CYBERLAW by CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

Do we have one real perception of the true degree of technological intrusiveness into the lives of citizens?

At this «Cyberlaw by CIJIC», 2nd edition, we intend to bring to one legal and technological debate some of the most worrying questions related with the weakness of the traditional concepts of public law. Take, for example, old problems where, alleged, threats to state security compress ordinary individual freedoms. Cyberspace currently dominates daily life. Where can we find the protection of the legal-subjective positions of individuals in it?

Traditional juridical and legal programs will lose all effectiveness, sliding into nominal, if the rule of law gives up to respond to the daily problems of netizens.

We all face new legal dimensions. In face of the ineluctable conclusion that the Internet is a global resource, which we dare say, incompatible, par excellence, with the old concept of territorial sovereignty of State, which scientific criteria need to be included in the construction of a dogmatic approach to the regulation of cyberspace? Furthermore, can it be regulated? Which - if any - new international, worldwide, legal solutions we must strive for?»

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

CYBERLAW by CIJIC

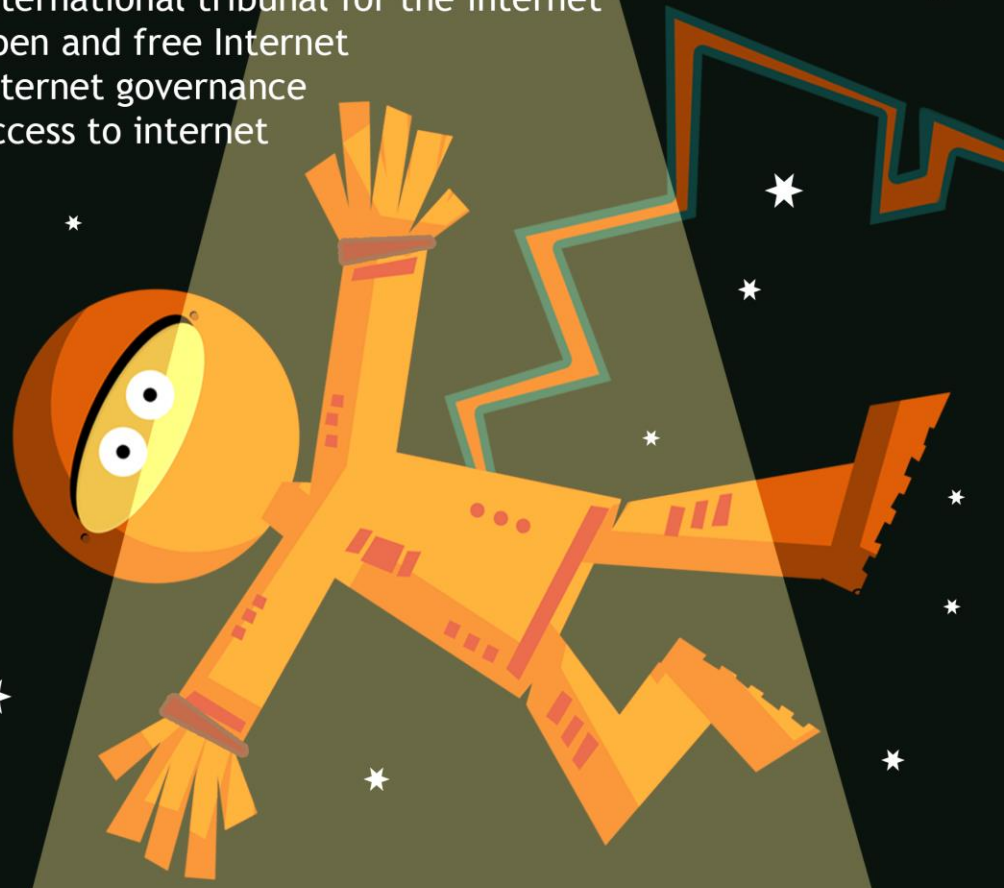
DIREITO: A PENSAR TECNOLOGICAMENTE

CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 02 junho 2016 | Grátis

DIREITO:
A PENSAR TECNOLOGICAMENTE

internet:

- international tribunal for the internet
- open and free Internet
- internet governance
- access to internet



outros: · international cooperation

CYBERLAW by CIJIC

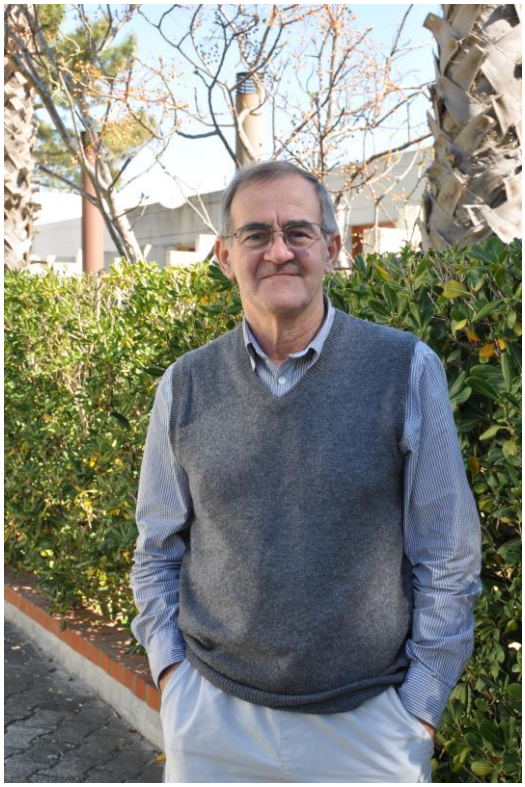
EDIÇÃO N.º II – JUNHO DE 2016

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

CYBERLAW by CIJIC

INTERVIEW WITH PORTUGUESE NATIONAL CYBERSECURITY CENTER COORDINATOR : PROFESSOR PEDRO VEIGA

ENTREVISTA COM O COORDENADOR DO CENTRO NACIONAL DE CIBERSEGURANÇA PORTUGUÊS: PROFESSOR PEDRO VEIGA



Professor PEDRO VEIGA

RESUMO

O novo Coordenador do Centro Nacional de Cibersegurança[1], Pedro Veiga, admite, à «*Ciberlaw By CIJIC*», que tem havido "défice de discussão" sobre a proteção dos Direitos Fundamentais no Ciberespaço. Garantiu-nos, todavia, que tudo fará para que a internet possa ser um espaço seguro e de confiança para todos os portugueses. Mais, após ter assumido funções há dois meses, Pedro Veiga apela, ainda, a um maior envolvimento de entidades públicas e privadas, prometendo um papel de charneira do CNCiber na divulgação das actuais leis e das boas práticas de Cibersegurança junto de todos os sectores da sociedade.

1 http://exameinformatica.sapo.pt/noticias/mercados/2016-04-18-Pedro-Veiga-e-o-novo-coordenador-do-Centro-Nacional-de-Cibersegurança

O catedrático apaixonado pela Cibersegurança revela que uma das suas prioridades é criar pontes com entidades públicas e privadas para trazer mais recursos humanos para uma área que considera ser "tão promissora, aliciante, de elevada empregabilidade e desafiante.". Pedro Veiga lembra que o factor humano é crucial para a Cibersegurança. Num paralelismo, questiona, "(D)e que serve um automóvel ter airbags, ABS, cintos de segurança e muitos outros dispositivos de segurança se o condutor estiver distraído a usar um telemóvel, não respeitar um sinal de proibição de ultrapassagem numa curva ou um semáforo no vermelho?". Podemos ter à mão tecnologias fantásticas, mas se não forem correctamente utilizadas, o resultado pode ser desastroso, conclui o recém-empossado Coordenador do CNCiber.

Ao longo da nossa conversa, Pedro Veiga revela as suas principais prioridades e mostra-se confiante no empenho do actual Governo na superação dos desafios, velhos e novos, do Ciberespaço.

