, o processo aberto, transparente, conduzido da base para o topo, com a participação “on equal footing” dos diversos atores, prosseguido na elaboração e aprovação das políticas públicas orientadoras, confirma a validade e eficácia do modelo multiparticipado para administrar os recursos críticos que, desde 1 de Outubro de 2016, lhe foram confiados, sem outra supervisão que não a da comunidade empoderada da Internet.

Madura, autónoma e financeiramente robusta, a ICANN atinge a maioria e sai de “casa dos pais” decidida a seguir rumo próprio. No percurso que trilhar, deve ter todavia presente que nenhum tratado internacional – fonte de autoridade, aceite e observada por todos – a legitima e que o regime regulatório que impõe coercivamente a quem com ela colabora, evidencia “características semelhantes às de um poder soberano” (Mueller, 2002), que ninguém lhe reconhece ou outorga.

Como conclui Hartwig (2010), a ICANN “institui regras potencialmente mais relevantes – a observar e cumprir de forma estrita – do que a maioria das emanadas pelas organizações internacionais”. A justificação está nessas regras se mostrarem “imprescindíveis à operabilidade da rede. Sem elas, a Internet não funciona e, sem a Internet, o mundo de hoje não trabalha”.

REFERÊNCIAS:

AUERBACH, Karl (2014), *Letter to Congress Regarding NTIA and ICANN*, The Amateur Computerist, Fall 2015, volume 26 No. 1; acedido em <http://www.ais.org/~jrh/acn/Acn26-1.pdf>

BURR, Becky (1998), *Internet Corporation for Assigned Names and Numbers (ICANN)*, U.S. DoC – National Telecommunications & Information Administration, press-release, October 20, 1998; acedido em <https://www.ntia.doc.gov/legacy/ntiahome/press/icann102098.htm>

BYGRAVE, Lee A., BING, Jon (2009), *Internet Governance, Infrastructure and Institutions*, Oxford: Oxford University Press

CSMONITOR (2016), *Yes, ICANN*, Monitor's Editorial Board, March 6, 2016; acedido em <http://www.csmonitor.com/Commentary/the-monitors-view/2016/0306/Yes-ICANN>

FULLER, Kathleen E. (2001), *ICANN: The Debate over Governing the Internet*, iBRIEF / Media & Communication Cite as 2001 Duke L. & Tech. Rev. 002; acedido em <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1000&context=dltr>

GAO (2016), *Department of Commerce – Property Implications of Proposed Transition of U.S. Government Oversight of Key Internet Technical Functions*; acedido em <http://www.gao.gov/products/B-327398>

IANA (2016), *PTI Mission Statement*; acedido em <https://www.iana.org/about>

ICANN (2012), *Articles of Incorporation of Internet Corporation for Assigned Names and Numbers*; acedido em <https://www.icann.org/resources/pages/articles-2012-02-25-en>

KAPLAN, Carl S. (1998), *A Kind of Constitutional Convention for the Internet*, Cyber Law Journal, October 23; acedido em <https://partners.nytimes.com/library/tech/98/10/cyber/cyberlaw/23law.html>

KLEINWACHTER, Wolfgang (2016), *Breaking Nonsense: Ted Cruz, IANA Transition and the Irony of Life*; acedido em http://www.circleid.com/posts/20160921_breaking_nonsense_ted_cruz_iana_transition_and_irony_of_life/

MUELLER, Milton L. (2002), *Ruling the Root, Internet Governance and the Taming of Cyberspace*, MA: The MIT Press

MUELLER, Milton L. (2015), *Does the IANA Transition Constitute a Transfer of US Government Property*; acedido em <http://www.internetgovernance.org/2015/09/29/does-the-iana-transition-constitute-a-transfer-of-us-government-property/>

MUELLER, Milton L. (2016), *“Inextricably Intertwined”: the ICANN-Verisign Root Zone Management Agreement*; acedido em <http://www.internetgovernance.org/2016/07/01/inextricably-intertwined-the-icann-verisign-root-zone-management-agreement/>

SZOKA, Berin, SCHAFFER, Brett, ROSENZWEIG, Paul (2016), *ICANN Transition is Premature. Unanswered Questions Regarding an Extension*; acedido em http://docs.techfreedom.org/TF_White_Paper_IANA_Transition.pdf

TELEANU, Sorina (2016), *The IANA Stewardship Transition: what is Happening?*; acedido em <http://www.diplomacy.edu/blog/iana-stewardship-transition-what-happening>

THUNE, John, GRASSLEY, Charles, UPTON, Fred, GOODLATE, Bob (2016), *Letter to Loretta Lynch and Penny Pritzker*; acedido em <https://energycommerce.house.gov/news-center/press-releases/senate-and-house-chairs-call-administration-reconsider-icann-internet>

WSIS (2005), *Tunis Agenda for the Information Society*, WSIS-05/Tunis/Doc/6 (Rev.1)-E, 18 November 2005; acedido em <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>

CYBERLAW

by CIJIC



«CONTRIBUTOS PARA O DEBATE SOBRE A "*GOVERNAÇÃO DA INTERNET*"»

- ANA CRISTINA NEVES

«CONTRIBUTOS PARA O DEBATE SOBRE A "GOVERNAÇÃO DA INTERNET"»*

Qualquer que seja a abordagem ao tema da Governação da Internet, esta começa sempre por levantar questões como “*para que serve a “Governação da Internet”?*”, “*que impacto tem a “Governação da Internet”?*” ou “*quem são os atores envolvidos na “Governação da Internet”?*”. Mas para responder a estas perguntas, importa colocar como questão de partida a seguinte: “*O que é a “Governação da Internet”?*”.

Na tentativa de contribuir para o debate sobre a Governação da Internet nesta I Conferência Internacional de Lisboa sobre Segurança da Informação e Direito Constitucional do Ciberespaço, esta comunicação está dividida em cinco partes e ainda uma sexta onde indicarei alguma da bibliografia recomendada para o aprofundamento do tema. Na 1.^a parte forçar-me-ei na evolução tecnológica da Internet, na 2.^a no seu impacto social e económico, na 3.^a aprofundo o tema da Governação da Internet e, na 4.^a, falarei sobre as implicações da Internet nas questões de Jurisdição. Por fim, darei sumariamente conta das iniciativas do IGF (*Internet Governance Forum*) aos níveis nacional e regional e mundial.

1. A EVOLUÇÃO TECNOLÓGICA DA INTERNET

As décadas de 1960 e 1970 são consideradas os pontos de partida da Internet, devido à criação da ARPANET (*Advanced Research Projects Agency*) e, posteriormente, da MILNET. Estes projetos de investigação, cujo objetivo passou pela ligação das redes académica e militar, foram altamente financiados pelo governo dos Estados Unidos, em pleno período de Guerra Fria, e antecederam o surgimento da NSF NET (*National Science Foundation Network*). Para este efeito

* Comunicação à «1.^a Conferência Internacional sobre Segurança da Informação e Direito Constitucional do Ciberespaço / Sessão V», Faculdade de Direito de Lisboa, 17 e 18 de Novembro de 2016.

Ana Cristina Neves, Diretora do Departamento da Sociedade da Informação, Fundação para a Ciência e a Tecnologia, I.P.

muito contribuíram cientistas como Vinton Gray Cerf (Vint Cerf) ou Robert Elliott Kahn (Bob Kahn)¹ que estiveram na génese dos protocolos TCP/IP.

Uma segunda fase desta evolução tecnológica, a do alargamento das suas funcionalidades e utilização, ocorre entre as décadas 1980 e 1990. É durante este período que se dá a fusão, ligação e alterações das arquiteturas das redes, e se inicia a sua fase de expansão, com a adesão do setor privado a esta “nova” ferramenta de comunicação e também de comercialização de produtos e serviços.

É, assim, a partir de meados da década de 1990 que a terceira fase se inicia com a Internet a tornar-se causa e efeito do desenvolvimento de novos dispositivos e serviços. O seu desenvolvimento tecnológico gera interesse e atrai novos *stakeholders* para a sua governação, para além das comunidades técnica e académica, como sejam, os utilizadores, as empresas, os governos, e as organizações internacionais. Esse movimento provoca uma maior consciencialização para a necessidade de investigação e desenvolvimento da Internet no sentido de responder aos desafios e necessidades que vão sendo identificados e sentidos. Ocorre, por isso, uma fase em que a Internet contribui significativamente para uma redução dos custos de produção, disponibiliza instrumentos em que os utilizadores e consumidores (de conteúdos) passam também a ser produtores, possibilita formas mais rápidas de comunicação e permite uma maior facilidade de acesso, não só à Internet mas, principalmente, ao Conhecimento, levando à democratização do mesmo.

2. O IMPACTO SOCIAL E ECONÓMICO

É inegável que este desenvolvimento tecnológico teve um grande impacto social e económico. Isso decorre da crescente dependência das Tecnologias de Informação e Comunicação (TIC) e da Internet, nomeadamente no aparecimento de novos modelos de negócio, de um novo paradigma social de interação e comunicação entre pessoas e instituições, de novas formas de perceção das realidades local, regional e mundial (“revolução” dos meios de comunicação social) e na identificação de novas necessidades de formação e capacitação.

Este processo conduz-nos para a chamada Sociedade da Informação e do Conhecimento, onde são cada vez mais os novos desafios tecnológicos e sociais, acompanhados, não obstante, de um acentuar da fratura digital.

¹ Bob Kahn continua ainda a desenvolver investigação na área da ligação dos objetos e páginas da Internet, nomeadamente no conceito da *Digital Object Architecture* (DOA).

Mas este desenvolvimento social e económico acrescenta um outro impacto: o político. Dada a rapidez do seu desenvolvimento, a tecnologia associada à Internet, cria a noção de que as políticas públicas se tornam rapidamente obsoletas ou a a noção de que a visão política não acompanha a visão daquela tecnologia e das suas necessidades. Encontram-se agora intervenientes não-governamentais ou institucionais, quando antes a intervenção política se encontrava quase exclusivamente na esfera dos Governos. Constatase também que o facto de a Internet não dispor de fronteiras como as que encontramos no espaço físico, levanta novas questões de soberania nacional, desafios às jurisdições nacionais, obrigando ao estabelecimento de uma nova forma de diplomacia/relações externas. Verifica-se, então, o surgimento de um novo conceito com que os governos e os países se veem confrontados neste espaço *ciberfísico*: a Partilha de Poder.

3. A “GOVERNAÇÃO DA INTERNET”

Face ao que antecede, o debate em torno da Governação da Internet é fundamental, não só para a compreensão de como a “rede das redes” é gerida e mantida, bem como determinante para a consciencialização dos riscos de uma Internet refém de interesses.

Inicialmente, o controlo e manutenção da Internet, não esquecendo as suas origens académicas e militares, foi assegurado pela DARPA (*Defense Advanced Research Projects Agency*). Posteriormente, e até final da década de 1990, esse controlo foi assegurado por entidades ou grupos técnicos (*task forces* técnicas) ligados ou promovidos pelo governo dos EUA. Em 1988, é criada a IANA (*Internet Assigned Numbers Authority*) com a função explícita de assegurar a gestão e atribuição de endereços de IP bem como outros aspetos técnicos relacionados com a infraestrutura. Uma década depois, em 1998, é finalmente criada a ICANN (*The Internet Corporation for Assigned Names and Numbers*), assinando um contrato com o governo dos EUA para a gestão dos nomes e números (endereços e IP’s na Internet) e o DNS (*Domain Name System*). Esta última, uma associação não-governamental sem fins lucrativos, assume uma função de maior decisão política no espaço do DNS, continuando a IANA a assegurar a vertente mais técnica, mas agora associada à ICANN.

A ideia de que a Internet está nas mãos de uma entidade controlada indiretamente pelo governo de um único país, neste caso o dos EUA, está assim na origem das pressões levadas a cabo por diversos Governos, por diversas associações oriundas da sociedade civil e das comunidades técnica e académica que conduziram aos primeiros passos da discussão do tema a nível global. Face ao que antecede, a Organização das Nações Unidas (ONU) promove a *World*

Summit on the Information Society (WSIS) que se deve realizar em duas fases, em 2003 e 2005. Em 2003, a WSIS tem lugar em Genebra, e foi o ponto de partida para uma discussão alargada, com vista a alcançar um entendimento global sobre a Governação da Internet. No final desta WSIS de 2003, foi criado o *Working Group on Internet Governance* (WGIG) que define que a «*Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*» Em 2005, a WSIS reúne-se em Tunes, e a Governação da Internet é assumida e reconhecida, a nível mundial, como um tema de extrema importância política, económica, social e geo-estratégica.

NA WSIS de 2005 é adotada a Agenda de Tunes onde é formalmente estabelecido um fórum mundial de discussão da Governação da Internet sob a égide do Secretário Geral da ONU, por um período de cinco anos: o *Internet Governance Forum* (IGF). Para este efeito, em particular o art.º 72.º da Agenda de Tunes, o IGF é definido como um espaço de discussão e debate abrangente, ao nível internacional, sobre princípios técnicos e políticos (política e políticas públicas) da Internet. Um dos aspetos bastante salientados é que nele devem participar todos os *stakeholders* em pé de igualdade. Desde então o IGF tem vindo a realizar-se anualmente². O primeiro mandato, que se iniciou em 2006, previa a realização do IGF por um período de 5 anos. O IGF acabou por ver o seu mandato prolongado por mais 5 anos em 2010 e, em 2015, a Assembleia Geral da ONU adotou uma Resolução para que o IGF se realize por um período de mais 10 anos³, até 2025.

A crescente importância e sucesso do IGF para a Governação da Internet, levou a um movimento espontâneo e voluntário muito interessante de multiplicação de iniciativas nacionais e regionais do IGF um pouco por todo o mundo. Não obstante, as preocupações sobre o controlo técnico da Internet continuaram e continuam presentes nestes debates. A ICANN, que participa ativamente nestas discussões a todos os níveis, nacional, regional e mundial, adota um modelo de gestão que, defende, inclui a participação de todos os setores. No entanto, apesar de estar organizado segundo o modelo *multistakeholder*, poder-se-á considerar que se trata de um modelo com evidentes desequilíbrios no que concerne ao poder de decisão. O *Governamental Advisory Committee* (GAC), que representa os governos, os principais responsáveis pela definição e

2 2006 – Athens, Grécia; 2007 – Rio de Janeiro, Brasil; 2008 – Hyderabad, Índia; 2009 – Sharm El Sheikh, Egito; 2010 – Vilnius, Lituânia; 2011 – Nairobi, Quénia (1.º de um novo ciclo de 5 anos); 2012 – Baku, Azerbaijão; 2013 – Bali, Indonésia; 2014 – Istanbul, Turquia; 2015 – João Pessoa, Brasil; 2016 – Guadalajara, México (1.º de um ciclo de 10 anos).

3 No decurso das discussões e negociações ocorridas num longo processo que foi intitulado de “WSIS +10”.

implementação de políticas públicas, não têm qualquer poder vinculativo nos pareceres que emite, ao contrário dos grupos que representam o setor privado.

Na sequência do fim do contrato de supervisão do governo dos EUA sobre a ICANN, foi definido um novo modelo de gestão da ICANN e da IANA, a partir de 1 de outubro 2016, após um longo processo de discussão e negociações, onde se redefiniu o papel de alguns *stakeholders* nos processos de decisão. É criada em Agosto de 2016 a corporação *Public Technical Identifiers* (PTI) que, com a privatização das funções da IANA a partir de 1 de Outubro de 2016, se tornou na organização responsável pela operação das funções da IANA, o que inclui principalmente a gestão dos identificadores únicos da Internet. A PTI é uma afiliada da ICANN.

Na sequência da aprovação dos novos estatutos da ICANN, os governos, representados pelo GAC, passaram a incorporar uma “comunidade mais empoderada” no processo de decisão, a *Empowered Community*, e onde adquiriram algum poder vinculativo nos seus pareceres em algumas matérias, desde que esses mereçam a concordância dos restantes *stakeholders* representados nessa “comunidade”, pois a *Empowered Community* age como um único órgão na gestão. Um desafio que continua em curso é a avaliação do impacto que estas alterações, tanto dos estatutos como da criação da nova “comunidade” terão no “modus operandi” do GAC.

