Exclusivo

SOCIEDADE

# Uma explicação muito técnica acompanhada de uma metáfora imobiliária para entender um dos grandes mistérios de 2021: o caso Censos

**Hugo Séneca**


Nuno Botelho

Os dados de seis milhões de portugueses que responderam aos Censos2021 estiveram ou não sob controlo momentâneo e exclusivo da empresa norte-americana Cloudflare? Esta é uma viagem ao coração da Internet - e da segurança, a sua segurança

Por mais de uma vez o INE garantiu que os serviços contratados à Cloudflare se limitavam a encaminhar dados entre internautas e servidores do Instituto. A resposta não surpreende, pois esse é o principal serviço prestado pela Cloudflare, mas confirma que durante um período indeterminado - que tanto poderá demorar apenas uma fração de segundo como todo o tempo de resposta aos formulários - a Cloudflare poderá ter assumido o controlo exclusivo de aceder aos dados dos cidadãos. E isso deve-se ao facto de ser

simultaneamente a gestora da rede que encaminha os dados e também a emissora do certificado que cifra essa informação. Hoje, o Censos 2021 opera de forma diferente – mas a cifra continua a ser emitida por uma empresa americana - a DigiCert.

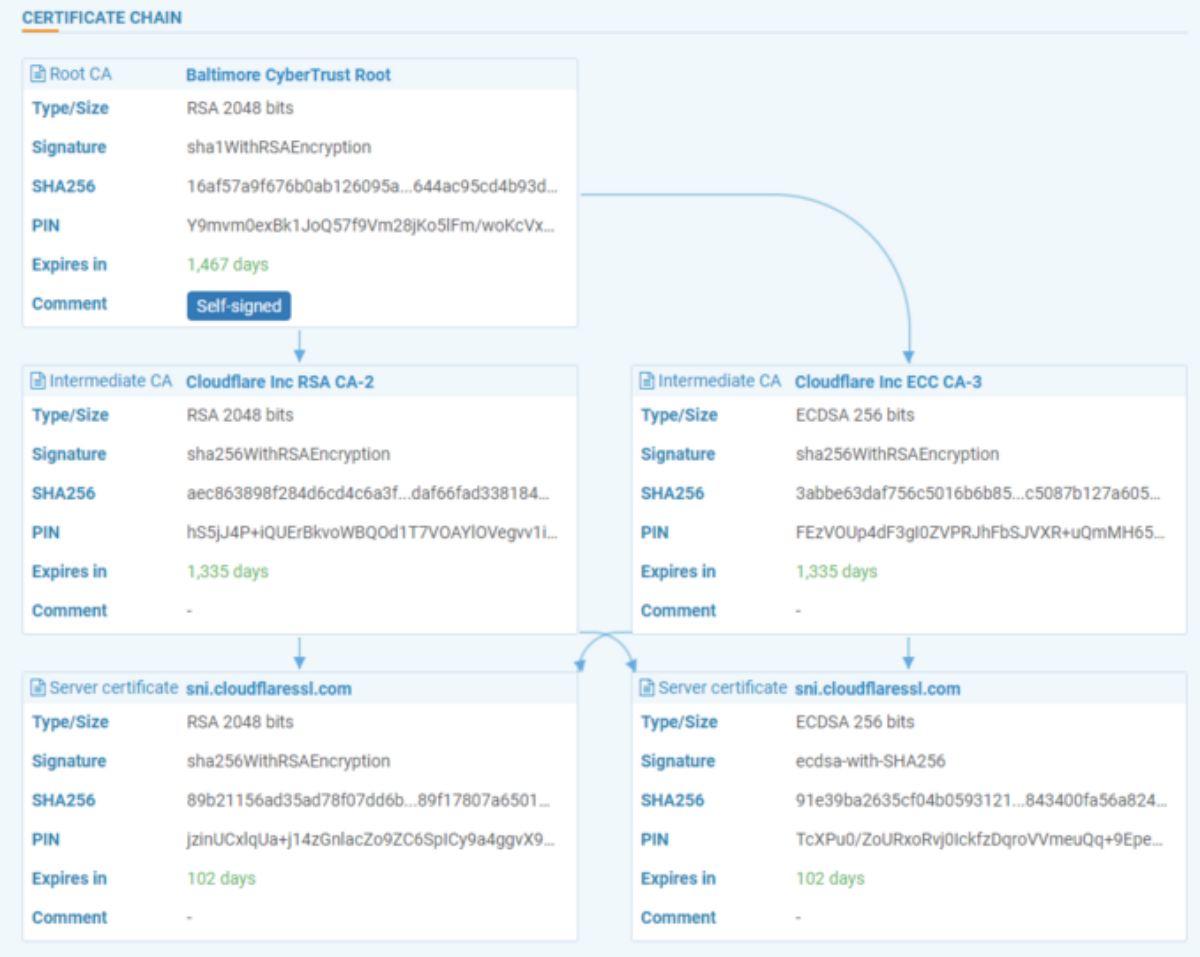
"Caberia ao INE saber por onde passam os dados dos Internautas. O problema nem é tanto o certificado TLS, mas sim o roteamento da informação. Se a informação passa por lá (pela rede de servidores da Cloudflare) então tem de ser decifrável. Logo há que saber para onde foi essa informação", explica Pedro Fortuna, diretor de Tecnologias da Jscrambler, empresa portuguesa que tem vindo a desenvolver soluções segurança para sites e plataformas que operam na Internet.