Interview Questions

Propusemos[2] uma conversa, ao Professor Pedro Veiga, subordinada a alguns tópicos, para que dela possamos suscitar discussões necessárias. Em traços gerais, pretendemos problematizar em torno da construção, do estabelecimento e do fomento de uma cultura de confiança (no anglicanismo de «*Trust*») do utilizador (em sentido lato, compreendendo desde o utilizador-médio, às organizações e ao próprio Estado) no uso da internet e na fruição do ciberespaço. Conseguiremos ancorá-la na vitalidade, que assim se espera, do nosso CNCiber?

Q) Comecemos, por exemplo, pela comparação, bastante *ilustrativa*, trazida a discussão por Peter Singer[3]. Poderemos esperar que o CNCiber tenha por «(...)*missão de contribuir para ganhos em* cibersegurança *pública, através de atividades de investigação e desenvolvimento tecnológico, atividade laboratorial de referência, observação da segurança e vigilância epidemiológica* informática, *bem como coordenar a avaliação externa da qualidade laboratorial, difundir a cultura científica, fomentar a capacitação e formação e ainda assegurar a prestação de serviços diferenciados, nos referidos domínios*[4]»? Agora que tomou as rédeas do CNCiber, o que podemos esperar deste?

P.V.) O CNCiber tem um mandato que está definido na Estratégia Nacional de Segurança no Ciberespaço (Resolução do Conselho de Ministros nº 36/2015) e esta estratégia deve ser alvo de uma revisão regular e periódica, segundo este diploma. Numa altura em que a crescente digitalização da sociedade avança, quando a informação sob a forma digital cresce a um ritmo muito elevado, e, quando cada vez mais serviços se desenvolvem sobre as redes globais, a missão central de garantir um ciberespaço nacional seguro e que inspire confiança aos cidadãos assume-se como muito importante. Não é só ao CNCiber que está atribuído o papel de garantir um ciberespaço seguro, na medida em que muitas outras entidades, públicas e privadas, tem que estar envolvidas e contribuir

2 Conduzida por Nuno Teixeira Castro.
3 *Singer, Peter W.*, em «*How to Save the Net: A CDC for Cybercrime*» em: http://www.wired.com/2014/08/save-the-net-peter-singer/
4 Embora adaptada à temática da cibersegurança, esta informação foi, *ipsis verbis* retirada do sítio do INSA - Instituto Nacional de Saúde Dr. Ricardo Jorge, e da missão a que este se propõe prosseguir. Disponível em: http://www.insa.pt/sites/INSA/Portugues/QuemSomos/Paginas/Missao.aspx

para elevados níveis de resiliência e robustez do nosso quotidiano neste mundo digital. Mas o CNCiber tem que contribuir para uma confluência de esforços na mesma direcção, quer através do desempenho de um papel charneira na difusão da legislação existente, quer levando o conhecimento das boas práticas de cibersegurança ao conhecimento de todos os sectores da sociedade. Há sectores e recursos que devem merecer uma especial importância como as infraestruturas críticas, a informação que é detida pelas instituições públicas ou a resiliência das redes que prestam os serviços aos cidadãos ou às empresas. A reduzida dimensão dos recursos humanos e materiais atribuídos ao CNCiber limitam a abrangência e diversidade da intervenção, por exemplo na vertente de investigação e desenvolvimento que é referida na sua questão, mas pela sua relevância é algo que será necessário repensar e reforçar no contexto da revisão regular e periódica atrás referida, sempre numa abordagem de colaboração e de procura pela excelência na implementação.

Q) - O factor humano continua a ser o «*tendão de Aquiles*». A este respeito, por um lado, comecemos com uma afirmação, *curiosa*, de Vint Cerf[(5)]: «(...) *"The thing I worry more than anything about is not the hackers and the people who are attempting to somehow change the function of the Internet. (…) Some of the worst problems that happen on the Internet are not because somebody deliberately caused the problem. It's because somebody made a mistake. We've lost half the networks ability to transport traffic or route it to the right destinations because somebody made a configuration mistake.*"». O que se passa? Ensino deficitário? Demasiada pressão organizacional focada no lucro? Incúria na segurança? *Maus* alunos?