A complexidade que podemos verificar que existe ao nível do processo de decisão espelha também uma outra complexidade já referida anteriormente: o elevado número de atores envolvidos e os múltiplos interesses que representam. A isto, pode-se também acrescentar outra variável de complexidade: o nível em que cada um deles atua. Seja ao nível das infraestruturas, seja ao nível técnico ou ao nível social e económico.

Face a esta rede de interesses, atores envolvidos e níveis de intervenção na discussão da Governação da Internet, pode considerar-se esta discussão como um processo passível de ser representado por:

- 1) Atores envolvidos

- a. Representantes dos diversos setores e grupos de interesse na sociedade: Sociedade Civil, Setor Privado, Governos, Comunidades Técnica e Académica, Organizações Internacionais;

- 2) Discussões Abertas - A discussão é conduzida de forma descentralizada por uma rede internacional *multistakeholder*

- a. Processos formais e informais de discussão sobre políticas públicas e normas: orientações, princípios e procedimentos sem poder vinculativo com vista

a alcançar níveis comuns de ação e interoperabilidade (documentos de trabalho, mensagens, declarações, etc.);

3) Políticas e Normas

a. Recomendações que acabam por ter influência nos processos de decisão (políticos e técnicos) porque têm por base um diálogo *multistakeholder* onde ganham legitimidade;

4) Operação, Equipamentos e Serviços

a. Determinante na interoperabilidade global da Internet e fortemente dependente dos níveis anteriores – com impacto social e económico.

Poder-se-á verificar, então, a pertinência do processo e a razão pelo qual a discussão da Governação da Internet deve continuar a ser fomentada, pois diz respeito aos processos que determinam a forma de gestão da Internet, às tomadas de decisão (técnicas ou políticas) que têm impacto em todos os setores da sociedade, à forma como a Internet é usada e como evolui, às discussões aos níveis nacional, regional e global que têm e terão uma influência determinante no presente e futuro da Internet, e porque as discussões ultrapassam as questões técnicas e cobrem todas as áreas e políticas⁴. Importa ainda referir que este tema tem continuado a despertar o interesse, e também desconfiança, por parte de vários países o que tem levado à realização de outras iniciativas⁵ com grande impacto a nível mundial, na discussão e resolução de questões relacionadas com a Governação da Internet.

4 E.g acesso e diversidade cultural / interconexão e regulação de preços / multilinguismo e conteúdos locais / reforçar acessibilidade para pessoas com necessidades especiais / literacia digital / segurança (safety) / cybersegurança / vigilância / privacidade / liberdade de expressão online / Internet & TICs para os *Sustainable Development Goals* (Agenda para o Desenvolvimento da ONU) / economia da Internet / direitos humanos online / envolvimento (compromisso) da juventude / questões de género / cooperação *multistakeholder* / recursos críticos da Internet / neutralidade da net / computação em nuvem / Internet das coisas.

5 Podem destacar-se as iniciativas IBSA – proposta de transferência das competências da ICANN para um comité da ONU em 2011, a *Montevideo Statement on the Future of Internet Cooperation* – defesa por um ambiente de discussão e decisão onde todos os *stakeholders* estivessem em pé de igualdade (contou com o apoio da ICANN e dos RIRs) em 2013, a *Global Multistakeholder Meeting on the Future of Internet Governance* (NETmundial) – discussão de políticas de Governação da Internet que contrariassem a hegemonia de alguns países em 2014 e a *NETmundial Initiative Conference* – tentativa da continuação da discussão anterior e discussão da perspetiva *multistakeholder* vs. perspetiva multilateral (envolvimento do WEF) também em 2014.

4. A INTERNET E A JURISDIÇÃO

A natureza global e transfronteiriça da Internet coloca obviamente questões de territorialidade e jurisdições aos Estados soberanos, o que constitui um tema novo e extremamente sensível para os Governos. Como podem ser geridos os abusos registados na rede e disputas jurídicas desencadeadas entre os utilizadores, os serviços que estes utilizam na Internet e as autoridades públicas entre os diferentes países? Qual a lei aplicável para regular condutas/comportamentos ilícitos na Internet? Como preservar a proteção dos direitos humanos *on-line*? Como gerir a coexistência de diferentes normas num espaço partilhado como a *Web*?

A necessidade de aprofundar a investigação nesta área tem originado iniciativas para tentar responder a estas e outras questões levantadas para ausência de fronteiras na Internet. A título de exemplo podemos destacar a “Internet & Jurisdiction (I&J)”⁶ que se constitui como uma rede global *multistakeholder* desde 2012, e que visa facilitar a cooperação transnacional, tendo como mote a preservação de uma Internet global. Para além de eventos⁷ que permitem a discussão de forma multidisciplinar nesta matéria, esta iniciativa disponibiliza também alguns instrumentos de utilidade como recursos e uma base de dados⁸ relativa a decisões judiciais.

Ainda um aspeto interessante de análise conceptual é a terminologia utilizada nesta discussão: “*Governance of the Internet*”, que admite a intervenção ao nível da governação dos protocolos, normas, endereços e evolução da arquitetura técnica, na qual existe um ecossistema de governação institucional complexo que inclui organizações tais como a W3C, IETF e ICANN; e “*Governance on the Internet*” que remete para a utilização da Internet, aplicações e serviços que funcionam por cima da dimensão física e lógica, bem como os comportamentos na Internet.

Identifica-se, nesta área, a existência de lacunas ao nível institucional, a necessidade de uma mudança de paradigma e de desenvolver novos mecanismos de cooperação institucionais inovadores, a passagem de uma cooperação internacional entre Estados para uma cooperação transnacional baseada em princípios de participação aberta e responsabilidade partilhada entre todos os *stakeholders* e, por fim, a passagem de Tratados intergovernamentais para novos mecanismos jurídicos de cooperação baseados em normas políticas que assegurem essa transnacionalidade.

6 www.internetjurisdiction.net

7 A 1ª Conferência “Global Internet and Jurisdiction” realizou-se de 14 a 16 de novembro 2016 identificando temas relacionados com Dados, Conteúdos/liberdade expressão e Domínios vs Jurisdição como áreas de possível cooperação.

8 <http://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTYtMTAifQ>

5. AS INICIATIVAS NACIONAIS E REGIONAIS DA “GOVERNAÇÃO DA INTERNET” - O CASO DA EUROPA E DE PORTUGAL

Como já foi atrás referido, o sucesso do IGF⁹ e da adoção de discussões assentes no modelo *multistakeholder* despoletou um conjunto de iniciativas com o objetivo de analisar e discutir a Governação da Internet levando em consideração as características nacionais e regionais.

Portugal não foi exceção e desde 2010 que organiza a iniciativa nacional da Governação da Internet¹⁰ inserida no Fórum para a Sociedade da Informação. Uma iniciativa que é atualmente coordenada pela Fundação para a Ciência e a Tecnologia e que procura envolver, não só na discussão mas também na estrutura da organização, para além do setor público, diversas outros atores oriundos do setor privado, das comunidades técnica e académica e da sociedade civil.

Ao nível regional da Europa existe, desde 2008, a iniciativa EuroDIG – *Pan-European Dialogue on Internet Governance*¹¹, cujo fórum de discussão decorre anualmente, em junho, de forma totalmente *multistakeholder*. Em 2016 realizou-se em Bruxelas, tendo sido o *host* a Comissão Europeia, e, em 2017, irá realizar-se em Talin, na Estónia. Portugal também já foi o anfitrião do EuroDIG, numa sessão realizada em Lisboa, em 2013.

Um pouco por todo o mundo e todos os continentes estas iniciativas têm vindo a ter uma importância crescente, pois trazem para o IGF as preocupações e posições muito concretas não só dos interesses de cada grupo de *stakeholders* mas também as preocupações desses mesmos *stakeholders* influenciados pelo ambiente nacional e regional.

9 www.intgovforum.org

10 www.governacaodainternet.pt (histórico anterior a 2012: www.unic.pt/index.php?option=com_content&task=section&id=29&Itemid=331)

11 www.eurodig.org

6. LEITURA RECOMENDADA

(ordem cronológica)

WSIS, 2003, “Declaration of Principles” (doc: WSIS-03/GENEVA/DOC/4-E)

WSIS, 2003, “Plan of action” (doc: WSIS-03/GENEVA/DOC/5-E)

WSIS, 2005, “Tunis Commitment” (doc: WSIS-05/TUNIS/DOC/7-E)

WSIS, 2005, “Tunis Agenda for the Information Society” (doc: WSIS-05/TUNIS/DOC/6(rev.1)-E)

OECD, 2008, “The Seoul Declaration for the Future of the Internet Economy”

COUNCIL OF EUROPE, 2011, “Declaration by the Committee of Ministers on Internet governance principles”

EUROPEAN COMMISSION, 2014, “... Internet Policy and Governance - Europe’s role in shaping the future of Internet Governance” (COM(2014)72 final)

NETmundial, 2014, “NETmundial Multistakeholder Statement”

OECD, 2014, “OECD Principles for Internet Policy Making”

UN General Assembly, 2016, “Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society” (A/RES/70/125)

COUNCIL OF EUROPE, 2016, “Internet Governance – Council of Europe Strategy 2016-2019” (CM(2016)10-final)

OECD, 2016, “Ministerial Declaration on the Digital Economy (“Cancún Declaration”)”.

CYBERLAW

by CIJIC



ALGUMAS REFLEXÕES SOBRE A GOVERNAÇÃO E A REGULAÇÃO DA INTERNET - LUÍS DE LIMA PINHEIRO

ALGUMAS REFLEXÕES SOBRE A GOVERNAÇÃO E A REGULAÇÃO DA INTERNET*

INTRODUÇÃO:

Fala-se por vezes de governação da internet numa aceção muito ampla, que abrange quer a regulação jurídica da internet quer a organização e atuação das entidades que coordenam o seu funcionamento (1). Sem colocar em dúvida a interligação entre estes dois aspetos, parece-me conveniente distingui-los, reservando o termo “governação” para a coordenação institucional da rede.

A *génese da internet* tem ainda hoje uma grande influência no modo como é governada e regulada. A internet surgiu historicamente nos EUA como um projeto da *Advanced Research Project Agency*, ligado ao Departamento de Defesa (2). Desenvolveu-se a partir daí por via da interconexão de redes criadas principalmente pela sociedade civil. O que deu origem a uma governação e regulação descentralizadas realizadas essencialmente por entidades autónomas. Estas entidades assumiram a tarefa de garantir o seu funcionamento e desenvolvimento, em especial no que toca à definição de padrões relativos aos protocolos de comunicação e à atribuição de nomes de domínio e de endereços que permitem a identificação de computadores ligados à rede, em articulação com as autoridades dos EUA.

* Luís de Lima Pinheiro. Professor Catedrático da Faculdade de Direito da Universidade de Lisboa. Texto que serviu de base à comunicação apresentada na I Conferência Internacional de Lisboa sobre Segurança da Informação e Direito Constitucional do Ciberespaço, organizada pelo Centro de Investigação Jurídica do Ciberespaço e pelo Centro de Investigação de Direito Público da Faculdade de Direito da Universidade de Lisboa, em novembro de 2016.

Esta comunicação resume e atualiza o estudo “Reflections on Internet Governance and Regulation with Special Consideration of the ICANN”, *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal*, Vol. 3 No. 41, 08/17/2016 (=CyberLaw by CIJIC 2 (Junho de 2016) 41-71, também acessível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2796402).

1 - Ver conclusões da Cimeira das Nações Unidas para a Sociedade da Informação – Genebra 2003/Tunis 2005, in <http://www.itu.int/wsis/index.html>.

2 - Ver “A Brief History of the Internet”, in <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet>.

Com a *globalização da rede*, e a sua crescente importância como meio de comunicação e informação utilizado em todas as esferas da vida social, política, económica e cultural, estas marcas de origem vieram colocar novos desafios.

Perante o carácter eminentemente privado da internet, o desafio da articulação com os valores e políticas públicas promovidos pelos Estados e organizações internacionais.

Perante a estrutura descentralizada de governação e regulação da rede, a necessidade de assegurar a sua coordenação.

Perante a ligação umbilical às autoridades dos EUA, a preocupação de globalizar e, para alguns, mesmo de intergovernamentalizar as entidades que coordenam a internet.

Na atualidade, os governos dos principais países democráticos, designadamente ao nível da União Europeia e dos EUA (3), bem como os principais foros em que se tem expressado a comunidade global da internet (4), convergem em que a internet deve ser governada segundo um *modelo de multiparticipantes* [*multistakeholders*], que inclui não só os governos e as organizações intergovernamentais, mas também a sociedade civil, designadamente as comunidades académica e técnica, os agentes económicos e as associações de utilizadores da internet.

Isto não exclui, naturalmente, algumas divergências sobre os contornos deste modelo.

A este modelo de multiparticipação corresponde, no plano da *regulação*, uma co-regulação em que as regras aplicáveis são criadas primariamente por fontes autónomas que constituem a expressão da comunidade global da internet, mas em que também é necessária uma regulação estadual e supraestadual que complemente essa regulação autónoma.

Este modelo de multiparticipação vingou na transferência do controlo do sistema de normas de domínio para a comunidade global da internet concretizada no mês passado nos termos que adiante referirei.

3 - Ver Comunicação da Comissão Europeia “A política e a governação da Internet. O papel da Europa na configuração da governação da Internet no futuro” COM (2014) 72 final e Press Release da U.S. Commerce Department’s National Telecommunications and Information Administration (NTIA) de 14/3/2014.

4 - Ver designadamente o NETmundial Multistakeholder Statement saído do Global Multistakeholder Meeting on the Future of Internet Governance realizado no Brasil em 2014, in <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>, o Report by the Panel on Global Internet Cooperation and Governance Mechanisms “Towards a Collaborative, Decentralized Internet Governance Ecosystem”, 2014, in http://internetgovernancepanel.org/sites/default/files/ipdf/XPL_ICAN1403_Internet%20Governance%20iPDF_06.pdf, e as “Perspectives on the IANA Stewardship Transition Principles”, publicadas pela Internet Society em 2015, in http://www.internetsociety.org/sites/default/files/IANA-Transition-Perspectives-20150728-en_0.pdf.

As minhas reflexões incidirão sobre aspetos muito gerais da governação e regulação da internet

A) GOVERNAÇÃO DA INTERNET

Enquanto *realidade global*, a internet deve ser objeto de uma governação e de uma regulação tendencialmente globais ⁽⁵⁾. A principal alternativa que se coloca a este respeito é entre a intergovernamentalização e a globalização baseada num modelo de multiparticipação de todos os interessados ⁽⁶⁾. É à luz dos *objetivos que devem nortear a governação da internet* que a questão tem de ser apreciada.

A governação da internet deve, em primeiro lugar, garantir a unidade, abertura, gratuidade e liberdade de acesso à internet, contrariando as tendências para segmentar ou restringir o acesso à internet por países que pretendem limitar as liberdades de expressão e informação na rede.

A governação da internet deve também assegurar a eficiência, estabilidade e segurança no funcionamento da rede, tirando o máximo partido das entidades e experiências que a têm garantido, e preservando o espírito inovador que tem marcado o desenvolvimento da internet.

Por último, mas não em último lugar, a governação da internet deve permitir que as entidades que têm a seu cargo a prossecução de interesses públicos legítimos tenham suficiente participação nos processos de decisão bem como uma adequada articulação entre os mecanismos de governação e regulação autónomas e o exercício das competências normativas dos Estados e organizações internacionais.

Será de seguir a via da intergovernamentalização?

Não existe uma organização intergovernamental em posição de satisfatoriamente assumir as tarefas de governação da internet.

A internet, afetando muitos aspetos da vida social, também toca a esfera de atuação de diversas organizações intergovernamentais, como é o caso da Organização Mundial do Comércio

5 - Ver, designadamente, as considerações que teci em “Portugal, Europe and Globalization in the Private Law Perspective”, in Portugal, Europe and the Globalization of the Law, org. por Vasco Pereira da Silva, 46-57, Ebook, Lisboa, 2015 (também acessível em SSRN: <http://ssrn.com/abstract=246534> 9, 52-53, com mais referências.

