



# Iniciativa Portuguesa do Fórum da Governação da Internet 2018

## Mensagens de Aveiro Messages from Aveiro

17 de outubro de 2018  
17 October 2018

**FCT** Fundação  
para a Ciência  
e a Tecnologia

**ANACOM** AUTORIDADE  
NACIONAL  
DE COMUNICAÇÕES

**apdsj** Associação para a  
Promoção e Desenvolvimento  
da Sociedade da Informação

**ASSOCIAÇÃO  
PORTUGUESA  
DE IMPRENSA**

**.pt**

**CIÊNCIA VIVA**  
Agência Nacional para a Cultura  
Científica e Tecnológica

**CNCS** Centro Nacional  
de Ciência e Tecnologia  
Portugal

**IAPMEI**

**Internet Society  
Portugal Chapter**

**tice.pt**  
Associação Portuguesa de  
Tecnologia da Comunicação e da Internet

**PRÉSIDÊNCIA DO CONSELHO DE MINISTROS**  
Portugal

**universidade  
de aveiro**

# Que tipo de Internet queremos? Governação e políticas públicas da Internet nos contextos nacional e global

A discussão sobre o modelo *multistakeholder* é complexa mas aberta e inclusiva. A responsabilidade e o papel de cada grupo de *stakeholders* é reconhecido, permitindo uma ampla participação da sociedade civil e diferentes perspectivas. Não obstante o modelo *multistakeholder*, a maior parte das decisões continuam a ser tomadas de forma unilateral na esfera dos setores privado e público.

Por outro lado, existem assimetrias mundiais entre os setores privado e público, quer a nível da informação, quer de recursos, o que fragiliza o modelo e aumenta as assimetrias que determinam o nível da capacidade de influência por parte dos vários *stakeholders*.

As vantagens do modelo *multistakeholder* só serão efetivas com a participação de todos os *stakeholders* no processo sendo que, atualmente, denota-se uma participação dos setores privado e público aquém das expectativas.

O modelo *multistakeholder* deve ser considerado não só como uma plataforma de discussão mas também como uma plataforma onde são tomadas decisões.

A Internet não é mesma para todos os utilizadores devido à fragmentação global, regional e nacional, bem como à concentração do poder económico num conjunto de plataformas da Internet que controlam a informação, acesso ao conteúdo, a limitações à neutralidade da Internet e políticas digitais nacionais.

O envolvimento dos jovens na discussão relativa a Governação da Internet é fundamental dado que são nativos digitais, agentes de inovação e “estarão” no futuro da Internet.

O controlo governamental das políticas de comunicação sempre existiu mas as questões de pluralismo e diversidade também sempre estiveram presentes e acompanharam a evolução tecnológica.

A resposta à pergunta “que tipo de internet queremos?” passa necessariamente pela definição de valores, ética, equidade e regulação.

## Inteligência artificial e Big Data

Cidadãos e objetos estão cada vez mais conectados e interligados através de uma realidade automatizada e robotizada. Os mecanismos de inteligência artificial foram, definitivamente, acrescentados aos computadores, e o impacto que daí resultou tem tanto de positivo como de perigoso. A tecnologia ainda não está suficientemente madura mas já a pusemos no terreno.

É necessário esclarecer, do ponto de vista judicial, quem é o responsável do que resulta dessa junção *machine learning/big data*, a par de fomentar o pensamento crítico, a colaboração, o “aprender a aprender” e a inteligência emocional. Esta parece ser a melhor atitude para encontrar o desejado equilíbrio entre Homem e máquina.

Por um lado, há quem considera que a acelerada evolução tecnológica irá impactar a nossa forma de decidir e, por outro, os que acreditam que o Ser Humano jamais será substituído pelos computadores, porque tem intencionalidade que deriva da consciência e da metacognição.

## Segurança no Ciberespaço: O dilema entre a privacidade do indivíduo e a segurança do Estado

Só organizando o papel de cada um no ciberespaço é possível assegurar níveis elevados e sustentáveis de segurança, e criar confiança para a sua expansão e utilização em novos serviços.

Perante os riscos colocados pela Internet, a sociedade deve refletir sobre como quer atuar para os mitigar. Essa reflexão deve passar pela opção de transformar a Internet em algo mais robusto tecnicamente, ou se, alternativamente, prefere “securizar” por pressão regulatória e pública.

A educação, competências e sensibilização da sociedade devem ser apostas sérias que permitam criar pensamento e promover o debate e uma cidadania mais ativa. Revela-se importante uma regulação independente, transparente e idónea, colocando-se assim o desafio de fixar regras que balancem o indivíduo e coletivo de forma transparente, envolvendo os cidadãos em processos de consulta pública.