P.V.) Em todas as áreas da segurança o factor humano é sempre um dos elos mais fracos. Na minha actividade de professor universitário costumo fazer analogias, na exposição nas aulas, com outros sectores da sociedade onde a segurança é um elemento crucial, tais como a segurança rodoviária, a segurança em edifícios ou a segurança contra os incêndios que nos devastam a cada verão. Nestas áreas podemos usar tecnologias fantásticas, mas se não forem aplicadas de modo adequado por todos os agentes envolvidos, o resultado final é desastroso. De que serve um automóvel ter *airbags*, ABS,

5 Mais em: https://www.washingtonpost.com/blogs/post-live/wp/2016/05/18/meet-father-of-the-internet-vinton-g-cerf/

cintos de segurança e muitos outros dispositivos de segurança se o condutor estiver distraído a usar um telemóvel, não respeitar um sinal de proibição de ultrapassagem numa curva ou um semáforo no vermelho? Também no ciberespaço existem soluções tecnológicas que podem mitigar muitos dos problemas que existem. Mas, se os gestores não estiverem cientes dos problemas não as aplicarão nas organizações e nas empresas que gerem, ou não atribuirão os recursos humanos e meios materiais necessários para garantir a cibersegurança organizacional. Os cidadãos não as usarão nos seus sistemas pessoais ou domésticos. Os técnicos informáticos não aplicarão as tecnologias necessárias por falta de meios materiais ou por puro desconhecimento. E a estonteante velocidade de evolução tecnológica, o crescente uso das tecnologias da informação em todos os sectores da nossa sociedade, não têm sido acompanhadas pela capacitação de recursos humanos em quantidade e com as competências necessárias, o que conduz a que o factor humano seja um dos principais problemas que urge resolver.

O nosso sistema de ensino não tem tido capacidade para formar todos os recursos humanos necessários para esta área; mais preocupante ainda quando aliado ao facto de os jovens não escolherem carreiras ligadas às tecnologias da informação e da comunicação (TIC). E isto parece um absurdo, na medida em que há muitas saídas profissionais nesta área e os estudos internacionais apontam para que o problema da falta de recursos humanos em TIC vá aumentar, em especial devido à, já referida, digitalização da economia. O CNCiber também procurará articular-se com outras iniciativas públicas e privadas para trazer mais recursos humanos para esta área tão promissora, aliciante, de elevada empregabilidade e desafiante.

Q) - Ainda e quanto ao factor humano. O comportamento e os hábitos, de uma grande parte dos *netizens* (autodidatas), resvalam para o risco. Como sabemos, o perigo não está somente no *software* e no *hardware*, mas, pelo contrário, antes e muito no *manware*. Sem uma formação de base mínima, muitas das vezes, pequenas dicas de comportamento *online* poderiam mitigar os efeitos associados a tais acções ou omissões. Poderá o CNCiber preencher esta falta de formação? Veja-se, por exemplo, o caso dos EUA, no seguimento da campanha levada a cabo pelo *DHS* (*Department of Homeland Security)- Stop.Think.Connect*[6], desde o seu lançamento em 2010, a mensagem de

6 Disponível em: http://www.dhs.gov/stopthinkconnect

divulgação e sensibilização assume uma dimensão nacional. O objectivo é o de criar uma verdadeira compreensão destas ameaças virtuais, segundo o *DHS*. A mensagem, forte, apela ao esforço de todos, cidadãos, organismos públicos e privados. Complementada com alguns recursos tecnológicos, regra geral ao nível de *software*, ainda segundo o *DHS*, tem permitido assegurar aos cidadãos comportamentos, recursos e ferramentas essenciais à sua protecção e, indirectamente, do próprio Estado, contra as crescentes ameaças cibernéticas. Um modelo que poderemos seguir?

