



Debate com Partidos Políticos “O Futuro da Regulação da Internet na Europa”

CONCLUSÕES

28 de maio de 2024

A 28 de maio a APDSI - Associação para a Promoção e Desenvolvimento da Sociedade da Informação - coorganizou com o Portugal Chapter da Internet Society, a Associação D3 - Defesa dos Direitos Digitais e a AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação, um debate online com Partidos Políticos sobre “O Futuro da Regulação da Internet na Europa”. PS e Chega não aceitaram participar no debate.

Este conjunto de associações considera fundamental que a União Europeia e os seus Estados-Membros adotem políticas que promovam desenvolvimentos tecnológicos e regulatórios na defesa dos cidadãos europeus, bem como a natureza aberta e sem fronteiras da Internet.

Com as eleições europeias no horizonte, aqui partilhamos as propostas deixadas pelos partidos portugueses com assento parlamentar relativamente ao futuro da Internet na Europa.

José Legatheaux Martins foi o moderador da sessão que introduziu os diferentes tópicos a discussão, começando por apresentar em relação a cada tópico as diferentes as diferentes perspectivas existentes. Introduziu então o primeiro tópico a debate.

As escutas telefónicas são um dos meios de investigação policial mais usados tradicionalmente, sob autorização do juiz de instrução.

Ao contrário do correio e telefone tradicionais, o uso de criptografia fim-a-fim (E2EE - End-to End Encryption) introduziu, através das suas potencialidades, dificuldades acrescidas à polícia para ter acesso às comunicações entre suspeitos, ou destes com as suas vítimas. No entanto, isso não invalida que outras técnicas de combate sejam usadas, como por exemplo a deteção de padrões e a infiltração. Fazer algo semelhante na Internet só seria possível com uma análise de todos os utilizadores, mantendo a criptografia, mas fazendo *upload analysis*. Sem esses mecanismos pouco a polícia poderá fazer para combater o crime online. A alternativa é **envolver as plataformas na análise de conteúdo suspeito**.

O outro lado argumenta que quebrar a criptografia fim-a-fim sem que haja suspeitas e autorização do juiz de instrução, constituiu uma medida desmesurada que coloca todos os cidadãos sob suspeita. O Parlamento Europeu, no final do ano passado, deliberou aceitar essa vigilância nas redes sociais, mas nas plataformas de mensagens não. Estas estão, pois, isentas desse controlo proposto para os *social media*. No entanto, a Comissão Europeia insiste numa variante da proposta que passa pela **análise dos conteúdos que são carregados nessas plataformas de mensagens**. Tendo as plataformas acesso aos dados, é fácil acrescentar aos meios de atuação policial o requisito da obrigatoriedade de deteção de conteúdos suspeitos pelas mesmas, através da análise dos conteúdos dos utilizadores através do recurso a ferramentas de IA. Deste modo, não só os suspeitos são sujeitos a vigilância, mas também todas as comunicações pessoais, faladas ou multimédia, o que levanta muitas questões de privacidade por oposição às necessidades do combate ao crime.

Vânia Neto, da Aliança Democrática (AD), tem uma visão otimista sobre a legislação atual que classifica como “um passo em frente” ao tentar proteger a privacidade das pessoas em geral, mas também os mais vulneráveis neste mundo digital. Cada um deve ter as suas cautelas, mas tem de haver mecanismos de proteção por parte das grandes plataformas que garantam que determinadas situações nas redes sociais não afetam os mais desprotegidos.

A UE é conhecida como um espaço de regulação, mas “eu não considero que a essa regulação seja incompatível com a inovação, desde que estejam assegurados os direitos das pessoas”. Vânia Neto considera que, neste momento, o caminho que a UE está a fazer na área da proteção, nomeadamente, das crianças no espaço digital, é o correto, embora daqui por alguns meses se possa estar a regular outros aspetos. A Europa deve ser um espaço global de segurança, portanto, também o deve ser na Internet. “Acredito que, de futuro, continue a haver mais legislação para proteger o espaço de direitos das pessoas e proteção da privacidade”, considera.