6 - Sobre os vários modelos de governação da internet, ver Michael RUSTAD – Global Internet Law, 2.^a ed., St. Paul, MN, 2016, 94 e segs.

(OMC), mas o âmbito de atuação destas organizações não abrange os aspetos centrais da governação e regulação da internet ⁽⁷⁾.

A organização intergovernamental que poderia estar mais vocacionada para o efeito é a União Internacional de Telecomunicações (UIT), que constitui hoje uma agência especializada das Nações Unidas ⁽⁸⁾. Entre outras atribuições, a UIT elabora padrões técnicos básicos do funcionamento da infraestrutura das comunicações. A UIT aspira a alargar a sua atividade aos padrões técnicos de todas as tecnologias de informação e comunicação, mas a sua estrutura organizativa, baseada em delegados dos Estados-Membros com igualdade de voto, tem-se mostrado inadequada à realidade da internet.

Como observa MIGUEL ASENSIO ⁽⁹⁾, a UIT não se mostra apta a superar as divergências importantes que se verificam à escala internacional em matéria de proteção dos direitos fundamentais e dos direitos de propriedade intelectual na internet e de garantia do acesso e do intercâmbio de informação na rede por parte de todas as pessoas. Isto refletiu-se na recusa de um grande número de Estados, entre os quais os Estados-Membros da UE, os EUA e o Japão em assinar as Atas Finais da Conferência Mundial de Telecomunicações Internacionais, realizada em 2012, que incluíam uma revisão do Regulamento das Telecomunicações Internacionais. Algumas regras deste instrumento suscitam dúvidas que podem facilitar um maior controlo do tráfego através da internet e a nova versão introduzia certas disposições sobre o controlo da rede de alcance incerto na sua aplicação por Estados que não são favoráveis à abertura da internet e não partilham das mesmas conceções em matéria proteção de direitos fundamentais.

Por conseguinte, *merece preferência uma globalização baseada num modelo de multiparticipação*. Assim, a governação da internet deve caber, em primeiro lugar, a entidades autónomas, inclusivas, transparentes e responsáveis, em que a comunidade global da internet esteja adequadamente representada ⁽¹⁰⁾.

Na realidade atual, a internet é governada principalmente por *entidades autónomas que formam uma estrutura descentralizada com correlações complexas* ⁽¹¹⁾.

7 - Ver também Pedro MIGUEL ASENSIO – Derecho Privado de Internet, 5.^a ed., Cizur Menor (Navarra), 2015, 43-44.

8 - Ver João MOTA DE CAMPOS (org.) – Organizações Internacionais, 4.^a ed., Coimbra, 2010, 601 e segs.

9 - N. 7, 44-45.

10 - Ver também Rolf WEBER – Shaping Internet Governance: Regulatory Challenges, em colaboração com Mirina Grosz e Romana Weber, Zurique, Basileia e Genebra, 2009, 63, 78 e 116-117.

11 - Cf. WEBER (n. 10) 43 e segs. e MIGUEL ASENSIO (n. 7) 46 e segs.

Uma destas entidades é a *Internet Corporation for Assigned Names and Numbers (ICANN)*, que apesar de ter *atribuições bastante limitadas*, desempenha funções particularmente importantes para o funcionamento da internet e pode constituir o embrião de uma entidade central de coordenação da mesma. Com efeito, a ICANN tem por missão coordenar, de forma geral, os sistemas de identificadores exclusivos da Internet globais e, particularmente, garantir a operação estável e segura dos sistemas de identificadores exclusivos da Internet (Art. 1.º/1 dos Estatutos da ICANN).

Uma parte importante das atribuições da ICANN, é desempenhada pela *Internet Assigned Numbers Authority (IANA)*, que constitui hoje um departamento da ICANN ⁽¹²⁾.

A ICANN é uma pessoa coletiva de Direito estadual, constituída em 1998 segundo o *California Corporation Code* como pessoa coletiva de fim não lucrativo e com sede em Los Angeles, na Califórnia.

O controlo da ICANN pelo Departamento do Comércio dos EUA terminou em 2009, mas a ICANN continuou ligada ao mesmo Departamento por um contrato [*Affirmation of Commitments*] que cessou neste ano de 2016. A Administração dos EUA optou pela transferência das funções de supervisão que desempenhava relativamente ao sistema de nomes de domínio para a comunidade global de multiparticipantes na internet e considerou a ICANN como a entidade mais bem colocada para gizar um plano para essa transição.

No entanto, o caminho que acabou por ser seguido foi o de confiar a dois grupos formados por representantes da comunidade global da internet – o *IANA Stewardship Transition Coordination Group (ICG)* e o *ICANN Cross Community Working Group on Accountability (CCWG)* – a elaboração de uma proposta com vista à transferência do controlo do sistema de nomes de domínio para a comunidade global da internet.

O IGP apresentou a *Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA)* em março de 2016 ⁽¹³⁾. Este documento é integrado por um relatório do ICG, que contém um sumário da proposta, e pelas propostas da *Domain Names Community*, da *Internet Number Community* e da *Protocol*

12 - Designadamente a coordenação da atribuição de endereços IP e de números autónomos e da gestão do servidor de raiz no DNS.

13 - <https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf>.

Parameters Registries Community, que o desenvolvem ⁽¹⁴⁾. Esta proposta obteve o apoio da *Internet Society* ⁽¹⁵⁾ e foi revista pela NTIA ⁽¹⁶⁾.

Seguindo-se esta proposta, foi criada uma filial da ICANN – *Post-Transition IANA (PTI)* – para atuar como operador das funções da IANA ⁽¹⁷⁾. A ICANN mantém a sua sede nos EUA e subcontrata a operação das funções da IANA com a PTI ⁽¹⁸⁾. A PTI é, à semelhança da ICANN, uma sociedade de fim não lucrativo constituída ao abrigo da lei da Califórnia ⁽¹⁹⁾, e a sua administração é nomeada pela ICANN ⁽²⁰⁾.

Em outubro de 2016, o contrato entre a ICANN e a Administração dos EUA caducou, por forma que a transição das funções IANA foi concretizada ⁽²¹⁾. Os estatutos da PTI - que correspondem aos pontos assinalados da proposta -, e os contratos entre a ICANN e a PTI foram aprovados pelos Conselhos de Administração do ICANN e da PTI ⁽²²⁾. Entretanto, em maio de 2016, o Conselho de Administração do ICANN já tinha aprovado novos estatutos contemplando o *Customer Standing Committee* ⁽²³⁾, composto principalmente por representantes de operadores de registo de nomes de domínio eleitos pelas respetivas comunidades ⁽²⁴⁾. A constituição deste Comité foi completada em agosto de 2016, com vista à sua entrada em funcionamento com a cessação do contrato entre a ICANN a Administração dos EUA ⁽²⁵⁾. Verificado este evento, *a função de supervisão até agora exercida pela Administração dos EUA quanto aos nomes de domínio passou para o Customer Standing Committee* ⁽²⁶⁾.

14 - N.º 12.

15 - Internet Society Statement in Support of the IANA Stewardship Transition, 24 de maio de 2016, in <https://www.internetsociety.org/news/internet-society-statement-support-iana-stewardship-transition>.

16 - Cf. Lawrence STRICKLING – “Reviewing the IANA Transition Proposal”, Blog de 11 de março de 2016, in <https://www.ntia.doc.gov/blog/2016/reviewing-iana-transition-proposal>.

17 - N.ºs 13 e 23.

18 - Ibidem.

19 - N.º 1108.

20 - N.º 1112.

21 - Cf. <https://www.icann.org/news/announcement-2016-10-01-en>.

22 - Cf. <https://www.icann.org/news/blog/final-implementation-update>.

23 - Art. 17.º dos Estatutos em vigor.

24 - N.ºs 1327 e 1328. O Comité é composto no mínimo por 2 representantes de operadores de registo nomes de domínio genéricos de topo, 2 representantes de operadores de registo de nomes de domínio geográficos, eventualmente 1 representante de operador de registo de nome de domínio não incluído nas categorias anteriores e 1 elemento de ligação da PTI. Podem ser designados elementos de ligação por outras organizações. Os membros e elementos de ligação do comité são designados pelas suas respetivas comunidades (n.º 1334), que são a *Country Code Names Supporting Organization*, o *Registry Stakeholder Group* e a *Generic Names Supporting Organization* (n.º 1336).

25 - Cf. *IANA Implementation Planning Status Report*, de 12 de Agosto de 2016, in <https://www.icann.org/en/system/files/files/iana-stewardship-implementation-planning-status-12aug16-en.pdf>.

26 - N.º 13 e P1. Annex G, n.ºs 1308 e segs.

A constituição da ICANN e da PTI segundo o Direito do Estado da Califórnia e a localização das suas sedes neste Estado não significa que toda a sua atividade seja regida pelas leis aí vigentes e que só os tribunais locais tenham competência para os litígios relativos a essa atividade.

Do ponto de vista do Direito Internacional Público, não é apenas a “nacionalidade” de uma pessoa coletiva de Direito privado que pode fundar a competência legislativa para regular a sua atividade e a competência jurisdicional para decidir litígios a ela relativos.

Do ponto de vista do Direito Internacional Privado, o Direito segundo o qual se constituiu a pessoa coletiva e o Direito do Estado da sua sede são decisivos em matéria do seu estatuto pessoal, mas já não são necessariamente aplicáveis noutras matérias, designadamente quanto aos contratos celebrados pela pessoa coletiva, à sua responsabilidade extracontratual e às questões relativas a propriedade intelectual. A localização da sede da pessoa coletiva também tem relevância para a determinação dos tribunais competentes nestas matérias mas, no que toca, designadamente, aos contratos, à responsabilidade extracontratual e à propriedade intelectual não exclui a competência de outras jurisdições nem, em princípio, o reconhecimento das suas decisões.

Nem sempre as críticas dirigidas à solução adotada têm em conta estas considerações.

O processo de transição das funções IANA abrange apenas um aspeto limitado da governação da internet, que diz principalmente respeito ao controlo do sistema de nomes de domínio. Mas a transferência deste controlo para a comunidade de multiparticipantes na internet pode representar *um primeiro passo no sentido da governação da internet por uma entidade autónoma globalizada baseada num modelo de multiparticipação*, que parece representar a opção mais adequada aos objetivos e valores que devem nortear a governação e a regulação da internet.

Perante as políticas anunciadas pela Comissão Europeia e pela Administração dos EUA, que acompanham as conclusões dos principais foros da comunidade global da internet, existe designadamente a possibilidade de a ICANN evoluir no sentido de uma estrutura de multiparticipação desta comunidade na governação da internet.

Nesta evolução, a assunção pela ICANN, ou pela entidade que lhe suceda, do papel de uma Organização Não-Governamental (ONG), e o reconhecimento a esta ONG, pelos Estados e pelas organizações internacionais, de um estatuto relevante perante o Direito Internacional Público, mostra-se idónea à sua consolidação como *entidade autónoma, global e multiparticipada*.

B) A REGULAÇÃO DA INTERNET

A regulação da internet depara com limites e condicionamentos dado:

- o carácter global da rede, que na maior parte dos casos põe em jogo mais de uma ordem jurídica estadual, e que *obsta à possibilidade de o seu funcionamento coordenado e harmonioso ser assegurado por regimes estaduais;*
- o reduzido significado que o território dos Estados assume no ciberespaço, que se projeta entre outros aspetos na *dificuldade em localizar os utilizadores da internet e as atividades que realizam no seu seio;* e
- a sua *estrutura descentralizada*, coordenada por diversas entidades em regra autónomas, com esferas de ação específicas e, por vezes, também geograficamente limitadas.

Verifica-se, por isso, uma *produção normativa por centros autónomos* que desempenham um papel de regulação da internet, embora de alcance limitado: trata-se essencialmente de definir os padrões técnicos necessários ao funcionamento da internet e da atribuição de nomes de domínio e de endereços IP.

Segundo o *princípio da subsidiariedade* ⁽²⁷⁾, a internet deve ser regulada por regras criadas por fontes autónomas que constituem a expressão da comunidade global da internet, designadamente regras emanadas de entidades que representam esta comunidade e costumes e usos observados pelos seus membros salvo na medida em que estejam em causa a proteção de direitos ou a prossecução de finalidades públicas que não possam ser adequadamente promovidos por Direito autónomo ⁽²⁸⁾.

A *prioridade da regulação autónoma*, além de corresponder a uma conceção democrática e aberta de sociedade ⁽²⁹⁾, é justificada por diversas vantagens, designadamente:

27 - Sobre o sentido e alcance do princípio da subsidiariedade na regulação das situações transnacionais, enquanto corolário do valor liberdade, ver Luís de LIMA PINHEIRO – Arbitragem Transnacional. A Determinação do Estatuto da Arbitragem, Coimbra, 2005, § 40, e Direito Internacional Privado, vol. I – Introdução e Direito de Conflitos/Parte Geral, 3.^a ed., Coimbra, 2014, 333-334. Mais em geral, sobre o seu significado para a teoria geral do Direito, ver Miguel TEIXEIRA DE SOUSA – Introdução ao Direito, Coimbra, 2012, 64 e segs.

28 - Ver também WEBER (n. 10) 17 e segs.

29 - Ver também WEBER (n. 10) 78-79.

- as regras autónomas são adaptadas à realidade técnica da internet, tendem a adequar-se aos interesses dos seus parceiros e estimulam a participação de todos os interessados na sua elaboração;

- a sua origem garante um elevado grau de efetividade;

- as regras criadas por entidades autónomas são mais facilmente modificáveis do que as regras criadas por instrumentos internacionais razão por que se mostram mais aptas a acompanhar a evolução da internet ⁽³⁰⁾.

Naturalmente que estas vantagens dependem, em maior ou menor medida, da representatividade equilibrada de todos os participantes; da eficiência, transparência e idoneidade do processo de produção normativa; e da atuação dos representantes dos participantes com base no respeito mútuo, na garantia de um núcleo essencial de direitos fundamentais e na devida consideração dos interesses dos outros participantes e do bem comum por forma a garantir que as regras adotadas são aptas para realizar valores comuns perante a consciência dos membros da comunidade global da internet e são compatíveis com as concepções dominantes na comunidade internacional ⁽³¹⁾.

Mas na regulação da internet não entram só em jogo valores jurídico-privados e os valores jurídico-privados a tutelar nem sempre podem ser adequadamente assegurados pela regulação autónoma.

A própria definição de padrões técnicos condiciona a contratação eletrónica, o modo como são oferecidos os bens e serviços em linha, o alcance de certos direitos fundamentais, como o direito à liberdade de informação, à liberdade de expressão, à intimidade da vida privada e à proteção de dados pessoais e, no caso do sistema de nomes de domínio e de endereços de internet, contende com importantes fins de política legislativa ⁽³²⁾.

Nas áreas em que é necessária uma regulação pública – mormente, no domínio do cibercrime, da proteção de direitos de personalidade e de propriedade intelectual ⁽³³⁾, da responsabilidade extracontratual e da proteção dos consumidores -, o caráter global da internet justifica, em princípio, esforços de unificação internacional mediante Convenções internacionais

30 - Os seus custos de produção também são inferiores aos das regras criadas por instrumentos internacionais.

31 - Ver as considerações convergentes de WEBER (n. 10) 22-23, 96 e segs., 120 e 207 e segs.

32 - Como observa MIGUEL ASENSIO (n. 7) 49-50.

33 - Ver, designadamente, Luís de LIMA PINHEIRO - “Algumas considerações sobre a lei aplicável ao direito de autor na internet”, ROA 74 (2014) 13-34, Introdução e I.B (quanto ao risco resultante da deslocalização dos operadores que fornecem acesso a obras protegidas, mediante o estabelecimento em Estados com baixo nível de proteção do direito de autor, para a tutela do direito à colocação da obra à disposição do público).

