

Exclusivo

SOCIEDADE

Lei portuguesa impede Apple de lançar detetor de pornografia infantil nos iPhones



O iPhone 12 Pro da Apple

Privacidade das telecomunicações está garantida pela Constituição. Apple, que vai lançar o detetor nos EUA (e não só), recorda que nunca tira os dados para fora da encriptação

O NeuralHash já fez estalar a polémica nos EUA, mas em Portugal é improvável que a ferramenta que a Apple desenvolveu para detetar imagens de pornografia infantil em iPhones venha alguma vez a ser lançada. A legislação nacional restringe o acesso a repositórios de dados e comunicações pessoais aos casos em que há uma mandado de um juiz. E esse requisito está protegido pela Constituição.

Raquel Brízida de Castro, constitucionalista e professora da Faculdade de Direito da Universidade de Lisboa, recorda que o acesso à correspondência e aos dados pessoais só pode ser levado a cabo em Portugal “com autorização de um juiz de instrução criminal - e no contexto de um processo penal”.



O direito à privacidade está consagrado pelo artigo 34º da Constituição da República Portuguesa, que, numa das alíneas, refere que “é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal”.

A Apple já fez saber que pretende lançar a ferramenta nos EUA no outono e que apenas deverá expandir a utilização aos países em que seja legal usá-la. Nas explicações que deu depois do início da polémica, a marca recordou ainda que a análise de imagens vai estar restringida aos ficheiros que são enviados por iPhones, tablets ou computadores da marca para os repositórios que operam na Internet com a denominação comercial iCloud – mas esta característica técnica de pouco vale perante a lei nacional, que dita que as comunicações de cidadãos e empresas só podem ser alvo de interceção ou escuta pelas autoridades e mediante mandado.

Luís Neto Galvão, especialista em questões de privacidade que trabalha na SRS Advogados, não tem dúvidas em considerar que a ferramenta NeuralHash não respeita o que determina a legislação nacional.

“É uma tecnologia perfeitamente intrusiva e ultrapassa todos os limites do que é admissível. Cabe às autoridades de investigação criminal, no quadro da lei, aceder às clouds (repositórios de dados) privadas e não podem ser as plataformas a fazê-lo de sua iniciativa”, refere o advogado, para depois acrescentar: “Houve um enorme avanço na responsabilização das plataformas quanto a disseminação de conteúdos ilegais, nomeadamente com o futuro Digital Rights Act, mas isto não é comparável dado o grau de intrusão. É uma intromissão na esfera privada de clientes ou utilizadores que claramente viola direitos, liberdades e garantias”.



Entre ativistas da privacidade e da proteção dos dados, a questão também não passou despercebida. “É uma questão que terá de ser tratada a um nível europeu”, refere Eduardo Santos, presidente da Associação de Defesa dos Direitos Digitais (D3).

O dirigente da associação D3 não tem dúvidas de que a NeuralHash contraria o posicionamento da Apple nos tempos mais recentes. “Apesar de todas as explicações e transparência da Apple, não deixa de ser um sistema que permite criar backdoor (portas traseiras) que permite vistoriar fotos que deveriam ser privadas. O que abre múltiplas possibilidades. Se calhar haverá Estados que vão querer alargar essa vistoria a conteúdos políticos... e também pode acontecer que hackers (cibercriminosos) ou entidades públicas tentem explorar igualmente essas backdoors”, alerta o ativista.

Entre quem tem por missão combater o abuso de crianças, a ferramenta NeuralHash não deve ser encarada como uma ameaça à privacidade. “A proteção expandida que a Apple disponibiliza para as crianças leva a uma mudança de paradigma”, refere John Clark, presidente do Centro Nacional de Crianças Desaparecidas ou Vítimas de Abuso dos EUA (NCMEC), citado pelo site *MIT Technology Review*.

O NCMEC é o parceiro escolhido pela Apple para implementar a vistoria automática da NeuralHash, mas John Clark não se coíbe de defender a ferramenta: “A realidade é que privacidade e proteção de crianças podem coexistir”.

E A ICLOUD COMO FICA?

A polémica em torno da nova ferramenta não tardou a levantar uma segunda dúvida: estará a Apple a fazer planos para encriptar os repositórios de dados que os consumidores vão debitando para o iCloud?



