

DELIBERAÇÃO/2021/533

I. Introdução

1. A Comissão Nacional de Proteção de Dados (CNPD) recebeu mais de uma dezena de participações relativas à operação censitária a decorrer – Censos 2021 – realizada pelo Instituto Nacional de Estatística, I.P. (INE), a qual em parte se concretiza através do preenchimento do formulário disponível *online* no endereço <https://censos2021.ine.pt/>. A maior das participações prende-se com o facto de o inquérito obrigar a fornecer dados de identificação dos cidadãos, designadamente o nome completo. Contudo, algumas participações associavam a obrigatoriedade de fornecimento de dados identificados com a transferência de dados para uma empresa sediada nos Estados Unidos da América.

2. Também nas redes sociais a mesma questão foi colocada, tendo órgãos de comunicação social relatado que a informação aí exposta não era exata.

3. A CNPD, ao abrigo dos poderes conferidos pelas alíneas *b)* e *e)* do n.º 1 do artigo 58.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º e da alínea *b)* do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto (a qual tem por objeto assegurar a execução, na ordem jurídica interna, do RGPD), procedeu à análise do sítio na Internet do INE e da plataforma aí disponibilizada, tendo concluído que esta entidade recorre a serviços prestados pela empresa Cloudflare. Foi ainda solicitada informação ao INE quanto a esta operação sobre os dados pessoais.

II. Análise

i. Factos apurados

4. O formulário para a recolha de dados dos Censos 2021 é acedido através da infraestrutura disponibilizada pela Cloudflare, Inc. (doravante, Cloudflare), uma empresa sediada em São Francisco, Califórnia, nos Estados Unidos da América. Esta empresa fornece vários serviços de segurança na Internet e de *Content Delivery Network* (CDN).

5. A CDN consiste numa rede de servidores que tem como objetivo diminuir a latência dos acessos aos servidores – *i.e.*, o período de tempo que medeia entre a ação do utilizador e a resposta a essa ação. Com efeito, através de um algoritmo que envia a informação simultaneamente para vários servidores, escolhe aquele que apresenta um tempo de resposta mais curto. Com isto, consegue-se a entrega da informação mais rápida e com maior robustez do ponto de vista de segurança.

6. A Cloudflare detém 200 (duzentos) *datacenters* localizados em mais de cem países, a grande maioria dos quais não tem um nível de proteção de dados adequado, nos termos previstos no artigo 45.º do RGPD.

7. O INE recorreu a serviços prestados pela empresa Cloudflare através da subscrição *online* do seu *Business Plan*¹. Este plano disponibiliza um conjunto de serviços, estando o INE atualmente a fazer uso da WAF², da CDN, e do *Rate Limit*³.

8. O referido plano rege-se pelo 'Self-Serve Subscription Agreement'⁴ (contrato principal de prestação de serviços) e pela adenda relativa ao tratamento de dados (Data Processing Addendum versão 3.0⁵), datada de 1 de outubro de 2020, a qual é parte integrante do contrato principal (cf. cláusula 6.1 do contrato principal).

9. O INE justificou a celebração deste contrato com o objetivo de "(...) *responder de forma eficaz às necessidades de desempenho e segurança da informação associadas à dimensão e complexidade da operação Censos 2021*".

10. Não obstante a utilização deste serviço, não está, nem nunca esteve em causa que a informação fornecida pelos cidadãos através dos formulários do Censos 2021 está alojada nos servidores do INE.

11. Quando o cidadão acede ao formulário do Censos 2021, é encaminhado para um dos servidores da Cloudflare de acordo com o referido algoritmo. Ainda que o critério subjacente a este algoritmo seja o da maior proximidade dos servidores em relação ao local da origem da invocação, não há garantia de que tal suceda, uma vez que depende da carga neles existente em cada momento. A infraestrutura da Cloudflare comunica com o servidor do INE por TLS.

12. O nome *censos2021.ine.pt* está associado ao IP 172.67.41.182, localizado nos Estados Unidos da América, estando atribuído à Cloudflare. Os clientes acedem ao sítio recorrendo ao protocolo de comunicação segura HTTPS, sendo que o certificado associado é emitido por Cloudflare, Inc ECC CA-3, uma entidade certificadora da própria Cloudflare. Deste modo, esta empresa é detentora tanto da chave privada como da chave pública,

¹ Este plano é apresentado no *website* da Cloudflare como destinado a pequenos negócios e *websites* de comércio eletrónico, que requerem um desempenho e segurança avançados, e que dão prioridade ao apoio de correio eletrónico. Ver <https://www.cloudflare.com/plans/business/>

² Uma WAF ajuda a proteger as aplicações *web* ao filtrar e monitorizar o tráfego HTTP. Protege dos ataques como *Cross Site Request Forgery*, *Cross Site Scripting*, *SQL Injection*, entre outros.

