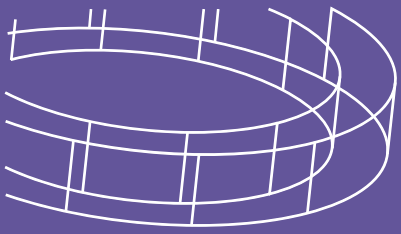


Iniciativa Portuguesa do Fórum da Governação da Internet 2018

FCT Fundação para a Ciência e a Tecnologia

ANACOM Autoridade Nacional de Comunicações

apdsi associação para a promoção e desenvolvimento da sociedade da informação

Associação Portuguesa de Imprensa

.pt

CNCS Centro Nacional de Cibersegurança Portugal

IAPMEI

Internet Society Portugal Chapter

Desde 1902 Instituto de Higiene e Medicina Tropical Universidade Nova de Lisboa

Presidência do Conselho de Ministros Secretaria-Geral

tice.pt Pólo de Competitividade das Tecnologias de Informação, Comunicação e Electrónica

universidade de aveiro theoria poiesis praxis

INICIATIVA PORTUGUESA SOBRE A
Governação da Internet

AVEIRO, 17 DE OUTUBRO DE 2018
AVEIRO, 17 OCTOBER 2018

ÍNDICE / *INDEX*

Mensagens de Aveiro

Messages from Aveiro

Mensagens 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 a inclusão de diferentes perspetivas. Não obstante o modelo *multistakeholder*, a maior parte das decisões continuam a ser tomadas de forma unilateral na esfera das comunidades técnica, privada e pública.

Por outro lado, existem assimetrias mundiais quer a nível de acesso à informação, quer de recursos, que fragilizam o modelo e aumentam as disparidades no 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 se está atualmente a assistir a uma redução da participação dos setores público e privado.

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, bem como à concentração do poder económico num conjunto de plataformas da Internet que controlam a informação e o acesso ao conteúdo, e à não neutralidade da Internet. Esta situação tem permitido políticas públicas nacionais que acabam por não cumprir todo o potencial estratégico e mais-valia inerentes à sua função junto da sociedade no âmbito da atual transformação digital.

O controlo governamental das políticas de comunicação foi sempre uma questão, mas o pluralismo e a diversidade também sempre estiveram presentes e acompanharam a evolução tecnológica.

O envolvimento dos jovens na discussão relativa a Governação da Internet é fundamental, pois serão os principais atores da governação da Internet num futuro próximo.

A resposta à pergunta "Que tipo de Internet queremos?" passa necessariamente por definir, em conjunto, com base num modelo *multistakeholder*, valores, princípios de 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 foi colocada no terreno.

É necessário esclarecer, do ponto de vista jurídico, 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

As dificuldades de controlo da segurança do ciberespaço vão originar episódios crescentes de acessos ilegais a volumes massivos de dados, o que vai criar uma maior consciência por parte das populações da proximidade da ameaça e do impacto nas suas vidas.

Por isso é importante que as instituições apostem seriamente na educação e na capacitação para uma melhor utilização da Internet.

Os atores devem articular-se, potenciando o conhecimento da academia, na construção de um edifício regulatório e de suporte à governação da Internet em Portugal.

A sofisticação crescente do crime (e do terrorismo) e a fragilidade dos utilizadores deve ser contrabalançada por uma atuação mais ativa da lei na Internet, bem como de regulamentação mais robusta.

Para suportar este processo é importante uma regulação independente, transparente e idónea, que fixe regras que balancem o indivíduo e o coletivo de forma equilibrada, envolvendo os cidadãos em processos de consulta pública.

GOVERNAÇÃO, CONFIANÇA, PRIVACIDADE E DESAFIOS NA ERA DA *INTERNET OF THINGS* (IoT)

Existe um crescimento exponencial de *"coisas"* na rede, um mercado em franco crescimento, ainda deficientemente regulado e pouco consciente dos problemas de confiabilidade, segurança e privacidade. Além do mais, a fronteira crítica 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 – *Internet of Things*.

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

O *digital twin* e a digitalização da sociedade comportam riscos mas também um leque abrangente de possibilidades. Neste conspecto, será crucial 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 tec-

nologias 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 a 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 e/ou contratos, sendo reconhecido que muitas questões jurídicas se irão colocar. As discussões neste campo salientam nestas tecnologias as suas principais caraterísticas 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.

Messages from Aveiro

WHAT KIND OF INTERNET DO WE WANT? GOVERNANCE AND INTERNET PUBLIC POLICIES AT THE NATIONAL AND GLOBAL LEVELS

The discussion about the multistakeholder model is complex, but open and inclusive. The responsibility and role of each stakeholder group is known, allowing civil society to participate and the representation of different perspectives. But despite the multistakeholder model, most decisions within the technical, private and public communities are still made unilaterally.

On the other side, the global asymmetries both at the levels of information and resource access weaken this model and raise divides on the influence capacity of the several stakeholders.

The advantages of the multistakeholder model will only be effective with the participation of all stakeholders involved in this process. But this participation is currently decreasing in the public and private sectors.

This model should be considered not only as a discussion platform, but also as a decision-making platform.

The Internet is perceived in different ways by users due to its global fragmentation and granularity at geo-political level, besides Internet non neutrality and the concentration of economic power in a group of platforms that control information and content access. This situation has allowed the non-compliance of national public policies with strategic potential and added-value that are inherent to their role in society, within the current digital transformation.

The Government control of communication policies has always been an issue. However, pluralism and diversity have always been there, accompanying technological evolution.

Engaging young people in this discussion about Internet Governance is essential, as they will be the main Internet Governance players in the near future.

The answer to the question "What kind of Internet do we want?" will necessarily involve the definition, in a collaborative way, of values, ethic, equity and regulation principles, based on a multistakeholder model.

ARTIFICIAL INTELLIGENCE AND BIG DATA

Citizens and objects are more and more connected and linked by an automated and robotic reality. Artificial intelligence mechanisms have definitely been added to computers, generating both a positive and dangerous impact. This technology is not ripe yet, but we have already put it in place.

Clarifying who is responsible for this machine learning/big data pairing from a legal point of view is essential. In addition, critical thinking, collaboration, "learning to learn" and emotional intelligence must be fostered. This seems to be the best approach to find the so much wanted balance between Man and Machine.

Some people think this accelerated technological evolution will impact our way of making decisions. Others believe human beings will never be replaced by computers because human intentionality derives from consciousness and metacognition.

SECURITY ON THE CYBERSPACE: DILEMMA BETWEEN THE PRIVACY OF THE INDIVIDUAL AND STATE SECURITY

Difficulties in controlling security on the cyberspace will result in an increasing of illegal access to massive data volumes. These events will rise the perception of the population of the close proximity of the threat and its impact on their lives.

This is why institutions should focus deeply on education and empowerment towards a better use of the Internet.