A questão permanece em aberto e é apontada pelos especialistas como o “próximo capítulo” a desvendar depois de a empresa ter confirmado que pretende estreitar a NeuralHash durante o outono, com o lançamento dos sistemas operativos usados nos iPhones, e também nos tablets, relógios inteligentes e computadores pessoais. iOS 15, iPadOS 15, watchOS 8 e macOS Monterey são os nomes dos sistemas operativos da Apple que devem estreitar a nova ferramenta no outono.

Depois do início da polémica desencadeada com uma primeira notícia no *Financial Times*, a Apple sentiu-se na obrigação de dar mais explicações sobre a ferramenta que consegue aceder aos repositórios alojados nos dispositivos da marca e, sem qualquer mandado judicial, verificar se existe alguma imagem de abuso sexual de menores arquivado. E as explicações da Apple acabaram por confirmar algo que não estava ainda bem presente na opinião pública: os repositórios de dados do iCloud não são encriptados – ou pelo menos não usam os mesmo níveis de criptografia que são disponibilizados na atualidade pelos iPhones.

Tendo em conta que os repositórios de dados de Microsoft, Google ou Amazon sempre disponibilizaram ferramentas similares de deteção de imagens associadas a abuso sexual de menores, não faltam analistas e observadores que admitem que a Apple pode avançar, nos tempos mais próximos, com a aplicação de cifra nos repositórios de dados que disponibiliza através da Internet com a marca iCloud.

Esta hipótese, caso venha a confirmar-se, pode fazer a diferença face à concorrência, ao mesmo tempo que garante o mesmo nível de encriptação das unidades de armazenamento do iPhone. E neste caso importa não esquecer que, no caso da Apple, a encriptação não é apenas proteção mas também posicionamento de marca.



Nas respostas dadas a críticos e jornalistas, a empresa garantiu, por mais de uma vez, que a ferramenta NeuralHash apenas procura imagens ou variantes de imagens que já foram previamente identificadas pelas autoridades ou entidades de proteção de menores.

No final essas suspeitas são encaminhadas para o NCMEC - e a Apple não chega a conhecer esses resultados apurados pelo sistema ou sequer a descriptar repositórios que se encontram em iPhones ou Macs.

As boas intenções não chegam para garantir que a privacidade não sai a perder. A concorrência da Apple não tardou muito a lembrá-lo. “Os países onde os iPhones são vendidos terão diferentes conceitos daquilo que é aceitável. Será este sistema usado na China? E, nesse caso, que conteúdos serão considerados ilegais e como é que nós alguma vez saberemos disso? Como é que eles (a Apple) vão gerir os pedidos de governos de vários pontos do mundo para que sejam adicionados outros tipos de conteúdos que podem vir a ser vistoriados?”, fez notar Will Cathcart, diretor do WhatsApp, numa publicação efetuada no Twitter.

Cathcart poderia estar a questionar a Apple com o objetivo de enaltecer a recusa do WhatsApp em adotar ferramentas de vistoria similares, mas não teve de demorar muito para ter uma potencial resposta da Apple: “No passado deparámo-nos com pedidos para o desenvolvimento e instalação de alterações mandatadas por governos que têm por objetivo diminuir a privacidade dos utilizadores e recusámos liminarmente esses pedidos”, referiu a Apple em comunicado, no qual reitera ainda a intenção de continuar a rejeitar os pedidos de governos para acesso indevido a dados dos utilizadores.

A questão é de sobremaneira delicada para a imagem de marca veiculada pela Apple. No passado recente, a Apple assumiu a



defesa da privacidade ao rejeitar as pretensões das polícias americanas no acesso a telemóveis de terroristas – e não se coibiu de assumir os danos colaterais desse braço-de-ferro lembrando os direitos civis instituídos nos EUA, mesmo durante investigações a casos de terrorismo que levaram à morte de inocentes.

Desde 2019 que a Apple tem vindo a desenvolver ferramentas que eliminam dados pessoais de navegação e reduzem o envio de informação pessoal para fora do ecossistema tecnológico que controla, elevando a fasquia no que toca à privacidade. Mas a defesa da privacidade poderá não ser totalmente uniforme à escala global: em paralelo com a defesa da privacidade, a marca também protagonizou uma entrada no mercado chinês – e, ao contrário do sucedido nos EUA, nunca houve notícia de a Apple se ter recusado a dar dados dos consumidores às autoridades chinesas.

O que levanta a questão: será que Apple está mesmo disposta a lutar pelos direitos individuais até às últimas consequências?
