

Iniciativa Portuguesa do Fórum da Governação da Internet 2026

Mensagens de Lisboa Messages from Lisbon

30 de junho de 2026
30 June 2026

Organizadores:



Apoio:



ABERTURA

A 14ª edição da Iniciativa Portuguesa do Fórum da Governação da Internet decorreu no dia 30 de junho no Fórum Picoas, em Lisboa.

Na abertura da sessão contámos com intervenções da Chief Executive Officer da MEO, Ana Figueiredo, da Presidente do Conselho de Administração da ANACOM, Sandra Maximiano, e uma Mensagem de Sua Excelência, o Presidente da República, António José Seguro.

"Nunca a tecnologia evoluiu tão depressa. E, provavelmente, nunca foi tão importante garantir que a nossa capacidade para a governar acompanha a velocidade da inovação. (...) Mas há algo que nunca mudou. A convicção de que a tecnologia só cria verdadeiro valor quando melhora a vida das pessoas. É precisamente essa responsabilidade que está no centro da governação digital. Durante muitos anos, a grande ambição foi levar a Internet a cada vez mais pessoas. Hoje, a questão é mais exigente. Como garantimos que este novo ecossistema digital continua a ser aberto, seguro, inclusivo e assente na confiança? Como conciliamos inovação com responsabilidade? Como protegemos direitos fundamentais sem comprometer a capacidade de inovar? E como asseguramos que ninguém fica para trás? São estas as questões que estão na agenda internacional. (...) A governação digital só será bem-sucedida se continuar a assentar num verdadeiro modelo multistakeholder, capaz de reunir governos, reguladores, empresas, academia, comunidade técnica e sociedade civil", referiu **Ana Figueiredo, Chief Executive Officer da MEO.**

"Este fórum realiza-se num momento particularmente importante. Estamos a mais de 20 anos da Cimeira Mundial sobre a Sociedade da Informação. No momento em que a União Europeia aprofunda o seu quadro regulatório digital, em que a inteligência artificial acelera também esta transformação tecnológica, em que a segurança das infraestruturas digitais se tornou uma prioridade geopolítica, em que a proteção de menores, integridade eleitoral, literacia digital e responsabilidade das plataformas estão no centro do debate público. A forma como governamos a Internet determinará em grande medida o tipo de sociedade digital que queremos construir. Uma sociedade digital aberta, segura, interoperável, inclusiva, inovadora, competitiva, resiliente, mas acima de tudo uma sociedade digital centrada nas pessoas. É essa vontade e responsabilidade que hoje nos reúne aqui", referiu **Sandra Maximiano, Presidente do Conselho de Administração da ANACOM.**



O Presidente da República

Mensagem por ocasião da 14.^a iniciativa portuguesa do Fórum da Governação da Internet | 30 de junho de 2026

Por me encontrar em representação do Estado português fora do país, não posso estar presente na 14.^a iniciativa portuguesa do Fórum da Governação da Internet. Agradeço ao .PT a sua organização e envio um cumprimento caloroso a todos os coorganizadores e participantes.

Há muito que a internet deixou de ser apenas uma ferramenta de trabalho e se tornou quase um bem essencial na vida de todos nós. Os dados sobre os hábitos digitais dos portugueses demonstram que o consumo de notícias, o contacto com familiares e amigos, o acesso a serviços, ao trabalho ou ao lazer, mas também a qualidade da nossa democracia, passam pela internet, dependendo dela em muitos casos.

É também por isso que hoje quando falamos de internet é incontornável abordar a sua governação, a inteligência artificial, a cibersegurança, a resiliência das infraestruturas digitais, a soberania tecnológica, a regulação das plataformas digitais, a proteção dos consumidores, a inclusão digital e o papel dos jovens na construção do futuro digital.

Sobre a governação da internet gostaria de vos deixar duas ideias que, para o Presidente da República, se revestem da maior relevância.

Em primeiro lugar, a importância de um modelo agregador dos diferentes parceiros. A construção de uma internet aberta, segura, resiliente, inclusiva e centrada nas pessoas não pode ser responsabilidade de uma única entidade ou setor, exigindo uma verdadeira cultura de diálogo e cooperação em torno dos desafios digitais. Trata-se de uma missão coletiva, que exige o contributo das instituições públicas, das empresas, da academia, da comunidade técnica, das organizações da sociedade civil e dos próprios cidadãos. Nem tão pouco pode ser uma missão apenas nacional, exigindo cooperação regional e global, como tão bem ilustra o Fórum Lusófono para a Governação da Internet.

Por fim, a segurança da internet como um caminho para um país justo e de excelência, para a qual é preciso aliar coração à razão. Um coração atento à exclusão digital, preocupado em não deixar ninguém para trás e defensor dos valores da nossa democracia. Uma razão focada na segurança das nossas infraestruturas digitais, garantindo a privacidade dos cidadãos, o seu acesso a serviços, mas também a defesa e soberania do Estado.

Conto com todos vós nesta caminhada que, não tendo começado hoje, sabemos que se prolongará por todas as nossas vidas.

António José Martins Seguro

DESAFIOS GLOBAIS DA GOVERNAÇÃO DA INTERNET

Keynote Speaker:

Pedro Siza Vieira, Partner, PLMJ e Professor na NOVA School of Law

Oradores:

Ana Neves, FCT I.P.

Manuel da Costa Cabral, ANACOM

Pitch: Inês Joaquim, fellow do .PT no YOUthDIG/EuroDIG

Quem governa a Internet? A resposta a esta pergunta continua a moldar um dos mais relevantes debates estratégicos do nosso tempo. Da criação da ICANN à World Summit on the Information Society (WSIS), que consagrou através da Agenda de Tunes uma visão multisetorial da governação da Internet e criou o Internet Governance Forum (IGF), até aos desafios contemporâneos da inteligência artificial, dos dados e das plataformas digitais, cuja relevância é hoje refletida no Global Digital Compact, a governação do digital tornou-se progressivamente mais complexa e multidimensional.

Num contexto em que as decisões sobre o digital influenciam cada vez mais a economia, a democracia, a segurança, o conhecimento e a vida quotidiana dos cidadãos, torna-se essencial promover um diálogo inclusivo entre governos, setor privado, comunidade técnica, academia, sociedade civil e juventude. Mais do que nunca, importa assegurar que a Internet permanece aberta, global, interoperável, segura, resiliente e acessível a todos, continuando a constituir um espaço de inovação, desenvolvimento, exercício de direitos fundamentais e criação de oportunidades.

A governação da Internet nunca foi apenas uma questão tecnológica. Desde a WSIS, tem sido entendida como um exercício de desenvolvimento humano, cooperação internacional, confiança, inclusão e responsabilidade partilhada. Os desafios evoluíram, mas a questão de fundo permanece a mesma: como garantir que a transformação digital continua ao serviço das pessoas, do desenvolvimento sustentável e das sociedades democráticas.