The different stakeholders have to collaborate and enhance academic knowledge to create a regulatory framework that supports Internet governance in Portugal.

The increasing sophistication of crime (and terrorism) together with users' fragility must be balanced with a better regulation on the Internet.

To this end, independent, transparent and appropriate regulation to balance both the individual and collective sides, are important, together with more engagement of the citizens through public consultation processes.

GOVERNANCE, TRUST, PRIVACY AND CHALLENGES IN THE ERA OF THE INTERNET OF THINGS (IoT)

There is an exponential growth on the number of interconnected things in the network. This rapidly increasing market is still poorly regulated and hardly aware of trust, security and privacy. Interoperability is crucial, as it will allow a more efficient communication infrastructure, which will benefit from the best practices as well as data security and communication standards at the several layers of the IoT – Internet of Things.

There is a need to promote collaboration and accountability frameworks to expand a sustainable IoT, by anticipating its gradual adoption in critical sectors that are increasingly demanding from the reliability, security, data privacy and operations standpoints.

The digital twin and society digitalization bring risks, but also a wide range of opportunities. In this scope, anticipating reflections and impact assessments in terms of sustainability, security and privacy will be vital.

FAKE NEWS, FAKE VIEWS – (DIS)INFORMATION SOCIETY

Fake news are a complex subject that brings not only new challenges but the continuation of other well known disinformation phenomena. Fake news should be fought by fostering critical media education.

Despite being mostly digital and online, fake news cannot be fought simply by developing more software and hardware. Technologies should be seen as tools to be used in a broader and more complex context in order to develop richer and more critic media practices.

WHAT ABOUT TOMORROW? TALKING ABOUT... BLOCKCHAIN

Distributed ledger technologies, and in particular Blockchain, still represent a conceptual and often operational unknown to many society sectors - except for a part of the academia and technical community - especially when it comes to their potential and challenges in this Digital Era.

"Cryptocurrencies" are the most well-known aspect of this technology. However, distributed ledger technologies´s potential for other types of transactions and/or contracts

were well underlined, bearing in mind that they will raise many legal questions. Discussions in this field highlighted the main features of such technologies as their main advantages: security, transparency and democracy.

It was well recognized that this subject deserves and needs in-depth discussion and higher degree of involvement of different stakeholders aiming at its acceptance, development and implementation.

This discussion will take place at the Portuguese Initiative of the Internet Governance Forum in 2019.

Contextualização

A Iniciativa Portuguesa do Fórum da Governação da Internet (PT – IGF) é uma plataforma nacional de diálogo que reúne todas as Partes Interessadas/*Stakeholders*, os setores público e privado, a academia, a comunidade técnica da Internet, os utilizadores e a sociedade civil em geral para informar, refletir e debater de forma aberta e interativa, questões políticas públicas sobre a utilização e a evolução da Internet.

A Governação da Internet começou a ser discutida, a nível global, com a criação do Fórum de Governação da Internet (IGF – *Internet Governance Forum*) em 2005, no âmbito da Cimeira Mundial sobre a Sociedade da Informação (WSIS – *World Summit on Information Society*) da Organização das Nações Unidas. O seu grande objetivo era o envolvimento de todos os *stakeholders*, nas suas respetivas funções e responsabilidades na discussão sobre a gestão da Internet, um recurso que se tornou global.

Neste contexto, surgiu um movimento a nível mundial que conduziu à organização, de forma voluntária, em várias partes do mundo, de Iniciativas Nacionais e Regionais (NRI – *National and Regional Initiatives*) do IGF. Este movimento levou a que fosse organizado, em 2010, pela primeira vez em Portugal, sob a alçada do Fórum para a Sociedade da Informação (previsto no Programa "Ligar Portugal", lançado em 2005), a "Iniciativa Portuguesa do Fórum da Governação da Internet" (PT – IGF).

A 1.ª edição da Iniciativa Portuguesa, baseada no modelo multissetorial (*multistakeholder*) realizou-se em 2010 (Lisboa, 8 de julho). Seguiram-se outras edições em 2012 (Lisboa, 10 de julho), em 2013 (aquando da realização do EuroDIG[1] em Lisboa), em 2014 (Lisboa, 4 de junho), em 2015 (Porto, 10 de setembro), em 2016 (Lisboa, 21 e 28 de outubro, 15, 16 e 23 de novembro) e em 2017 (Lisboa, 29 de setembro).

Todas as Iniciativas Nacionais e Regionais aderem aos princípios do IGF, espelhados nos artigos 72.º e 73.º da Agenda de Tunes[2] adotada na WSIS de 2005.

A edição 2018 realizou-se em Aveiro, a 17 de outubro, com o mote "A Internet um jogo de sombras?". O evento foi organizado pela FCT (Fundação para a Ciência e a

---

1 *Iniciativa Regional Europeia de Governação da Internet: https://www.eurodig.org/index.php?id=1*
2 *https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html*

Tecnologia I.P), em parceria com a ANACOM (Autoridade Nacional de Comunicações), APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da Informação), API (Associação Portuguesa de Imprensa), Associação DNS.PT, Ciência Viva (Agência Nacional para a Cultura Científica e Tecnológica), CNCS (Centro Nacional de Cibersegurança), IAPMEI (Agência para a Competitividade e Inovação), IHMT (Instituto de Higiene e Medicina Tropical), ISOC – PT (Capítulo Português da Internet Society), Polo TICE.PT, Secretaria Geral da Presidência do Conselho de Ministros, e Sociedade Civil. Este movimento é a prova que a PT – IGF reúne algumas das Partes Interessadas mais significativas a nível nacional no âmbito da cooperação digital, neste caso para debater a Governação da Internet e o futuro das políticas públicas da Internet.

No seguimento de um convite à participação pública que decorreu entre 23 de março e 12 de abril de 2018 e de várias reuniões com os parceiros do IGF – PT 2018, foram definidos um conjunto de temas a serem discutidos, na perspetiva da Governação da Internet, permitindo assim uma melhor compreensão sobre as respetivas funções e responsabilidades dos vários grupos de *stakeholders*.

Os temas focados foram os seguintes: a Internet das coisas (IoT – *Internet of Things*), os megadados (*Big Data*), a Inteligência Artificial, a *Blockchain*, a Segurança no Ciberespaço e a Desinformação, alguns particularmente relevantes no âmbito das prioridades definidas pelo Governo através do programa INCoDe.2030 - Iniciativa Nacional em Competências Digitais e.2030.

A reflexão nacional *multistakeholder* e as principais mensagens de Portugal, que resultaram desta edição, contribuíram para a discussão que decorreu a nível mundial, no âmbito das NRI, na 13.ª edição do IGF, em Paris, de 12 a 14 de novembro 2018, sob o tema "*The Internet of Trust*", em particular na Sessão Plenária "*Evolution of Internet Governance, focus on the multistakeholder approach*".

