Pedro Veiga
Marta Dias

A Internet e as novas dimensões legais

NA EUROPA TAMBÉM EXISTE, de igual modo, uma crescente atenção para os problemas na área da governação da Internet. A Europa será, quiçá, a região do globo onde há uma maior estruturação do pensamento nesta área. Foi criado um fórum de discussão destes temas, o EuroDIG (European Dialogue on Internet Governance), onde se estudam e discutem os desafios presentes e futuros que a Internet está a trazer para a agenda da sociedade europeia.

Alguns aspectos Legais da rede global

A constatação do poder e do crescimento da Internet levou à suposta necessidade da sua governação. Quando se fala de governação, a lei é de imediato chamada à colação, seguem-se os órgãos de polícia criminal e, em última instância, os tribunais. Nesta matéria identificam-se duas posições opostas: por um lado a que defende que a governação da Internet é um imperativo de segurança, sendo que esta só existe se houver regulação e se houver controlo sancionatório. Por outro lado, a posição que defende que a governação é contranatura, assumindo-se mesmo, na vertente mais radical, como um meio de censura à própria Internet. Entre nós a posição dominante é hoje a da governação mínima que concilie a liberdade de cada um com a necessária privacidade, segurança e respeito pelos direitos, liberdades e garantias de cada um e de terceiros.

A protecção dos dados pessoais, a defesa dos direitos de propriedade intelectual e direitos conexos, a luta contra a cibercriminalidade, a protecção dos menores a quem é reconhecida especial debilidade no âmbito da utilização diária dos recursos da rede, em particular as redes sociais, os direitos dos consumidores em geral, os eventuais constrangimentos no acesso comercial aos serviços Internet e a respectiva regulação pelas autoridades competentes em cada país, são algumas das pedras de toque quando se aborda os aspectos legais da Internet.

No domínio da Internet as fronteiras esbatem-se ou simplesmente desaparecem, e nem sempre o direito internacional tem respostas para as questões que se levantam. Acresce o facto de a nível nacional não haver lei específica ou, havendo-a, poderem levantar-se dúvidas sobre a sua aplicação.

Ao nível da protecção dos dados pessoais, a Comissão Nacional de Protecção de Dados, enquanto entidade nacional de controlo dos dados pessoais, tem lançado várias campanhas de sensibilização tendo em vista alertar o público em geral para o perigo da circulação de dados pessoais na Internet. O regime jurídico aplicável nesta sede limita a possibilidade de tratamento de dados a duas situações concretas: as que resultam da lei e aquelas que advêm do consentimento livre, informado e expresso de cada um. Fora destas situações ficamos num terreno lodoso que merece e se espera ter tutela jurídica. Ora, aqui a indefinição surge quando, por exemplo, o sistema jurídico aplicável é o de um país onde pode simplesmente não haver lei que regule o tratamento de dados pessoais; veja-se o caso dos Estados Unidos da América, onde prevalece um puro modelo de mera "accountability" em detrimento da protecção dos dados pessoais, como a temos hoje em países como Portugal e como a Alemanha.

Em 1991, através da Lei n.º 109/91, de 17 de Agosto, foi publicada a Lei da Criminalidade Informática (LCI); esta lei inspirou-se na Recomendação 89/9 do Conselho Europeu, tendo adoptado a lista facultativa dos tipos criminais constantes daquela Recomendação, a título de exemplo: falsidade informática; dano relativo a dados ou programas informáticos; sabotagem informática; acesso ilegítimo; intercepção ilegítima e reprodução ilegítima de programa protegido. As molduras penais dos crimes de base iam entre pena de multa a pena de prisão até três anos, com excepção dos casos em que os crimes eram qualificados, podendo a pena ir até 10 anos (na sabotagem informática). A Lei da Criminalidade Informática previa ainda a responsabilidade criminal das pessoas colectivas que pratiquem estes crimes (e diversas penas acessórias), isto é, pelos crimes respondem os administradores das empresas, mas também as próprias empresas. Mas a lei nacional não se ficava por aqui e o Código Penal fixava o regime jurídico da burla informática, onde, diga-se, ao contrário da LCI, não há a responsabilidade da pessoa colectiva.

Entretanto, a 23 de Novembro de 2001 Portugal aderiu à Convenção do Cibercrime, a qual tinha como principal meta a harmonização das legislações nacionais dos Estados-membros da União Europeia em matéria de criminalidade cometida por estes meios, bem como facilitar a cooperação internacional e as investigações de natureza criminal.

> "No domínio da Internet as fronteiras esbatem-se, ou simplesmente desaparecem, e nem sempre o direito internacional tem respostas para as questões que se levantam."