Ao assinalar os vinte anos da WSIS, a WSIS+20 veio reafirmar a atualidade desta visão, reforçando o papel do IGF como fórum permanente das Nações Unidas para o diálogo multisetorial sobre questões de política pública relacionadas com a Internet e o digital. Reconheceu igualmente a importância das Iniciativas Nacionais e Regionais do IGF (NRIs) como espaços essenciais para assegurar uma discussão contínua, inclusiva e próxima das realidades locais, criando pontes entre os debates globais e os desafios concretos enfrentados pelos diferentes países e regiões.

INFRAESTRUTURA, RESILIÊNCIA E SOBERANIA DIGITAL

Oradores:

Ana Aguiar, ISOC PT

Ana Carla Sousa, MEO

Augusto Fragoso, ANACOM

Luís Bernardino, Observatório dos Ecossistemas e Infraestruturas Digitais

Moderação: Sandra Fazenda Almeida, APDC

Relatora: Isabel Travessa, APDC

A internet é uma infraestrutura crítica e deve ser reconhecida como tal nas políticas públicas nacionais e europeias

A internet deixou há muito de ser apenas uma plataforma de comunicação. É hoje uma infraestrutura crítica para o funcionamento da economia e da sociedade, sustentando áreas essenciais como os serviços públicos, os sistemas financeiros, a energia, a saúde, a educação, os transportes e a segurança. Quanto maior é a nossa dependência do digital, maior é também a necessidade de proteger as infraestruturas que o suportam. Por isso, estas infraestruturas devem ser encaradas como ativos estratégicos críticos, com uma visão de longo prazo e investimento continuado.

A resiliência digital exige uma abordagem integrada e uma dimensão europeia

A internet assenta em infraestruturas interdependentes operadas por entidades diferentes: redes de comunicações, cabos submarinos, satélites, centros de dados, energia, pontos de troca de tráfego, serviços cloud e muitos outros sistemas de suporte. Basta que um destes elementos falhe para afetar todo o ecossistema. Reforçar a resiliência exige uma abordagem integrada, cooperação público-privada, redundância e capacidade de prevenção, resposta e recuperação. A resiliência deve ser encarada como um objetivo europeu comum, com maior coordenação entre Estados-Membros, interoperabilidade das infraestruturas críticas e mecanismos de resposta conjunta a incidentes.

A soberania digital constrói-se com capacidades próprias, sem fragmentação

A fragmentação geopolítica da internet constitui um dos maiores riscos para a economia digital global. Reforçar a soberania digital não significa fragmentar: significa dotar a Europa de maior capacidade para desenvolver infraestruturas, tecnologia, investigação, talento e inovação, reduzindo dependências estratégicas face a países terceiros sem comprometer a natureza aberta, global e interoperável da internet. A Europa deve criar condições para que soluções europeias e assentes na lei europeia se possam estabelecer, escalar, e ser alternativas credíveis na Europa e no mercado competitivo internacional.

Portugal tem ativos estratégicos que deve transformar em vantagem competitiva

Os cabos submarinos são essenciais à conectividade global e à autonomia digital europeia, exigindo políticas específicas de proteção, investimento e diversificação. Portugal, um dos principais polos europeus de amarração de cabos internacionais, com crescente capacidade de acolher centros de dados e conhecimento técnico reconhecido, deve adotar uma estratégia nacional integrada que capitalize estes ativos e reforce o seu papel como hub digital atlântico e europeu.

A confiança na internet depende do investimento, regulação e literacia digital

Uma internet segura e resiliente não depende apenas da tecnologia. Requer um investimento contínuo nas infraestruturas, regras simplificadas e capazes de acompanhar a aceleração da evolução tecnológica e uma sociedade mais preparada para o mundo digital. Sem infraestruturas resilientes não existe internet. A regulação deve garantir acesso justo a um ecossistema de infraestruturas eficientes e seguras pelas empresas e pelos consumidores. Uma regulação potenciadora da inovação e dos investimentos, garantindo sempre a defesa dos direitos fundamentais, da sustentabilidade e a existência de um paradigma que não deixe ninguém para trás. Reforçar a literacia digital é essencial para que cidadãos, empresas e Administração Pública compreendam melhor os riscos, os direitos e as responsabilidades associados à utilização da internet, contribuindo para um ambiente digital mais seguro e mais confiável.

A governação da internet continua a depender de um modelo multistakeholder

A inteligência artificial, a automatização crescente da internet, a concentração tecnológica, a cibersegurança e o atual contexto geopolítico tornam ainda mais importante preservar um modelo de governação aberto, colaborativo e multissetorial. O futuro da internet dependerá da capacidade dos governos, reguladores, operadores, comunidade técnica, academia, empresas e sociedade civil continuarem a trabalhar em conjunto para garantir uma internet aberta, resiliente, segura e orientada para o interesse público.

REGULAÇÃO DIGITAL, PLATAFORMAS E CIBERSEGURANÇA

Oradores:

Magda Cocco, VdA

Miguel Pupo Correia, Instituto Superior Técnico

Paula Leal Monteiro, Siemens

Moderação: Maria João Nogueira, Women in Tech

Relatora: Fernanda Ledesma, ANPRI

Regulação Digital, Plataformas e Cibersegurança: uma abordagem integrada para um ecossistema digital mais seguro e competitivo

A transformação digital veio alterar profundamente a forma como cidadãos, empresas e administrações públicas comunicam, trabalham e acedem a serviços. Em resposta a esta evolução, a União Europeia tem vindo a construir um quadro regulatório abrangente, que integra instrumentos como a Diretiva NIS2, o Regulamento dos Serviços Digitais (DSA), o Regulamento Geral sobre a Proteção de Dados (RGPD) e o Regulamento da Inteligência Artificial (AI Act). Embora cada um destes instrumentos tenha objetivos próprios, todos contribuem para um propósito comum: reforçar a segurança, proteger os direitos fundamentais e promover um ambiente digital mais transparente, resiliente e confiável.

O debate desta sessão evidenciou a urgência de abandonar a visão fragmentada da regulação. Em vez de tratar cada norma como uma peça isolada com o seu próprio calendário e regulador, é imperativo adotar uma abordagem sistémica.

O ecossistema digital estrutura-se em três camadas interdependentes: (i) Infraestrutura de comunicações e armazenamento, (ii) Plataformas e (iii) Conteúdos. Qualquer intervenção numa destas camadas gera impactos diretos nas restantes. Consequentemente, a eficácia das políticas públicas depende cada vez mais da adoção de uma abordagem integrada, capaz de assegurar coerência entre os diferentes instrumentos legislativos e reduzir os custos de implementação para as organizações. Abordagens isoladas resultam em burocracia, contradições legais e até entraves à inovação.

Promover uma governação integrada do ecossistema regulatório digital

A multiplicidade de diplomas atualmente em vigor representa um avanço significativo na proteção dos cidadãos e das infraestruturas críticas. Contudo, a sua implementação isolada pode originar sobreposição de obrigações, aumento da carga administrativa e dificuldades de conformidade, sobretudo para as pequenas e médias empresas. Uma visão sistémica da regulação permitirá conciliar segurança, inovação, competitividade e proteção dos direitos fundamentais, assegurando que os diferentes instrumentos legais funcionam de forma complementar e não como regimes independentes.