Para os leigos, os termos "certificado TLS" e "roteamento" podem dizer pouco, mas para os departamentos de informática e alguns gabinetes jurídicos especializados já não são novidade. A Cloudflare tem vindo a ganhar mercado como empresa que disponibiliza Redes de Distribuição de Conteúdos (CDN, na sigla em inglês), que suportam aquilo que se conhece na gíria como "roteamento", que encaminha dados através de canais próprios dentro da Internet. Estes canais de roteamento funcionam como túneis virtuais que distinguem os dados de um ou mais clientes do restante tráfego da Internet, mas exigem certificados TLS (sigla de Transport Layer Security, ou Camada de Segurança do Transporte, numa das traduções possíveis).

No caso do Censos 2021, o certificado TLS é gerido pela Cloudflare, que é a única detentora das chaves de cifra.

Os certificados TLS cifram as comunicações e só são atribuídos às diferentes entidades que usam a Internet quando há garantias da identidade de quem os pede, mas porque a Cloudflare tem de assumir por várias vezes a função de veículo das comunicações e dados de outras entidades usa o seu certificado TLS como forma de garantir a cifra. E quem quiser usar os serviços de roteamento

terá sempre de usar também os certificados TLS da Cloudflare – e sujeitar-se ao já mencionado período indeterminado em que a empresa americana tem o poder exclusivo de decifrar a informação em trânsito.




O certificado usado pela Cloudflare para veicular os dados do Censos 2021. O certificado pode ser obtido através de ferramentas de cibersegurança que estão disponíveis na Internet

A deliberação que a CNPD emitiu com a ordem de suspensão do envio de dados através da Cloudflare confirma precisamente as suspeitas de que a empresa americana, que tem vindo a ganhar mercado no segmento do roteamento e proteção de comunicações e é hoje apontada como uma referência no que toca à captação de investimentos para Portugal, terá tido o acesso exclusivo aos dados – e tanto o INE como as autoridades nacionais pouco poderiam fazer além de confiar na boa-fé ou na política interna da Cloudflare - que prevê a emissão de alertas para os clientes sempre que há pedidos de acesso a dados com base em mandados da justiça nacional ou estrangeira.

"O facto de a chave de a cifragem utilizada ser da Cloudflare significa que a cifra é aplicada por esta entidade, mantendo-se durante o trânsito da informação, e é por ela e só por ela decifrada - ou seja, antes da entrega do conjunto da informação (os pacotes de dados) ao lNE, a Cloudflare tem de proceder à sua decifragem, não tendo o INE qualquer intervenção neste processo", refere a deliberação da CNPD.

As dúvidas levantadas pela deliberação da CNPD também podem ser apresentadas em jeito de metáfora: "Era como se uma agência imobiliária me vendesse uma casa e dissesse que ficava com as chaves da casa para evitar assaltos. Se quiser, essa agência imobiliária consegue entrar na casa que comprei? Sim, consegue. O que significa que fiquei a saber que continua a haver possibilidade de alguém entrar na minha casa, mas fico sem a possibilidade de tentar saber quem terá sido, pois a chave não é minha", explica David Russo, diretor de Tecnologias da empresa CyberS3C.

No caso de se confirmar que houve uma fuga de dados de mais de seis milhões de portugueses que já tinham respondido ao Censos 2021 até o serviço da Cloudflare ser suspenso, o INE poderá ter de se explicar em audição com a CNPD a fim de evitar uma multa que pode chegar a um máximo de 20 milhões de euros.

O INE responde às suspeitas de perda de controlo no envio dos dados lembrando que os dados do Censos 2021 são sempre alojados nos servidores do Instituto. "É preciso compreender que as funções de cibersegurança que haviam sido contratadas à Cloudflare são um complemento às medidas adotadas pelo INE, cuja definição foi acompanhada pelo Gabinete Nacional de Segurança / Centro Nacional de Cibersegurança. Com a cessação dos serviços da Cloudflare, o INE adotou medidas adicionais no seu próprio sistema", refere por e-mail fonte institucional do INE.