(³⁴). Com efeito, só regimes internacionais podem proporcionar a eficácia, certeza e previsibilidade das soluções jurídicas nessas matérias, bem como a harmonia jurídica internacional, evitar cumulos de normas e conflitos de deveres que onerem os utilizadores e fornecedores de serviços da rede.

Quando a criação de um regime internacional de âmbito universal depare com dificuldades ponderosas, e haja interesse numa regulação de âmbito regional, também é de admitir, nas áreas em que seja necessária uma regulação pública, a elaboração de Convenções internacionais regionais ou de legislação emanada de organizações regionais, como é o caso da legislação da União Europeia.

Em suma, se a internet deve, no essencial, ser governada autonomamente, será mais apropriado encarar a sua regulação numa perspetiva de complementaridade da regulação autónoma e da regulação pública e, por conseguinte, de *co-regulação* (³⁵).

34 - Ver também WEBER (n. 10) 16-17.

35 - No mesmo sentido, WEBER (n. 10) 5. Em sentido parcialmente diferente, Alexandre DIAS PEREIRA – “Direito Ciberespacial: ‘Soft Law’ or ‘Hard Law’?”, in Est. José Gomes Canotilho, vol. I., 685-710, Coimbra, 2012, 704 e segs., com base em preocupações legítimas, mas sem ter em devida conta, em minha opinião, as decorrências do princípio da subsidiariedade e a relatividade que na esfera global ou transnacional assumem os interesses e políticas públicas de Estados singularmente considerados.



***O PARTILHADOR ENQUANTO “HOMO RECIPROCANS”:
MOTIVAÇÕES E JUSTIFICAÇÕES DOS UTILIZADORES
PORTUGUESES E BRASILEIROS DE INTERNET PARA A PARTILHA
NÃO AUTORIZADA DE OBRAS PROTEGIDAS POR DIREITOS DE
AUTOR ****

MIGUEL CAETANO

* Artigo Peer-review.

RESUMO

Com base nas respostas de 301 indivíduos de nacionalidade portuguesa e brasileira a um inquérito online com amostra por autosselecção, bem como nas declarações posteriores de 16 desses participantes recolhidas por intermédio de entrevistas online -, este artigo visa traçar um retrato mais fidedigno do grau de consciencialização dos utilizadores portugueses e brasileiros de Internet relativamente à natureza ilícita ou lícita dos conteúdos, assim como das verdadeiras motivações, justificações e racionalizações dos que entre estes se assumem como partilhadores:

- Quais as razões que invocam para justificar o download de conteúdos protegidos por direitos de autor?

- O que pensam das consequências dos seus hábitos de partilha nos criadores, editores e o futuro da criação cultural em geral?

- Como encaram as medidas repressivas fomentadas pelas indústrias culturais e implementadas pelos diferentes estados nacionais?

- Que soluções e modelos de negócio apontam para as empresas e associações representantes das indústrias culturais?

Palavras-Chave: partilha de ficheiros; direito de autor; pirataria; Portugal; Brasil

ABSTRACT

Building on a online survey with 301 respondents of Portuguese and Brazilian nationality as well as on a set of 16 online interviews subsequently arranged with some of these individuals, this article aims to draw a more accurate picture not only of the level of awareness of Portuguese and Brazilian Internet users concerning the unlawful or lawful nature of the content downloaded and/or shared by them, but also of the true motives and rationales of those who identify as file-sharers:

- *What rationales do they use for justifying the downloading of copyrighted content?*

- *What is their opinion regarding the consequences of their sharing habits in the lives of creators, publishers and the future of cultural creativity in general?*

- *What do they think of the enforcement measures proposed by copyright industries?*

- *What solutions and business models do they propose to businesses and trade associations representing rights holders?*

Keywords: file sharing; copyright; piracy; Portugal; Brazil

1. INTRODUÇÃO

A 12 de Maio de 2009, a Assembleia Nacional de França aprovou o projeto de lei “Criação e Internet” relativo à implementação de um mecanismo de resposta gradual naquele país europeu prevendo o corte da ligação de banda larga dos utilizadores que fossem apanhados três vezes a descarregar conteúdos protegidos por direitos de autor a partir da Internet. Nesse mesmo dia, quando interrogado sobre a sua opinião a respeito desse sistema, o então ministro da Cultura de Portugal José Pinto Ribeiro considerou que não fazia sentido em Portugal, chegando mesmo a comentar que tal atitude – a “expulsão” de utilizadores da Internet – não era coisa de um Estado de direito:

Nós somos um país que tem uma história e um regime de Estado de Direito específicos. A história é que vivemos 48 anos sobre a ditadura e portanto não compreendemos facilmente soluções que tenham uma leitura possível censória – que alguém está a ver o que estamos a fazer. (Rosário 2009)

Na sua opinião, a partir do momento em que os conteúdos se encontram disponíveis *online* eles deviam poder ser usufruídos por qualquer pessoa que tivesse acesso à rede pelo que qualquer tentativa de impor sanções seria censória:

Estamos a tratar de um área [filmes e música] em que de facto as pessoas, têm a sensação de que alguém lá pós e eles limitam-se apenas a usar o que está disponível: como alguém encontra notas de banco no chão. (Rosário idem)

Ainda de acordo com Pinto Ribeiro, somente a utilização da Internet para a prática de crimes como a pedofilia ou o tráfico de seres humanos devia ser investigada e punida. Em contrapartida, os filmes e as músicas disponíveis *online* seriam “*de quem os agarrasse.*” À luz da natureza não-rival e não exclusiva dos bens informacionais (Benkler 2006, p. 36; Quiggin 2013, p. 91; Rosa 2006, p. 90; Rosa 2009, p. 31), a analogia escolhida pelo ex-governante deve ser entendida como plausível – se não totalmente, pelo menos parcialmente: tal como as notas de dinheiro encontradas no chão depois de terem sido colocadas intencionalmente ou perdidas de forma involuntária por outrem são objetos cuja propriedade só muito dificilmente pode ser associada de forma estável e permanente à identidade de alguém - sendo por definição objetos

anónimos e com elevado grau de fungibilidade -, também músicas, filmes e livros em formato digital “achados” na Internet dizem respeito a ficheiros cujo “proprietário” original só muito dificilmente pode ser identificado. Mas se por um lado em ambos os tipos de situações encontramos a mesma dificuldade em assegurar a exclusividade, por outro os ficheiros digitais distinguem-se de notas de dinheiro emitidas pelo Banco Central Europeu encontradas ao acaso no meio da rua pela sua natureza não-rival que faz com que o seu consumo por uma pessoa não reduza o consumo por outra.

Independentemente da sua plausibilidade, tais afirmações relativamente inesperadas da parte de um governante com tão elevadas responsabilidades no tema em questão foram rapidamente condenadas e repudiadas pelo MAPiNET¹ no seu blogue, recorrendo para tal à analogia já habitual nas associações representantes de detentores de direitos entre ficheiros digitais e objetos físicos:

As notas caídas no chão poderão ser consideradas objetos perdidos, mas os filmes e as músicas disponibilizados ilegalmente na Internet e que são objeto de download têm donos bem identificados, que foram roubados, aparentemente com o apoio do Ministro que devia protegê-los: estará o Ministro a equacionar a sua continuidade na titularidade desta pasta? (MAPiNET 2009)

Embora se desconheçam os dotes divinatórios dos elementos do MAPINET, o que é facto é que na sequência desta e de outras críticas de teor semelhante tecidas pela Sociedade Portuguesa de Autores – através do seu administrador Tozé Brito – e pela Associação do Comércio Audiovisual de Portugal, dois dias depois Pinto Ribeiro sentiu necessidade de esclarecer melhor o sentido das suas afirmações, explicando que “obviamente” não era favorável à prática de ilegalidades. Na mesma entrevista, Pinto Ribeiro aproveitou para matizar ainda mais a sua posição de defesa da liberdade na Internet ao acrescentar que “aquilo que nos parece especialmente grave é quem faz o *upload*, é quem põe coisas na Internet para que elas possam ser descarregadas ouvidas, lidas” (Coutinho 2009).

Não obstante o facto de, no seguimento das eleições legislativas de 27 de Setembro de 2009 que deram nova vitória – com maioria relativa – ao Partido Socialista, Pinto Ribeiro não ter sido reconduzido no cargo de ministro da Cultura, forçoso é notar que o momento acima descrito

¹ Movimento Cívico Antipirataria na Internet composto por diversas associações portuguesas de representantes dos detentores de direitos de autor.

marcou o fim de um período de afastamento da agenda do executivo português face aos interesses das associações dos detentores de direitos no que diz respeito à prática da partilha de ficheiros protegidos por direitos de autor. Com efeito, longe da tolerância ou aceitação passiva expressa por Pinto Ribeiro, as subsequentes tutelas da pasta da Cultura tenderam visivelmente para um estreitamento dos esforços com as associações do setor no sentido do combate àquilo que estas designam de “pirataria digital”.

Um sinal inequívoco dessa postura repressiva pode ser encontrado num acordo assinado a 30 de Julho de 2015 entre a Inspeção Geral das Atividades Culturais (IGAC) da Secretaria de Estado da Cultura de Portugal, a Associação Portuguesa de Operadores de Telecomunicações (APRITEL), a Direção Geral do Consumidor, a DNS.pt (organização responsável por gerir o domínio.pt) e uma série de associações de gestão de direitos de autor. Tendo como objetivo o bloqueio pelos quatro grandes fornecedores de acesso à Internet (NOS, Meo, Vodafone e Cabovisão) de todos os sites que possam disponibilizar ligações, indexar ou alojar conteúdos que infrinjam os direitos de autor, tal acordo torna desnecessária a obtenção de uma ordem de bloqueio junto de um juiz de um tribunal. Neste sentido, trata-se de uma iniciativa ímpar a nível europeu: pela primeira vez em acordos deste tipo, para que o bloqueio passe a vigorar basta que uma entidade de direito privado com interesses óbvios na matéria (o MAPiNET) apresente a uma entidade administrativa dependente do poder político (a IGAC) as “provas” necessárias que fundamentem as queixas de distribuição não autorizada de obras protegidas por parte de um site apresentadas pelos detentores de direitos e as entregue².

2.OBJETIVOS E METODOLOGIA

Perante tal ofensiva - que já demonstrou ser pouco mais do que um mecanismo de censura indiscriminada e sem qualquer controlo judicial (Revolução dos Bytes 2016; Simões 2016a e 2016b) -, e face à grave lacuna de estudos empíricos realizados a nível académico sobre a partilha de ficheiros e pirataria digital em Portugal, este artigo visa traçar um retrato mais fidedigno do

² Depois de recolher estas “provas”, o MAPiNET encarrega-se de enviar mensalmente até duas listas com um máximo de 50 dos sites em questão à IGAC, de modo a que esta entidade notifique as operadoras dos sites em causa de modo a que os endereços IP relativos aos domínios em causa sejam bloqueados. Futuramente, sempre que um utilizador a um desses URLs bloqueados, ser-lhe-á exibida a mensagem “site indisponível” ou “site não encontrado”. Para que o site passe a integrar a lista dos bloqueados, o único critério necessário é que aquele contenha mais de 500 ligações para conteúdos alegadamente ilegais ou cujo indexador contenha mais de 66% de conteúdos alegadamente ilícitos (Caçador 2015; Andy 2015).

grau de consciencialização dos utilizadores portugueses e brasileiros de Internet relativamente à natureza ilícita ou lícita dos conteúdos que encontram *online*, assim como das verdadeiras motivações, justificações e racionalizações dos que entre estes se assumem como partilhadores:

- *Quais as razões que invocam para justificar o download de conteúdos protegidos por direitos de autor?*
- *O que pensam das consequências dos seus hábitos de partilha nos criadores, editores e o futuro da criação cultural em geral?*
- *Como encaram as medidas repressivas fomentadas pelas indústrias culturais e implementadas pelos diferentes estados nacionais?*
- *Que soluções e modelos de negócio apontam para as empresas e associações representantes das indústrias culturais?*

No intuito de responder a estas questões, iremos recorrer aos dados empíricos recolhidos no âmbito de um projeto de doutoramento em Ciências da Comunicação onde se tentou traçar um retrato demográfico e sociológico o mais fiel possível dos “partilhadores” portugueses e brasileiros de modo a saber mais sobre os seus usos de Internet e práticas de consumo – tanto *online* como *offline*, autorizadas ou não autorizadas à luz das leis de direito de autor de Portugal e Brasil - de três tipos de conteúdos (música, filmes e livros), sem no entanto descurar a eventual importância de outros tipos de obras protegidas por direitos de autor como jornais, revistas, videojogos e software informático.

Um primeiro pilar metodológico da análise empírica que irá ocupar o grosso deste artigo consiste nos resultados de um questionário *online* em língua portuguesa constituído por perguntas fechadas e dirigido a utilizadores portugueses e brasileiros de Internet. De modo a melhor adaptar as questões aos idiomas nacionais em questão, foram elaboradas duas versões do mesmo inquérito: uma em português de Portugal e outra em português do Brasil. Em ambas as versões, as amostras consistiram em indivíduos que se auto-selecionaram ao responderem aos apelos lançados em várias redes sociais (Facebook, Twitter, Google Plus e LinkedIn) com vista ao preenchimento do questionário.

A ativação da versão em português de Portugal do questionário ao público deu-se a 2 de Abril de 2014, tendo a desativação ocorrido a 10 de Junho desse mesmo ano. Durante esse período, foram submetidos 203 formulários completos contra 135 que ficaram por completar de um total de 339 iniciados, o que corresponde a uma taxa de resposta de 60%. Esta versão foi composta por

36 questões fechadas (sendo 16 de índole sociodemográfica), a maioria das quais de resposta obrigatória.

Tal como no caso da versão em português de Portugal, a versão do questionário em português do Brasil manteve-se ativa durante aproximadamente dois meses: de 13 de Maio a 25 de Junho de 2014. A taxa de resposta ficou contudo ligeiramente aquém do esperado: 58,3%. No total, foram submetidos (completos) 98 formulários de um total de 168 iniciados. Esta versão acabou por integrar 29 questões (nove das quais de índole sociodemográfica).

A segunda vertente da pesquisa empírica centrar-se-á nas respostas a entrevistas *online* dadas por participantes em ambas as versões do questionário que concordaram em ser posteriormente contactados. Entre Julho e Setembro de 2014, foram entrevistados nove utilizadores de Internet residentes em Portugal (de um total de 33 que tinham indicado o seu endereço de email no formulário do inquérito) e sete utilizadores brasileiros (de um total de 25 participantes da versão em português do Brasil do questionário que disponibilizaram o seu endereço de email para posterior contacto. Estas entrevistas foram efetuadas através de plataformas de conversação textual escrita tipo chat (Google Hangout, Facebook Chat e Skype). Com uma estrutura semi-fechada, as entrevistas destinaram-se a explorar com maior profundidade as temáticas abordadas no questionário. De forma a garantir o anonimato dos participantes da pesquisa, os excertos retirados das respostas às questões colocadas no âmbito das entrevistas serão apenas identificados pelo sexo, nacionalidade, idade, profissão e nível de escolaridade dos autores das declarações. No intuito de melhorar a precisão ortográfica e tornar mais clara a leitura, serão efetuadas pequenas alterações pontuais às frases originais.

De modo a contextualizar devidamente tal análise empírica sobre o universo da partilha em Portugal e no Brasil, começaremos por apresentar de seguida algumas das principais conclusões a retirar da leitura da literatura empírica mais relevante sobre a relação entre vendas e cópias não autorizadas de bens informacionais, seguindo-se uma exposição dos resultados de centenas de estudos quantitativos realizados até hoje incidindo nos comportamentos reais dos utilizadores e nas motivações que os levam a descarregar ficheiros relativos a obras protegidas por direitos de autor.