Reforçar a maturidade em cibersegurança através das pessoas e da capacitação das organizações

A transposição da NIS2 em Portugal através do novo Regime Jurídico da Cibersegurança alargou significativamente o leque de entidades abrangidas e reforçou as obrigações de governação, gestão do risco e reporte de incidentes. O maior fosso de preparação não reside nas grandes empresas, mas sim nas PME que integram a sua cadeia de fornecedores.

A aquisição de *software* e a adoção de mecanismos tecnológicos são apenas uma parte da resposta. A principal dificuldade reside na escassez de recursos humanos qualificados, na insuficiente literacia digital e na capacidade das organizações para incorporar práticas permanentes de gestão do risco, monitorização e resposta a incidentes. A falta de literacia digital infiltra-se nas práticas profissionais e constitui a principal vulnerabilidade do ecossistema. Assim, o investimento em competências, formação e sensibilização deve assumir um papel central nas estratégias nacionais de cibersegurança, envolvendo trabalhadores, gestores e órgãos de administração.

Reforçar a transparência das plataformas e investir na literacia digital desde cedo

O DSA introduz novas obrigações de transparência e responsabilização das plataformas digitais, procurando criar um ambiente *online* mais seguro para todos os utilizadores. Persistem, porém, desafios relevantes, nomeadamente na proteção de menores, na definição de mecanismos eficazes de verificação da idade, na utilização responsável dos dados pessoais e na mitigação das dinâmicas que incentivam uma utilização excessiva das plataformas.

A discussão sobre a limitação do acesso a menores (ex.: fixação de idade mínima em 16 anos) expõe um dilema crítico: para verificar a idade e aplicar restrições, as plataformas necessitam de recolher mais dados pessoais e identificadores. Isto contradiz frontalmente o princípio básico da cibersegurança: "*menos dados recolhidos, menos dados para proteger*". A solução pode passar pela utilização de ferramentas de "*selective disclosure*" (divulgação seletiva) e identidades soberanas (como a Carteira Digital Europeia), permitindo validar atributos essenciais sem ceder o controlo da informação às plataformas.

Execução regulatória e literacia vs. hiper-regulamentação

Existe um consenso de que não são necessárias mais leis, mas sim maior capacidade técnica e institucional para fiscalizar e fazer cumprir os regulamentos existentes, como o DSA. Os participantes no painel defenderam que a resposta não deverá assentar na produção de mais legislação, mas sobretudo na aplicação efetiva das normas existentes, na recolha do mínimo indispensável de dados pessoais e na promoção da literacia digital

desde os primeiros anos de escolaridade, capacitando os cidadãos para identificar ameaças e dotando as organizações com conhecimentos técnicos aprofundados. Uma cidadania digital informada constitui o principal fator de resiliência perante os riscos associados à utilização das plataformas e da inteligência artificial.

Considerações finais

O debate demonstrou que o futuro da governação digital depende da capacidade de equilibrar inovação, segurança e direitos fundamentais. A consolidação de um ecossistema digital resiliente exige uma visão integrada da regulação, maior coordenação entre políticas públicas e reguladores, reforço das competências digitais e mecanismos eficazes de fiscalização e cumprimento das normas já existentes. Mais do que criar novas obrigações, importa assegurar que as soluções tecnológicas e regulatórias contribuem para aumentar a confiança dos cidadãos, apoiar a competitividade das empresas e promover um espaço digital mais seguro, transparente e responsável.

RECOMENDAÇÕES:

Mapeamento integrado: Mapear os riscos regulatórios de forma integrada, unificando a conformidade de NIS2, DSA, RGPD e AI Act.

Capacitação humana: Investir na literacia digital contínua dos alunos desde cedo, e simultaneamente das equipas e dos órgãos sociais das instituições, reconhecendo o fator humano como a primeira linha de defesa.

Minimização de dados: Adotar o princípio da minimização de dados e arquiteturas de privacidade por conceção (*privacy by design*) em todos os processos e serviços.

INTELIGÊNCIA ARTIFICIAL E PODER ALGORÍTMICO

Keynote Speaker:

Adolfo Mesquita Nunes, Co-Chair e sócio da área de Direito Público e Regulatório na Pérez-Llorca

Oradores:

Luís Moniz Pereira, Professor Emérito da Universidade Nova de Lisboa

Rita Barbosa, Guardião

Rui Dias Ferreira, Palko.ai e APDSI

Moderação: Luisa Ribeiro Lopes, .PT

Relator: Raúl Oliveira, IPBRICK

A IA de uma forma muito simples, pode ser resumida em duas vertentes principais, grandes quantidades de dados, e a capacidade de processar ou tratar essas enormes quantidades de dados usando ferramentas matemáticas. Podemos até chamar a essas ferramentas matemáticas de algoritmos, que estão organizados em camadas, mais básicas ou gerais e mais avançadas ou específicas. Mas no fundo o que estas ferramentas manipulam são dados. E a grande questão que se pode colocar, é se o poder vem das ferramentas matemáticas ou dos dados recolhidos, tratados e armazenados. Por conseguinte da possibilidade de obter deles informações preciosas, das quais se pode obter vantagens para o bem e para o mal, ou se quisermos com boas ou más intenções.

1. IA tem limites no seu conhecimento e dados de treino

Quando se consegue armazenar tanta quantidade de informação em modelos como aqueles que estão disponíveis hoje e são usados pela IA generativa, corre-se o risco de pensar que a IA sabe tudo. Mas na realidade não sabe tudo, porque está limitada no seu conhecimento pelos dados usados para realizar o seu treino. A IA generativa não tem informação sobre conhecimento resultante de dados que não foram usados durante o seu treino. Por exemplo, não podemos esperar que a IA possa tomar decisões sobre conhecimento de que não dispõe. Portanto, a supervisão humana é mandatória sempre que se recorre à IA.

Por isso, apesar de haver IA vamos ter de continuar a investigar, inovar e criar dados, informações e conhecimentos novos, que mais tarde ou mais cedo aparecerão em modelos de IA generativa.

Portanto, a IA não tem conhecimento profundo do que se passa em todas as empresas, mas sim e unicamente daquelas cujos dados estão disponíveis. Portanto, será crucial formar as pessoas das empresas para aprenderem a usar a IA para os ajudar a decidir,

para os ajudar a delegar tarefas, executar tarefas sem valor acrescentado, e não tanto colocar a IA a fazer aquilo que distingue uma empresa das demais, porque inevitavelmente se perderá o valor da empresa.

2. A influência exercida pelos algoritmos mediante o acesso exaustivo aos dados pessoais.

Na verdade o poder do conhecimento não está unicamente nos algoritmos mas sobretudo nos dados a que os algoritmos têm acesso. O que é absolutamente incrível, é a quantidade de dados que é possível recolher através de uma panóplia de aplicações, e a possibilidade que existe de tratar e relacionar os dados recolhidos por tantas aplicações. Quem são os proprietários desses dados, como os partilham com quem decide ter acesso a eles para os tratar, e assim obter as vantagens que daí resultam, nomeadamente a influência que podem ter sobre as pessoas?