A Governação da Internet é um processo de diálogo contínuo tendo, neste momento, atingindo um maior nível da maturidade, que tem levado atualmente a uma discussão sobre o futuro do IGF.

Context

The Portuguese Initiative of the Internet Governance Forum (PT – IGF) is a national dialogue platform that gathers all Interested Parties/Stakeholders, public and private sectors, academia, technical Internet community, users and civil society. This platform aims at informing, reflecting and debating political issues in an open and interactive way on the use and evolution of the Internet.

Global debates about Internet Governance began in 2005 with the creation of the Internet Governance Forum (IGF) in the scope of the World Summit on Information Society (WSIS) of the United Nations (UN). The IGF major objective was to engage all stakeholders, in their respective roles and responsibilities, in a discussion on Internet management, a resource that became global.

In this scope, a global movement led to the voluntary organization of National and Regional Initiatives (NRI) of the IGF all over the world. This movement, led Portugal to host in 2010, for the first time under the Information Society Forum (established by the "Ligar Portugal" Programme, launched in 2005) the "Portuguese Initiative for the Internet Governance Forum" (PT – IGF).

The 1st edition of the Portuguese Initiative was based on the multistakeholder model and took place in 2010 (Lisbon, 8 July). More editions took place in 2012 (Lisbon, 10 July), 2013 (in the scope of EuroDIG[1] in Lisbon), 2014 (Lisbon, 4 June), 2015 (Oporto, 10 September), 2016 (Lisbon, 21 and 28 October and 15, 16 and 23 November) and 2017 (Lisbon, 29 September).

All National and Regional Initiatives observe the principles of the IGF that are reflected by articles 72 and 73 of the Tunis Agenda[2] adopted during WSIS in 2005.

The 2018 edition took place in Aveiro, 17 October under the overarching theme "Internet: A Game of Shadows?". This edition was hosted by FCT (Fundação para a Ciência e a Tecnologia I.P.) in partnership with ANACOM (Autoridade Nacional de Comunicações), APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da Informação),

---

1 *European IG Initiatives: https://www.eurodig.org/index.php?id=1*
2 *https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html*

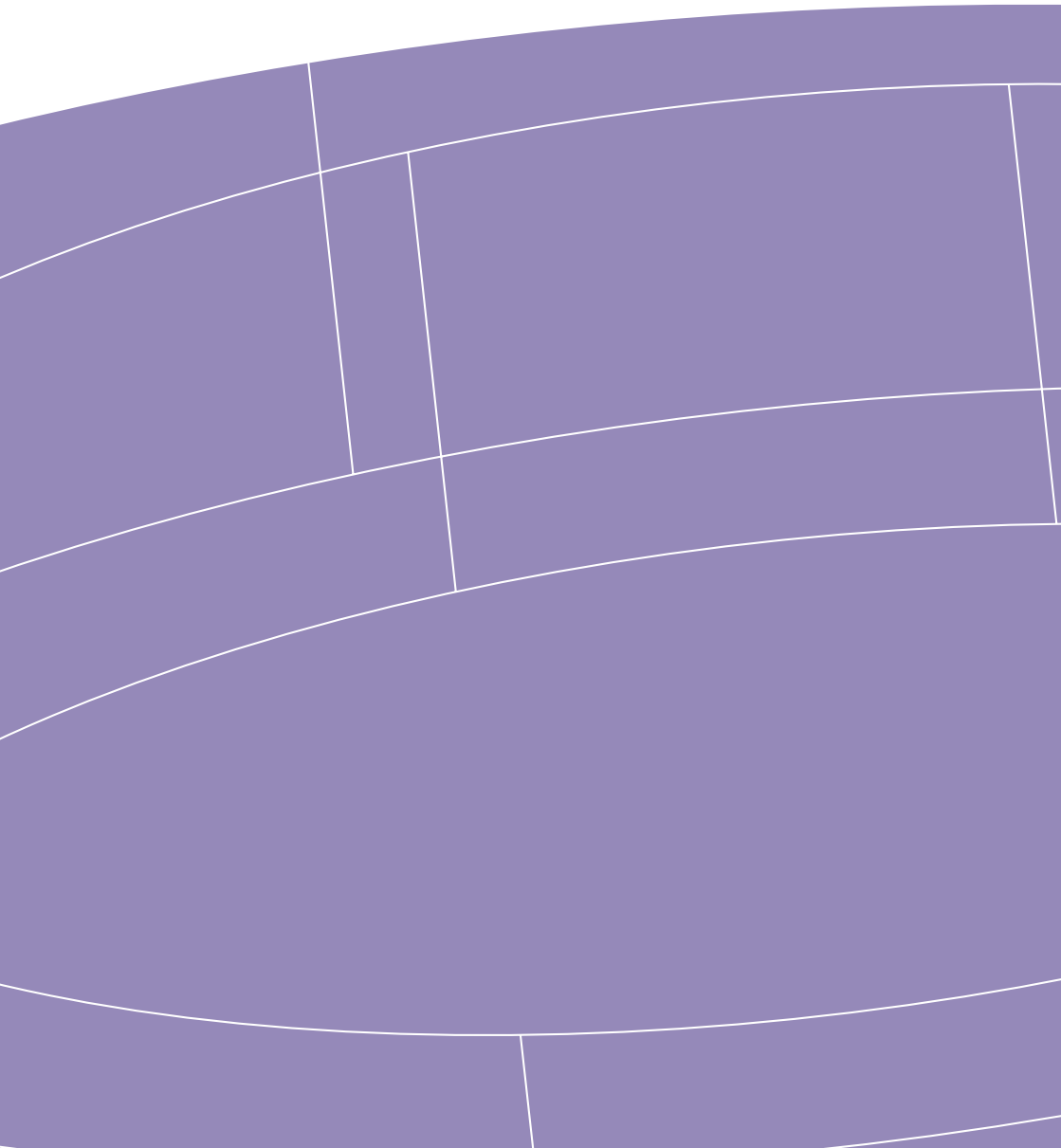
API (Associação Portuguesa de Imprensa), Associação DNS.PT, Ciência Viva (Agência Nacional para a Cultura Científica e Tecnológica), CNCS (Centro Nacional de Cibersegurança), IAPMEI (Agência para a Competitividade e Inovação), IHMT (Instituto de Higiene e Medicina Tropical), ISOC – PT (Portuguese Chapter of Internet Society), TICE.PT, Secretaria Geral da Presidência do Conselho de Ministros and Civil Society. This movement is the evidence that PT – IGF puts together some of the most important players in the context of digital cooperation, in this case to discuss Internet Governance and Internet public policies.

A list of subjects to discuss in the scope of Internet Governance was defined after the call for public participation between March 23rd and April 28th and several meetings with the IGF – PT 2018 partners. This allowed a better understanding about roles and responsibilities of the several groups of stakeholders.