Quebras de privacidade não são aceitáveis, todos concordam. Proteger a criptografia quanto à sua eficácia é essencial para garantir a segurança e a privacidade online. Mas há quem olhe para a criptografia como uma barreira à aplicação da lei. **É aceitável fazer-se o varrimento sistemático das comunicações de todos os cidadãos?**

Do Bloco de Esquerda (BE), Pedro Filipe Soares, lamenta que do ponto de vista político esta questão seja pouco discutida para o público em geral. O compromisso agora alcançado, diz-nos, é um mau compromisso porque parte do pressuposto que não são consideradas comunicações feitas através das redes sociais e só as outras de mensagens mais formais, de ponta a ponta, são invioláveis. As outras podem ser, pois não se considera que tenham valor legal. Esta diferenciação do que é e não é considerado comunicação é a abertura da caixa de pandora. Sublinha o BE que, deste modo, a sociedade passa a estar sob suspeita e as suas informações a serem escalpelizadas por quem quer que seja.

Da CDU, Manuel Gouveia defende que as alterações tecnológicas não podem ser uma permanente diminuição da privacidade e aumento dos limites de fiscalização prévia: “devemos criar condições para não estarmos permanentemente numa sociedade securitária que previamente pode controlar as nossas informações e diminuir a nossa privacidade face a multinacionais, por exemplo. Batemo-nos contra isso”.

Do Livre, Raquel Pichel diz que o acesso a indiscriminado a este tipo de informação é desproporcionado e iniciativas como o *chat control* não são aceitáveis.

No entender do Livre a informação ponta a ponta é um direito e tudo o que a ameace deve ser rejeitada. “Do ponto de vista legal quase que o ónus da prova é feito de forma invertida”, afirma.

Passou-se então à segunda questão.

Alguns consideram que o DSA - Digital Services Act - em conjunto com o RGPD - Regulamento Geral sobre a Proteção de Dados - são uma espécie de constituição da Internet Europeia, uma resposta europeia contra o “Far West” criado por Silicon Valley. O RGPD baseia-se na noção de consentimento avisado e consciente, esclarece José Legateaux. Basta para isso ir, em função da experiência, melhorando e densificando estas regulamentações ou outras equivalentes.

Por outro lado, há quem julgue que as plataformas continuam a analisar os comportamentos dos utilizadores, sendo que o problema de fundo é o modelo que preside à operação dos grandes grupos: tudo é bom desde que aumente os seus lucros. Esse modelo tem tornado **o RGPD, na prática, incapaz de combater a recolha real de dados dos utilizadores. Já o DSA visa obrigar as plataformas a moderarem os conteúdos disseminados online. Será necessário ir mais longe no RGPD e no DSA?**

Vânia Neto, da AD, volta a valorizar a regulação, mas considera que tem de ser adaptável à evolução das situações. É favorável à obrigatoriedade de identificação dos conteúdos publicitários para cada pessoa saber exatamente onde está a ser feito o *tracking* sobre a sua navegação.

O reforço da resiliência dos cidadãos na luta contra a utilização dos seus dados passa por garantir o alerta contra a desinformação. E sim, “é preciso responsabilizar as plataformas contra a desinformação. Compete à UE reforçar as regulações que estão implementadas”, reforça.

Pedro Filipe Soares, do BE, também acha melhor o que a UE tem e que não existe no resto do mundo, mas, ainda assim, não é suficiente. Os direitos são legitimados pelos próprios cidadãos “e infelizmente há muito pouca informação, valorização e formação sobre os direitos individuais. Os cidadãos mais informados têm consciência dos seus direitos e como os podem usar. Os *tracking free ads* referem direitos para que essa exposição não nos torne tipificáveis e inundados de publicidade”, esclarece. Os grandes detentores desta informação, refira-se, geram verba com estes dados. Pedro Filipe Soares acrescenta que, uma vez que os cidadãos estão pouco ativos, tem de ser a lei mais ativa para os ajudar a fazer valer os seus direitos: “na redistribuição da riqueza, acho que a UE está a defender-se dos *players* norte-americanos e chineses motivada pelas questões de concentração de riqueza. Devia haver uma taxação destas empresas, o que não está a acontecer na UE. Teríamos melhor democracia e cidadãos mais protegidos”.