No futuro vamos ter de ter cada vez mais critério sobre as aplicações que deveremos usar, por forma a restringir quem tem acesso aos dados que geramos. Mais do que esperar pela regulação, teremos de saber proteger os dados sobre os quais consideramos que é importante restringir o acesso para manter a soberania digital.

Escolher as aplicações que tem formas de controlar quais os dados que podem ser recolhidos de forma a beneficiar o nosso dia a dia, mas sem permitir influenciá-lo.

3. Como em qualquer tecnologia, a IA também pode ser usada para o bem como para o mal

Desde o início dos tempos que as tecnologias que o homem foi desenvolvendo, têm vindo a ser usadas tanto para o bem como para o mal. Podemos recuar até à idade do ferro, passando pela revolução industrial, e chegando à introdução da computação, etc.

O exemplo da aplicação Guardião, é um excelente exemplo da utilização da IA para o bem, acedendo a dados e recorrendo a algoritmos para adquirir a capacidade de detetar burlas. Mas a IA também é usada para processar dados referentes a doenças e os algoritmos nesta situação são usados para detetar de forma precoce doenças, até uma das que mais nos atormentam, como é o caso do cancro. É possível também o acesso a dados para treinar equipamentos, que usados de forma positiva conduzem à redução de erros humanos (condução automática, cirurgias feitas com a precisão do melhor cirurgião do mundo, etc).

4. O risco da IA afetar o desenvolvimento cognitivo das próximas gerações

Claro que dispor de tanto conhecimento à distância de um clique é uma situação nova, que numa primeira fase condiciona os métodos de aprendizagem existentes à época do aparecimento da IA generativa. Mas nos próximos anos iremos aprender a conviver com a IA, como aprendemos a conviver com a máquina de calcular, com o computador e com os motores de pesquisa. O papel do ensino será também explicar como é que os alunos devem tirar partido da IA, como podem de forma crítica supervisionar as suas respostas, para assim se ensinar cada vez mais e melhor.

5. Quando se usa o poder dos algoritmos para influenciar ou aconselhar

A grande questão é quem tem a posse dos dados, quem tem acesso aos mesmos, juntamente com a capacidade de recorrer a algoritmos para conseguir gerar riqueza a partir deles. Normalmente as entidades envolvidas são estrangeiras, estando os portugueses sempre numa posição passiva.

O exemplo da Palko.ai, contraria esta passividade portuguesa e até europeia, e demonstra bem que em Portugal também é possível fazermos parte de um ecossistema empresarial que também é capaz de retirar partido do poder algorítmico.

OS CONSUMIDORES, AS EMPRESAS E A SOCIEDADE DIGITAL

Oradores:

Eliza Tarzia, 351 Associação Portuguesa de Startups

Jorge Morais Carvalho, Faculdade de Direito da Universidade NOVA de Lisboa
Paulo Fonseca, DECO

Moderação: Fátima Caçador, Tek Notícias

Relator: Luís Pisco, DECO

Neste painel promoveu-se uma reflexão crítica sobre o estado atual da governação da qualidade dos serviços digitais, a suficiência do quadro regulamentar e as soluções possíveis para garantir que o ecossistema digital serve os consumidores e as empresas. Perante tendências atuais como a degradação intencional da qualidade de serviços digitais (*enshitification*), torna-se essencial debater que modelos de responsabilidade são necessários; que padrões mínimos de qualidade devem ser exigidos; como se garante a transparência e a auditabilidade dos algoritmos de que forma a interoperabilidade e a portabilidade podem libertar os consumidores dos designados "walled gardens" das grandes plataformas.

Consumidores e Startups concordam que a degradação progressiva e deliberada dos serviços digitais, por parte de certas tecnológicas, não afeta apenas os direitos dos consumidores, mas ainda os modelos de negócio das pequenas empresas também utilizadoras dessas plataformas. O DMA veio fixar obrigações de interoperabilidade, portabilidade de dados e condições equitativas de acesso, mas a governação deve ser global e não apenas europeia.

Do ponto de vista jurídico, este fenómeno de degradação da qualidade dos serviços digitais deve ser também enquadrado e interpretado no regime das práticas comerciais desleais, porquanto a qualidade é um direito de todos que não deve e não pode ser monetizado. Sem prejuízo da sua eventual densificação no futuro "Digital Fairness Act", a sua avaliação não deve passar apenas por uma questão de leis, mas também de comportamentos e de apreciação valorativa dos danos causados por essa degradação de qualidade.

A degradação intencional da qualidade dos serviços digitais afeta consumidores e pequenas empresas sem capacidade negocial, devendo ser encarada e combatida enquanto estratégia deliberada de algumas tecnológicas e não como uma consequência inevitável da evolução tecnológica, dificultando o exercício de direitos pelos utilizadores. O DMA foi um importante primeiro passo na fixação de obrigações aos grandes controladores de acesso, mas sendo o digital global, as obrigações terão de ser igualmente globais.

JOVENS E O FUTURO DA INTERNET

Oradores:

João Barroso, Farfetch

João Trocado, YouthDIG 2024

Susana Henriques, Universidade Aberta

Moderação: João Martins, Embaixador Europeu da Juventude para a Segurança na Internet, Rede Europeia de Centros de Internet Segura

Relatora: Priscila Andrade, CDI Portugal

Os jovens são hoje os principais utilizadores da Internet e das tecnologias digitais, mas continuam sub-representados nos processos de decisão que definem as regras, plataformas e políticas que moldam o ecossistema digital. Uma governação da Internet verdadeiramente multissetorial exige que os jovens sejam reconhecidos não apenas como destinatários das políticas públicas, mas como participantes ativos na sua conceção e implementação.

O debate evidenciou que as preocupações dos jovens nem sempre coincidem com aquelas que dominam o debate público e regulatório. Enquanto as políticas tendem a privilegiar os riscos associados ao ambiente digital, como a dependência, o cyberbullying ou a fraude, os jovens valorizam igualmente as oportunidades de aprendizagem, participação, ligação e inclusão proporcionadas pela Internet. Integrar estas perspetivas é essencial para desenvolver políticas públicas mais equilibradas e eficazes.

Foi igualmente destacado que a participação jovem pode assumir diferentes níveis de envolvimento, desde iniciativas de capacitação e programas de formação até mecanismos permanentes de consulta e participação na definição de políticas. Contudo, a participação meramente simbólica, em que os jovens são ouvidos sem influência efetiva nas decisões, compromete a legitimidade dos processos participativos. Importa, por isso, criar modelos de participação contínuos, transparentes e orientados para resultados.

No domínio da inovação tecnológica, foi defendido que a inteligência artificial deve reforçar as capacidades humanas e não substituir os percursos de aprendizagem e desenvolvimento profissional. A adoção destas tecnologias deve preservar oportunidades de formação para as novas gerações, assegurando que o desenvolvimento de competências acompanha a evolução tecnológica.

O painel identificou ainda a reduzida visibilidade pública da governação da Internet como uma barreira à participação dos jovens. Reforçar a literacia digital, o pensamento crítico e a educação para a cidadania digital desde cedo constitui uma condição essencial para promover uma participação mais informada e representativa nos processos de governação.

