Debate eleitoral sobre

"O Futuro da Regulação da internet na Europa"

Temas para Discussão na Sessão

No presente ciclo político elegemos um conjunto de temas cuja importância nos parece mais relevante e para o qual vos convidamos a apresentarem a vossa opinião e, eventualmente, confrontá-la com as diferentes abordagens das mesmas. Para esse efeito apresentamos a seguir cada um desses temas, referimos visões alternativas sobre o mesmo, e avançamos uma ou duas perguntas, cuja resposta poderia constituir o essencial da vossa participação.

1) Criptografia, privacidade e combate ao crime

Apresentação

Dada a centralidade que a Internet assumiu nas comunicações interpessoais, esta deu meios suplementares aos criminosos para atuarem e expandirem as suas atividades, e por isso introduziu um novo ambiente onde as polícias têm de desenvolver as suas atividades de vigilância e investigação.

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 prevenção, deteção de padrões e a infiltração.

Colocar atualmente a polícia numa situação equivalente à da interceção, legalmente autorizada, de chamadas telefónicas, implica impedir o uso de E2EE, ou usar outras alternativas. A mais referida

atualmente é “client-side scanning” (“inspeção do lado do cliente”), que dá acesso ao conteúdo das comunicações antes de estas serem cifradas. Neste caso, as plataformas têm de ter acesso aos dados antes de estes serem cifrados.

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 com recurso a “aprendizagem automática” (vulgo IA), dos conteúdos dos utilizadores. Ou seja, estaremos numa situação em que não só os suspeitos são sujeitos a vigilância, mas esta se generaliza a todas as comunicações pessoais, faladas ou usando outros suportes (texto, imagem, vídeo, etc.).

A privacidade e as necessidades do combate ao crime, através da mitigação da privacidade, estão sempre em confronto. Os Estados modernos baseados no conceito de Estado-de-Direito, dão a primazia à presunção da inocência, à condenação através de provas, e ao direito à privacidade dos cidadãos. No outro extremo, todas as casas estariam sujeitas à instalação de câmeras pela polícia por exemplo. Com efeito, “se a polícia não reclamar mais meios de investigação sacrificando a privacidade, é porque já estaremos num Estado policial”.

Com o aparecimento da Internet, e a sua centralizada na Sociedade, os Estados têm também de velar para que esta gigantesca infraestrutura seja confiável, segura e previsível. Algo que está dependente de um funcionamento protegido, seguro e fiável de todas as suas componentes. Introduzir “client-side scanning” por exemplo, é considerado um meio por excelência para tornar mais frágeis e inseguros os dispositivos usados pelos utilizadores como o afirmaram recentemente um conjunto de reputados especialistas em segurança.

Visões alternativas

Proteger a criptografia quanto à sua eficácia é essencial para garantir a segurança e a privacidade online. Outros vêm a criptografia como uma barreira à aplicação da lei.

O enfraquecimento da criptografia E2EE apresenta na realidade sérios riscos para a privacidade e a segurança de milhões de utilizadores europeus na Internet, bem como dos seus dados e comunicações, e até paradoxalmente especialmente as crianças. No outro extremo, outros acham que violá-las , sob controlo judicial, seria um meio suplementar e muito eficaz de combater o crime.

Embora se reconheçam as preocupações sobre as dificuldades de aplicação da lei, é vital compreender que comprometer sistematicamente a segurança digital não é uma solução viável e constitui uma perigosa rampa deslizante. Qualquer solução tem de ser proporcional e pesar os prós e contras da sua aplicação.

As soluções preconizadas pelos que dão primazia às necessidades da polícia, introduzem mecanismos de vigilância generalizada e dão às plataformas, e aos seus funcionários, meios de acesso generalizado às comunicações interpessoais e às comunicações empresariais. Tal constituí um risco desmedido e desproporcional que põe em perigo até os negócios e as atividades empresariais que envolvem projetos e colaborações distribuídas geograficamente.

Existe a argumentação de que o "client-side scanning" ("inspeção do lado do cliente") é compatível com a continuação do uso de E2EE. No entanto, isso constituí um mal-entendido comum pois tal prejudica a própria essência da criptografia e constitui um elevado perigo do ponto de vista da segurança. A seguinte analogia pode ajudar a esclarecer o equívoco: quebrar a criptografia é abrir uma carta lacrada e ler o conteúdo antes que ela chegue ao destinatário; a inspeção do lado do cliente é ter alguém olhando por cima do ombro enquanto se escreve a carta. O objetivo da criptografia é assim fundamentalmente prejudicado, bem como todos os seus benefícios.

Repare-se que a E2EE não só protege a confidencialidade das comunicações. Ela é também essencial para garantir a sua integridade (que as mensagens não foram adulteradas) e a autenticação (que as mensagens têm por origem quem se apresenta como o emissor das mesmas). Sem E2EE os utilizadores passam a responsabilidade da verificação destas propriedades para terceiras partes (as plataformas e as polícias).

O lado oposto contrapõe que para combater os crimes de pedofilia e terrorismo é necessário obrigar os serviços de comunicação pessoa a pessoa, através dos seus sistemas e plataformas, a darem acesso a registos das comunicações privadas dos seus utilizadores de forma que, em caso de necessidade, seja possível fazer a sua análise e usá-las como meio de prova.

