Internet Society
Portugal Chapter

# Plano de trabalhos para o ano de 2018

## Os Novos (velhos?) Desafios - Cibersegurança e Confiança Online

### As nossas principais preocupações em 2018

Em 2017 o tema "Fake News" emergiu como um testemunho marcante do impacto da Internet nas nossa vidas, com especial realce ao nível político e dos media, como se verificou recentemente com as revelações sobre as relações do Facebook com a empresa Cambridge Analytica.

Quando chegarmos ao fim de 2018 qual será o tema com maior impacto na Internet neste ano? Do ponto de vista da Internet Society, a possibilidade de esse tema ser a "Cibersegurança" é um cenário bastante provável. Todas as facetas com impacto real na "confiabilidade online (online trust)" terão também uma grande importância.

Em 2018, a ISOC, e naturalmente também o Capítulo Português da Internet Society (ISOC-PT), elegeram os problemas ligados à Cibersegurança como o principal eixo da sua atividade. Assumem neste quadro especial realce a emergência da IoT (Internet of Things), a segurança do backbone da Internet, as implicações da cibersegurança na segurança dos Estados, mas também na vida dos cidadãos e nas suas liberdades. Continua também a ter importância o tema recorrente da confiança e abertura da Internet, com impactos aos mais diversos níveis: político, das liberdades dos cidadãos e da economia.

## Internet of Things (IoT) igual a Internet of Insecure Things?

A IoT pode ser caracterizada como uma "poeira" de pequenos objetos (sensores e controladores ou atuadores) globalmente interligados com infraestruturas computacionais, e a produzirem dados e ações, consolidadas através da Cloud. Esta "poeira" está sub repticiamente a invadir as nossas vidas. A indústria automóvel está a investir fortemente nesses dispositivos e na interligação dos carros com os seus centros de dados. A domótica é outro campo de excelência para a aplicação da IoT. É bastante provável que apareçam em breve ofertas em que a partir do seu telemóvel possa controlar remotamente todos os aspectos do funcionamento da sua casa. Só que para tal terá de instalar um *hub* (no seu *router* doméstico?) interligado com o operador de uma aplicação para o seu telemóvel, que operará a partir da *Cloud*. As aplicações de vigilância doméstica e pública são já bem conhecidas. As aplicações industriais e na produção agrícola começam a ser uma realidade também.

Infelizmente a IoT coloca nas nossas casas, nas ruas, e nas infraestruturas críticas de que dependemos, dispositivos computacionais ligados à Internet que, para serem baratos e consumirem pouco, têm software de má qualidade, dificilmente atualizável quando se descobrem *bugs*, e com imensos potenciais "buracos de segurança", dada a necessidade de instalação agilizada (por exemplo: *passwords* conhecidas colocadas na fábrica que os seus utilizadores não vão mudar). Tais dispositivos, são uma benção para a constituição de *botnets* e outras infraestruturas *underground* de ataque, como foi demonstrado por um ataque de negação de serviço em larga escala (DDoS), que teve lugar em outubro de 2016 com base na *botnet* Mirai.

O risco real é a que a IoT, devido às pressões económicas no sentido de baixar os preços, e substituir rapidamente a intervenção humana, seja caracterizada pelo epíteto "*Insecurity by Design*", dado que neste campo a "*Security by Design*" encarece os sistemas e defere o retorno dos investimentos.

Para a ISOC e para a sua iniciativa Online Trust Alliance (OTA - https://otalliance.org), um consórcio de empresas envolvidas em iniciativas de promoção das boas práticas de segurança, os problemas levantados pela IoT têm de ser enfrentados com um conjunto alargado de ferramentas: regulação e certificação formal, educação e boas práticas dos utilizadores e também auto-regulação da própria indústria. A intervenção coordenada neste conjunto de facetas é um enorme desafio e compreende os seguintes objetivos:

- Divulgar o "IoT Trust Framework" da Online Trust Alliance e promover a sua adopção a nível global,
- Incrementar a exigência dos utilizadores de segurança e garantias de privacidade nos dispositivos e aplicações,
- Desencadear iniciativas regulatórias para incrementar a segurança e a privacidade dos dispositivos IoT.

O ISOC PT tentará, na medida das suas possibilidades, desenvolver este programa a nível nacional, estando já a contactar outras instituições com vista a desenvolver uma frente comum de ação.

## Estabilidade e segurança do backbone e dos serviços da Internet

A Internet é uma interconexão de redes. Só a estabilidade e fiabilidade desta interconexão pode garantir a funcionalidade global do sistema. Como várias outras facetas da Internet, os mecanismos e protocolos que sustentam a interligação das redes foram concebidos com fragilidades do ponto de vista de segurança. Mas, como também é comum na Internet, o desejo de colaboração, motivado pelo interesse comum, tem minorado o impacto dessas fragilidades.