P.V.) Esta pergunta já foi, em parte, respondida anteriormente. Com efeito é crucial criar uma cultura de segurança no ciberespaço. Mas chegar a todos é um desafio monumental, que obriga a recorrer a meios e a instrumentos que são difíceis de serem geridos por um centro com a nossa dimensão e os nossos recursos. Mas é uma vertente que pode marcar a diferença, pelo que iremos tentar reunir esforços de outras entidades, como o sistema de ensino superior (politécnico e universitário) e não superior ou ainda, por exemplo, associações de vários tipos para podermos atingir os vários actores que são mais relevantes. Desde associações empresariais, associações sem fins lucrativos do terceiro sector ou empresas interessadas em contribuir para uma sociedade digital mais segura, tentaremos uma confluência de esforços e acções para que todos tenhamos um uso mais seguro do ciberespaço.

Q) – Quanto ao contexto empresarial. O CNCiber, sendo vitalíssimo para todas as nossas organizações, à semelhança da estratégia nacional de cibersegurança alemã[7], poderia assumir uma postura activa - eventualmente por equipas especializadas CERT ou CSIRTS - de especial "policiamento" e/ou apoio às nossas PME's[8]? Ainda a tempo para construirmos um CNCiber útil e vital[9], para que Portugal não perca as inúmeras potencialidades do, já prometido, Mercado Único Digital para a Europa, estará o caminho

7Em: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Germancybersecuritystrategy20111.pdf

8 Um *ciberpolícia* para as PME's? O tecido empresarial português é essencialmente composto por PME's. Precisamente pelo peso que estas representam na nossa economia e pela dimensão da sua estrutura - a qual mais das vezes relega a sua ciberprotecçao para segundo plano - as recentes e constantes notícias sobre ataques de *ramsomware têm privilegiado o ataque a estas.* Os riscos associados a tais omissões de protecção estarão devidamente consciencializados?

9 Enquanto farol coordenador, especializado, entre o governo-sector público, as empresas, a academia e o cidadão.

para essa construção e os objectivos últimos suficientemente definidos para a prossecução dos mais elementares fins do estado? E de todos?

P.V.) O CERT.PT, que foi criado no seio da FCCN enquanto a dirigi, é uma peça importante mas não a única. Claro que a existência de CERTs é reconhecida pela ENISA como de especial importância, mas há outras formas de preparação das organizações e de resposta a incidentes que podem ser exploradas. Aliás, várias iniciativas europeias sugerem o modelo de parcerias público-privadas para reforçar a capacidade de garantir segurança no ciberespaço. O modelo alemão é um dos que estudaremos para ver qual o mais adequado a Portugal. Não há modelos óptimos e o que venha a ser decidido deve ter em conta a estrutura e as entidades nacionais. Ainda e em relação ao caso que refere, da Alemanha, há dimensões que se justificam num estado federal e que não podem ser transpostos de modo directo para a nossa realidade. Mas, sem dúvida que o desenvolvimento do Mercado Único Digital exige, de todos, uma confiança acrescida em relação à segurança do ciberespaço.

Q) – Um pouco de contexto da política legislativa e a essencialidade de mecanismos legislativos de cibersegurança, eficientes, perceptíveis e concretos no terreno da acção, quer para juristas quer para engenheiros, quer para o utilizador-médio-comum. Reflexo da crescente dependência tecnológica, as infraestruturas críticas, enquanto manifestações essenciais no regular funcionamento do estado, encontram-se cada vez mais manietadas por esta, carecendo de uma efectiva e eficaz protecção (por cada dia que passa, a tónica deverá incidir mais sobre a ciberprotecção[10]. Só assim o Estado poderá estar melhor capacitado para alcançar os seus fins. Existirá uma percepção correcta, por parte da vontade política, sobre a necessidade de legislar sobre cibersegurança e sobre as nossas infraestruturas críticas?