3. ANÁLISE DA PESQUISA EMPÍRICA PRÉVIA SOBRE PARTILHA DE FICHEIROS

Um elemento comum a todos os processos instaurados a nível internacional até hoje pelas indústrias culturais visando responsáveis por redes ou aplicações de partilha de ficheiros consiste na apresentação de números relativos a alegadas vendas perdidas no valor de várias centenas de milhões de euros em razão da possibilidade oferecida por essas tecnologias de realizar um número ilimitado de *downloads* não autorizados. Não estranha por isso que ao longo da última década e meia e a par com uma série de estudos de âmbito jurídico destinados a avaliar a licitude ou ilicitude da cópia não autorizada de obras protegidas por direitos de autor à luz da legislação das diferentes jurisdições nacionais³, tenha despontado uma vasta literatura dedicada ao tema, na sua maioria composta por estudos empíricos de índole económico dedicados a analisar os efeitos deste tipo de práticas *online* nos modelos de negócio das indústrias culturais, nomeadamente nas suas vendas.

Ainda que na maioria dos estudos empíricos se detete uma relação negativa entre a partilha de ficheiros e a venda de música e filmes (Smith e Telang 2012⁴), a literatura teórica aponta para a possibilidade de a cópia não autorizada poder não só contribuir para aumentar os lucros dos detentores de direitos como também melhorar o bem-estar social. Ao mesmo tempo, em virtude de deficiências inerentes aos dados disponíveis publicamente e às metodologias empregues na sua recolha, esta relação negativa encontrada entre vendas legítimas e cópia não autorizada pode ocultar mais do aquilo que revela. É assim por exemplo que Dejean (2009) coloca a possibilidade daquilo a que designa de “pirataria digital” criar novas ocasiões de consumo e alterar a relação de forças dos diferentes intervenientes na indústria cultural (p. 346). Por outro lado, o ênfase excessivo do debate público na questão de saber se a partilha de ficheiros prejudica ou beneficia as indústrias culturais e em que medida faz com que os contributos oriundos do campo da economia sejam de uma utilidade limitada quando se trata de determinar medidas que tenham em conta tanto o bem-estar do utilizador como a sustentabilidade da produção cultural a longo prazo (em termos da produção de novas obras), sem descurar os custos financeiros e sociais (maior vigilância e enor privacidade, colocando desta forma em risco direitos e liberdades civis) que a aplicação dos direitos de autor num contexto digital de abundância acarreta (Handke 2012, p. 48). Daí a importância, em termos de políticas públicas, de ter em linha de conta não só a relação entre

3 Ainda que quase sempre ignorando a questão da legitimidade dessas regras jurídicas face às normas sociais predominantes (Larsson 2011).

4 Valerá talvez a pena salientar o facto desta revisão da literatura académica ter sido financiada pela *Motion Picture Association of America* (MPAA), a associação industrial que representa os interesses dos seis maiores estúdios cinematográficos de Hollywood.

vendas e cópias não autorizadas, mas também os comportamentos reais dos utilizadores, bem como as razões que os levam a descarregar ficheiros relativos a obras protegidas por direitos de autor. Desta perspetiva mais holística, a relevância dos contributos de outros campos do conhecimento – Sociologia, Ciências da Comunicação, Psicologia, Direito, Engenharia Informática, Estudos Culturais, etc. – torna-se inegável (Grassmuck 2010, p. 43).

4.EFEITOS NO BEM-ESTAR

O ênfase excessivo nos prejuízos dos detentores de direitos por parte da literatura empírica sobre as consequências económicas da cópia não autorizada é aliás confirmado por Christian Handke numa análise de 33 estudos empíricos de índole quantitativa publicados entre 1985 e 2012 (Handke 2012). Partindo de três grandes tipos de distinções relativas aos efeitos económicos dos direitos de autor - 1) efeitos de curto e longo alcance; 2) efeitos para os detentores de direitos e para os utilizadores; 3) efeitos da cópia não autorizada, dos direitos de autor e da aplicação dos direitos de autor -, Handke chega à conclusão que 21 dos 33 estudos incidem nos efeitos de curto prazo da cópia ilícita no bem-estar dos detentores de direitos, ou seja, nas suas receitas. Outras consequências dos direitos de autor, nomeadamente a nível do bem-estar dos utilizadores (tanto a curto prazo, em termos de acesso, como a longo prazo, em termos da qualidade ou quantidade das obras publicadas), assim como da reação das indústrias dependentes dos direitos de autor às novas tecnologias de cópia e reprodução digital, foram alvo de um grau muito menor de atenção⁵. O vazio de dados empíricos chega a ser absoluto no caso dos efeitos da aplicação dos direitos de autor em termos dos custos administrativos e de transação associados aos sistemas de direitos de autor⁶ Para além disso e apesar destas indústrias “diferirem substancialmente entre si, por exemplo em termos de dimensão, ritmo de crescimento, estrutura de custos e condições de procura relevantes como seja o nível de substituição das cópias autorizadas e não autorizadas (...) o grosso da literatura económico-empírica sobre a cópia digital não autorizada” tem como único objeto de estudo a indústria discográfica: 20 dos 33 estudos incidem sobre a música, seguindo-se-lhe de muito longe os filmes com sete estudos (Handke 2012, p. 53-54). Uma vez que é bastante discutível

5 “As escassas provas disponíveis até ao momento suscitam dúvidas sobre se quaisquer perdas para os detentores de direitos se traduzem numa perda no bem-estar social nas atuais condições de mercado. Por exemplo, não existem quase provas nenhuma de que o reforço dos direitos de autor estaria positivamente associado à quantidade ou qualidade das obras intelectuais produzidas.” (Handke 2012, p. 83)

6 Isto é, custos em termos de despesa pública.

extrapolar os resultados relativos a uma indústria às restantes indústrias dependentes dos direitos de autor, quaisquer eventuais conclusões a que possamos chegar após a leitura da pesquisa académica nesta área estarão logo à partida condicionadas por esta limitação.

A preponderância da música na literatura empírica publicada até hoje é também salientada por Watson, Zizzo e Fleming (2014) numa revisão bibliográfica abrangente⁷. Com base numa análise de 209 artigos publicados entre Janeiro de 2003 e Fevereiro de 2013 sobre a partilha não autorizada de conteúdos digitais incidindo sobre os comportamentos, intenções e atitudes dos partilhadores⁸, os autores concluem que as evidências relativas aos efeitos positivos ou negativos deste tipo de práticas se concentram fortemente nos ficheiros de música, surgindo os filmes e o software num distante segundo lugar. Em contrapartida, a pesquisa em torno de videojogos, *software*, livros ou conteúdos televisivos é muito escassa. Um facto notório é a ausência total da pornografia, especialmente tendo em conta não só a vasta quantidade de conteúdos pornográficos disponíveis em redes e *sites* de partilha de ficheiros mas também a popularidade dos sites de streaming de vídeos deste teor. Tal como Handke, Watson *et al.* salientam o perigo de fundamentar medidas públicas em dados bastante limitados a uma única categoria de obras quando as evidências indiciam que os fatores determinantes e as implicações no bem-estar da partilha não autorizada de uma determinada categoria de obras podem não ser extensíveis a outra categoria.

De acordo com a mesma revisão abrangente da literatura, 33 dos 209 artigos incluídos na amostra incidem especificamente nas implicações do *download* não autorizado a nível do bem-estar social⁹. Segundo os autores, a maioria dos estudos adotam uma de duas abordagens. Uma primeira assenta na análise dos efeitos da partilha não autorizada de ficheiros nas vendas num determinado mercado, correspondendo assim na taxonomia de Handke à categoria de efeitos de curto prazo no bem-estar dos produtores. Tal como Handke, Watson *et al.* chegam à conclusão que neste tipo de estudos existe uma clara negligência do bem-estar obtido pelos consumidores com a partilha não autorizada. Se a segunda abordagem, associada a indicadores do nível de disponibilidade para pagar pelos bens, se encontra mais focada no bem-estar dos consumidores, ela apresenta contudo o inconveniente de ser empregue por apenas um pequeno número de estudos.

⁷ *Scoping review* em inglês.

⁸ Seleccionados de entre 54.441 fontes obtidas em resultado de uma pesquisa metódica em bases de dados académicas e um repositório de pré-publicações, bem como em sites de centros de investigação e de entidades representantes das diferentes indústrias em questão.

⁹ Os autores apresentam uma definição de bem-estar com conotações micro-económicas, em termos dos benefícios obtidos por consumidores e produtores. Esta definição faz corresponder os benefícios retirados pelos consumidores à disponibilidade destes para pagar pela versão original dos ficheiros que descarregaram. Quanto aos benefícios obtidos pelos produtores, estes correspondem às receitas resultantes do consumo lícito das obras.

Watson *et al.* referem em seguida uma série de dificuldades e limitações metodológicas encontradas nos dois grandes tipos de estudos.

No que diz respeito aos estudos que tentam quantificar o efeito da partilha nas vendas, considera-se que os tipos de dados disponíveis aos investigadores são bastante inadequados para calcular de forma fiável esse impacto. Dado que a maioria dos estudos que visam analisar o benefício ou prejuízo baseiam-se no comportamento expresso de participantes em inquéritos¹⁰ e não em comportamentos diretamente observados por indivíduos (através de experiências) ou populações (obtidos a partir de dados sobre vendas), a validade das suas conclusões poderá restringir-se a uma amostra específica, tendo em conta as diferenças nas percentagens de partilha não autorizada de ficheiros entre diferentes países e grupos sociodemográficos como é o caso dos estudantes.

Mesmo quando os investigadores têm acesso a dados relativos a comportamentos observados, tal não significa que estes sejam por si só mais rigorosos. Não só porque é frequentemente difícil senão mesmo impossível confirmar as estimativas de vendas ou taxas de partilha não autorizada com origem nas indústria dependentes dos direitos de autor, mas também porque os instrumentos metodológicos com origem na ciência económica empregues para calcular os prejuízos a par com a escolha das variáveis instrumentais¹¹ contribuem para um enviesamento:

A ausência de controlos adequados e verificáveis em experiências naturais, comparações entre países e modelos integrando variáveis instrumentais faz com que quaisquer atribuições de causa e efeito sejam extremamente ténues, tendo resultado de forma não surpreendente num vasto leque de diferentes graus de estimativas de efeitos (...) A definição de prejuízo adotada pelos estudos atuais é

¹⁰ Isto é, em relatos pessoais de comportamentos exibidos no passado.

¹¹ Neste tipo de estudos baseados em variáveis instrumentais, é usual escolher-se uma variável que se pressupõe que tenha um efeito indireto nas vendas legais, apenas através da sua relação com a partilha não autorizada de ficheiros. Um dos estudos mais conhecidos assente nesta abordagem é o de Oberholzer-Gee e Strumpf (2007) no qual os seus autores revelam ter descoberto que em 2002, durante o período correspondente às férias escolares na Alemanha, o nível de oferta de ficheiros não autorizados disponíveis na rede OpenNap aumentou, levando assim a uma subida do número de *downloads* ilícitos nos Estados Unidos. De acordo com Oberholzer-Gee e Strumpf (*idem*), não foi no entanto descoberta qualquer correlação com as vendas legais nos EUA. A seleção desta variável instrumental foi justificada pelos autores pelo facto de muitos dos ficheiros descarregados nos EUA se encontrarem alojados na Alemanha, com especial incidência para o período das férias escolares, durante o qual o tempo que demora a efetuar cada *download* e o número de *downloads* incompletos tendem a diminuir. Apesar de Oberholzer-Gee e Strumpf não terem descoberto qualquer impacto estatisticamente significativo da partilha de ficheiros nas vendas de discos, o seu estudo foi sujeito a severas críticas. A principal delas partiu de Stan Liebowitz que num artigo de 2007 desmonta o pressuposto dos dois economistas de que o nível de partilha não autorizada nos EUA se encontrava fortemente associado ao número de estudantes alemães em férias (Liebowitz 2007).

extremamente limitada e na maior parte dos casos encontra-se restrita às vendas físicas, com um número relativamente inferior de estudos a investigar as vendas digitais. Tentativas futuras de realizar estimativas empíricas do impacto (...) deverão ter em conta a vasta gama de fontes de financiamento disponíveis atualmente para a produção de conteúdos, incluindo serviços digitais de streaming e projetos de crowdfunding, uma vez que – assim como as vendas físicas e digitais – todas elas contribuem para a economia criativa. Não só os impactos da partilha não autorizada de ficheiros deveriam ser analisados numa perspetiva mais vasta, como as implicações em termos de bem-estar para os vários agentes relevantes deveriam ser igualmente consideradas, tendo em conta que o impacto nos artistas e criadores constitui uma importante omissão de boa parte da literatura. (Watson, Zizzo e Fleming 2014, p. 47-48).

Relativamente aos estudos que visam averiguar o grau de disponibilidade dos utilizadores para pagar pelos conteúdos, apenas quatro incluem uma estimativa das implicações da partilha de ficheiros no bem-estar, sendo que todos eles concluem no sentido da existência de um benefício social líquido. Contudo tal como no caso dos estudos centrados nas vendas, também aqui Watson *et al.* encontram deficiências graves nos dados:

1. Embora todas as estimativas de bem-estar se centrem exclusivamente na indústria discográfica, os dados podem não ser aplicáveis a todas as restantes indústrias dependentes dos direitos de autor;

2. As taxas de substituição de obras adquiridas legitimamente por ficheiros ilícitos empregues para calcular os efeitos a nível do bem-estar referem-se apenas a estudantes, o que dificulta a generalização dos seus resultados a populações de maior dimensão em outros países;

3. Os estudos não contemplam quaisquer mecanismos de incentivo nas suas estimativas do nível de disponibilidade dos participantes para pagar pelos conteúdos originais. Uma vez que a metodologia não envolve o dispêndio de dinheiro, dependendo antes de cenários puramente hipotéticos, é provável que exista uma sobrevalorização dos montantes indicados;

4. Apesar das estimativas realizadas partirem do princípio que a produção musical não é afetada pela partilha não autorizada de ficheiros (tanto pelo lado da quantidade como

da qualidade), de momento a investigação relativa à relação entre o nível da oferta musical e este tipo de práticas permanece bastante incipiente. Ora, é apenas mediante a incorporação dos efeitos dinâmicos (a longo prazo) da transferência de bem-estar dos produtores para os consumidores - em resultado da substituição de uma venda por um download - na criação e distribuição de novos conteúdos que qualquer potencial diminuição do bem-estar pode ser identificada.

Após elencarem as deficiências inerentes a cada uma das duas grandes abordagens (vendas e nível de disponibilidade para pagar), Watson *et al.* chegam a uma conclusão bastante semelhante à de Handke (2012), apontando para o facto de ambas não contemplarem quaisquer estimativas relativas às implicações a longo prazo a nível do bem-estar que um mercado com um reforço dos direitos de autor ou, em alternativa, um mercado dominado por modelos de negócio que privilegiem o acesso aberto teriam (Watson, Zizzo e Fleming 2014, p. 48).

Muitas das críticas tecidas nos artigos de Handke e Watson *et al.*, às deficiências encontradas na pesquisa empírica quantitativa sobre a partilha não autorizada de ficheiros tinham sido aliás já expostas em revisões da literatura anteriores. É o caso de Dejean 2009, Grassmuck 2010 ou Tschmuck 2010. Não obstante, os artigos de Handke (2012) e Watson *et. al.* (2014) destacam-se não só por serem mais recentes, mas também por procederem a uma análise mais abrangente, rigorosa e sistemática da literatura sobre o tema.

5.MOTIVAÇÕES E PERFIL SOCIODEMOGRÁFICO DOS UTILIZADORES: BREVE REVISÃO DA LITERATURA

Uma vantagem acrescida da revisão bibliográfica da autoria de Watson *et al.* é o facto – raro entre a maioria das revisões de literatura publicadas até hoje, de pendor excessivamente economicista - de se debruçar igualmente sobre a literatura em torno das motivações e do perfil sociodemográfico dos utilizadores que acedem a redes e *sites* de partilha de ficheiros para efetuar o *download* não autorizado de obras protegidas por direitos de autor¹². De modo a atribuir um

¹² Embora esta análise deixe de lado os estudos relativos ao upload de ficheiros protegidos por direitos de autor, os autores não deixam contudo de constatar que algumas das suas conclusões são de igual forma aplicáveis a esta dimensão.

maior grau de sistematicidade à análise, os autores elaboraram um quadro conceptual que modela teoricamente os tipos de razões por detrás da decisão de cada utilizador obter uma cópia não autorizada, adquirir uma versão lícita do conteúdo em causa ou não fazer nada. Partindo de cinco grandes tipos de fatores potencialmente preditivos (financeiros e jurídicos, experienciais, técnicos, sociais e morais)¹³ destacados na pesquisa sobre o tema, Watson *et al.* elaboram um gráfico em forma de cubo destinado a representar visualmente os dados disponíveis a partir de 186 dos 206 estudos inicialmente selecionados de acordo com três categorias: utilidade; conteúdo (música, software, filmes, televisão, livros, videojogos); e medição de resultados (qualitativa, preferências enunciadas, intenções, nível de disponibilidade para pagar, comportamento indicado e comportamento observado – seguindo uma ordem crescente de acordo com a qualidade dos dados).