Com a importância crucial que a Internet está a ter para as pessoas, a sua vida social, a ecnomia, o comércio mundial e muitas outras facetas da actividade humana, este frágil equilíbrio entre, por uma lado, simplicidade e descentralização, e por outro o incentivo para ataques massivos, pode ser destruído.

A ISOC apoia a iniciativa Mutually Agreed Norms for Routing Security (MANRS - https://www.manrs.org), um conjunto de normas e boas práticas para combater a introdução de rotas falsas, o desvio de tráfego e a introdução de endereços falsos, que constituem a base dos ataques de negação de serviço cujos custos são elevadíssimos.

A boas práticas propostas dizem respeito à adopção de normas de controlo e filtragem dos anúncios de encaminhamento no backbone e esta iniciativa tem a colaboração do RIPE (Réseaux IP Européens - https://www.ripe.net) Network Coordination Centre, que é a organização de coordenação dos operadores Internet na Europa, Médio Oriente e Ásia Central. O RIPE actua também como organização de distribuição de espaço de endereçamento IP nas sua área de actuação e de coordenação técnica entre os operadores.

Para o sucesso desta iniciativa, assume também a maior importância a coordenação entre os diferentes operadores regionais e os PIXs (Public or Private Internet Interchanges), segundo o mote "Pense globalmente, mas actue localmente". Por isso a ISOC PT tentará promover boas práticas a nível nacional, com apoio internacional, para que as normas MANRS sejam adoptadas pelos operadores e PIXs nacionais, sem excepção.

Os operadores de rede e de serviços da Internet têm também especial responsabilidade na adoção de normas modernas (e.g. IPv6) e também de segurança, nos serviços que prestam aos seus utilizadores. Assim, integrada com a ação MANRS deverão igualmente ser promovidas ações para incrementar a adoção de IPv6, assim como todos os protocolos de segurança para suporte de serviços essenciais, de criptografia (HTTPS) e autenticação do correio electrónico: DKIM, SPF, DMARC e IMAPS.

## Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (RGPD ou GRDP no acrónimo inglês), aprovado pela União Europeia (UE), entrará em pleno funcionamento no próximo dia 25 de maio. Segundo um artigo de 2017 do "The Economist", os dados são o petróleo do séc. XXI, que é uma forma simples de pôr em evidência a centralidade que a informação assume na nossa sociedade.

O RGPD constitui o primeiro regulamento abrangente para a regulação da propriedade, proteção e circulação da informação privada das pessoas. Ele vai ter impacto na cibersegurança, na economia digital e nos direitos individuais. O RGPD é também o primeiro regulamento europeu com um claro impacto mundial, na medida em que estende o seu âmbito de aplicação à circulação de informação dos cidadãos da UE fora da UE, sendo quase certo que se advinham batalhas importantes entre a UE e os gigantes da Internet, dos quais nenhum é europeu. Adivinham-se também contra-ofensivas ao nível do impacto do RGPD no comércio internacional.

O RGPD privilegia a privacidade e os direitos e controlo dos cidadãos sobre os seus dados. Ele estabelece regras básicas para o consentimento à memorização, manipulação, destruição e conhecimento pelos próprios da informação que lhes diz respeito. Isso vai contra as práticas instaladas em que a informação sobre os cidadãos é colectada, agregada sem o conhecimento destes, e vendida para promoção da publicidade. Sem o saberem, os cidadãos pagam os serviços que utilizam em troca dos seus dados, colectados por uma indústria cujo modelo de negócio depende de quebrar a privacidade dos utilizadores dos seus serviços "gratuitos".

# Governação da Internet

A Internet evoluiu como uma plataforma aberta e colaborativa, que nasceu com uma forma de governação multi-participada e multifacetada, geralmente designada pelo acrónimo em Inglês: *multistakeholder governance.*

Esta forma de governação, defendida por vários organismos, entre os quais a Internet Society e as Nações Unidas, foi adoptada com maior ou menor sucesso, mesmo para além do período inicial da comercialização e da generalização de acesso que a Internet conheceu até ao final do Séc. XX. No entanto, mais recentemente, com a explosão do acesso à Internet, o surgimento de gigantescas companhias, sobretudo com base nos EUA e na China, que a procuram controlar em seu proveito próprio, a importância da Internet para o comércio mundial, e o seu impacto no dia a dia dos serviços e infraestruturas críticas de que dependem a vida dos cidadãos e a organização dos estados, o ideal da *multistakeholder governance* está a enfraquecer, se é que alguma vez se tornou uma realidade generalizada.

Por um lado formaram-se gigantescos monopólios que procuram defender os seus negócios, influenciando diretamente a opinião pública e a política dos estados. Se não o fazem diretamente, pelo menos permitem que outros o façam com base nos seus serviços.