The highlighted themes were the following: IoT – Internet of Things, Big Data, Artificial Intelligence, Blockchain, Cybersecurity, and Disinformation. Some of these were particularly relevant in the scope of priorities defined by the Government in the INCoDE.2030 programme (National Digital Competences Initiative e.2030).

National multistakeholder reflections and key messages arising from this edition contributed to the NRI global discussion that took place during the 13th edition of the IGF that took place in Paris, from 12 to 14 November, under the overarching theme "The Internet of Trust", in particular in the Plenary Session "Evolution of Internet Governance, focus on the multistakeholder approach".

Internet Governance is a continuous dialogue that has now reached its highest level of maturity leading currently to a discussion about the future of the IGF.



Relatos das Sessões

Report from the Sessions

BOAS VINDAS */ WELCOME REMARKS*

Paulo Jorge Ferreira, Reitor da Universidade de Aveiro
Ana Sánchez, Vogal do Conselho Diretivo da FCT – Fundação para a Ciência e a Tecnologia, I.P.

SESSÃO INAUGURAL */ OPENING SESSION*

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

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

KEYNOTE
Ana Cristina Neves, FCT – Fundação para a Ciência e a Tecnologia, I.P.

MODERADOR */ MODERATOR*
Nuno Garcia, Universidade da Beira Interior

ORADORES */ SPEAKERS*
Elsa Costa e Silva, Universidade do Minho
João Romão, GetSocial.io, *World Economic Forum Global Shaper*
Sandra Hoferichter, EuroDIG
Vania Baldi, Universidade de Aveiro
Yuliya Morenets, TaC – *Together Against Cybercrime, Leader of the Youth IGF Movement*

RELATOR */ RAPPORTEUR*
Charlotte Simões, FCT – Fundação para a Ciência e a Tecnologia, I.P.

Existe uma dificuldade geral de perceção do conceito de "Governação da Internet" que tem significados e conotações diferentes em várias línguas e culturas, levando a vários equívocos, nomeadamente como estando relacionado com as autoridades governamentais.

A essência da "Governação da Internet" prende-se com a necessidade de ser discutido, a nível global, o impacto da transformação digital nas nossas vidas. Esta discussão

ocorre em vários fora internacionais, tais como, o Fórum de Governação da Internet (IGF – *Internet Governance Forum*) da Organização das Nações Unidas, *European Dialogue on Internet Governance* (EuroDIG) e nas Iniciativas Nacionais e Regionais (NRI – National and Regional Initiatives) do IGF, que são particularmente importantes para envolver a comunidade local nas discussões na sua própria língua.

O modelo *multistakeholder* em que se baseia a discussão sobre a Governação da Internet é um modelo complexo que envolve vários níveis designadamente: infraestrutura, técnica/académica e a dimensão económica/social.

As vantagens do modelo *multistakeholder* encontram-se no facto de ser um modelo aberto e inclusivo, onde a responsabilidade e o papel de cada grupo de *stakeholders* são reconhecidos, permitindo uma ampla participação da sociedade civil, e no qual se pretende reunir diferentes perspetivas.

No entanto, o funcionamento do modelo *multistakeholder* tem demonstrado algumas limitações. Existem assimetrias no acesso à informação, conhecimento e recursos económicos que determinam o nível de participação, a capacidade de influência e o poder por parte dos vários *stakeholders*. Para além disso, muitas questões continuam a ser reguladas a nível dos Estados, das grandes empresas da Internet e da comunidade técnica.

Assim, as vantagens do modelo *multistakeholder* só se tornam efetivas com a participação de todos os stakeholders no processo de discussão, sendo que, atualmente, denota-se uma participação dos setores público e privado aquém das expetativas. Todos os *stakeholders* devem assumir as suas responsabilidades e envolver-se na discussão sobre a Governação da Internet.

As soluções que resultam das discussões, com base no modelo *multistakeholder*, são mais sustentáveis que qualquer outra solução que envolve só um ou dois grupos de *stakeholders*.

O modelo *multistakeholder*, idealmente, deveria evoluir para uma plataforma não só de discussão mas onde as decisões são tomadas em conjunto de formal consensual.

A Internet não é mesma para todos os utilizadores devido à fragmentação global e polarização a nível geopolítico, bem como à concentração do poder económico num conjunto de plataformas da Internet que controlam a informação e o acesso ao conteúdo, e à não neutralidade da Internet. Esta situação tem permitido políticas públicas nacio-

nais que acabam por não cumprir todo o potencial estratégico e mais-valia inerentes à sua função junto da sociedade no âmbito da atual transformação digital.

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.

O envolvimento dos jovens na discussão relativa à Governação da Internet é fundamental, pois serão os principais atores da Governação da Internet num futuro próximo. A primeira edição do "Youth IGF" português, realizou-se na Universidade da Beira Interior, na Covilhã, no dia 15 de outubro de 2018. As Mensagens que resultaram deste debate propõem soluções para resolver questões e desafios em matéria de privacidade, supervisão e controlo de conteúdos na Internet, desinformação, direitos de autor e IoT.

A resposta à pergunta "Que tipo de Internet queremos?" passa necessariamente por definir, em conjunto, com base num modelo *multistakeholder*, valores, princípios de ética, equidade e regulação.

In general, "Internet Governance" is a concept that is hardly perceived. Its different meanings and connotations in distinct languages and cultures leads to several misconceptions, namely its relation to governmental authorities.

The very essence of "Internet Governance" concerns the need of a global discussion on the impact of digital transformation happening in our lives. This discussion has been going on in several international fora, such as the Internet Governance Forum (IGF) of the United Nations, the European Dialogue on Internet Governance (EuroDIG), and the National and Regional Initiatives (NRI). These are particularly important for the engagement of local communities in discussion in their own languages.

The multistakeholder model, which Internet Governance discussions are based, is a complex model composed of several levels: infrastructure, technical/academic and economic/social dimension.

This model's advantages rely on its openness and inclusiveness. The responsibility and role of each group of stakeholders are recognised, allowing civil society to participate in a large-scale and enabling the representation of different perspectives.

The multistakeholder model has however shown some limitations. There are asymmetries regarding access to information, knowledge and economic resources that determine stakeholders' participation levels, influence capacity and power. In addition, there are many issues still being regulated at the level of States, large Internet companies and technical community.

This way, this model's advantages will only become effective with the participation of all stakeholders involved in the discussion. This participation has however been decreasing for the public and private sectors. Stakeholders must take responsibility and get involved in this discussion about Internet Governance.

Solutions arising from discussions based on this multistakeholder model are more sustainable than any other solution involving just one or two groups of stakeholders.

This model should ideally evolve towards a platform that should include not only a debate but the preparation of consensus-based proposals for decision makers.