Concluiu-se que uma Internet mais inclusiva depende da criação de mecanismos permanentes de participação jovem, capazes de transformar a consulta em influência efetiva. Garantir que as novas gerações participam na definição das políticas e tecnologias que moldam o futuro digital constitui uma condição fundamental para uma governação da Internet mais democrática, inclusiva e sustentável.

ENCERRAMENTO

No encerramento contámos com a intervenção do **Senhor Secretário de Estado para a Digitalização, Bernardo Correia.**

"A Internet que nós conhecemos foi feita por académicos, pessoas com espírito de busca de conhecimento, e por isso nasceu como uma comunidade de partilha e colaboração. Conseguimos ainda hoje ver alguns lampejos desse mundo original: os projetos à volta da ciência, os sistemas de inteligência artificial, o conhecimento e o ensino levados ao mundo inteiro de forma democrática, as descobertas no campo da saúde... enfim, a Internet como o mecanismo para um mundo melhor.

Bem governada, a Internet torna-nos mais próximos e cria prosperidade na aldeia global. O digital, em particular, permite-nos corrigir a nossa desvantagem histórica: a produtividade. Para isso, apostamos em competências e literacia, infraestrutura e soberania, e em criar mais valor económico a partir dos dados, aplicações ou serviços e produtos, como por exemplo a aplicação gov.pt."



OPENING SESSION

The 14th edition of the Portuguese Initiative of the Internet Governance Forum took place on 30 June in Lisbon.

At the opening of the session, we heard remarks from MEO Chief Executive Officer Ana Figueiredo, ANACOM Chairwoman Sandra Maximiano, and a message from the President of the Portuguese Republic, António José Seguro.

"Technology has never evolved so quickly. And it has probably never been more important to ensure that our ability to govern it keeps pace with the speed of innovation. (...) But one thing has never changed: the conviction that technology only creates real value when it improves people's lives. That responsibility lies at the very heart of digital governance. For many years, the great ambition was to bring the Internet to as many people as possible. Today, the challenge is even greater. How do we ensure that this new digital ecosystem remains open, secure, inclusive and built on trust? How do we reconcile innovation with responsibility? How do we protect fundamental rights without compromising our ability to innovate? And how do we ensure that no one is left behind? These are the questions shaping the international agenda. (...) Digital governance will only succeed if it continues to be grounded in a genuine multistakeholder model, bringing together governments, regulators, businesses, academia, the technical community and civil society," said **Ana Figueiredo, Chief Executive Officer of MEO**.

"This forum is taking place at a particularly significant moment. More than 20 years have passed since the World Summit on the Information Society. At a time when the European Union is further strengthening its digital regulatory framework, artificial intelligence is accelerating technological transformation, digital infrastructure security has become a geopolitical priority, and the protection of minors, electoral integrity, digital literacy and platform accountability are at the heart of public debate. The way we govern the Internet will largely determine the kind of digital society we want to build: one that is open, secure, interoperable, inclusive, innovative, competitive, resilient, and, above all, people-centred. It is this shared commitment and sense of responsibility that brings us together here today," said **Sandra Maximiano, Chair of ANACOM's Board of Directors**.

Message from the President of the Portuguese Republic, António José Seguro

"The internet has long ceased to be merely a working tool and has become almost an essential part of all our lives. Data on the digital habits of the Portuguese show that our consumption of news, our contact with family and friends, our access to services, our work and leisure, as well as the quality of our democracy, all depend on the internet, in many cases.

This is also why, when we speak about the internet today, we must inevitably address its governance, artificial intelligence, cybersecurity, the resilience of digital infrastructures, technological sovereignty, the regulation of digital platforms, consumer protection, digital inclusion and the role of young people in shaping the digital future.

Regarding internet governance, I would like to leave you with two thoughts which, for the President of the Republic, are of the utmost importance.

First, the importance of a model that brings together the various stakeholders. Building an open, secure, resilient, inclusive and people-centred internet cannot be the responsibility of any single entity or sector. It requires a genuine culture of dialogue and cooperation in addressing digital challenges. This is a collective mission that calls for contributions from public institutions, businesses, academia, the technical community, civil society organisations and citizens themselves. Nor can it be solely a national mission: it requires regional and global cooperation, as the Lusophone Internet Governance Forum so aptly demonstrates.

Finally, ensuring that the internet serves as a pathway towards a fair and excellent country requires us to combine heart with reason. A heart attentive to digital exclusion, committed to leaving no one behind and to upholding the values of our democracy. A reason focused on the security of our digital infrastructures, safeguarding citizens' privacy and their access to services, while also protecting the defence and sovereignty of the State."

Note: Excerpt from the message of His Excellency the President of the Republic. The English version is provided for information purposes only. In the event of any discrepancy or inconsistency, the Portuguese version shall prevail for all purposes.

GLOBAL CHALLENGES OF INTERNET GOVERNANCE

Keynote Speaker:

Pedro Siza Vieira, Partner, PLMJ e Professor na NOVA School of Law

Speakers:

Ana Neves, FCT I.P.

Manuel da Costa Cabral, ANACOM

Pitch: Inês Joaquim, fellow do .PT no YOUTHDIG/EuroDIG

Who governs the Internet? The answer to this question continues to shape one of the most significant strategic debates of our time. From the creation of ICANN to the World Summit on the Information Society (WSIS), which established a multistakeholder vision of Internet governance through the Tunis Agenda and created the Internet Governance Forum (IGF), to the contemporary challenges posed by artificial intelligence, data, and digital platforms, whose growing importance is now reflected in the Global Digital Compact, digital governance has become increasingly complex and multidimensional.

In a context where decisions about the digital sphere increasingly influence the economy, democracy, security, knowledge, and the everyday lives of citizens, it is essential to foster an inclusive dialogue among governments, the private sector, the technical community, academia, civil society, and youth. More than ever, it is crucial to ensure that the Internet remains open, global, interoperable, secure, resilient, and accessible to all, continuing to serve as a platform for innovation, development, the exercise of fundamental rights, and the creation of opportunities.

Internet governance has never been solely a technological issue. Since WSIS, it has been understood as an endeavour rooted in human development, international cooperation, trust, inclusion, and shared responsibility. While the challenges have evolved, the fundamental question remains the same: how can we ensure that digital transformation continues to serve people, sustainable development, and democratic societies?

Marking the twentieth anniversary of WSIS, the WSIS+20 process reaffirmed the continued relevance of this vision, reinforcing the role of the Internet Governance Forum (IGF) as the United Nations' permanent multistakeholder forum for dialogue on public policy issues related to the Internet and the digital environment. It also recognised the importance of the IGF's National and Regional Initiatives (NRIs) as essential platforms for ensuring continuous, inclusive discussions that are closely connected to local realities, bridging global debates with the concrete challenges faced by different countries and regions.