P.V.) Em primeiro lugar e relativamente ao aspeto da "*vontade política*" tenho dificuldade em responder de modo directo, na medida em que as múltiplas dimensões dos

10 Assustador? http://exameinformatica.sapo.pt/noticias/internet/2016-05-24-Internet-das-coisas-em-Portugal-ha-redes-de-agua-gas-e-centrais-eletricas-sem-autenticacao

problemas ligados ao *ciber* são tratados por muitas entidades e para umas o tema terá mais relevância do que para outras. Mas do ponto de vista da Ministra da Presidência e da Modernização Administrativa, que me desafiou para estas funções, sempre senti que atribui uma enorme importância a esta área, na medida em que o crescente uso da internet e dos paradigmas associados ao digital são fundamentais para uma administração mais ágil, eficiente e eficaz. Acresce que a directiva NIS, cuja versão final foi terminada há pouco tempo, contempla uma série de aspectos que têm de ser transpostos para a legislação nacional e que terão implicações em várias vertentes legais e em que muito trabalho terá de ser feito.

Em relação às infraestruturas críticas devo dizer que se trata de algo em que já estamos a desenvolver actividades, mais especificamente, com reuniões com várias entidades que têm responsabilidade em relação a este tipo de recursos, para ver como nos podemos articular para termos garantias de que são resilientes relativamente aos diversos desafios que podem surgir.

Q) – Por fim, a temática mais apetecível aos juristas: os Direitos fundamentais. Na senda da ideia da edificação de uma *Magna Carta*[11] para a internet, *Stefan Decker*, membro do Centro irlandês *Insight Centre for Data Analytics*, proferiu uma afirmação deveras pertinente. As pessoas «*are not looking for web protection and web privacy. They are looking for data protection and data privacy.*"[12]». Concorda? Protecção da rede e da sua privacidade, ou, Protecção de dados e da privacidade das pessoas? E por falarmos em protecção, com tantas formas, estaduais ou não, de interferência na normalidade *online*, no mundo *virtual* e no processo completo de transmissão da Informação e na garantia da sua ulterior superioridade, até que ponto fará sentido a exigência de um centro nacional cripto?

11 http://www.theguardian.com/technology/2014/sep/28/tim-berners-lee-internet-bill-of-rights-greater-privacy e http://www.networkworld.com/article/2688401/microsoft-subnet/tim-berners-lee-wants-internet-magna-carta-to-guarantee-netizens-privacy.html

12 *Stefan Decker*, ao *Irishtimes* em: http://www.irishtimes.com/business/technology/how-collective-insight-could-make-the-data-deluge-work-to-society-s-advantage-1.2108295

P.V.) Concordo com a afirmação e queria salientar que é uma área em que creio que existem múltiplas dificuldades. E até diria que o que as pessoas querem é poder beneficiar do mundo digital em segurança, sem saberem, sequer, o que são dados. E estarem protegidos de intrusos ou criminosos.

É difícil o equilíbrio entre, por exemplo, o que está preconizado no documento do Conselho da Europa "Guia dos Direitos Humanos para os Utilizadores da Internet" e a necessidade da protecção e da segurança do ciberespaço. Diferentes entidades, públicas e privadas, ou diferentes indivíduos, consoante o seu domínio de responsabilidade e a sua visão do Mundo, têm diferentes abordagens sobre os instrumentos que se podem, ou não, usar para que o uso do ciberespaço seja de progresso para a humanidade. É algo em que tem havido défice de discussão e é algo onde ainda não tenho ideias sólidas sobre o papel que deve ter o CNCiber, especialmente porque o nosso mandato e os recursos que temos disponíveis não nos permitem abrir áreas de intervenção em todas as vertentes possíveis neste mundo cada vez mais digital. As alterações relativamente à protecção de dados, e que são da responsabilidade directa de outras entidades, também são uma das frentes a que temos que estar atentos pelas implicações que pode ter no modo como o ciberespaço se desenvolve.

Quanto ao Centro nacional de criptografia, não considero que seja necessária a existência de um centro assim. É uma área de investigação que deve ser financiada como outras áreas já são financiadas, numa base competitiva a nível nacional ou internacional, mas considero que a tecnologia criptográfica que existe a nível internacional é adequada às exigências de privacidade e segurança do ciberespaço. O que considero que é muito relevante é o uso livre, adequado e apoiado em tecnologias de *software* robustas que assegurem implementações sólidas.