The Internet is perceived in different ways by users due to its global fragmentation and granularity at geo-political level, besides Internet non neutrality and the concentration of economic power in a group of platforms that control information and content access. This situation has allowed the non-compliance of national public policies with strategic potential and added-value that are inherent to their role in society, within the current digital transformation.

The Government control of communication policies has always been an issue. However, pluralism and diversity have always been there, accompanying technological evolution.

Engaging young people in this discussion about Internet Governance is essential, because they will be the main Internet governance players in the near future. The first Portuguese edition of the "Youth IGF" took place on 15 October, in University of Beira Interior, Covilhã. The Messages that came up from the debate suggest solutions to address issues and challenges concerning privacy, supervision and control of Internet content, disinformation, copyright and IoT – Internet of Things.

The answer to the question "What kind of Internet do we want?" will necessarily involve the definition, in a collaborative way, of values, ethic, equity and regulation principles, based on a multistakeholder model.

SESSÃO PARALELA / *PARALLEL SESSION*

Inteligência Artificial e *Big Data*

Artificial Intelligence and Big Data

MODERADOR / ***MODERATOR***

Miguel Brito Campos, APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação

KEYNOTE

Ernesto Costa, Universidade de Coimbra

ORADORES / ***SPEAKERS***

António Castro, Masdima
Carlos Paiva, TAP Portugal
José Amaral Gomes, APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação
Nuno Nogueira, Rebis Consulting
Zaida Chora, AMA – Agência para a Modernização Administrativa, I.P.

RELATOR / ***RAPPORTEUR***

Daniela Azevedo, APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação

Para o bem e para o mal, cidadãos e objetos estão cada vez mais conectados e interligados através de uma realidade automatizada e robotizada. Aplicações móveis, plataformas da IoT e *big data*, com maior ou menor influência humana, foram os temas que, neste painel, levaram à discussão sobre os seus impactos nos relacionamentos sociais, bem como as suas implicações legislativas e governativas.

Os mecanismos de inteligência artificial foram, definitivamente, acrescentados aos computadores, e o impacto que daí resultou tem tanto de positivo como de perigoso. Estamos constantemente a descoberto e a informação está sempre a ser produzida.

Foram descritas três formas de Inteligência Artificial: a simbólica (agentes de decisão num computador que seguem o caminho dos humanos), a conexionista (abordagem que apareceu nos anos 80, sendo um modelo assente na maneira como o cérebro funciona e como os neurónios se interligam para resolver problemas complexos) e a evolutiva (uma nova maneira de encarar esta arquitetura com base em ligações neuronais; as soluções são criadas pelo computador com base numa seleção natural – *deep learning*; não há *raw data*).

Houve quem defendesse que perante a acelerada evolução tecnológica os assistentes virtuais estão a tomar conta das nossas decisões mas, por outro lado, a generalidade das opiniões não acredita num futuro em que as máquinas tomem conta de nós.

A utilização inteligente e preditiva dos carros, por exemplo, foi outra preocupação aqui destacada, sobretudo pela necessária evolução para uma tomada de decisão do aparelho em tempo real (o carro tem de processar dados no imediato), ao invés da massificada aprendizagem pela máquina supervisionada, na qual um Ser Humano ensina a um computador como distinguir características básicas, de onde resulta o perigo dos dados por enviesamento.

Para enfrentar estes desafios, foi sublinhada a necessidade de se esclarecer, do ponto de vista jurídico, quem é o responsável que resulta desse juntar de *machine learning* a *big data*. A tecnologia ainda não está suficientemente madura e nós já a pusemos no terreno, concluiu-se.

Fomentar o pensamento crítico, a colaboração, o "aprender a aprender" e a inteligência emocional parece ser a atitude determinante na procura pelo desejado equilíbrio entre Homem e máquina.

Esta procura pelo balanço ainda trouxe ao debate a questão da utilização militar da tecnologia de Inteligência Artificial, algo considerado, unanimemente, muito perigoso e preocupante porque as implicações da utilização militar de sistemas autónomos são enormes e com um efeito devastador. O seu comportamento é fortemente regulado mas o desenvolvimento tecnológico também é muito acelerado, pelo que apostar na capacitação interna em competências digitais parece ser o caminho a seguir quer neste campo, na Administração Pública e até em empresas privadas.

Em suma, foi consensual a crença de que o Ser Humano jamais será substituído pelos computadores porque tem intencionalidade que deriva da consciência e da metacognição. Os assistentes virtuais não resolvem o problema da solidão e a Inteligência Artificial depende da política e da sensibilidade do Homem.

———

For better or for worse, citizens and objects are more and more connected and inter-linked by an automated and robotic reality. Mobile apps, IoT – Internet of Things

platforms and big data, with more or less human intervention, were the themes discussed by this panel, in particular their impacts on social relationships, and legislative and governmental implications.

Artificial intelligence mechanisms were definitively added to computers, generating both a positive and dangerous impact. We are constantly exposed and information is continuously being generated.

Three types of Artificial Intelligence were described: symbolic (decision agents in a computer that follow human tracks), connectionist (approach that appeared in the 80's and relied on the functioning of brain and how neurons connected themselves to solve complex problems), and evolutionary (a new way of facing this architecture based on neural connections; solutions are created by computers based on natural selection - deep learning; there is no raw data).

Some participants stated that, in this rapid technological evolution, virtual assistants are taking over our decisions. However, in general, participants did not believe in a future where machines take over humans.

The intelligent and predictive use of cars was other concerns debated. Mainly due to the required evolution to real-time decision-making (vehicles must process data immediately) as opposed to the massive learning of the supervised machine in which humans teach computers how to differentiate between basic features, resulting in the risk of data bias.

The need to clarify who is responsible for this machine learning and big data pairing, from the legal point of view, was also highlighted as a way to face these challenges. They reached the conclusion that this technology is not ripe yet, but we have already put it in use.

Fostering critical thinking, collaboration, "learning to learn" and emotional intelligence seems to be the decisive attitude when seeking the much-wanted balance between Man and machines.

This search for balance has also brought to debate the use of Artificial Intelligence in military technology. This was unanimously deemed very dangerous and worrisome, because the implications of the use of autonomous systems by the military can be huge and devastating. This use is strongly regulated but technological development moves also very fast. Therefore, focusing on empowerment in digital com-

petences seems to be the way to go, whether in the military, Public Administration or private companies.

In short, there was a consensus between participants that humans will not be replaced by computers, due to our intention that derives from conscience and metacognition. Virtual assistants do not seem to solve the loneliness problem and Artificial Intelligence depends on Man's policies and sensitivity.