INFRASTRUCTURE, RESILIENCE AND DIGITAL SOVEREIGNTY

Speakers:

Ana Aguiar, ISOC PT

Ana Carla Sousa, MEO

Augusto Fragoso, ANACOM

Luís Bernardino, Observatório dos Ecossistemas e Infraestruturas Digitais

Moderation: Sandra Fazenda Almeida, APDC

Rapporteur: Isabel Travessa, APDC

Internet is critical infrastructure and must be recognised as such in national and European public policies

The internet has long ceased to be merely a communications platform. Today, it is critical infrastructure underpinning the economy and society, supporting essential sectors such as public services, financial systems, energy, healthcare, education, transport and security. As our dependence on digital technologies continues to grow, so too does the need to protect the infrastructures that support them. These infrastructures must therefore be regarded as critical strategic assets, requiring a long-term vision and sustained investment.

Digital resilience requires an integrated approach and a European dimension

The internet relies on a network of interdependent infrastructures operated by different entities, including communications networks, submarine cables, satellites, data centres, energy systems, Internet Exchange Points (IXPs), cloud services and many other supporting systems. The failure of just one of these components can affect the entire ecosystem. Strengthening resilience requires an integrated approach, public-private cooperation, redundancy, and strong capabilities for prevention, response and recovery. Digital resilience should be pursued as a common European objective, with greater coordination among Member States, interoperability of critical infrastructures and joint mechanisms for responding to incidents.

Digital sovereignty is built through strategic capabilities, not fragmentation

The geopolitical fragmentation of the internet is one of the greatest risks facing the global digital economy. Strengthening digital sovereignty does not mean fragmenting the internet. Rather, it means equipping Europe with stronger capabilities to develop its own infrastructures, technologies, research, talent and innovation, reducing strategic dependencies on third countries while preserving the internet's open, global and interoperable nature. Europe must create the conditions for European solutions governed by European law to emerge, scale and become credible alternatives across Europe and in global markets.

Portugal has strategic assets that should be transformed into competitive advantage

Submarine cables are essential to global connectivity and European digital autonomy, requiring dedicated policies for protection, investment and diversification. As one of Europe's main landing hubs for international submarine cables, with growing capacity to host data centres and internationally recognised technical expertise, Portugal should adopt an integrated national strategy that leverages these assets and strengthens its role as an Atlantic and European digital hub.

Trust in the internet depends on investment, regulation and digital literacy

A secure and resilient internet depends on far more than technology alone. It requires sustained investment in infrastructure, simplified regulatory frameworks capable of keeping pace with rapid technological change, and a society that is better prepared for the digital world. Without resilient infrastructures, there is no internet. Regulation must ensure fair access to an ecosystem of efficient and secure infrastructures for both businesses and consumers. It should also foster innovation and investment while safeguarding fundamental rights, sustainability and an inclusive digital paradigm that leaves no one behind. Strengthening digital literacy is essential to enable citizens, businesses and public administrations to better understand the risks, rights and responsibilities associated with internet use, contributing to a safer and more trustworthy digital environment.

Internet governance continues to depend on a multistakeholder model

Artificial intelligence, the increasing automation of the internet, technological concentration, cybersecurity challenges and the current geopolitical context make it more important than ever to preserve an open, collaborative and multistakeholder model of internet governance. The future of the internet will depend on the ability of governments, regulators, operators, the technical community, academia, businesses and civil society to continue working together to ensure that the internet remains open, resilient, secure and aligned with the public interest.

DIGITAL REGULATION, PLATFORMS AND CYBERSECURITY

Speakers:

Magda Cocco, VdA

Miguel Pupo Correia, Instituto Superior Técnico

Paula Leal Monteiro, Siemens

Moderation: Maria João Nogueira, Women in Tech

Rapporteur: Fernanda Ledesma, ANPRI

Digital Regulation, Platforms and Cybersecurity: An Integrated Approach to a Safer and More Competitive Digital Ecosystem

Digital transformation has fundamentally changed the way citizens, businesses, and public administrations communicate, work, and access services. In response to this evolution, the European Union has developed a comprehensive regulatory framework encompassing instruments such as the NIS2 Directive, the Digital Services Act (DSA), the General Data Protection Regulation (GDPR), and the Artificial Intelligence Act (AI Act). Although each of these instruments has its own specific objectives, they all contribute to a common goal: strengthening security, safeguarding fundamental rights, and fostering a more transparent, resilient, and trustworthy digital environment.

The discussion highlighted the urgent need to move beyond a fragmented view of digital regulation. Rather than treating each legal instrument as a separate framework with its own timeline and regulator, participants emphasized the importance of adopting a systemic approach.

The digital ecosystem is structured around three interdependent layers: (i) communications and data storage infrastructure, (ii) digital platforms, and (iii) content. Any intervention in one of these layers has direct implications for the others. Consequently, the effectiveness of public policies increasingly depends on an integrated approach capable of ensuring coherence across legislative instruments while reducing implementation costs for organisations. Fragmented approaches lead to regulatory overlap, legal inconsistencies, excessive bureaucracy, and barriers to innovation.

Promoting Integrated Governance of the Digital Regulatory Ecosystem

The wide range of regulatory instruments currently in force represents a significant step forward in protecting citizens and critical infrastructure. However, their isolated implementation may result in overlapping obligations, increased administrative burdens, and compliance challenges, particularly for small and medium-sized enterprises (SMEs). A systemic approach to regulation can better reconcile security, innovation, competitiveness, and the protection of fundamental rights by ensuring that different legal instruments operate as complementary components of a coherent regulatory framework rather than as independent regimes.

Strengthening Cybersecurity Maturity through People and Organisational Capacity Building

The transposition of the NIS2 Directive into Portuguese law through the new Cybersecurity Legal Framework has significantly expanded the number of entities covered while reinforcing obligations related to governance, risk management, and incident reporting. The greatest preparedness gap does not lie within large organisations but rather among the SMEs that form part of their supply chains.

Acquiring security software and deploying technological solutions represents only part of the response. The greatest challenge remains the shortage of qualified professionals, insufficient digital literacy, and organisations' limited ability to embed continuous risk management, monitoring, and incident response practices. Low levels of digital literacy permeate professional environments and constitute one of the most significant vulnerabilities within the digital ecosystem. Investment in skills development, training, and awareness should therefore become a central pillar of national cybersecurity strategies, engaging employees, managers, and corporate boards alike.

Enhancing Platform Transparency and Investing in Digital Literacy from an Early Age

The Digital Services Act introduces new obligations regarding transparency and accountability for online platforms, aiming to create a safer digital environment for all users. Nevertheless, significant challenges remain, particularly concerning the protection of minors, the development of effective age verification mechanisms, the responsible use of personal data, and the mitigation of platform design features that encourage excessive engagement.

The debate surrounding restrictions on minors' access to social media—for example, establishing a minimum age of 16—illustrates a critical dilemma. To verify users' age and enforce restrictions, platforms must collect additional personal data and identifiers. This directly conflicts with a fundamental cybersecurity principle: the less data collected, the less data there is to protect. Possible solutions include the adoption of selective disclosure technologies and self-sovereign digital identities, such as the European Digital Identity Wallet, enabling essential attributes to be verified without transferring unnecessary personal information or control to digital platforms.