De modo semelhante ao verificado na sua análise da literatura a respeito dos efeitos da partilha não autorizada no bem-estar social, Watson *et al.* concluem que a música é igualmente o tipo de suporte mais alvo de pesquisas empíricas em todos os tipos de fatores preditivos ou fontes de utilidade. Apesar da existência de um número razoável de estudos centrados no software e – com menor peso - nos filmes, suportes como videojogos, livros ou programas televisivos são praticamente ignorados. Outra crítica tecida por Watson *et al.* aos estudos empíricos sobre o tema que vai ao encontro do alerta feito por Peter Tschmuck (2010) é o facto de a maioria empregar descrições genéricas do comportamento em causa nas questões colocadas ao participante: “pirataria digital”, “utilização de P2P” ou “download de conteúdos digitais.” Com efeito, a escolha por termos genéricos em vez de referências específicas a determinados tipos de conteúdos tende a gerar erros de medição e a reduzir a fiabilidade das estimativas:

De modo a demonstrar a existência de uma relação entre uma causa hipotética de um comportamento e o próprio comportamento, é muito importante ser bastante específico a respeito do comportamento alvo. Os motivos que levam alguém a descarregar música de modo ilícito podem ser diferentes dos motivos dos motivos para descarregar filmes ou software. Daí que perguntar aos participantes sobre as razões que os levam a descarregar conteúdos em geral faça com que tanto os participantes como os investigadores sejam incapazes de especificar quais os

13 Para além destes cinco tipos de fatores relativos a diferentes tipos de utilidade, alguns dos estudos mencionados aludem ainda àquilo que Watson *et al.* designam de estimativas de utilidade total líquida, um conceito utilizado para determinar o benefício ou prejuízo que os participantes consideram obter com a partilha não autorizada de ficheiros em comparação com a decisão de adquirir uma versão autorizada do conteúdo ou de não tomar qualquer ação.

comportamentos em causa, introduzindo assim ruído nas estimativas... (Watson, Zizzo e Fleming 2014, p. 28).

Tal como no caso dos estudos centrados na determinação do grau de benefício ou prejuízo, Watson *et al.* criticam a escassez de estudos sobre as motivação dos participantes baseados em comportamentos realmente observados, sendo particularmente notória a sua quase total ausência no caso de fontes morais, experienciais e sociais de utilidade – o que, como referem, não deixa de ser surpreendente se tivermos em conta que estes fatores são frequentemente os mais realçados nas campanhas educativas contra a partilha de ficheiros promovidas pelas indústrias de conteúdos, nomeadamente através da tentativa de moralizar o download não autorizado ao compará-lo com o roubo de bens materiais e tangíveis. Na medida em que a maioria das observações se limitam apenas a registar atitudes (na forma de preferências expressas) e intenções, existem razões para duvidar que daqui resulte um comportamento real (Watson, Zizzo e Fleming *idem*). Outra crítica tecida por Watson *et al.* aos estudos sobre as motivações dos partilhadores reside no facto da grande maioria destes se basearem em inquéritos transversais¹⁴ e não em questionários longitudinais, uma abordagem metodológica que, na sua opinião, contribui para identificar as causas dos comportamentos registados. Mormente estas observações, não deixa de ser possível extrair algumas conclusões a respeito dos fatores potencialmente preditivos da partilha não autorizada de ficheiros, de acordo com a exposição de Watson *et al.* (*ibidem*, p. 36-42). Dada a especificidade do ângulo de análise deste artigo, optei por destacar em seguida as conclusões dos autores relativos aos estudos incidindo na utilidade financeira/jurídica e moral:

- *Utilidade financeira e jurídica: no total foram registadas 187 observações empíricas envolvendo fatores deste tipo. Destas, metade (50%) centraram-se na partilha não autorizada de música, seguindo-se-lhe muito de longe o software (19%) e os filmes (13%). De resto somente quatro estudos incidiram em programas televisivos e videojogos, sendo apenas três os que abordaram a partilha de livros.*

- *Dos nove estudos que compararam o grau de cumprimento das leis de propriedade intelectual em diferentes países para estimar os níveis de partilha não autorizada ou vendas legais, a maioria concluiu pela existência de uma relação entre*

¹⁴ Tipo de inquérito baseado na comparação de diferentes grupos populacionais num determinado momento, permitindo assim obter um retrato no tempo desses grupos e, ao mesmo tempo, comparar múltiplas variáveis ao mesmo tempo.

indicadores como a adesão a tratados internacionais, o nível dos custos de aplicação da lei e o grau de eficácia da lei por um lado e mais vendas legais/taxas menores de partilha não autorizada por outro. Duas possíveis objeções a essa conclusão são em primeiro lugar, o facto desses estudos empregarem estimativas dos níveis de partilha não autorizada fornecidas pelas associações de detentores de direitos como IFPI, BSA e IIPA e, em segundo, a possibilidade da influência de outras variáveis independentes como o grau de desenvolvimento económico. Um dado nesse sentido consiste na existência de uma correlação entre o grau de cumprimento das leis de propriedade intelectual e o nível de rendimento de um país.

- *No que diz respeito à introdução de leis mais severas de propriedade intelectual num só país, os dados disponíveis relativamente às suas implicações nos níveis de partilha não autorizada de conteúdos são bastante limitados.*

- *Na maioria dos estudos, apenas uma minoria dos participantes foi da opinião que as leis constituem um meio de dissuasão contra a partilha não autorizada. Em geral, uma percentagem inferior de inquiridos atribuiu maior importância aos riscos jurídicos deste tipo de práticas do que a riscos técnicos como a possibilidade de infectar o seu computador com um vírus informático.*

- *A partir de uma leitura dos 12 estudos que analisaram o nível de conhecimentos legais dos inquiridos, é possível concluir que muitas pessoas não têm consciência do que é ou não é ilícito à luz das respetivas legislações nacionais.*

- *Na maioria dos 53 estudos – tanto pesquisas qualitativas como inquéritos - que examinaram as implicações a nível de preços, o preço dos conteúdos autorizados foi bastante indicado pelos participantes como uma motivação para a partilha não autorizada. “Contudo, no que diz respeito ao comportamento, embora tenhamos encontrado uma relação uniforme entre preços mais elevados e vendas autorizadas inferiores, a relação com níveis de partilha não autorizada foi muito menos nítida, com apenas cinco entre 11 estudos a descobrir uma relação entre preços mais elevados e níveis acrescidos de partilha de ficheiros.” (Watson, Zizzo e Fleming, ibidem, p. 34). De acordo com Watson et al. tal discrepância poderá apenas ser um reflexo das deficiências inerentes a métodos que dependem da colocação de cenários hipotéticos aos participantes em lugar do recurso a experiências envolvendo preços e orçamentos reais.*

- Dos 27 estudos que analisaram as implicações do rendimento individual de cada participante na partilha não autorizada, não foi possível observar qualquer efeito nítido. Mais uma vez, a quase inexistência de estudos baseados na observação direta de comportamentos torna difícil extrair qualquer conclusão.

- *Utilidade moral:* os fatores preditivos de natureza moral foram alvo de análise em 154 observações. Mais uma vez, a música foi o tipo de conteúdos mais pesquisado com 42% das observações, seguindo-se-lhe de longe o software (23%) e os filmes (12%). Porém, não só os videojogos, programas televisivos e livros foram apenas incluídos em três estudos cada, como também uma parte não negligível (17%) das pesquisas incidindo nas questões morais não chegaram a especificar quaisquer tipos de conteúdos em particular.

- Dos seis estudos que investigaram os efeitos da legalidade ou ilegalidade de determinadas práticas nas convicções morais dos participantes, uma maioria concluiu que os inquiridos que se apoiavam na legislação para enquadrar as suas próprias crenças morais eram mais propensos a considerar a partilha não autorizada de ficheiros uma prática moralmente reprovável.

- O potencial impacto de diferentes conjuntos de valores morais na partilha não autorizada de ficheiros foi analisado por 12 estudos, ressaltando-se daqui a ideia de que enquanto os argumentos contra este tipo de práticas tendem a focar-se em valores morais absolutos, exibindo uma razoável estabilidade, já as justificações a favor tendem a ser mais relativas, evidenciando uma maior fluidez e variando de acordo com o contexto em análise. Para além disso, tanto estudos qualitativos como pesquisas de natureza quantitativa identificaram uma relação entre a recusa em considerar a partilha não autorizada um problema ético e comportamentos associados a esse tipo de práticas.

- Dos 37 estudos que tentaram estimar os efeitos das convicções morais dos participantes a respeito da partilha não autorizada de ficheiros e vários tipos de perceções referentes a esta prática, sete estudos tentaram analisar especificamente o impacto da primeira variável em avaliações de atitudes relativas ao comportamento dos inquiridos, tendo todos os sete confirmado a existência de uma relação entre ambas. Não obstante, no que concerne ao impacto das convicções morais em geral os

resultados foram algo contraditórios, dependendo do tipo de conteúdos em análise. Se por um lado tanto as pesquisas centradas na partilha de software como as que combinaram vários tipos de conteúdos numa designação genérica evidenciaram na esmagadora maioria dos casos que quem considera a partilha de ficheiros uma prática mais moralmente reprovável é menos suscetível de manifestar a sua intenção de descarregar ficheiros de modo ilícito, por outro, no caso dos estudos centrados na música os efeitos apresentaram um menor grau de consistência: apenas dois de um total de cinco pesquisas encontraram uma relação entre a primeira variável e a intenção de realizar downloads não autorizados, ao passo que sete em 13 estudos detetaram uma relação entre essa variável e o comportamento expresso pelos participantes.

- *Nove estudos estimaram diretamente a possibilidade da existência de uma relação entre a opinião expressa pelos participantes de que a partilha não autorizada de ficheiros contribui para uma melhoria do bem-estar social e uma série de atitudes, intenções e comportamento expressos favoráveis a este tipo de práticas, tendo os dados recolhidos apontado de forma consistente nesse sentido.*

- *Dos 15 estudos que investigaram o papel da consciencialização dos participantes para o prejuízo gerado pela partilha não autorizada de ficheiros, a generalidade concluiu que a perceção dos participantes é de que o prejuízo em causa é muito reduzido ou mesmo nulo. Ainda que os participantes tenham manifestado uma maior preocupação sempre que o dano era apresentado como afetando os criadores de conteúdos em vez da indústria, a perceção dominante foi a de que essas perdas podiam ser facilmente absorvidas.*

6.PERCEPÇÕES DOS UTILIZADORES PORTUGUESES E BRASILEIROS DE INTERNET SOBRE A ILICITUDE DA PARTILHA DE FICHEIROS PROTEGIDOS POR DIREITOS DE AUTOR

No intuito de aferir de modo preliminar o nível de conhecimentos das respetivas legislações nacionais de direitos de autor, foi perguntado aos inquiridos se sabiam distinguir entre os conteúdos distribuídos com autorização dos detentores de direitos e os que são distribuídos sem autorização dos detentores de direitos que descarregam ou acedem via *streaming*. Os resultados

obtidos indicam que em ambas as amostras mais de metade dos inquiridos têm de facto sempre ou frequentemente consciência da natureza lícita ou ilícita das obras que descarregam: 68,5% (139) no inquérito pt_PT e 55,1% (54) no inquérito pt_BR.

Quadro 1. Quando descarrega/acede a conteúdos através da Internet, consegue habitualmente distinguir entre aqueles que são distribuídos com autorização e os que são distribuídos sem autorização? - Portugal (n= 203)

	Frequência	Percentagem
Sempre	55	27,1%
Frequentemente	84	41,4%
Por vezes	33	16,3%
Raramente	18	8,9%
Nunca	5	2,5%
Não sabe	8	3,9%

Quadro 2. Quando descarrega/acede a conteúdos através da Internet, consegue habitualmente distinguir entre aqueles que são distribuídos com autorização e os que são distribuídos sem autorização? - Brasil (n= 98)

	Frequência	Percentagem
Sempre	22	22,4%
Frequentemente	32	32,7%
Por vezes	19	19,4%
Raramente	16	16,3%
Nunca	6	6,1%
Não sabe	3	3,1%

Ainda assim, tal consciencialização não parece constituir um impedimento ao *download* ou acesso não autorizado, na medida em que apenas 15,7% (32) dos inquiridos portugueses e 11,2% (11) dos inquiridos brasileiros reconheceram desistir sempre ou frequentemente de descarregar ou aceder a um conteúdo que é disponibilizado sem autorização dos detentores direitos

Quadro 3. Normalmente, o facto de um conteúdo ser disponibilizado sem autorização leva-o a desistir de o descarregar/aceder através da Internet - Portugal (n= 203)

	Frequência	Percentagem
Sempre	10	4,9%
Frequentemente	22	10,8%
Por vezes	53	26,1%
Raramente	55	27,1%
Nunca	54	26,6%
Não sabe	9	4,4%

Quadro 4. Normalmente, o facto de um conteúdo ser disponibilizado sem autorização leva-o a desistir de o descarregar/aceder através da Internet - Brasil (n= 98)

	Frequência	Percentagem
Sempre	5	5,1%
Frequentemente	6	6,1%
Por vezes	14	14,3%
Raramente	29	29,6%
Nunca	44	44,9%
Não sabe	0	0,0%

No que diz concretamente respeito ao cenário português, esta percepção de que a partilha de conteúdos audiovisuais na Internet é uma prática corriqueira e sem grandes implicações morais é aliás confirmada pelos resultados representativos do universo dos utilizadores nacionais de Internet relativos à edição de 2013 do inquérito Sociedade em Rede em Portugal:

Cerca de 40% dos utilizadores de Internet afirmam que quando encontram um ficheiro na Internet que lhes interessa usam-no e partilham-no com os seus amigos, sem se questionarem sobre se é legal fazê-lo. Representam também pouco mais de 40% da amostra aqueles que dizem que não há problema em partilhar ficheiros de filmes ou séries de televisão na Internet, e aqueles que indicam fazer downloads de música não pagos. (Cardoso et al. 2015, p. 165).

A hipótese do recurso irrefletido ao *download* e ao acesso via streaming não autorizados é igualmente corroborada por essa pesquisa que aponta para o facto de a partilha ser uma prática incrustada no quotidiano de um cada vez maior número de internautas portugueses:

Cerca de 70% dos inquiridos concordam em parte ou totalmente que quando alguém se depara com um conteúdo digital na Internet, seja de música, vídeo ou livro, não se questiona se o seu uso é legal antes de utilizá-lo (...) O facto de o nível declarado de adesão a esta prática ser mais reduzido do que a ideia generalizada de que a mesma está fortemente difundida entre os internautas, sugere que o primeiro pode estar subdimensionado.

Adicionalmente, 83% dos utilizadores têm a percepção de que a maioria das pessoas que utiliza a Internet usa conteúdos livres em vez de conteúdos pagos (...) Da mesma forma, 69% concordam ou concordam totalmente com a ideia de que a pirataria de música, livros e vídeos, desde que acontece na Internet, já não é considerada negativa pelos jovens; 68% desvalorizam a importância das queixas contra a partilha online; e 61% acedem à ideia de que mais de metade dos downloads de conteúdos audiovisuais são em violação dos direitos de autor. Destaque ainda para os 51% de utilizadores que declaram que partilhar a sua música, vídeos e livros digitalmente faz parte da sua vida quotidiana atual, percentagem que é de 60% entre os indivíduos na faixa etária dos 15 aos 34 anos. (Cardoso et al. idem).