SESSÃO PARALELA */ PARALLEL SESSION*

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

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

MODERADOR */ MODERATOR*

Lino Santos, CNCS – Centro Nacional de Cibersegurança

ORADORES */ SPEAKERS*

João Barreto, S21sec
Manuel Pedrosa de Barros, ANACOM – Autoridade Nacional de Comunicações
Pedro Martins, Openlimits
Sérgio Nunes, Instituto Superior de Economia e Gestão, Universidade de Lisboa

RELATOR */ RAPPORTEUR*

Luís Velez Lapão, Instituto de Higiene e Medicina Tropical, Universidade Nova de Lisboa

A cibersegurança é uma nova realidade. Desde Snowden[3], dos ataques de hackers a bancos e do caso da interferência nas últimas eleições dos EUA[4], este tema tomou conta dos media e das preocupações de pessoas e das organizações.

A perceção é que o risco de segurança é cada vez maior e que urge conhecer os métodos de mitigação destes riscos. A cibersegurança pode ser vista como uma gestão do ciber-risco.

---

3 Referência a Edward Snowden que, em 2013, protagonizou um episódio de apropriação e disponibilização pública de informação considerada confidencial relativa a programas de vigilância conduzidos por agências governamentais dos Estados Unidos da América.

4 No decurso da campanha eleitoral para a presidência dos EUA, em 2016, foram identificadas, pelas agências governamentais norte-americanas, ações de propagação de mensagens com vista a influenciar a decisão dos eleitores. Uma matéria que ainda se encontra envolta em polémica e investigação pelas autoridades dos EUA.

Perante os riscos que podem ser potenciados, 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.

Uma boa base de conhecimento ajuda na perceção do risco. A educação, competências e sensibilização da sociedade devem ser apostas sérias para permitir criar pensamento e promover o debate e uma cidadania mais ativa. A dificuldade de consciencializar a linha fina entre liberdade e a segurança deve ser mitigada pela capacitação, sobretudo quando a privacidade está um pouco a desvanecer-se culturalmente.

A sofisticação do crime e do terrorismo e a fragilidade dos utilizadores deve ser contrabalançada por uma atuação mais ativa da lei na Internet, bem como de regulamentação mais sofisticada através de auditorias e mais responsabilização das empresas. Hoje as ameaças podem alargar-se à IoT até aos veículos autónomos.

Deve melhorar-se a capacidade de resiliência das infraestruturas, nomeadamente através da implementação da Lei n.º 46/2018 que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, e potenciando a lei da proteção de dados.

As entidades lidam de forma distinta com a cibersegurança pelo que conflituam. O potencial de conflitos de interesse pode ser mitigado por uma abordagem *multistakeholder* que promova a comunicação e a tomada de decisão com maior consenso.

Só definindo e organizando o papel de cada um no ciberespaço será possível assegurar níveis elevados e sustentáveis de segurança, e criar confiança para a sua expansão e a utilização de novos serviços fundamentais para o desenvolvimento da sociedade e de economia digital.

———

Cybersecurity is a recent reality. From Snowden[3], to hacker attacks to banks, to the interferences in the last US elections[4], this cybersecurity issue has taken over the media and the minds of people and organizations.

People are becoming more and more aware of security risks. This way, it is urgent to know how to mitigate these risks. Cybersecurity can be seen as cyber risk management.

Some risks can be magnified and that is why society must reflect on how to act in order to mitigate such risks. This reflection must help to decide whether opting to transform the Internet into something technically more robust or alternatively "securing" the Internet due to regulatory and public pressure.

A good knowledge base helps understand this risk. Education, competences and raising society's awareness must be taken seriously to create thought and to promote discussion and a more active citizenship. The difficulty in imagining this fine line between freedom and security must be mitigated by training, mostly when privacy is beginning to fade culturally.

The increasing sophistication of crime and terrorism and user fragility must be balance by a more active action of law on the Internet and a more sophisticated regulation, through auditing and greater accountability of companies. Nowadays, threats may spread to IoT – Internet of Things and even autonomous vehicles.

The capacity of infrastructure resilience must be improved, namely by implementing the Law 46/2018 that established the legal regime for cybersecurity (transposing the Directive (EU) 2016/1148, of the European Parliament and of the Council of July 6, 2016), and by strengthening the data protection law.

Entities deal with cybersecurity differently and this generates conflicts. These potential conflicts of interest can be mitigated by a multistakeholder approach that promotes communication and consensus decision-making.

---

3 Reference to Edward Snowden who was involved in an episode of appropriation and disclosure of public information deemed confidential concerning surveillance programmes run by US government agencies in 2013.

4 The US government agencies identified actions designed to propagate messages in order to influence voters, during the US presidential electoral campaign of 2016. A matter that still generates controversy and that is still under investigation by US authorities.

Only by defining and organizing the role of each one in cyberspace we can create high, sustainable security levels and generate trust to expand it, enabling to spread the use of new essential services that are fundamental to the development of digital society and economy.

SESSÃO PARALELA */ PARALLEL SESSION*

Governação, confiança, privacidade e desafios na era da Internet das Coisas (IoT)

Governance, trust, privacy and challenges in the Era of the Internet of Things (IoT)

MODERADOR ***/ MODERATOR***

Augusto Casaca, INESC–ID/IST – Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento, Instituto Superior Técnico

KEYNOTE ***/ MODERATOR***

Henrique João Domingos, ISOC – PT – Capítulo Português da *Internet Society*

ORADORES ***/ SPEAKERS***

Luis Lamela, GoLabs IoT (Altice)
Manuel Ricardo, INESC TEC / Universidade do Porto
Pedro Diogo, Ubiwhere
Susana Sargento, Universidade de Aveiro / Veniam

RELATOR ***/ RAPPORTEUR***

Nuno Teixeira de Castro, ISOC – PT – Capítulo Português da *Internet Society*

Na apresentação de abertura, foi brevemente apresentado o «*IoT trust framework v2.5*», da Internet Society/Online Trust Alliance (ISOC/OTA), tendo sido focados:

- O IoT – *Internet of Things* numa visão integradora, como ecossistema integrando diferentes dispositivos, incluindo sensores, atuadores e processadores, funcionando de forma cada vez mais autónoma e sem supervisão humana;

- As oportunidades, ameaças e desafios decorrentes da explosão em larga escala de soluções IoT e os indissociáveis problemas de segurança, fiabilidade e privacidade;

- A necessidade de refletir sobre a efetividade de quadros regulatórios, quer no plano da qualidade ou certificação de tecnologias, quer no impacto da IoT na gestão de serviços e infraestruturas críticos.