Manuel Gouveia, da CDU, sobre a recolha de dados, entende se devia ir mais longe porque “os dados não estão a ser comercializados apenas por razões comerciais, mas sim para questões para perigosas que ameaçam os direitos, liberdades e garantias dos cidadãos”. Os softwares deviam ser menos opacos e atentar menos contra a liberdade dos cidadãos. O combate à desinformação é outra luta com a qual é preciso ter cuidado. “De vez em quando há *fake news*, mas os mecanismos de censura historicamente sempre se viraram contra nós”, recorda.

Raquel Pichel admite que o Livre não tem nenhuma medida que proíba algoritmos específicos, mas defende a transparência nos algoritmos que condicionam o acesso à informação e serviços. “Promoção da literacia digital é um ponto básico para nós, porque quem não tem conhecimento e faz os cliques, fica muito desprotegido e as leis devem fazer um maior acompanhamento da literacia digital para proteger as pessoas”, resume.

A independência dos media pode ser uma forma de combater a sua utilização indevida. Se for vista como mais uma forma publicitária, ameaça o jornalismo independente. Também se deve apostar na transferência de software livre e de código aberto em todas as instituições públicas, o que pode valorizar a segurança e privacidade de quem utiliza estes programas.

Nuno Guimarães, do ISOC PT, exulta os representantes dos partidos políticos a tomarem uma posição face às multas que a UE aplica aos grandes operadores em valores impressionantes, mas essas multas diluem-se no orçamento da União Europeia. Era importante canalizar esse rendimento para reforçar os agentes de controlo da regulação porque não tem capacidade de proteger a nossa informação quotidiana.

Para finalizar passou-se à discussão da terceira questão colocada inicialmente aos partidos.

No que concerne ao desenvolvimento e expansão da cobertura de acesso à Internet, é consensual que a conectividade é fundamental para a educação, o desenvolvimento económico e o envolvimento social. Existe, todavia, um problema relacionado com o financiamento da expansão do serviço de Internet. Nas regiões onde existe uma grande densidade de utilizadores, esses viabilizam os investimentos necessários e fornecem as bases para um equilíbrio económico dos serviços. Nas zonas de menor densidade de consumidores, ou para facultar este acesso a famílias com menores recursos, ponderou-se os *sender pay taxes*, ou a partilha justa (mecanismo que garanta que os fornecedores de conteúdos paguem aos operadores de telecomunicações uma taxa pela expansão e melhoria da infraestrutura de rede). Quem os critica, argumenta que os operadores já são pagos pelos utilizadores para encaminharem o tráfego e que essa solução iria ferir a *net neutrality*. Alternativa? Reconhecer que a rentabilidade deste tipo de infraestruturas é deficitária nas zonas do interior e terá de ser subsidiária pelos Estados, mas é necessário clarificar com que modelo.

Por conseguinte, a UE tem como objetivo para 2030 que o acesso Gigabit seja universal no espaço europeu. No entanto, garantir o acesso digital Gigabit universal aos cidadãos europeus, por exemplo em zonas rurais ou remotas, exige investimentos substanciais.

O caminho para viabilizar a conectividade Gigabit universal no espaço europeu pode passar pela viabilização de taxas do tipo "remetente paga" a cobrar pelos operadores de telecomunicações aos operadores de conteúdos ou deve, em alternativa, basear-se numa intervenção dos poderes públicos que tomem medidas para viabilizar essa conectividade sem distorcer o mercado, e sem favorecer os ativos dos operadores de telecomunicações privados atuais e futuros?