O INE também lembra que a Cloudflare é uma empresa com delegações em Portugal e noutros países da UE e rejeita ceder aos pedidos de acesso à informação que se encontra na UE por parte de entidade externas. Sobre os Censos 2021, o INE garante ainda que "a nível de desempenho a questão do roteamento dos dados tem impacto apenas em relação a dados estáticos, como por exemplo imagens ou logotipos (não está relacionada os dados recolhidos no contexto do Censos)" - o que contradiz, pelo menos, parte da deliberação da CNPD.

A Cloudflare também nega qualquer ireregularidade ou fuga de dados: "Apesar de continuarmos a analisar a nossa posição, estamos preocupados com esta abordagem restritiva que foi levada a cabo pelas autoridades portuguesas (a CNPD) neste caso delicado que, no limite, poderá minar, em vez de melhorar, a privacidade dos utilizadores, ao tornar os dados vulneráveis perante ameaças de segurança", refere a empresa numa resposta oficial, que também reitera o empenho em respeitar o RGPD (Regulamento Geral de Proteção de Dados).

## E EM BRUXELAS?

A hipotética fuga de dados do Censos 2021 não desencadeou qualquer notificação para a Comissão Europeia, uma vez que o processo foi desencadeado pela entidade supervisora (a CNPD) e não o Governo de um Estado-membro. A Comissão prefere não se pronunciar sobre o assunto – mas em Bruxelas toda a gente sabe qual o princípio dominante a seguir pelas autoridades dos 27 países: tanto Estados como entidades privadas têm de garantir o respeito pelo RGPD quando estão a lidar com o envio de dados para fora da UE.

Nos gabinetes de advogados, o "caso" assume especial importância – até porque pode vir a produzir efeitos na forma como as empresas que operam em Portugal e na UE terão de lidar com as fornecedoras tecnológicas. Luís Neto Galvão, especialista em questões jurídicas relacionadas com as

tecnologias que trabalha com a SRS Advogados, admite que o INE ainda possa apresentar uma versão diferente no caso de ser aberto um processo pela CNPD, mas lembra que a deliberação da entidade supervisora do respeito pela privacidade aponta para indícios de irregularidades.

"É manifesto que, na investigação efetuada pela CNPD, constataram-se pelo menos duas irregularidades: a contratação de serviços na cloud sem proteção adequada e a não realização de uma avaliação de impacto sobre a proteção de dados especificamente sobre o tema do transporte de dados para os servidores da Cloudflare", explica por e-mail o advogado. Por sua vez, Pedro Fortuna diz que a Cloudflare poucas responsabilidades terá na matéria – e que é ao INE que cabe tomar as devidas precauções: "Toda a gente sabe que as coisas funcionam assim. [O uso de um certificado TLS da Cloudflare] é uma das condições para se usar aquele serviço. E o INE tinha obrigação de saber disso", refere Pedro Fortuna.

Francisco Lima, presidente do INE, nega qualquer fuga de dados para os EUA

Com mais de 200 servidores dispersos pelo mundo, a Cloudflare garante a disponibilidade de serviço a plataformas, apps, formulários ou sites através de cópias que permanecem em cache. Por norma, estas cópias ficam alojadas nos servidores mais acessíveis para cada internauta em cada momento – e com isso se garante menos tempos de espera e evita-se congestionamentos ao distribuir os pontos de acesso pelo mundo.

A este processo de replicação de endereços, plataformas e sites dá-se o nome "cache". É algo corriqueiro mas há uma variante a ter em conta: há uma diferença entre usar a cache de um formulário ou usar uma cache para as respostas que os cidadãos dão aos formulários. Os formulários são públicos e não deverão ser muito diferentes daquilo que se faz noutros países; as respostas aos formulários são obrigatórias por lei nacional e já contêm informação pessoal, que nalguns casos pode ser considerada “sensível”.

Pedro Fortuna considera que o INE poderia ter mantido o roteamento dos formulários do Censos 2021 mas deveria ter evitado que as respostas dos internautas fossem “roteadas” através da rede da Cloudflare. “Os dados dos utilizadores não têm de passar por servidores que asseguram o serviço do CDN [que a Cloudflare disponibiliza]. É possível especificar que os dados dos utilizadores não passam por esses servidores, mas nesse caso da aplicação [do Censos 2021] tem de ser desenhada e preparada para isso”, refere o especialista em questões de cibersegurança.