No painel e debate que se seguiram, as principais ideias expressas foram:

- Apesar do crescimento exponencial da IoT, a maioria dos utilizadores não está ainda ciente das suas implicações de segurança e privacidade, estando os princípios regulatórios ainda mal definidos;

- É indispensável promover princípios de interoperabilidade que permitam beneficiar das melhores práticas de comunicação e segurança nas diversas camadas de operação, bem como permitir a sua convergência com as plataformas de serviços já existentes;

- É necessário promover a cooperação e sinergias entre os diversos *stakeholders*, o que contribuirá para a interoperabilidade e adoção da IoT em serviços críticos, onde fiabilidade e segurança são requisitos indispensáveis;

- O protocolo IPv6, com o seu maior espaço de endereçamento, suporte nativo de segurança e flexibilidade de encaminhamento é fundamental para o desenvolvimento da IoT;

- Deverão ser prosseguidos os esforços de normalização definidos no âmbito do *Internet Engineering Task Force* (IETF), nomeadamente os que afectam a interoperabilidade e segurança da IoT;

- O *digital twin* e a extensão da digitalização potenciado pela explosão de dispositivos IoT implicam riscos de privacidade e segurança, mas abrirão igualmente um vasto número de possibilidades, sendo necessário encontrar o desejável balanço entre riscos e benefícios sociais esperados.

———

The «IoT trust framework v2.5» from Internet Society/Online Trust Alliance (ISOC/OTA) was briefly presented in the opening session. The highlighted matters were:

- *An integrated vision of the IoT – Internet of Things as an ecosystem that incorporates different devices, including sensors, actuators and processors and that operates in an increasingly autonomous way without human intervention;*

- *Opportunities, threats and challenges arising from the widespread increase of IoT solutions and inextricable security, reliability and privacy problems;*

- *The need to reflect on the effectiveness of regulatory frameworks, both in relation to technology quality and certification and the impact of the IoT on the management of critical services and infrastructures.*

The panel and the participants in the debate expressed the ideas below:

- *Despite the exponential growth of the IoT, most users are not quite aware of security and private implications, and regulatory principles are still ill-defined;*

- *Interoperability principles must be promoted for the several operation layers to benefit from the best communication and security practices, and to allow their convergence with existing service platforms;*

- *Promoting cooperation and synergies between the several stakeholders is required and will contribute to the interoperability and adoption of the IoT in essential services, where reliability and security are absolute requirements.*

- *Protocol IPv6, with its increased address space, native security support, and forwarding flexibility is crucial for the development of the IoT.*

- *Standardization efforts in the scope of the Internet Engineering Task Force (IEFT) must continue, namely those affecting the interoperability and security of the IoT;*

- *The expansion of digital twin and digitalization strengthened by the widespread increase of IoT devices bring privacy and security risks, but will open doors to a number of opportunities. Nevertheless, it will be necessary to find the balance between expected risks and social benefits.*

SESSÃO PARALELA */ PARALLEL SESSION*

Fake news, fake views – Sociedade da (Des)Informação
Fake news, fake views – (Dis)Information Society

MODERADOR */ MODERATOR*
Sérgio Gomes da Silva, Direção de Serviços de Política Legislativa para os Media, Secretaria-Geral da Presidência de Conselho de Ministros

ORADORES */ SPEAKERS*
Clara Rodrigues, *Future Ballloons*
Francisco Teixeira, *HK Strategies*
Francisco Teixeira da Mota, Teixeira da Mota Advogados
Gustavo Cardoso, Obercom
João Palmeiro, Associação Portuguesa de Imprensa
Manuel Pinto, Universidade do Minho

RELATOR */ RAPPORTEUR*
Pedro Moura, Universidade do Minho

Do debate a que se assistiu na sessão *Fake news, fake views – Sociedade da (Des)Informação* sobressaiu uma conclusão: a natureza intrinsecamente complexa dos conteúdos manipuladores com ares de notícia, facto que dificulta o seu combate. Esta complexidade manifesta-se, desde logo, na sua difícil conceptualização. Apesar de popular, *fake news* é uma expressão ambígua, que remete para ideias dificilmente conciliáveis, encontrando-se a conjugação dos conceitos de "notícia" e de "falsidade" à cabeça. Para além disto, é só parcialmente nova: apesar das diferentes e desafiantes potencialidades associadas à natureza eminentemente digital e *online* das *fake news*, estas decorrem de estratégias de desinformação há muito conhecidas e adotadas por diferentes atores globais. Consequentemente, vocábulos alternativos e familiares – como propaganda ou, sobretudo, desinformação – foram sugeridos como opções viáveis, mas que não eliminam a necessidade de se continuar a trabalhar na conceptualização das *fake news*.

A formação crítica dos públicos foi a ferramenta de combate à desinformação mais comungada pelos intervenientes no debate: educar para os *media*, isto é, desenvolver competências muito para lá do acesso e do domínio técnico dos meios de comunicação, terá de assumir um lugar cimeiro na luta contra as *fake news*. Desde logo pela não existência de soluções garantidamente eficazes e, sobretudo, com efeitos colaterais de somenos ao nível da governação da Internet. Ou seja, as hipóteses avançadas na sessão – como a defesa de um mercado livre de ideias (em oposição à

limitação por algoritmos dos conteúdos), de uma maior regulação das empresas de distribuição e produção de conteúdos online ou da premente colaboração entre os diferentes agentes tecnológicos e mediáticos – não garantem, por si só, o fracasso das *fake news*. Para além de não assegurarem necessariamente eficácia no combate, podem colocar em causa valores fundamentais como a liberdade de expressão e o direito ao anonimato.

———

One conclusion stood out from the debate that took place in the session Fake news, fake views – (Dis)Information Society: the fight against fake news is hard to manage by the intrinsically complex nature of manipulative content disguised as news. This complexity is rapidly demonstrated by its hard conceptualization. Although popular, the term fake news is ambiguous and refers to ideas that are hard to reconcile, because it combines "news" and "falsehood". Also, this term is only partially new: despite the different and challenging potentials associated to digital and online fake news, these are disinformation strategies that are have been long known and adopted by different global players. Consequently, alternative and familiar wordings – like propaganda or, mainly, disinformation – were suggested as viable options that however do not eliminate the need to keep working in the conceptualization of fake news.

The critical training of audiences was the tool that was referred more often during the debate to fight disinformation: educating people to deal with the media, i.e., developing skills that go beyond access and technical aspects of communication means must be prioritized in the fight against fake news. Starting with the fact that no solutions are guaranteed to be effective and, mostly, because there are minor collateral effects at the Internet governance level. That is, the hypotheses presented in this session - such as a free marketplace of ideas (as opposed to the limitations imposed by content algorithms), improved regulation for distribution companies and companies that create online content, or the urgent collaboration between the several technological and media agents - do not represent, on their own, a positive assurance that fake news will fail. In addition to not guaranteeing effectiveness in the fight against fake news, they may also jeopardize fundamental values like freedom of speech and the right to anonymity.

SESSÃO PLENÁRIA */ PLENARY SESSION*

E amanhã? À conversa sobre... Blockchain

What about tomorrow? Talking about ... Blockchain

Helena Correia Mendonça, VdA – Vieira de Almeida
Mário Romão, Instituto Superior de Economia e Gestão, Universidade de Lisboa
Rui Serapicos, Aliança Portuguesa de Blockchain

RELATOR */ RAPPORTEUR*
Pedro Matos, FCT – Fundação para a Ciência e a Tecnologia, I.P.