Raquel Pichel, do Livre, refere que o partido se identifica mais com o direito de acesso à Internet de forma livre e universal. Entende que tem de se criar legislação que permita aos estados-membros desenvolver a sua infraestrutura digital: “o acesso à internet, como direito que reconhecemos, não pode estar dependente de questões de ordem económica ou localização das pessoas. As empresas devem tratar da transmissão de dados na sua rede de forma igual, independentemente da sua aplicação ou a quem são destinados com vista a uma internet livre e universal para todos”.

Para Manuel Gouveia, da CDU, não se deve equacionar a subsidiarização por parte do Estado, porque as empresas estão a usar um bem público, o espaço eletromagnético, além do conhecimento científico da humanidade. As empresas, não podem só ter lucro e mais lucro e quando têm prejuízo ser o Estado a pagar; a sua atividade deve ser feita de forma equilibrada. A CDU defende que a Internet deve ser crescentemente socializada e evoluir para um serviço gratuito de telecomunicações acessíveis a todos e em todos os lugares. “A questão do fim da neutralidade da rede traz perigos enormes, somos contra qualquer medida que ponha fim à neutralidade da rede para dar mais benefícios a quem já tem mais dinheiro”, conclui.

Pedro Filipe Soares, do BE, ressalva que a neutralidade da internet é um valor fundamental cujo ataque pode pôr em causa o futuro da Internet, pelo que a sua dimensão não pode ser desvalorizada. Os poderes públicos têm a responsabilidade perante os cidadãos de ter Internet de alta velocidade até 2030. Essa resposta deve vir

através da taxação e não deve ser feita de “forma oportunista”, nomeadamente através de poderes que nem são europeus.

Ainda assim, Portugal está no pelotão da frente no acesso a Internet de alta velocidade no território europeu.

Vânia Neto, da AD, concorda que é de importância crucial o espaço europeu poder aumentar e melhorar a sua conectividade à Internet. Grande parte da inovação tecnológica passa pela Internet que já é quase um bem de 1.ª necessidade. Na Europa, 90% dos lares já têm acesso à Internet. Ainda assim, é necessária uma nova geração de conectividade. “Naturalmente, este é um tema em que vai valer a autonomia dos Estados e cada um pode customizar a sua realidade local, mas não faz sentido serem os utilizadores a pagar, e sim os operadores”, refere. Os reguladores devem garantir que não há zonas cinzentas sem internet. É fundamental para a coesão territorial tal como é fundamental o reforço dos recursos da Agência Europeia para a cibersegurança porque “sabemos que esta Internet de largo espectro também traz mais riscos em matéria de cibersegurança”.

Ricardo Lafuente, da D3, traz à discussão as questões de vigilância e securitarismo que se estão a levantar em França, com os Jogos Olímpicos no país a implicarem um enorme aparato securitário, vigilância muito apertada das comunicações e outros atropelos da liberdade. “Estamos a assistir a um ampliar do alcance dos mecanismos securitários, preocupa-nos a videovigilância porque parece haver vontade de a normalizar através de mecanismos de reconhecimento facial automatizado com métodos de análise cruzados entre várias entidades e massificação de internet of things”, descreve. **A D3 questiona qual o posicionamento dos partidos na ampliação deste âmbito securitário.**

Pedro Filipe Soares, acompanha muito estas preocupações e acredita que numa democracia não se devem abandonar os direitos fundamentais.

Manuel Gouveia duvida que a Europa esteja assim tão à frente de outros países do mundo e, portanto, deve ter cuidado com estes desenvolvimentos tecnológicos, que “devem ser travadas ou passamos a viver numa sociedade de vigia, que atribui pontuação e etiquetagem constantes e a seguir estamos a ser reprimidos. Se os cidadãos deixarem de consentir a utilização sistemática dos seus dados, algo tem de mudar”. Com

os Jogos Olímpicos, estamos a viver um “momento terrível” porque são mais um instrumento de guerra: “temos de instar as Nações Unidas e traçarem um caminho de paz e não o da concorrência, competição e luta entre todos. Este modelo de Jogos Olímpicos não foi o que construímos”.

Raquel Pichel também não se revê neste caminho. “Os direitos dos utilizadores têm de ser garantidos na nossa vida online e offline”, finaliza.