Perguntas

- O caminho para combater os crimes de pedofilia e terrorismo passa por obrigar os serviços de comunicação pessoa a pessoa a darem acesso, a pedido da polícia, a registos das

comunicações privadas dos seus utilizadores, mesmo que isso implique aceder a todas as comunicações, analisá-las e registá-las generalizada e sistematicamente?

- Dado que esse acesso implica quebrar sistematicamente, ou a criptografia fim-a-fim, ou introduzir mecanismos inseguros e perigosos de "client-side scanning", essa solução não é proporcional e configura o varrimento sistemático das comunicações de todos os cidadãos e por isso deve ser rejeitada?

2) Desinformação, Polarização da Sociedade e Redes Sociais

Apresentação

As redes sociais alteraram profundamente a forma como as pessoas comunicam e se informam. Se por um lado é de saudar aquela que é uma das facetas mais interessantes da Internet, a saber, a banalização da comunicação interpessoal e do acesso à informação, não podemos ignorar que essas plataformas têm contribuído de forma não desprezável para a disseminação de desinformação em massa, e contribuído para a fragilidade e ineficiência dos intermediários de filtragem e análise e dos curadores da informação, nomeadamente da imprensa tradicional.

Em particular, existe hoje liberdade para se difamar, injuriar e ofender, propagar falsidades e soluções de "banha da cobra" sem que se seja responsabilizado por isso. Canais de difusão capazes de alcançarem milhões, sem qualquer responsabilização semelhante à que é imposta à imprensa tradicional, são acessíveis a nacionais e estrangeiros, desde que disponham dos meios financeiros adequados.

Associadas a estas plataformas, e outras similares, foram também desenvolvidos mecanismos de análise de perfis individuais, em clara violação do direito à privacidade dos cidadãos, para os catalogar e classificar com o objetivo de rentabilizar novos e sofisticados meios de fazer publicidade e de apropriação de informação pública e privada, em vastos repositórios de dados, propriedade das plataformas, potenciando todo o tipo de ganhos futuros.

O DSA (Digital Services Act) da UE entrou, em fevereiro passado, em plena aplicação. Há vários anos já entrou em aplicação o RGPD. Estes novos e ambiciosos pacotes legislativos da UE visam regular a atividade das plataformas de forma que os direitos das crianças e dos consumidores sejam

respeitados, nomeadamente banindo venda de bens e difusão de conteúdos perigosos, protegendo a privacidade dos utilizadores e combatendo as bolhas de informação das redes sociais.

Visões alternativas

Alguns consideram que o DSA, em conjunto com o RGPD, são uma espécie de constituição da Internet Europeia, uma resposta europeia contra o "Far West" criado por Silicon Valley. Basta para isso ir, em função da experiência, melhorando e densificando estas regulamentações ou outras equivalentes.

Outros acham que o problema de fundo é o modelo que preside à operação das grandes plataformas: 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. Adicionalmente, os modelos de promoção das publicações nas redes sociais obedecem à necessidade de viciar os utilizadores online, sem atender às consequências, independentemente da natureza da informação propagada.

Perguntas

- O caminho traçado pelo RGPD é suficiente? ou é necessário ir mais longe e introduzir medidas concretas que limitem a viabilidade de as plataformas extraírem lucros sem limitações, como por exemplo algumas semelhantes à proposta "Tracking-Free Ads"?

- Será necessário ir mais longe que o RGPD e o DSA e introduzir medidas concretas como por exemplo: a proibição de algoritmos de "ranking de notícias" com base em critérios psico-sociológicos de envolvimento emocional do utilizador, introduzir limitações sérias de todos os canais de difusão em grupo anónimos que ultrapassem a dimensão de um grupo de amigos, e também introduzir a exigência de identificação clara como publicidade de todos os conteúdos subsidiados?

3) Desenvolvimento e expansão da cobertura de acesso à Internet

Apresentação

A conectividade é fundamental para a educação, o desenvolvimento económico e o envolvimento social. 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 por parte dos operadores de telecomunicações e é imperativo expandir os investimentos.

Visões alternativas

Alguns consideram que a melhor maneira de resolver este problema consiste em introduzir, por via legal, um mecanismo que permita aos operadores de telecomunicações cobrarem uma taxa do tipo "remetente paga" / “sender-pays” (ou a chamada "partilha justa") para o tráfego da Internet. Esse mecanismo garante que os fornecedores de conteúdos paguem aos operadores de telecomunicações uma taxa pela expansão e melhoria da infraestrutura de rede, resolvendo desta forma o problema da viabilidade do desenvolvimento do acesso digital Gigabit universal aos cidadãos europeus.

Outros acham que tal solução poderia prejudicar gravemente o ecossistema da Internet, o princípio da neutralidade da rede, permitiria o aprofundamento de oligopólios de telecomunicações e distorceria o funcionamento do mercado.

Esta segunda visão considera que nos casos em que o fornecimento da conectividade a Gigabit se revelar economicamente inviável, por exemplo por manifesta baixa densidade de clientes, deve o Estado, no âmbito da sua legítima responsabilidade, liderar o desenho das soluções e controlar a sua execução com os mecanismos ao seu dispor, por exemplo taxas, sem condicionar o modelo de sustentação da conetividade universal aos interesses empresariais dos operadores de telecomunicações privados e dos gigantes digitais e sem interferências artificiais nas relações contratuais entre agentes económicos.

Perguntas

- 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?