A conversa sobre a *blockchain* partiu do mote "mas, afinal, como é que ela se governa?". É, no entanto, uma pergunta para a qual não se encontra uma resposta clara. Desde logo pela utilização que se lhe dá: se se trata de uma *blockchain* pública ou privada. Sendo privada, a sua governação é assumida pela entidade proprietária. Sendo pública, ela terá, na linha do que foi debatido, de assentar num princípio básico: o do consenso entre todos os intervenientes – só assim se obterá a validação das transações nas suas múltiplas utilizações, por todos. Mas esta é, também, uma questão que provoca antagonismos dado que há quem considere difícil a obtenção deste nível de consenso em torno de regras. E esta dificuldade pode criar as condições ideais para o surgimento de atores que assumam um papel de domínio nesta matéria, à semelhança do que aconteceu em outras áreas tecnológicas, impondo os seus protocolos e regras e criando potenciais problemas ao nível da interoperabilidade, em função dos tipos de *blockchain* que venham a surgir.

Um outro aspeto em aberto na discussão é o de se se deve adotar ou não um modelo de governação centralizado, à semelhança de outras tecnologias e protocolos. Como exemplo foi referido o modelo da ICANN[5], de tecnologias *ledger* centralizadas. Mas que poderão evoluir na próxima década, para tecnologias de registo descentralizadas.

Acredita-se que a *blockchain* traga um maior grau de segurança na certificação de ações. No entanto, é errado assumir-se que a descentralização destes processos signifique uma ausência de regras ou protocolos, muito pelo contrário. A transparência e a democracia são outros dois aspetos considerados positivos: as transações e o

---

5 A ICANN (Internet Corporation for Assigned Names and Numbers) centraliza a governação dos nomes de endereços de IP (Internet Protocol).

papel de cada interveniente são claros. Os custos energéticos associados são uma outra problemática da *blockchain*, podendo potenciar ainda mais assimetrias entre países: países com acesso a recursos energéticos mais baratos terão mais condições para utilizar a *blockchain* do que países com custos energéticos mais elevados.

Constata-se que há ainda trabalho que deve ser desenvolvido para que as empresas adotem esta tecnologia, nomeadamente ao nível dos modelos de negócio. Contrastado com a incerteza do caminho que a *blockchain* seguirá, se pela via da regulação ou da desregulação em termos jurídicos e de governação, a certeza que o painel transmitiu foi a de que este é um tema que terá que permanecer na agenda política e a ser discutido de forma aberta com todos os *stakeholders*.

The conversation about blockchain started with the question "but after all, how does it govern itself?" But this question has no clear answer and depends on whether we are talking about a public or private blockchain. For private blockchain, governance is the responsibility of their owners. In line with what was discussed, for public blockchain, governance must rely on a basic principle: consensus between all players is the only way to get transactions validated by everybody. This is also a matter that generates conflicts, because some people find this level of consensus around rules hard to get. And this difficulty may as well generate the ideal conditions for players to take power positions like it happened before with other technological areas. This would lead to the imposition of their protocols and rules, creating potential interoperability problems, depending on the type of blockchain that may arise.

Another issue addressed in this discussion was whether a centralized governance model should be adopted, alike for other technologies and protocols. The centralized ledger technology model of ICANN[5] was mentioned as an example, but it may turn into a decentralized ledger technology in the next decade.

It is believed that blockchain may bring a higher degree of security in share certification. However, it is wrong to assume that decentralizing these processes will result in the absence of rules or protocols. Transparency and democracy are two blockchain aspects

---

5 Governance of IP (Internet Protocol) address names is made by the ICANN (Internet Corporation for Assigned Names and Numbers).

deemed positive: transactions and the role of each player are clear. Associated energy costs are another blockchain-related problem, as these may end up boosting differences between countries i.e. countries with access to cheaper energy resources will benefit from more favourable conditions to use blockchain than those countries with access to more expensive energy resources.

It is clear that there is still much work to be done in order to make companies adopt blockchain technologies, namely at the level of business models. Whether blockchain will be regulated or not in legal and governance terms is uncertain, but the panel was confident that this subject will remain in political agendas and continue to be discussed with all stakeholders openly.

SESSÃO DE ENCERRAMENTO / *CLOSING SESSION*

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

Nuno Garcia, Vice-Presidente da Faculdade de Engenharia da Universidade da Beira Interior

Eduardo Anselmo Moreira Fernandes de Castro, Vice-Reitor da Universidade de Aveiro

Ana Cristina Neves, Diretora do Departamento para a Sociedade da Informação da FCT, lançou um repto à audiência para fazer parte da organização dos próximos PT – IGF anuais. Sublinhou que as questões relacionadas com a *blockchain* serão discutidas na edição 2019 do PT – IGF, de forma mais aprofundada.

Nuno Garcia, Vice-Presidente da Faculdade de Engenharia da Universidade da Beira Interior, convidou a audiência a fazer parte da organização do PT-IGF 2019, que se realizará na Covilhã.

Eduardo Anselmo Moreira Fernandes de Castro, Vice-Reitor da Universidade de Aveiro, demonstrou contentamento por a Universidade de Aveiro ter sido anfitriã do PT – IGF 2018, que abordou temas que se integram na filosofia da instituição, na interseção da tecnologia, ética, questões de governação. Salientou a ideia de que a tecnologia é demasiado importante para ficar reduzida à discussão de especialistas em tecnologia e manifestou interesse da Universidade de Aveiro em envolver as áreas sociais no debate sobre as questões tecnológicas, a governação da Internet, o uso da informação e outras questões sociais. Realçou a necessidade das novas tecnologias serem utilizadas pelos cidadãos comuns, evitando uma potencial maior divisão na sociedade.

———

Ana Cristina Neves, the Director of the Department for the Information Society at FCT, I.P. challenged the audience to take part in the organization of the next annual PT – IGF. Moreover, she highlighted that blockchain related matters will be deepened in the 2019 edition of the PT – IGF.

Nuno Garcia, the Vice-President of the Faculty of Engineering of University of Beira Interior invited the audience to take part in the organization of the PT-IGF 2019 which will take place in Covilhã.

Eduardo Anselmo Moreira Fernandes de Castro, Vice-Rector of University of Aveiro, was pleased that the University of Aveiro was chosen to be the host the PT-IGF 2018, addressing subjects that combine technology, ethics and governance that are aligned with its university's philosophy. He highlighted that technology is too important to be limited among technology experts discussions and expressed University of Aveiro interest in engaging in social debates about technology, Internet governance, information use and other social matters. He also emphasized the need of new technologies being used by common citizens, thereby preventing a potential major of division of society.

INICIATIVA PORTUGUESA SOBRE A
Governação da Internet 2018

Esta publicação pode ser descarregada no website da FCT,
em www.fct.pt.

www.governacaointernet.pt