# Governança, Confiança, Privacidade e Desafios na Era da IoT

Crescimento exponencial de “coisas” na rede, um mercado em franco crescimento, ainda deficientemente regulado e pouco consciente dos problemas de confiabilidade, segurança e privacidade - critérios-chave para uma IoT de base sustentável e com equilíbrio de visões e interesses entre todos os intervenientes.

A fronteira a ultrapassar tem, necessariamente, de ser a interoperabilidade, para que a infraestrutura comunicacional seja mais eficiente e beneficie das melhores práticas de interoperabilidade e/ou *standards* de segurança de dados e comunicações, aos diversos níveis de intervenção da IoT: desde as tecnologias na periferia (*things / edge-IoT communication environments*) à sua convergência e integração em plataformas de serviços e soluções na Internet.

Necessidade de articulação e promoção sinérgica de quadros de colaboração e de responsabilidades *multistakeholder* que salvaguardem a expansão de uma IoT sustentável, antecipando a adopção progressiva em sectores críticos, cada vez mais exigentes do ponto de vista da confiabilidade, segurança e privacidade de dados e operações.

O IPv6 (bem como suas repercussões nas áreas de IPSec e tecnologias relacionadas - ex., EDGE ou 6LowPan, bem como a normalização do encapsulamento de diferentes protocolos IoT *data-link* e encaminhamento IP) é vital para o desenvolvimento da IoT, podendo suavizar as dificuldades de interoperabilidade de protocolos de comunicação ao comportar mecanismos mais flexíveis na questão do endereçamento e encaminhamento seguros.

Será interessante seguir com atenção os esforços de normalização aberta no quadro dos standards de interoperabilidade e segurança IETF, em relação às iniciativas desenvolvidas para a IoT no quadro de protocolos do nível rede, nível sessão e nível de suporte aplicação.

O *digital twin* e a digitalização da sociedade comportam riscos mas também um leque abrangente de possibilidades, para os quais será necessário antecipar reflexões e avaliações de impacto nos requisitos de sustentabilidade, segurança e privacidade.

## Fake news, fake views Sociedade da (Des)Informação

As *fake news* são um tema complexo, apresentando simultaneamente desafios novos e continuidade face a outros fenómenos de desinformação já conhecidos. O seu combate deve assentar no fomento de uma educação crítica para os media.

Apesar de serem maioritariamente digitais e online, as *fake news* não podem ser combatidas somente pelo desenvolvimento de mais *softwares* e *hardwares*. As tecnologias devem ser vistas como ferramentas a usar num quadro mais alargado e complexo para desenvolvimento de práticas mediáticas mais ricas e críticas.

## E amanhã? À conversa sobre...Blockchain

As *distributed ledger technologies* e em particular, a *Blockchain*, representam ainda incógnita conceptual e até operacional para muitos setores da sociedade, com exceção de uma parte da academia e da comunidade técnica, em especial sobre as suas potencialidades e desafios nesta era do Digital.

A sua faceta mais conhecida são as criptomoedas mas existe um reconhecimento do potencial da tecnologia para outro tipo de transações, contratos sendo reconhecido que muitas questões jurídicas se irão colocar. As discussões neste campo salientam nestas tecnologias as suas principais características como vantagens: segurança, transparência e caráter democrático.

É reconhecidamente um tema que merece e necessita de uma discussão mais aprofundada e dum maior envolvimento dos vários *stakeholders* com vista ao seu reconhecimento, desenvolvimento e implementação

Esta será uma discussão a desenvolver na Iniciativa Portuguesa do Fórum da Governação da Internet 2019.

# What kind of Internet do we want? Internet Governance and public policies at national and global levels

The discussion on the multistakeholder model is complex, yet open and inclusive. The responsibility and role of each stakeholder group is recognized, allowing broad participation of civil society and different perspectives.

Despite the multistakeholder model, the majority of the decisions continue to be taken unilaterally in the private and public sectors. There are global asymmetries between the private and public sectors at information and resource level that weaken the model and increase the asymmetries that determine the level of influence of the various stakeholders.

The advantages of the multistakeholder model will only be effective with the participation of all the stakeholders in the process. Currently there is a participation of the private and public sector that falls short of expectations.

The multistakeholder model should be considered not only as a discussion platform but also as a platform where decisions are made.

The Internet is not the same for all users due to global, regional and national fragmentation and concentration of economic power on a set of Internet platforms that control information, access to content, limitations on Internet neutrality and national digital policies.

The involvement of young people in the discussion on Internet Governance is crucial as they are digital natives, agents of innovation and will be part in the future of the Internet.



Government control of communication policies has always existed but issues of pluralism and diversity have also always been present and followed technological development.