A 15 de Setembro de 2009 foi publicada a Lei nº 109/2009, também denominada Lei do Cibercrime. Esta nova lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa. É pois revogada a Lei da Criminalidade Informática, que já tinha atingido a maioridade. Simultaneamente com a publicação da Lei do Cibercrime, foram no mesmo dia aprovadas e ratificadas a Convenção sobre o Cibercrime (passados oito anos) e o Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adoptado em Estrasburgo em 28 de Janeiro de 2003. Esta lei concretiza aquilo a que Portugal se obrigou no âmbito da convenção do cibercrime. Trata-se de um instrumento de cooperação internacional, já que se prevê que mais de 40 países possam adoptar um regime legal similar no domínio do cibercrime e da recolha de prova em suporte electrónico, em matéria relativa a ataques contra sistemas de informação.

O que esta lei traz de novo é, nomeadamente, a tipificação de novos crimes que visam fazer face a novos paradigmas como a Internet, por exemplo o crime de "phishing"; o facto da mera propagação de vírus informáticos passar a ser punida, mesmo sem haver danos informáticos; a possibilidade de o tribunal decretar a perda a favor do Estado dos objectos, equipamentos ou dispositivos que tiverem servido para a prática dos crimes nela tipificados. Trata-se de uma lei aplicável aos crimes informáticos, àqueles que sejam cometidos electronicamente e, ainda aos ilícitos cuja prova esteja guardada em suporte digital. Mas, reforçando tudo aquilo que já tivemos oportunidade de expor acima, esta lei vem de forma expressa e inequívoca salientar e formalizar o papel da cooperação internacional. Fá-lo ao longo de seis artigos onde são estabelecidas as formas e meios com as quais as autoridades nacionais competentes cooperam com as suas congéneres internacionais. Mais ainda, prevê-se a preservação e revelação expedita de dados informáticos para efeitos de investigação criminal, fixando-se prazos rigorosos para a salvaguarda dos mesmos. Neste campo a cooperação vai assim para além dos operadores da justiça, abrangendo os prestadores de serviços de comunicações electrónicas. Por fim, a título de regime geral aplicável prevê-se que em tudo o que não contrarie o disposto na lei da cibercriminalidade, aplicam-se aos crimes, medidas processuais e cooperação, as disposições do Código Penal, do Código do Processo Penal e da Lei n.º 144/99, de 31 de Agosto. Reforça-se por fim o facto de o tratamento de dados pessoais, a que acima já fizemos menção, se dever regular pelos termos do disposto na Lei n.º 67/98, de 26 de Outubro.

Em suma, dizer que hoje o legislador está de costas voltadas para a Internet é fazer letra morta do quadro legal vigente. Resta a questão da morosidade na aplicação da justiça; essa sim, continua a ser incontornável.

Não sendo possível aqui explorar exaustivamente todo o referido quadro legal, não podemos ainda deixar de fazer menção a algumas das disposições da lei fundamental:

a Constituição da Republica Portuguesa. Ao longo de todo o seu articulado encontramos disposições como o artigo 35.º e o artigo 37.º O n.º 6 do artigo 35.º dispõe que "A todos é garantido livre acesso às redes informáticas de uso público (…)", o artigo 37.º estabelece na sua epígrafe a liberdade de expressão e informação, e concretiza na sua redacção que todos têm o direito de exprimir e divulgar livremente o seu pensamento, por qualquer meio, sem impedimentos nem discriminações. Sabendo nós que, como regra, as normas legais não podem prevalecer sobre os princípios fundamentais do Estado de Direito democrático protegidos pela Constituição, facilmente entendemos a dicotomia segurança/liberdade e a necessidade de balancear estes valores quando falamos em governação da Internet.

Já tivemos oportunidade de identificar o papel que determinadas entidades têm em matéria de governação da Internet, destacámos oportunamente a intervenção dos "registries" nacionais a quem cabe a responsabilidade pela gestão do ccTLD de cada país. Assim sendo, cumpre-nos fazer uma breve análise do que em Portugal se tem feito a este propósito.

O registo de nomes de domínio em Portugal

De 1991 a 1996 o registo de nomes de domínio sob .PT baseava-se numa análise meramente técnica. Com a evolução do número de registos, surgem em 1996 as primeiras regras para registo de domínios sob .PT, ainda muito incipientes e adaptadas às necessidades da época, cuja principal preocupação era o combate ao *cybersquating*.

A Resolução do Conselho de Ministros n.º 69/97, de 5 de Maio, veio clarificar, na ordem jurídica portuguesa, os termos e abrangência da responsabilidade e papel da FCCN e remeteu para o ministro da Ciência e da Tecnologia a competência para "dirimir todas as divergências que possam vir a existir entre a FCCN e os requerentes ou beneficiários dos domínios ou subdomínios Internet específicos de Portugal."