Francisco Lima, presidente do INE, forneceu algumas pistas no rescaldo deste caso, admitindo que a plataforma do Censos 2021 possa ter ficado algo mais lenta – possivelmente porque os dados dos internautas começaram a ser roteados por outras vias que garantem que a informação não é veiculada para fora da UE.

Perante as restrições legais atuais, e sem se saber quando haverá um acordo entre EUA e UE para uma transferência de dados mais

expedita entre os dois lados do Atlântico, começa a ganhar forma a ideia de se criar uma infraestrutura que garanta funcionalidades similares às que são providenciadas por serviços como o da Cloudflare. "Não faz sentido serviços do Estado como o Censos 2021 não terem um certificado [TLS] próprio. Deveria haver uma infraestrutura nacional para o suporte de roteamento e certificados TLS. Seria algo que deveria ser aplicado em diferentes serviços do Estado, até por uma questão de soberania digital", refere David Russo.

## O CERTIFICADO DA CLOUDFLARE

Através de ferramentas de uso comum para os especialistas de cibersegurança é possível aceder ao certificado da Cloudflare que foi usado pelo Censos 2021. O certificado TLS usado pela Cloudflare está dependente de uma entidade conhecida por Baltimore CyberTrust Root e é composto por uma chave RSA de 2048 bits. Eventualmente, o roteamento dos dados deixou de recorrer a redes que têm servidores fora da UE, mas o Censos 2021 passou a usar o certificado TLS da também americana Digicert. O que levanta a questão sobre a dependência que entidades nacionais e europeias têm das empresas americanas. Até porque a Cloudflare não é a única que opera nos moldes que levaram à intervenção da CNPD. Akamai, Fastly e serviços especializados da Google ou Amazon também prestam serviços em Portugal e na UE – e estão sujeitas à mesma incompatibilidade que hoje se verifica nas legislações americana e europeia.

"Há muitas outras empresas e organizações portuguesas que fazem o mesmo que fez o INE. Se levarmos ao limite a posição que a CNPD assumiu com base na análise da decisão Schrems II do Tribunal de Justiça da UE, torna-se muito difícil continuar a enviar dados para os EUA", refere Sofia de Vasconcelos Casimiro, advogada e professora da Faculdade de Direito da Universidade de Lisboa e da Academia Militar.

Roteamento e certificados TLS são termos desconhecidos para os leigos, mas a decisão Schrems II também não será propriamente assunto de conhecimento geral. A decisão Schrems II foi anunciada pelo TJUE no verão de 2020, na sequência de uma queixa do ativista austríaco Max Schrems. Antes desta decisão, o mesmo jovem já havia ficado conhecido por ter levado o TJUE a declarar inválido o acordo Safe Harbor, que permitia o envio expedito de dados entre Europa e EUA. Com a decisão Schrems II, o TJUE declarou inválido o acordo Privacy Shield que substituiu com propósitos similares o Safe Harbor. Com esta decisão, as empresas que pretendam enviar dados para os EUA passaram a ter de assinar contratos para os diferentes casos de envio – mas há condições a serem respeitadas.

"O INE só poderia avançar com este tipo de contrato se houvesse garantia da outra empresa cumprir os requisitos (equivalentes aos do RGPD)", refere Sofia de Vasconcelos Casimiro. "São dados relativos a toda a população portuguesa e contêm informação considerada "sensível"", acrescenta a jurista.

A decisão Schrems II não afeta apenas a informação mais pessoal e é também uma questão de geopolítica. Schrems é o apelido que fez a queixa nos tribunais europeus, mas a decisão está diretamente ligada às revelações do ex-agente da Agência de Segurança Nacional dos EUA Edward Snowden sobre a facilidade com que as autoridades judiciais e os serviços de informação americanos acedem a dados veiculados na Internet – a partir de qualquer ponto do mundo.

Luís Neto Galvão recorda que a decisão Schrems II foi justificada pelo TJUE pelo facto de a lei Foreign Intelligence Surveillance Act (FISA) e o Decreto Executivo n.º 12333, da presidência dos EUA, darem às autoridades americanas poderes que não se compadecem com o que determina o Regulamento Geral de Proteção de Dados (RGPD) "Estão em causa não só a possibilidade de acesso aos dados como a insuficiência dos meios

concedidos aos titulares dos dados não americanos para se defenderem de intrusões por parte das autoridades de informação americanas. Não há assim em tese um nível de proteção dos dados importados a partir da União Europeia equivalente ao que é exigido pelo direito europeu. O que, segundo o TJUE, obriga a que sejam adotadas medidas de salvaguarda adicionais", descreve por e-mail Luís Neto Galvão.