A hipótese de que a maioria dos partilhadores possui consciência de que a cópia ou o acesso via *streaming* a ficheiros protegidos por direitos de autor a partir da Internet constitui uma

ilegalidade logo quando começa a realizar esse tipo de práticas foi no entanto comprovada pelos testemunhos obtidos dos entrevistados: quando interrogados sobre se já tinham noção de que esses ficheiros eram disponibilizados sem autorização dos detentores de direitos ou se só progressivamente é que se aperceberam desse facto, todos os entrevistados à exceção de um manifestaram ter um conhecimento pelo menos rudimentar da ilicitude de tal ato. Saliente-se, contudo, que as respostas dos entrevistados portugueses foram aqui, regra geral, mais extensas do que as dos brasileiros, pautando-se por uma necessidade de desculpabilizar ou pelo menos justificar moralmente o comportamento descrito:

Sempre tive noção que não seria correto ter acesso aquelas coisas. Se na loja custavam x€ e eu tinha de graça, alguma coisa estava errada! Mas no início não tinha 1/10 dos conhecimentos que tenho hoje nem sabia que existiam direitos de autor. Pensava que, no máximo, estava a prejudicar aquelas grandes e ricas cadeias de vendas que ganhavam aos milhões nunca pensava na pessoa pequena...na base...que aquele conteúdo surge do trabalho de alguém que tem de ser compensado/pago por isso. (Português, 27 anos, bacharelato/licenciatura, gestor de projetos)

Tinha noção, mas a consciência só começou a pesar mais tarde... Quando comecei a fazer downloads isto era tudo muito novo. Ainda me lembro de usar o Napster. Teria cerca de 20 anos, ou seja há 12 anos atrás. Na altura os CDs eram caríssimos (custavam mais do que hoje em termos nominais, cerca de 15 euros) As empresas discográficas eram grandes multinacionais, o cinema dava muito dinheiro. Aos poucos fui lendo que estas indústrias estavam a sofrer e fui tendo consciência da importância de pagar por conteúdos. (Português, 33 anos, doutoramento, investigador associado)

Apesar dos inquiridos portugueses terem afirmado possuir um maior discernimento do que os inquiridos brasileiros sobre a natureza ilícita ou lícita dos conteúdos que encontram na Internet, quando foi colocada aos entrevistados a questão de saber se se consideravam esclarecidos a respeito da legislação de direitos de autor do respetivo país, os resultados obtidos foram quase antagónicos, com cinco dos entrevistados portugueses a responderem que não se consideravam informados, dois a considerarem-se mais ou menos informados e outros dois a afirmarem possuírem conhecimento das leis nacionais. Em contraste, cinco dos entrevistados brasileiros

responderam sentirem-se bem informados sobre este tópico contra apenas dois que confessaram ter um nível de conhecimento intermédio.

De forma a comprovar a veracidade desse auto-diagnóstico, foi em seguida lhes perguntado que opinião tinham dessa legislação. Nas situações em que as respostas iniciais revelavam ser algo evasivas, foi-lhes diretamente perguntado se consideravam que a cópia *online* de obras protegidas por direitos de autor deviam ser consideradas uma ilegalidade. Tanto no caso português como no brasileiro, as respostas pareceram corroborar a tese de quanto maior é o nível de esclarecimento percecionado pelos indivíduos a respeito de um tema emergente em termos de mobilização social, maior é a percepção da urgência de efetuar mudanças drásticas na legislação e políticas públicas:

Acho que essa legislação deve ser revista urgentemente. É um dos vários campos em que a tecnologia está bem à frente da legislação, o que provavelmente será uma inevitabilidade.

(...)

Da maneira como o sistema está construído e tendo em vista o cair do "preço por unidade de trabalho" na área profissional onde me movimento (tenho que trabalhar o triplo do que trabalhava há uns 15 anos para receber o mesmo, sem levar em conta a inflação), não sei se a liberalização do consumo de conteúdo protegido por direito autoral traria algum benefício à atividade criativa e, por arrasto, aos consumidores desse conteúdo. É um assunto delicado que requer muitíssima reflexão.

(...)

Se a mudança de paradigma de consumo desse conteúdo se deslocar de um paradigma baseado na posse para outro baseado no acesso (como os serviços de streaming), essa questão da cópia poderá tornar-se obsoleta. A grande questão está em definir uma melhor maneira de distribuição de riqueza proveniente desse acesso {pois} a que se tem vindo a desenhar até agora está bastante aquém do ideal.

(...)

Por outro lado, agrada-me a ideia de se pagar (seja lá de que maneira for) por cada vez que se "tira proveito" dum conteúdo. Pode-se comprar um álbum e ouvi-lo uma vez ou ouvi-lo 24 horas por dia durante um ano inteiro e não se paga nem mais nem menos por isso, enquanto com o streaming é eventualmente mais justo. (Português, 42 anos, ensino secundário, músico – entrevistado via Google Hangout)

Na realidade, pensava que era uma coisa até mais simples mas aparentemente temos de estar sempre a pagar às pessoas que fazem essas coisas (filmes e músicas). Uma pessoa vai descobrindo por necessidade...mas nada é claro. Mesmo quando surgiram algumas campanhas sobre o ilegal, faz já uns anos, explicaram muito pouco. Diziam 'é crime, punível até x anos de cadeia' mas nada era claro. Era muito alarmista... Conheci muita gente que parou/reduziu os downloads nessa altura.

(...)

Por um lado, as pessoas e empresas que dedicam horas e horas de trabalho para produzirem algo têm de ser pagas. E uma parte disso é através das vendas. Portanto, se estamos a ter acesso às coisas e não estamos a pagar nada em troca, não é correto. Nessa lógica, deveria ser crime, é de alguma forma roubo. Agora, também me parece que os preços das coisas são demasiado caros porque toda a gente fica com uma parte do custo final de um conteúdo. Comprar um CD de música por 20-25€ é caro. Um jogo por 60€ é uma loucura. Porque a pessoa da loja leva uma parte, o distribuidor leva outra, os acionistas da empresa-mãe levam outra, a empresa leva outra e a pobre alma que fez o serviço leva o quê?...1/100? (Português, 27 anos, bacharelato/licenciatura, gestor de projetos – entrevistado via Google Hangout)

[A legislação brasileira de direito autoral] é bastante ruim; as limitações são restritas e ambíguas (o que provavelmente é intencional ou resultado de soluções de compromisso na esfera legislativa). A última reforma (1998) contribuiu negativamente. Poucas salvaguardas ao criador como restrições à amplitude dos contratos, possibilidades de cessão presumida de direitos, etc. (Brasileiro, 35 anos, mestrado/pós-graduação, editor de textos – entrevistado via Google Hangout)

Bem, nossa atual lei dos direitos autorais é a 9.610/98, de 1998, claro, e por isso mesmo está bastante aquém da realidade que hoje se mostra. A legislação está desatualizadíssima e necessita de revisões urgentes. Sei que esse questionamento pode ser feito a toda a legislação mas não é fácil aceitar um atraso tão grande em uma legislação de direitos autorais, em um mundo de tecnologia como esse.

(Brasileira, 26 anos, mestrado/pós-graduação, assessora de comunicação - entrevistada via Skype)

Daquilo que conheço [da legislação], penso que defende bem os direitos dos autores das obras. E acho bem que recebam pelo facto dos seus trabalhos estarem online. Só acho é que se devia seguir o exemplo do Spotify para os filmes e séries, em que se tem acesso a esses conteúdos gratuitamente, estando os direitos autorais assegurados. (Portuguesa, 31 anos, mestrado/pós-graduação, desempregada – entrevistada via Google Hangout)

Não sei se a legislação como um todo faz sentido, mas sim, acho que partilhar conteúdos protegidos por direitos de autor é uma ilegalidade. A não ser que os próprios autores decidam que queiram partilhar livremente. Já existem opções para isso. (Português, 33 anos, doutoramento, investigador associado - entrevistado via Google Hangout)

Acho que não faz sentido a proibição: é como um sinal de sentido proibido no meio do deserto. Respeita-o?

(...)

Compreendo a dificuldade em remunerar os autores e em proteger os seus direitos mas, nos dias de hoje, parece-me impossível controlar o acesso, ou melhor, todas as possibilidades que há de acesso e partilha. (Português, 46 anos, mestrado/pós-graduação, advogado - entrevistado via Google Hangout).

Ainda a respeito das perceções dos entrevistados sobre a partilha de conteúdos protegidos por direitos de autor enquanto prática social, foram lhes colocadas duas questões destinadas a averiguar a sua opinião sobre os efeitos económicos em causa para os produtores de conteúdos e os argumentos de natureza moral frequentemente avançados pelos detentores de direitos no sentido da aplicação de penas mais duras contra os partilhadores que fazem equivaler o download não autorizado de conteúdos a uma forma de roubo. Relativamente à primeira questão, à exceção de dois entrevistados brasileiros, todos os restantes admitiram que tal tipo de práticas representa um prejuízo económico. Ainda assim, muitos fizeram questão de estabelecer uma distinção entre editoras e outros intermediários tradicionais no processo de produção de conteúdos por um lado e

os autores e criadores de conteúdos propriamente ditos, por outro, esclarecendo que para estes a Internet e a partilha por ela proporcionada oferece significativas vantagens promocionais. Outra diferenciação avançada foi entre os criadores que sempre dispuseram de outras fontes adicionais de rendimento e aqueles cujo principal meio de subsistência consistiu tradicionalmente na venda de cópias das suas obras:

Sim, alguns mais do que outros, mas sim prejudica-os. Os músicos por exemplo têm a alternativa dos concertos, mas um escritor não tem alternativa. Ou vende os livros ou não ganha dinheiro. Com o cinema e a televisão continuam a haver várias fontes de rendimento, mas seja como for já se vê que no cinema americano apenas dão dinheiro os filmes de super-heróis, os filmes de terror e as comédias baratas. O cinema independente que aspire a um financiamento um pouco mais elevado sai prejudicado. Ou seja, há consequências reais, que põem em causa a produção de conteúdos de qualidade. (Português, 33 anos, doutoramento, investigador associado)

Prejudicar prejudica, claro...em vez de faturarem 1 bilião de euros com algo podem faturar "apenas" 500 milhões. A meu ver, apesar de prejudicar, acaba por ser uma ação minimamente aceitável... Se eles ganham tanto tanto tanto, é aceitável que alguém tire um conteúdo sem pagar. É um pouco na lógica de 'eu sou pequeno, gastar 100€ mês em entretenimento faz-me moça no orçamento, eles que são grandes, perderem os meus 100€ não faz diferença nenhuma, porque recuperam isso de n outras formas' (...) Custa-me muito menos tirar um conteúdo de uma empresa enorme, cheia de recursos e dinheiro, que a uma pequena, que acaba de começar mas, mesmo apesar de me custar mais...continuo a optar pelo download... Apesar do pequeno tamanho, isso não tem um impacto tão grande que me faça pensar "epá, eles são novos, vou ajudar ao crescimento comprando em vez de fazer o download"...não acontece... (Português, 27 anos, bacharelato/licenciatura, gestor de projetos)

Acho que prejudica sim, mas considero que é uma realidade com a qual precisamos aprender a lidar. O mundo não vai voltar atrás, então não acho que seja possível simplesmente tentar fingir que tudo continua como era... principalmente no segmento musical, vemos que os artistas mais do circuito comercial têm vivido muito mais dos shows do que dos álbuns. É uma tendência

cada vez mais forte. Por outro lado, temos na rede uma possibilidade de acesso infinitamente maior do que tínhamos antes, inclusive que beneficia os músicos e artistas que não teriam as mesmas oportunidades no mercado tradicional. Acho que o mundo atual exige novas formas de consumo e dinâmicas mais condizentes com a realidade do que muitos insistem em pregar. (Brasileira, 26 anos, mestrado/pós-graduação, jornalista).

Penso que pode prejudicar, sim; mas em geral, menos do que às empresas que explorava os conteúdos protegidos.

(...)

Acho que a situação também varia muito de setor para setor: o cinema é uma arte muito mais industrial, por exemplo. E mesmo dentro de cada setor, também variará muito: grandes produções requerem grandes vendas, grandes investimentos de marketing, e fica – creio – mais difícil garantir sua produção como investimento rentável quando há o download não autorizado.

Acho que os pequenos produtores/criadores tendem a ser menos afetados (até porque na situação [anterior] recebiam uma parcela pequena do bolo, comparado às empresas); mas ao mesmo tempo, é necessário um grande esforço deles para que encontrem modos de custear sua produção na situação atual.

Em certas esferas isso é viável, ou até muito próximo do que esses criadores já faziam (como no caso do músico que já tirava seu sustento de shows); em outros, é bem mais difícil (como no caso dos autores de livros (Brasileiro, 35 anos, mestrado/pós-graduação, editor de textos)

A Internet tornou verdade aquela premonição do Andy Warhol, não é? [Isto é,] a história de que um dia toda a gente seria famosa por 15 minutos... Por isso é que há milhares de artistas novos por todo o lado... se isso é um ganho ou não depende de cada um, dos [seus] objetivos. (Portuguesa, 31 anos, mestrado/pós-graduação, arquiteta)

Quanto à dimensão da empresa ou artista, é claro que faz toda a diferença. O Moby, por exemplo, que nem é um dos artistas mais populares que andam por

aí, ofereceu uma cópia de uma das músicas dele no seu próprio web site enquanto que a música estava à venda no iTunes. A música ficou em primeiro lugar no top do iTunes enquanto estava a ser oferecida no site do artista. Há coisas estranhas... É claro que o potencial de promoção da distribuição não autorizada de conteúdo protegido não é para ser desprezado, mas no caso de artistas emergentes, as coisas podem tornar-se um pouco mais complicadas. Isto é tanto mais complicado no caso de artistas emergentes que se movimentam em nichos de mercado onde os consumidores habituais têm menor afluência económica. As músicas acabam por ser descarregadas ilegalmente sem que os artistas sejam compensados e eventualmente chega o momento fatídico em que cessam atividades por não as poderem suportar. Em Portugal então, onde não há o hábito das pessoas fomentarem o que quer que seja através da sua própria contribuição económica, a situação é ainda mais complicada. (Português, 42 anos, ensino secundário, músico)

Creio que não prejudica. Não sei se te contei, mas uma das moderadoras do [nome de tracker privado de BitTorrent] trabalhava para a Sony/BMG, e ela dizia que relatórios internos falavam dos benefícios da pirataria que ajuda bem na promoção dos artistas, acho que artistas de música eletrônica são mais atualizados em relação a isso. E até certo ponto é verdade, sim. São os que mais aparecem no [site] pedindo lançamento dos CDs (Brasileiro, 28 anos, bacharelato/licenciatura, coordenador de secção de município).