Também os poderes executivos e legislativos, confrontados com o impacto avassalador dos problemas de ciberterrorismo, a segurança das infraestruturas críticas, o impacto da Internet nos media e na economia, mas sobretudo a emergência de um estado de alerta criado pela possibilidade de a Internet ser usada na guerra e pelas organizações terroristas, optam por privilegiar formas não proporcionais de vigilância massiva, menosprezam a necessidade da defesa dos direitos dos cidadãos e promovem um debate fechado e longe do escrutínio público. Este eco sistema de governação é um campo privilegiado em que esses poderes podem facilmente ceder a lóbis poderosos e bem financiados.

Esse estado de coisas não é compatível com as promessas de contínua inovação ao serviço do bem comum, com que a Internet foi idealizada por muitos dos defensores da ideia da *multistakeholder governance*.

Em Portugal estas facetas estão particularmente agravadas pela crónica falta de participação cívica, a crise da imprensa de investigação e de opinião, e pelo fato de a maioria da legislação mais relevante para a governação da Internet ter origem externa, nomeadamente ao nível dos organismos da UE.

A Internet Society considera que só um debate alargado, com participação activa de toda a sociedade civil e dos poderes públicos, que promova formas de educação, de consciencialização e de regulação efectiva, podem contribuir para que a Internet seja uma plataforma aberta, ao serviço da Inovação, ao serviço dos Cidadãos e ao serviço do Bem Público.

O Capítulo Português da Internet Society procurará promover debates e participar em todas as iniciativas que no espírito e na prática possam contribuir para a concretização da visão: a Internet é de todos e deve estar ao serviço dos cidadãos.

As nossas preocupações imediatas dirigem-se para os seguintes temas: o RGPD e a defesa do direito à privacidade; a introdução de medidas de segurança equilibradas e proporcionais que respeitem os direitos dos cidadãos; a defesa de abertura, equilíbrio, transparência e capacidade de proporcionar inovação na Internet, de forma alinhada com os princípios da Neutralidade da Rede; a defesa da liberdade de expressão e de formas de defesa do direito de copyright que não redundem em censura exercida por entidades privadas; e finalmente o combate a todas as formas de apropriação privada e sem regulação de recursos públicos ligados à Internet.

## Plano de ação para 2018

Estão previstas, ou já foram realizadas, as seguintes ações:

- Apoio à campanha para a manutenção em Portugal da idade mínima de dispensa de autorização parental para o acesso à Internet, nos 13 anos - janeiro de 2018.
- Apoio, durante todo o ano, à campanha para a defesa da neutralidade da rede. Resposta à consulta pública da ANACOM - março / abril de 2018.
- Apoio, durante todo o ano, à campanha para não permitir a privatização da defesa do Direito do Copyright e a introdução de censura de base privada.
- Continuação da chamada de atenção que os recursos públicos da Internet Portuguesa, nomeadamente o monopólio da gestão do domínio .PT, não podem ser privatizados sem regulação, nem supervisão.
- Co-organização de um evento de recepção do RGDP em 25 de maio, data da sua entrada em vigor, em conjunto com a Faculdade de Direito da Universidade de Lisboa, Centro de Investigação Jurídica do Ciber Espaço (CIJIC), ISOC Europa e ISOC Suiça.
- Participação, a convite do Centro Nacional de Ciber Segurança, numa sessão plenária, e organização de uma sessão temática sobre IoT, no evento C-DAYs, que tem lugar em 20 e 21 de junho em Coimbra.
- Atribuição do prémio INForum / ISOC 2018, no valor de 1.000 €, para distinguir o trabalho apresentado ao Simpósio INForum 2018 que melhor defenda os princípios da ISOC.
- Co-organização, em outubro, com o RIPE, e outras entidades ainda a definir, de um evento sobre segurança e boas práticas para as diferentes categorias de operadores de rede e serviços da Internet.
- Participação na organização do IGF Portugal que terá lugar em outubro. Intervenção da ISOC central na sessão de abertura sobre a governação da Internet e organização de uma sessão sobre IoT pela ISOC PT.

- Apoio a todas as iniciativas que surjam para a uma governação aberta da Internet de acordo com os princípios acima expostos, nomeadamente, as relacionados com a Internet e os media, a defesa da liberdade de expressão na Internet, o debate sobre a Internet e a privacidade, a defesa da Net Neutrality, etc.

A Internet Society (ISOC - http://internetsociety.org) é uma associação internacional, sem fins lucrativos, fundada pelos pioneiros da Internet, que é a organização "chapéu de chuva" do IETF - Internet Engineering Task Force, o organismo mais relevante no estabelecimento de normas abertas para o funcionamento da Internet. Para além desta faceta, a ISOC intervém a nível social, político e cívico com o propósito de manter a Internet como uma infraestrutura aberta, universal e ao serviço do conjunto da Humanidade sem excepções de raças, credos ou países. A ISOC tem capítulos nacionais, entre as quais o Capítulo Português da ISOC (ISOC-PT - http://isoc.pt) que desenvolve actividades com os mesmos objectivos a nível nacional.