## OS BLOCOS CONTINENTAIS DA PRIVACIDADE

A equivalência no tratamento de dados está prevista pelo RGPD, tal como foi aprovado pela Comissão e o Parlamento Europeu, para a informação que é enviada para fora da UE. O requisito não é exclusivo para o alojamento e o tráfego de dados que passa pelo EUA – e também poderá colocar-se nas marcas asiáticas que operam na UE, entre muitas de outras proveniências, mas a predominância dos serviços baseados na Internet que foi assumida, nos últimos anos, e o próprio escândalo iniciado por Edward Snowden colocaram as marcas americanas no centro das atenções.

Ciente destas limitações, a Microsoft anunciou recentemente que iria passar a alojar os dados provenientes da UE no espaço comunitário, para evitar questões legais como a que assolou o Censos 2021. Esta decisão de manter os dados europeus dentro da UE vai ficar totalmente operacional até ao final do ano através da instalação de 13 centros de dados em diferentes Estados-membros (o mais próximo de Portugal vai ficar situado em Madrid, Espanha).

Hoje, os dados dos clientes da Microsoft são armazenados na Irlanda e têm uma cópia de segurança na Holanda. Com a expansão da rede de alojamento de informação para mais países, os clientes da Microsoft vão poder indicar os servidores onde podem armazenar os dados e, no limite, até podem ser ressarcidos no caso de haver um acesso indevido por autoridades externas que não respeite o RGPD.

"Não é uma resposta a qualquer decisão de um governo de um Estado-membro, porque já cumpríamos a lei europeia, mas sentíamos que os nossos clientes pretendem manter os dados dentro da UE", explica Pedro Duarte, diretor da Microsoft Portugal, que assume a pasta dos Assuntos Externos e Legais.

Pedro Duarte faz notar que não conhece o "caso" Censos 2021 mas recorda que, no passado, a gigante do software já tinha feito finca-pé no fornecimento de dados de clientes que se encontravam em servidores sediados na Irlanda mas que foram solicitados pela justiça americana. O "caso" mais emblemático foi encaminhado até ao Supremo Tribunal dos EUA – e acabou por ficar sanado em 2018 depois de ser aprovada uma legislação conhecida como Clarifying Lawful Overseas Use of Data Act (CLOUD Act), que esclareceu algumas dúvidas mas que pode dar às autoridades americanas uma potencial jurisdição à escala mundial, uma vez que, aparentemente, continua a permitir o acesso a dados que se encontram alojados fora dos EUA.

"Com a jurisprudência Schrems II tornou-se bastante complexo justificar transferências internacionais para destinos que, como os Estados Unidos ou uma parte significativa do mundo, não oferecem um nível de proteção adequado. Nessa medida, quando estejam em causa os dados de muitos cidadãos confiados à administração pública, julgo que o princípio da prudência deve levar a que esta opte por soluções na nuvem que assegurem a localização dos dados exclusivamente no espaço europeu", refere Luís Neto Galvão.

As restrições impostas pelo TJUE com a decisão Schrems II põem em evidência a necessidade de se criar uma nova ordem mundial que tenha em conta as transferências de dados – que são hoje a principal "matéria prima" da Internet. Pedro Duarte admite que os conflitos gerados por diferentes governos e legislações possam estar a abrir caminho à formação de blocos continentais que têm regras próprias e limitam o envio de dados quando não há

garantias de reciprocidade ou equivalência, mas também defende que é chegada a hora de atuar sobre a matéria. "Temos grande esperança de que a UE e os EUA estabeleçam um novo acordo [para a troca de dados]. Ambas as partes ganham com isso. As empresas dos EUA têm interesse em continuar a fazer negócio na UE e as startups europeias têm interesse em ter acesso a um mercado enorme como é o americano", conclui.

A polémica sobre o Censos 2021 chegou em plena presidência portuguesa da UE e a Associação para o Desenvolvimento e Promoção da Sociedade da Informação (APDSI) não quis deixar passar o "caso" em claro, aproveitando a realização da cimeira de chefes de Estado e Comissão Europeia no Porto, durante o passado fim de semana.

"A APDSI apela a que os legisladores da UE e dos EUA acelerem as negociações com vista a encontrar-se uma solução política para este impasse regulatório nas transferências de dados entre os dois lados do Atlântico", referiu o comunicado da Associação, dando voz aos anseios de profissionais e empresas das tecnologias.

A Comissão Europeia responde a este e outros reptos lembrando que as conversações estão em curso para o desenvolvimento de um novo acordo entre EUA e UE. Resta saber quando é que esse eventual acordo poderá ser implementado.