The answer to the question "what kind of internet do we want?" necessarily involves the definition of values, ethics, equity and regulation.

## Artificial Intelligence and Big Data

Citizens and objects are increasingly connected and interconnected through an automated and robotized reality. Artificial intelligence mechanisms have definitely been added to computers, and the resulting impact is both positive and dangerous. The technology is not yet mature enough but we've already put it on the ground.

It is necessary to clarify, from the legal point of view, who is responsible for the combination machine learning/ big data, besides fostering critical thinking, collaboration, "learning to learn" and emotional intelligence. This seems to be the better approach to achieve the desired balance between Man and machine.

While some argue that the fast technological development will impact our decisions, others believe that the Human Being will never be replaced by computers since he has intentionality that derives from consciousness and metacognition.

## Security on the Cyberspace: Dilemma between the privacy of the individual and State security

Only by organizing each one's role in cyberspace can it be possible to ensure high and sustainable levels of security, and to build confidence in its expansion and use for new services.

Faced with the risks posed by the Internet, society must reflect on how to act to mitigate them. This reflection should be made with the option of transforming the Internet into something more technically robust, or if, alternatively, it prefers to "secure" by regulatory and public pressure.

Education, skills and awareness of the society should be a serious commitment to create thinking and promote a debate and a more active citizenship. An independent, transparent and appropriate regulation is important, putting the challenge of establishing rules that balance the individual and collective in a transparent way, involving citizens in public consultation processes.

## Governance, trust, privacy and challenges in the IoT age

There is an exponential growth on the number of interconnected things in the Internet, a market in accelerated development and where most regulatory principles are still ill defined. In particular, most IoT users are still not aware of reliability, security and privacy issues, which are key components of a sustainable IOT landscape, where a reasonable balance between different visions, usefulness and goals of all participants and stakeholders is a main requirement.

One of the main problems that IoT needs to address is interoperability, in order to benefit from a more efficient communication infrastructure. This will also enable IoT to benefit from the best practices concerning interoperability, communications and security standards at the several IoT operation layers: from peripheric technologies (things / edge-IoT communication environments) to convergence and its integration in platforms of services and solutions available in the Internet.

It is mandatory to articulate and promote the cooperation and synergies in a multi-stakeholder framework, which may contribute to the expansion of a sustainable IoT. This will enable IoT adoption in critical services where reliability, security and privacy are increasingly demanding mandatory requirements.

IPv6, with its enlarged address space and native security support through IPsec, as well as related technologies (such as EDGE and 6LowPan), and its capability of encapsulating different protocols layers, namely data-link and network layers, is crucial for the development of IoT. IPv6 may also contribute to smooth out difficulties on the interoperability of different communication protocols, since it supports more flexible addressing and routing solutions.

It is crucial to follow the standardization efforts developed in the scope of IETF with impact on the interoperability and security of IoT, namely the initiatives developed by IETF for IoT with impact on network, session and application protocol layers.

The digital twin and the extension of digitalization to many society activities and areas enabled by the explosion of IoT devices encompass privacy and security risks. However, it will also open a vast number of possibilities, for which it will be required to anticipate and discuss societal impacts, namely on the sustainability, security and privacy fronts.

## Fake news, fake views (Dis)Information Society

Fake news is a complex subject, one that simultaneously presents new challenges and continuities from other and already known misinformation phenomena. They should be fought by fostering a critical media education.

Despite being mostly digital and online, fake news cannot be fought simply by developing more software and hardware. Technologies should be regarded as tools to be used within a broader and more complex context for the development of richer and more critical media practices.

## And tomorrow? A talk on... Blockchain.

Distributed ledger technologies, and in particular Blockchain, still represent a conceptual and even operational uncertainty for many sectors of society, with the exception of a part of academia and the technical community, especially about their capabilities and challenges in this Digital era.

Its most well-known facet is the crypto-currency but there is a recognition of the potential of ledger technologies for other types of transactions, contracts. Besides, it is also acknowledged that many legal questions will arise. The discussions in this field emphasize the main characteristics of these technologies as advantages: security, transparency and democratic character.

It is recognized as a topic that deserves and needs more in-depth discussion and greater involvement of the various stakeholders bearing in mind its recognition, development and implementation.

This will be a discussion to put forward in the Portuguese Initiative of the Internet Governance Forum in 2019.

The image features a solid blue background with several white, curved lines that intersect and overlap, creating a sense of movement and depth. The lines are of varying thickness and curvature, some appearing as simple arcs while others form more complex, interconnected shapes. The overall composition is abstract and modern.

[www.governacaointernet.pt](http://www.governacaointernet.pt)