Regulatory Enforcement and Digital Literacy versus Over-Regulation

Participants broadly agreed that the priority is not to introduce additional legislation but to strengthen the technical and institutional capacity required to enforce existing regulations effectively, particularly the DSA. Rather than creating new legal obligations, efforts should focus on ensuring compliance with current legislation, minimising the collection of personal data, and promoting digital literacy from the earliest stages of education. Empowering citizens to recognise digital threats and equipping organisations with advanced technical expertise are essential prerequisites for building resilience. An informed and digitally literate society remains the strongest defence against the risks associated with digital platforms and artificial intelligence.

Final Remarks

The discussion demonstrated that the future of digital governance depends on achieving the right balance between innovation, security, and the protection of fundamental rights. Building a resilient digital ecosystem requires an integrated regulatory vision, stronger coordination among policymakers and regulators, enhanced digital skills, and effective enforcement of the existing legal framework. Rather than creating additional regulatory obligations, priority should be given to ensuring that technological and regulatory solutions strengthen citizens' trust, enhance business competitiveness, and promote a safer, more transparent, and more accountable digital environment.

RECOMMENDATIONS

Integrated Regulatory Mapping: Develop an integrated approach to regulatory risk mapping by aligning compliance efforts across the NIS2 Directive, the Digital Services Act (DSA), the General Data Protection Regulation (GDPR), and the Artificial Intelligence Act (AI Act).

Human Capacity Building: Invest in continuous digital literacy for students, employees, executives, and governing bodies, recognising the human factor as the first line of defence in cybersecurity.

Data Minimisation: Embed the principles of data minimisation and **privacy by design** across all digital processes and services to reduce risks while safeguarding users' fundamental rights.

ARTIFICIAL INTELLIGENCE AND ALGORITHMIC POWER

Keynote Speaker:

Adolfo Mesquita Nunes, Co-Chair and partner in the Public and Regulatory Law area at Pérez-Llorca

Speakers:

Luís Moniz Pereira, Professor Emeritus at the Nova University of Lisbon

Rita Barbosa, Guardiã

Rui Dias Ferreira, Palko.ai and APDSI

Moderation: Luisa Ribeiro Lopes, .PT

Rapporteur: Raúl Oliveira, IPBRICK

In a very simple way, AI can be summarised in two main aspects: large amounts of data, and the ability to process or handle these enormous amounts of data using mathematical tools. We can even call these mathematical tools algorithms, which are organised in layers, more basic or general and more advanced or specific. But fundamentally, what these tools manipulate is data. And the big question that can be asked is whether the power comes from the mathematical tools or from the data collected, processed, and stored. Consequently, from the possibility of obtaining valuable information from them, from which one can gain advantages for good and for evil, or if we want, with good or bad intentions.

1. AI has limits in its knowledge and training data

When you can store so much information in models as those available today and used by generative AI, you run the risk of thinking that AI knows everything. But in reality, it doesn't know everything, because its knowledge is limited by the data used to train it. Generative AI lacks knowledge derived from data that wasn't used during its training. For example, we cannot expect AI to make decisions based on knowledge it doesn't possess. Therefore, human oversight is mandatory whenever AI is used.

Thus, despite the existence of AI, we will have to continue to investigate, innovate, and create new data, information, and knowledge, which sooner or later will appear in generative AI models.

Therefore, AI doesn't have in-depth knowledge of what happens in all companies, but only in those whose data is available. Therefore, it will be crucial to train people in companies to learn how to use AI to help them make decisions, to help them delegate tasks, to perform tasks without added value, and not so much to have AI do what distinguishes a company from others, because inevitably the company's value will be lost.

2. The influence exerted by algorithms through exhaustive access to personal data

In reality, the power of knowledge lies not only in algorithms but, above all, in the data to which algorithms have access. What is absolutely incredible is the amount of data that can be collected through a plethora of applications, and the possibility of processing and relating the data collected by so many applications. Who owns this data, how do they share it with those who decide to access it to process it, and thus obtain the resulting advantages, namely the influence they can have over people?

In the future, we will have to be increasingly discerning about the applications we use, in order to restrict who has access to the data we generate. More than waiting for regulation, we will have to know how to protect the data to which we consider it important to restrict access in order to maintain digital sovereignty.

Choosing applications that have ways to control what data can be collected in order to benefit our daily lives, but without allowing them to influence it.

3. As with any technology, AI can be used for good as well as evil

Since the beginning of time, the technologies that humankind has developed have been used for both good and evil. We can go back to the Iron Age, through the Industrial Revolution, and to the introduction of computing, etc.

The example of the Guardiã application is an excellent example of the use of AI for good, accessing data and using algorithms to acquire the ability to detect scams. But AI is also used to process data related to diseases, and algorithms in this situation are used to detect diseases early, even one of the most tormenting, such as cancer. It is also possible to access data to train equipment, which, when used positively, leads to a reduction in human error (automated driving, surgeries performed with the precision of the world's best surgeon, etc.).

4. The Risk of AI Affecting the Cognitive Development of Future Generations

Of course, having so much knowledge at the click of a button is a new situation, which initially conditions the learning methods that existed at the time of the emergence of generative AI. But in the coming years we will learn to live with AI, as we have learned to live with calculators, computers, and search engines. The role of education will also be to explain how students should take advantage of AI, how they can critically monitor their responses, so that they can learn more and better.

5. When you use the power of algorithms to influence or advise

The big question is who owns the data, who has access to it, along with the ability to use algorithms to generate wealth from it. Usually, the entities involved are foreign, with the Portuguese always in a passive position.

The example of Palko.ai contradicts this Portuguese and even European passivity, and clearly demonstrates that in Portugal it is also possible to be part of a business ecosystem that is also capable of taking advantage of algorithmic power.

CONSUMERS, BUSINESSES AND THE DIGITAL SOCIETY

Speakers:

Eliza Tarzia, 351 Associação Portuguesa de Startups

Jorge Morais Carvalho, NOVA School of Law

Paulo Fonseca, DECO

Moderation: Fátima Caçador, Tek Notícias

Rapporteur: Luís Pisco, DECO

This panel promoted a critical reflection on the current state of governance of digital service quality, the adequacy of the regulatory framework, and possible solutions to ensure that the digital ecosystem serves consumers and businesses. Given current trends such as the intentional degradation of digital service quality (enshittification), it becomes essential to debate what accountability models are needed; what minimum quality standards should be demanded; how to guarantee the transparency and auditability of algorithms; and how interoperability and portability can free consumers from the so-called "walled gardens" of large platforms.

Consumers and startups agree that the progressive and deliberate degradation of digital services by certain technology companies affects not only consumer rights but also the business models of small businesses that use these platforms. The European Digital Market Act (DMA) established obligations for interoperability, data portability, and equitable access conditions, but governance must be global, not just European.

From a legal standpoint, this phenomenon of degradation in the quality of digital services should also be framed and interpreted within the framework of unfair commercial practices, since quality is a right of all that should not and cannot be monetised. Without prejudice to its potential expansion in the future "Digital Fairness Act," its assessment should not only be a matter of laws but also of behaviours and a value judgment of the damages caused by this degradation of quality.