Não obstante, na opinião dos entrevistados quaisquer prejuízos provocados eventualmente pela partilha de ficheiros não parecem legitimar o recurso à metáfora do *download* não autorizado como uma espécie de roubo que é empregue por detentores de direitos como companhias discográficas e produtoras de cinema e que faz equivaler uma cópia ilícita a uma venda perdida. Com efeito, ao longo das entrevistas palavras como “exagero” e “absurdo” foram não raramente utilizadas para descrever tal pretensão retórica. Um pormenor que não penso deva ser menosprezado é o facto das respostas dos entrevistados portugueses a esta questão em concreto terem sido mais uma vez muito mais longas do que as dos entrevistados brasileiros que na maior parte dos casos se limitaram a rejeitar categoricamente a hipótese do “efeito de substituição”:

Parece-me difícil que um produtor de uma imagem saia fortemente prejudicado pela divulgação da mesma, uma vez que na maior parte das vezes a cópia não tem a qualidade do original e a procura deste se mantém. Compreendo que eles tenham tentado essa via como forma de condicionar o destinatário das mensagens. Mas acho que [isso] não tem efeito na sociedade atual. Ou seja, percebo que eles recorram à via 'intimidatória'/criminalizadora para tentar proteger um interesse económico forte. Mas acho que durante muitos anos beneficiaram grandemente dos preços absurdos a que vendiam vinis/CD's/DVD's. Naturalmente que perdendo essa fonte de (enormes) receitas, não estarão felizes com a facilidade de acesso e cópia que agora existe. Nesse aspeto, julgo que o iTunes foi bastante inteligente. (Português, 46 anos, mestrado/pós-graduação, advogado)

É um exagero. O problema do roubo é a violência que normalmente acompanha o ato. O medo de ser magoado fisicamente e o sentimento de impotência. No caso dos downloads isso não existe. Parece-me que eles [detentores de direitos] querem criar uma consciência que não existia antes, apelando a algo que assusta as pessoas. Mas na verdade acho que em parte o uso de downloads ilegais é culpa dos detentores de direitos de autor. Muitos têm demorado a adaptar-se ao novo contexto da Internet. Não entendo porque ainda é tão difícil ver séries e filmes online em streaming, pagos através de publicidade. Muitos conteúdos ainda são difíceis de aceder ou demasiado caros. (Português, 33 anos, doutoramento, investigador associado)

A questão de a situação ficar um pouco melhor porque afinal há mais concertos e música ao vivo não se aplica muito em Portugal: Vivemos décadas num sistema em que câmaras municipais pagavam a artistas para concertos que ofereciam aos seus munícipes. Isso sabotou o circuito de concertos pagos. Agora que o estado não tem dinheiro e os municípios também, esse esquema acabou e os concertos que restam são muito menos bem pagos. As pessoas, por seu lado, nunca criaram o hábito de pagar para ir ver um artista Português. Quanto às editoras e a essa estratégia, acho absolutamente descabida. É claro que a indústria sofreu muito com a disponibilização de música online de forma gratuita e não autorizada, mas eles são eventualmente uns dos principais culpados pelo estado da coisa. Além

disso, é só analisar os contratos das editoras até ao fim dos anos 90 para perceber quem são os originais piratas da indústria

A BMG (agora Sony) ainda me deve dinheiro que nunca irei ver. Eles só são os representantes dos artistas em papel. Na realidade só zelam pelos seus próprios interesses. (Português, 42 anos, ensino secundário, músico)

Acho exagerado

(...)

No caso da música, penso que em alguns casos isso acontece [muitos utilizadores recorrem ao download não autorizado como forma de experimentar antes de comprar os conteúdos em causa]. No caso dos filmes, sei que muitas vezes acedem ao download e se gostam, acabam por comprar o DVD. Mas neste caso, é verdade que se deixou de ir ver os filmes nas salas de cinema e passou-se a fazer o download (o que não é o meu caso, que ainda frequento [as salas de cinema] com alguma assiduidade). No caso das séries, não. Penso que não se está à espera que [a série] seja transmitida na televisão por cá. (Portuguesa, 31 anos, mestrado/pós-graduação, desempregada)

Acho que é em grande medida fruto de uma campanha retórica das grandes empresas. Para além da discussão sobre o carácter não-exclusivo da cópia, duvido que no passado esses criadores pensavam no empréstimo de uma obra, na gravação de uma cassete para um amigo como equivalente a um roubo. (Brasileiro, 35 anos, mestrado/pós-graduação, editor de textos).

7.CONCLUSÃO: A RECIPROCIDADE ENQUANTO MOTOR DE UMA CULTURA DA PARTILHA

No decurso do processo de elaboração da pesquisa da qual os dados expostos em cima foram retirados, fomos confrontados com algumas limitações metodológicas, situação que nos levou a adotar um método misto (inquérito e entrevistas *online*). Uma primeira dessas limitações está relacionada com o recurso a amostras não probabilística, ou seja, não representativas das populações em questão, tendo aquelas sido constituídas exclusivamente por indivíduos que se auto-selecionaram ao responderem aos apelos lançados em várias redes sociais solicitando o preenchimento do questionário. A segunda resulta de uma consequência indireta da primeira e consiste na desproporcionalidade da dimensão das duas amostras dos inquéritos *online* (203 inquiridos no caso do questionário pt_PT e 98 inquiridos no caso do questionário pt_BR) em contraposição com o conjunto total de utilizadores da Internet de Portugal e Brasil. Apesar dessas deficiências, pensamos que a riqueza e a qualidade das declarações de 16 dos participantes recolhidos por entrevista *online* contêm aportes empíricos bastante valiosos sobre o modo como utilizadores portugueses e brasileiros incorporaram a Internet nos seus hábitos quotidianos de consumo de obras culturais.

Ao mesmo tempo, não sendo esta uma pesquisa inspirada por um cientifismo extremista, não pode deixar de ser relevante o facto das respostas tanto ao inquérito *online* como à entrevista se coadunarem com algumas das conclusões dos estudos analisados por Watson *et al.* Assim, se por um lado em ambas as amostras a percentagem de inquiridos que têm sempre ou frequentemente consciência da natureza lícita ou ilícita das obras que descarregam aparenta ser superior à média dos 12 estudos citados por Watson *et al.* que analisaram o nível de conhecimentos legais dos inquiridos, por outro tanto os resultados do nosso questionário como as opiniões avançadas pelos 16 entrevistados indiciam estar em linha com o facto de na maioria dos estudos referidos por Watson *et al.* apenas uma minoria dos participantes ser da opinião que as leis constituem um meio de dissuasão contra a partilha não autorizada. Outro ponto comum identificado entre esta pesquisa empírica e os estudos analisados por Watson *et al.* é o ênfase no preço elevado dos conteúdos autorizados enquanto motivação adicional para a partilha não autorizada. Tal fator encontra-se particularmente presente nas declarações dos participantes nas entrevistas. Relacionado com este fator está a percepção maioritária – visível tanto nos dados empíricos da nossa pesquisa, como nas observações empíricas alvo da revisão de Watson *et al.* - de que o prejuízo em causa é muito

reduzido ou mesmo nulo e de que, a verificar-se a existência de danos, tais perdas podem ser facilmente absorvidas, nomeadamente mediante a adoção de modelos de negócio inovadores.

Ainda que o conjunto de motivações e justificações dos utilizadores para a partilha não autorizada de ficheiros que acabámos de expor seja por si só relevante, pensamos que a total compreensão das suas implicações sociais e culturais ficará incompleta se não acrescentarmos a este quadro outro conjunto de fatores centrados nas relações sociais formadas a partir das redes de partilha de ficheiros. Com efeito, uma das conclusões destacadas na revisão bibliográfica de Watson *et al.* refere-se à presença entre os utilizadores de redes de partilha de ficheiros da noção de que quem tirou partido dos recursos disponíveis numa rede deve contribuir com a sua parte, disponibilizando recursos como largura de banda e ficheiros aos restantes utilizadores. Esta noção permite-nos assim falar da existência de uma Cultura P2P associada às próprias características técnicas das redes P2P, bem como à Internet em geral. Ao assegurarem a democratização da capacidade de reprodução de obras intelectuais, estas redes permitem que pela primeira vez na história da humanidade cada utilizador passe a poder copiar em simultâneo informação de milhões de outros utilizadores sem necessitar de saber quem eles são ou onde se encontram. Esta democratização expressa-se sobretudo pelo facto da distribuição dos conteúdos dispensar o recurso a agentes estabelecidos como grandes indústrias culturais ou órgãos de comunicação social pertencentes ao Estado ou a poderosos grupos económicos privados.

Tal cultura é particularmente visível nas comunidades de partilha de ficheiros sem fins comerciais de acesso fechado ao público como *trackers* privados de BitTorrent. Para evitar uma “tragédia dos comuns”, isto é, uma situação de défice de produção – fracos níveis de upload de novos conteúdos - e consumo excessivo – de largura de banda, estas comunidades adotam e fazem cumprir um conjunto de regras mais ou menos complexas, ajudando deste modo a criar e a manter um conjunto de recursos comuns. Na esteira de Ostrom (1990), Bodó considera que estamos perante regimes de produção entre pares baseados em bens comuns (Bodó 2013).

A noção de reciprocidade é aqui chave na medida em que nos remete para um modelo diferente do *homo economicus*, o ideal-tipo característico da economia neoclássica de agente humano associal, egoísta e movido exclusivamente pelo interesse próprio que serve de inspiração a boa parte dos estudos sobre os efeitos da partilha não-autorizada de ficheiros protegidos por direitos de autor no bem-estar social. Com base em dados empíricos relativos a dezenas de estudos sobre teoria dos jogos que demonstram o interesse da maioria das pessoas por valores como justiça, reciprocidade e a participação em grupos, os economistas Samuel Bowles e Herbert Gintis propõem a existência de um segundo ideal-tipo, o *homo reciprocans*. Para Bowles e Gintis, o *homo*

reciprocans distingue-se do *homo economicus* por ser movido por um princípio de reciprocidade, ou seja “uma propensão para cooperar e partilha com outros com a mesma disposição, mesmo a custo pessoal, e uma vontade de punir aqueles que violam normas sociais cooperativas e de outro tipo, mesmo quando a punição acarrete custos pessoais” (Bowles e Gintis 1998, p. 2-3). Em situações experimentais, “quando outras formas de sanção não se encontram disponíveis, o *homo reciprocans* reage à deserção com deserção, conduzindo assim a uma espiral descendente de não-cooperação.” Daí que Gintis conclua que longe de ser o altruísta desinteressado da teoria utópica ou o hedonista egoísta da economia neoclássica, o *homo reciprocans* seja antes um cooperador condicional (Gintis 2000, p. 277-278).

Perante o contraste entre as conclusões das revisões bibliográficas de Handke (2012) e Watson *et al.* (2014) por um lado, e os dados empíricos da nossa investigação aqui destacados por outro, o ideal-tipo do *homo reciprocans* avançado por Bowles e Gintis apresenta-se assim como uma fonte de inspiração não só para pesquisadores nos efeitos e motivações para a partilha não-autorizada de ficheiros como também para o processo de formação de políticas públicas em torno dos direitos de propriedade intelectual.

REFERÊNCIAS BIBLIOGRÁFICAS

- Andy (2015). “Rapid Pirate Site Blocking Mechanism Introduced By Portugal”. *TorrentFreak*, 31 de Julho. <https://torrentfreak.com/rapid-pirate-site-blocking-mechanism-introduced-by-portugal-150731/>.
- Benkler, Yochai (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press.
- Bodó, Balázs (2013), “Set the Fox to Watch the Geese: Voluntary IP Regimes in Piratical File-Sharing Communities”, em Fredriksson, Martin e James Arvanitakis (eds.). *Piracy: Leakages from Modernity*, Sacramento, CA: Litwin Books. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2261679.
- Bowles, Samuel e Herbert Gintis (1998). “Is Equality Passé? Homo Reciprocans and the Future of Egalitarian Politics”, 19 de Outubro. Amherst, Massachusetts: Universidade do Massachusetts. <http://www.umass.edu/preferen/gintis/isinequa.pdf>.
- Caçador, Fátima (2015). “A pirataria online tem os dias contados em Portugal? Acordo facilita bloqueio de sites pelos operadores”. *SAPO TEK*, 30 de Julho. http://tek.sapo.pt/noticias/internet/artigo/a_pirataria_online_tem_os_dias_contados_em_portugal_acordo_facilita_bloqueio_de_-43609kkc.html.
- Cardoso, Gustavo, António Firmino da Costa, Ana Rita Coelho e André Pereira (2015). *A Sociedade em Rede em Portugal - Uma Década de Transição*. Coimbra: Edições Almedina.
- Coutinho, Isabel (2009). “Governo procura solução para proteger artistas”. *Público*, 14 de Maio. <https://web.archive.org/web/20091001052557/http://ultimahora.publico.clx.pt/noticia.aspx?id=1380516>.
- Dejean, Sylvain (2009). “What Can We Learn from Empirical Studies About Piracy”. *CESifo Economic Studies*, 55(2), pp. 326-352. <http://cesifo.oxfordjournals.org/content/55/2/326.abstract>.
- Gintis, Herbert (2000). *Game Theory Evolving: A Problem-Centered Introduction to Modeling Strategic Interaction*. Princeton, Nova Jersey: Princeton University Press.
- Grassmuck, Volker R. (2010). “Academic Studies on the Effect of File-Sharing on the Recorded Music Industry: A Literature Review”. Social Science Research Network, 14 de Maio. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1749579.

- Handke, Christian (2012). “A Taxonomy of Empirical Research on Copyright – How Do We Inform Policy?”. *Review of Economic Research on Copyright Issues*, 9(1), pp. 47-92. <http://ssrn.com/abstract=2101084>.
- Larsson, Stefan (2011). *Metaphors and Norms – Understanding Copyright Law in a Digital Society* (tese de doutoramento). Lund Studies in Sociology of Law 36, Lund University. <http://lup.lub.lu.se/record/2157989>.
- Liebowitz, Stan J. (2007). “How Reliable is the Oberholzer-Gee and Strumpf Paper on File-Sharing?”. *Social Science Research Network*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1014399.
- MAPiNET – Movimento Cívico Anti-Pirataria na Internet (2009). “O MAPiNET condena e repudia as declarações do Ministro da Cultura a propósito da aprovação da Lei Criação e Internet em França”, 12 de Maio. <https://web.archive.org/web/20090518064631/http://www.mapinet.org/2009/05/o-mapinet-condena-e-repudia-as-declaracoes-do-ministro-da-cultura-a-proposito-da-aprovacao-da-lei-criacao-e-internet-em-franca/>.
- Oberholzer-Gee, Felix e Koleman S. Strumpf (2007). “The Effect of File Sharing on Record Sales: An Empirical Analysis”. *Journal of Political Economy*, 115(1), pp. 1-42. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=961830.
- Ostrom, Elinor (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Nova Iorque: Cambridge University Press.
- Quiggin, John (2013). “The Economics of New Media”, em John Hartley, Jean Burgess e Axel Bruns (eds.). *A Companion to New Media Dynamics*. Oxford: Wiley-Blackwell, pp. 90-103.
- Revolução dos Bytes (2016). “Novo site legítimo bloqueado e sujeito a duplo pagamento”. 28 de Janeiro. <https://revolucaodosbytes.pt/novo-site-legitimo-bloqueado-e-sujeito-a-duplo-pagamento/>.
- Rosa, António M. (2006), *Cinco Lições sobre Comunicação, Redes e Tecnologias da Informação: da Cibernética ao Copyright*. Lisboa: Vega.
- Rosa, António M. (2009). *Os Direitos de Autor e os Novos Media*,. Coimbra: Angelus Novus.
- Rosário, Daniel (2009). “Liberdade acima de tudo, defende ministro”. *Rádio Renascença*, 12 de Maio.

<https://web.archive.org/web/20090605214716/http://www.rr.pt/InformacaoDetalhe.aspx?AreaId=23&SubAreaId=79&ContentId=286462>.

Simões, Paula (2016a). “Mais um site legítimo bloqueado”. *Paula simoes’ blog*, 28 de Janeiro. <https://paulasimoesblog.wordpress.com/2016/01/28/mais-um-site-legitimo-bloqueado/>.

Simões, Paula (2016b). “IGAC e MAPiNET não cumprem Memorando de Entendimento”. *Paula simoes’ blog*, 10 de Março. <https://paulasimoesblog.wordpress.com/2016/03/10/igac-e-mapinet-nao-cumprem-memorando-de-entendimento/>.

Smith, Michael D. e Rahul Telang (2012). “Assessing the Academic Literature Regarding the Impact of Media Piracy on Sales”. *Social Science Research Network*, 19 de Agosto. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2132153.

Tschmuck, Peter (2010). “The Economics of Music File Sharing – A Literature Overview”. Vienna Music Business Research Days, University of Music and Performing Arts, Viena, 9-10 de Junho. <http://musikwirtschaftsforschung.files.wordpress.com/2010/06/tschmuck-the-economics-of-file-sharing-end.doc>.

Watson, Steven J., Daniel J. Zizzo e Piers Fleming (2014). “Determinants and welfare implications of unlawful file sharing: a scoping review.” *CREATE Working Paper*, 14(5). <http://zenodo.org/record/8553/files/CREATE-Working-Paper-2014-05.pdf>.

CYBERLAW

by CIJIC