Vânia Neto mostra-se contra a videovigilância embora reconheça que nos casos em que é imperativo garantir a segurança e integridade física das pessoas possa fazer sentido. Essas imagens não devem ser guardadas, refere, mas admite que não é fácil atingir este equilíbrio.

Miguel Gonçalves, da AP2SI, é da opinião que a literacia tem de sofrer um upgrade ao nível nacional; têm de ser especialistas a discutir estas pastas “cruciais na sociedade”. O que está em causa nem sempre é a segurança dos dados, essa está garantida; “é a privacidade a que todos os cidadãos têm direito”. Para Miguel Gonçalves o tema da Internet livre não deve ser delegado apenas nas instituições privadas; deve sim haver um acordo para se estabelecer acesso livre em todo o nosso país.

Pergunta da audiência:

- **De que forma entendem que a polarização nas redes sociais afeta a democracia e que estratégias se podem seguir para mitigar estes efeitos?**

“A polarização dos discursos é algo que nos preocupa bastante”, diz Vânia Neto. As plataformas devem evitar discursos de ódio, mas para isso temos de apostar na educação dos cidadãos. Devemos tentar educá-los o quanto antes para uma utilização segura, educada e saber distinguir o que é verdadeiro do que é falso. Urge implementar educação para a cidadania digital nas escolas e na população me geral.

Pedro Filipe Soares diz que a democracia forte tem de vir de cidadãos que vejam as suas condições de vida melhoradas e só assim nasce coesão nas sociedades. Por outro lado, estudos recentes mostram que os discursos amplificados de polarização das redes sociais, servem para tirar do escuro ideias que existiam, mas estavam disfarçadas. “A

falta de coesão das sociedades não vem das redes sociais, elas só vieram amplificar um descontentamento crescente”, esclarece.

Raquel Pichel não vê que haja uma solução milagrosa, mas o caminho passa pela literacia.

Manuel Gouveia tem noção que a polarização é real, mas a culpa não é das redes sociais. “Até no local de trabalho estamos todos contra todos e se promove a concorrência em vez da construção de locais coletivos e sociais. Será este o caminho que a nossa sociedade quer?”, interroga, em jeito de desafio final para o debate.

SOBRE A APDSI

Criada em 2001, a Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) tem por objetivo a promoção e desenvolvimento da transformação e inclusão digital em Portugal, reunindo com este interesse comum profissionais, académicos, empresas, organismos públicos e cidadãos em geral.

Na linha destes propósitos a APDSI tem vindo a desenvolver diversas atividades em torno de causas tecnológicas e sociais, que se traduzem num conjunto de eventos, recomendações e estudos realizados por grupos de trabalho multidisciplinares em diversas áreas de intervenção, como a Segurança e Privacidade, a Ética no Digital, os Serviços Públicos Digitais, a Saúde, a Cidadania e Inovação Social, o Território Inteligente, as Tecnologias de Inteligência Digital, a Política Digital e Governança, os Futuros da Sociedade da Informação, as Competências digitais e o Ambiente e Energia.

Em todos estes trabalhos a APDSI procura identificar as tendências de evolução e também as interações entre as tecnologias e outras dimensões sociais e económicas, contribuindo com uma visão mais aberta para a discussão e tendo como meta a eficaz perceção e implementação destes conceitos na Sociedade Portuguesa. A APDSI tem o Estatuto de Utilidade Pública e foi em 2008 reconhecida como ONGD.

ASSOCIE-SE

URL | www.apdsi.pt

email | secretariado@apdsi.pt

APDSI

ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO



Associação de Utilidade Pública
ONG – Organização Não Governamental

Rua Alexandre Cabral, 2C – Loja A
1600-803 Lisboa – Portugal
URL: www.apdsi.pt

Tel.: (+351) 217 510 762
Fax: (+351) 217 570 516
E-mail: secretariado@apdsi.pt

Coorganização



Patrocinadores Globais da APDSI

Platina



Ouro