The intentional degradation of the quality of digital services affects consumers and small businesses without bargaining power, and should be viewed and fought as a deliberate strategy of some technology companies, not as an inevitable consequence of technological evolution, hindering the exercise of users' rights. The DMA was an important first step in establishing obligations for gatekeepers, but since the digital world is global, the obligations must also be global.

YOUTH AND THE FUTURE OF THE INTERNET

Speakers:

João Barroso, Farfetch

João Trocado, YouthDIG 2024

Susana Henriques, Universidade Aberta

Moderation: João Martins, European Youth Ambassador for Children Internet Safety, Safer Internet Centre network

Rapporteur: Priscila Andrade, CDI Portugal

Young people are now the primary users of the Internet and digital technologies, yet they remain underrepresented in the decision-making processes that shape the rules, platforms, and policies governing the digital ecosystem. A truly multistakeholder approach to Internet governance requires that young people be recognised not merely as beneficiaries of public policies, but as active participants in their design and implementation.

The discussion highlighted that young people's concerns do not always align with those that dominate public and regulatory debates. While policy discussions tend to focus on the risks associated with the digital environment, such as addiction, cyberbullying, and online fraud, young people also value the opportunities for learning, participation, connection, and inclusion enabled by the Internet. Incorporating these perspectives is essential to developing more balanced and effective public policies.

It was also emphasised that youth participation can take different forms, ranging from capacity-building initiatives and training programmes to permanent consultation mechanisms and direct involvement in policy development. However, purely symbolic participation, in which young people are consulted without having any meaningful influence over decisions, undermines the legitimacy of participatory processes. It is therefore essential to establish participation mechanisms that are continuous, transparent, and results-oriented.

With regard to technological innovation, the panel argued that artificial intelligence should enhance human capabilities rather than replace learning pathways and professional development. The adoption of these technologies should preserve opportunities for education and skills development for younger generations, ensuring that the development of human capabilities keeps pace with technological progress.

The panel also identified the limited public visibility of Internet governance as a barrier to youth participation. Strengthening digital literacy, critical thinking, and digital citizenship education from an early age is essential to fostering more informed and representative participation in Internet governance processes.

The discussion concluded that a more inclusive Internet depends on the establishment of permanent mechanisms for youth participation capable of transforming consultation into meaningful influence. Ensuring that younger generations take part in shaping the policies and technologies that define the digital future is a fundamental prerequisite for a more democratic, inclusive, and sustainable model of Internet governance.

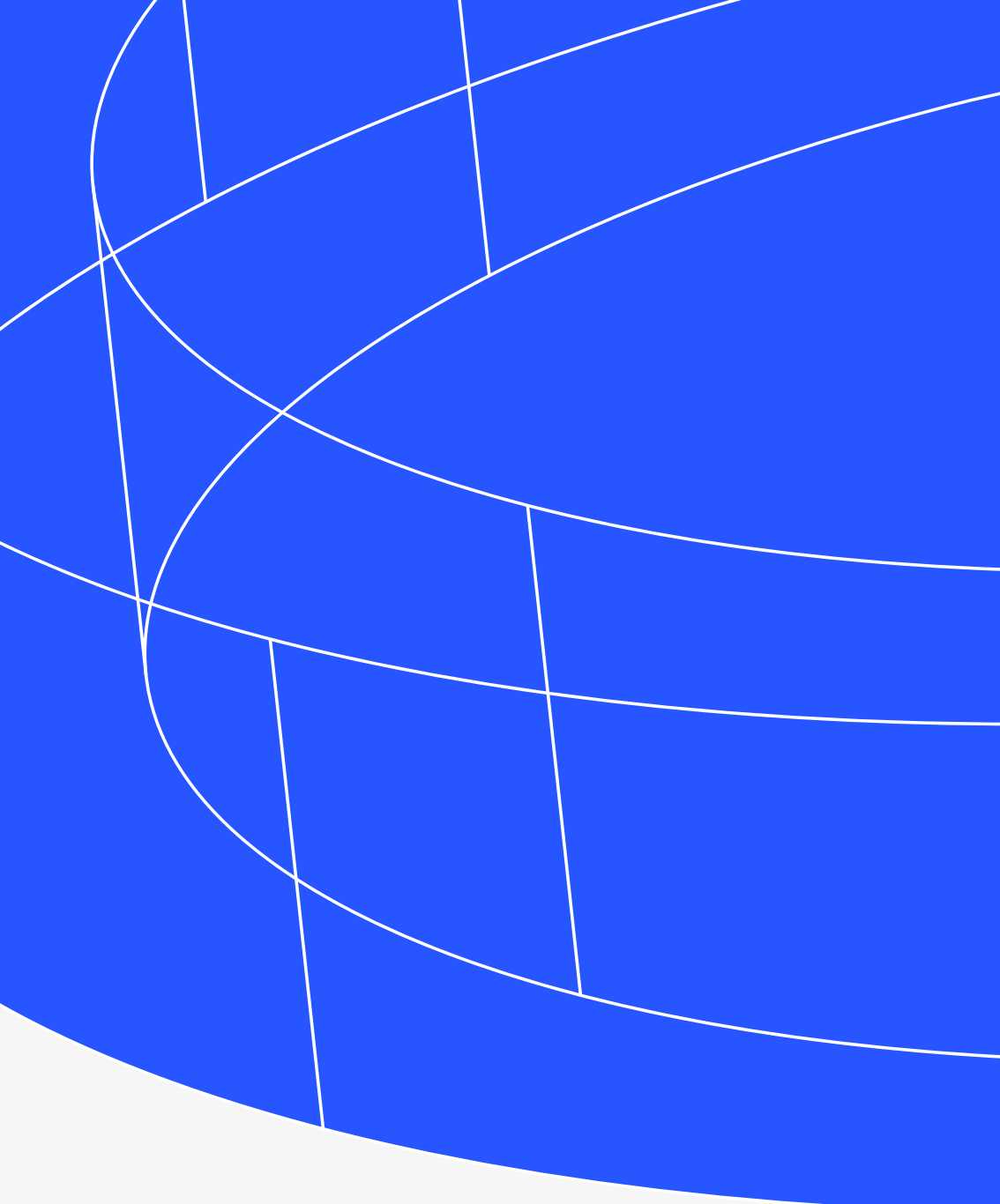
CLOSING SESSION

The closing session featured remarks by the **Secretary of State for Digitalisation, Bernardo Correia**.

"The Internet as we know it was created by academics, people driven by a desire to seek knowledge, and so it was born as a community built around sharing and collaboration. Even today, we can still see glimpses of that original vision: projects centered on science, artificial intelligence systems, knowledge and education made democratically accessible to people around the world, breakthroughs in healthcare... in short, the Internet as a mechanism for building a better world.

When properly governed, the Internet brings us closer together and creates prosperity across the global village. Digital technologies, in particular, allow us to address our historical disadvantage: productivity. To achieve this, we are investing in skills and literacy, infrastructure and sovereignty, and in creating greater economic value from data, applications, services and products, such as the gov.pt app."

Note: The English version is provided for information purposes only. In the event of any discrepancy or inconsistency, the Portuguese version shall prevail for all purposes.



www.governacaointernet.pt