É então criado o Conselho Consultivo do DNS de .PT, órgão com funções de consulta composto por entidades de reconhecido mérito na área da Internet, da propriedade intelectual e industrial e das telecomunicações e que são sempre chamadas a propor e dar parecer sobre alterações ao regulamento aplicável. Este órgão acaba por ser o exemplo do modelo hoje entendido como sendo a base de uma "boa" governação da Internet, já que tem uma composição *multistakeholder* onde estão representadas entidades como o INPI – Instituto Nacional da Propriedade Industrial, a Associação Portuguesa para a Defesa do Consumidor – DECO; a ANACOM – Autoridade Nacional de Comunicações, a Direcção Geral do consumidor, a APREGI – Associação de Prestadores de Registos de Domínios e Alojamento, assim como entidades de reconhecido mérito na área da Internet.

Com a consciencialização do impacto da Internet e do valor jurídico e económico dos nomes de domínio nos finais dos anos 90, a FCCN, enquanto Registry de .PT, publica um novo regulamento com o objectivo de facilitar e acomodar os registos sob .PT consoante a actividade e público-alvo dos mesmos, sendo então criados os seguintes classificadores: .org.pt, .publ.pt, .gov.pt, .net.pt, .nome.pt, .int.pt, .edu.pt, .com.pt (este último sem restrições ao registo, flexibilizando assim o acesso ao registo de nomes de domínio, o que veio a verificar-se, tornando-se este classificador a primeira escolha logo abaixo do registo directamente sob .PT).

Em 2003 são de novo revistas as regras de registo de nomes de domínio de .PT, destacando-se então a introdução de um sistema de arbitragem na resolução de litígios no âmbito dos nomes de domínio, a abolição de algumas proibições e a redução do preço de submissão e manutenção de domínios, medidas que favoreceram o aumento do número de registos sob o TLD .PT. Nova alteração em 2006, que acaba por consolidar um conjunto de princípios: a prossecução de uma política que visa evitar o registo especulativo e abusivo de nomes de domínios sob .PT, conforme com as melhores práticas, incluindo as recomendações da Organização Mundial da Propriedade Intelectual (OMPI); a utilização de uma política de resolução extrajudicial de litígios – processo de arbitragem; a possibilidade de registo de nomes de domínios/subdomínios com caracteres especiais do alfabeto português; a correcta configuração e operação do servidor primário da zona DNS PT, e a assunção prioritária da segurança nessa operação com a implementação das extensões DNSSEC. Desde o dia 1 de Julho de 2010, encontra-se em vigor o novo regulamento de registo de domínios de .pt marcado pela maior flexibilização dos subdomínios .com.pt e .org.pt, mais segurança para o .pt, e adopção formal do centro de arbitragem ARBITRARE para a resolução de conflitos nessa área

Notas Finais

A promoção da sociedade digital é uma das bandeiras da Estratégia Europa 2020, lançada no passado mês de Março pela Comissão Europeia (CE). Nesse seguimento, foi publicada pela CE, no passado dia 19 de Maio, a Agenda Digital que, no seu todo, prevê 100 medidas, com um calendário de aplicação que vai até 2015. A Agenda está dividida em sete domínios prioritários que passam pela criação de um mercado único digital, maior interoperabilidade, reforço da confiança na Internet e da sua segurança e o acesso muito mais rápido à Internet para todos os cidadãos.

O papel crescente que a Internet tem na nossa sociedade tem levado a um maior envolvimento dos governos nos diversos aspectos desta rede. Se alguns governos se preocupam sobre o impacto económico e social da rede, do seu uso como instrumento de desenvolvimento e democraticidade, outros procuram controlar a rede para evitar que esta seja usada para fins políticos contrários aos seus interesses. É neste mundo de enorme diversidade que o problema da governação da Internet se move, procurando seguir aborgadens inovadoras e que garantam um crescente uso da rede com segurança, estabilidade e abrangência universal. ■

Lista de Acrónimos

ICANN – Internet Corporation for Assigned Names and Numbers
gTLD – Generic Top-Level Domain
ccTLD – Country Code Top-Level Domain
ITU – International Telecommunications Union
ISOC – Internet Society
IGF – Internet Governance Forum
EuroDIG – European Dialogue on Internet Governance
IPv4 - Internet Protocol Version 4
IPv6 – Internet Protocol Version 6

Este texto está publicado, na integra, na revista *JANUS. NET, e-journal of International Relations, Vol. 1, n.º 1 (Outono 2010)*. Disponível em: http://observare.ual.pt/janus.net/pt_vol1_n1_art6