³ *Rate limiting* protege contra ataques de *Denial of Service* (DoS), ataques de força bruta e outros tipos de comportamentos malignos.

⁴ <https://www.cloudflare.com/terms/>

⁵

https://www.cloudflare.com/resources/assets/slt3lc6tev37/1M1j5uuFDuLTyZJJDPBag/bda8d591447971b3df2bccf5aa4e0916/Customer_DPA_v.3.1_-_en_1_Oct_2020.pdf

ficando assim habilitada à cifragem e decifragem de todas as comunicações entre os cidadãos que acedem ao formulário e enviam dados para o servidor do INE.

13. Note-se que o facto de a chave de 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 INE, a Cloudflare tem de proceder à sua decifragem, não tendo o INE qualquer intervenção neste processo.

14. Aliás, o INE admite não ter controlo sobre a transmissão da informação entre os cidadãos e o seu servidor. Uma vez dentro da rede CDN da Cloudflare, o INE não tem forma de saber se o tráfego está a ser dirigido para servidores situados no território de países da União Europeia, ou residentes em qualquer outra zona do globo.

15. Até à data da presente deliberação, foram recolhidos dados pessoais de mais de seis milhões de cidadãos residentes em território nacional.

ii. Apreciação à luz do RGPD

16. Não sobrando dúvidas que as informações fornecidas pelos cidadãos no preenchimento dos formulários Censos 2021 constituem dados pessoais, nos termos do artigo 4.º, alínea 1), do RGPD – por corresponderem a informações relativas a pessoas singulares identificadas –, a operação censitária está sujeita ao RGPD, sendo o INE o responsável pelo tratamento, de acordo com as alíneas 2) e 7) do mesmo artigo.

17. Sendo ainda certo que algumas das informações cabem na categoria de dados pessoais especiais prevista no n.º 1 do artigo 9.º do RGPD, estando por isso o tratamento de dados sujeito a um regime de proteção mais rigoroso e, desde logo, à obrigação de realização de uma avaliação de impacto sobre a proteção de dados (AIPD), conforme o n.º 1 e a alínea b) do n.º 3 do artigo 9.º do RGPD.

18. Assinala-se que a AIPD tem de abranger todas as operações sobre os dados pessoais, incluindo, portanto, a operação correspondente ao transporte da informação para e dos servidores da Cloudflare, no âmbito da relação de subcontratação.

19. Quanto a este ponto, o INE declarou à CNPD que *"(...) optou pela realização de uma Avaliação de Impacto sobre a Proteção de Dados apenas à operação estatística principal. Isto ficou a dever-se ao facto de os testes (2016, 2018, 2020) visarem apenas testar processos de recolha e funcionalidades aplicacionais, e serem, no que toca às soluções aplicacionais, parciais. Por conseguinte não permitiam testar e avaliar o risco inerente a todos os processos. Nesse sentido, apenas a operação final permitiu realizar uma avaliação completa e abrangente*

num cenário em que as decisões tomadas, dado o contexto pandémico, foram sendo alteradas e otimizadas. No entanto, os respetivos conteúdos não se encontram ainda integrados de forma a serem disponibilizados de imediato. Embora esteja garantido o acompanhamento sistemático e contínuo do EPD e do RSI aos Censos 2021."

20. Não tendo sido realizada uma avaliação de impacto quanto a esta específica operação sobre os dados pessoais, o INE não concretizou uma ponderação dos riscos para os direitos dos titulares dos dados e, consequentemente, não adotou quanto a esta operação qualquer medida suplementar mitigadora desses riscos, tendo-se apenas centrado sobre o desempenho e a segurança do sistema, promovendo inclusive uma consulta ao Gabinete Nacional de Segurança.

21. Sobre esta operação, o INE não consultou a CNPD, o que teria permitido à CNPD pronunciar-se e assim procurar acautelar os direitos dos titulares dos dados.

22. No entanto, mesmo considerando a finalidade visada com esta operação, havia outras soluções que permitiriam mitigar os riscos, garantindo ao INE um maior controlo sobre os dados, e, desde logo, limitar o trânsito dos dados pessoais ao território dos Estados-Membros da União Europeia, não implicando o seu envio para Estados terceiros.

23. Ora, a opção do INE implica, como se demonstrará, o trânsito de dados pessoais por países terceiros em relação à União Europeia e que não possuem o nível de proteção adequado. Implica também, por força do contrato celebrado, uma específica autorização do INE para transferência de dados pessoais para os Estados Unidos da América (EUA) e para os demais países onde estejam localizados os servidores utilizados pela Cloudflare (nomeadamente, África do Sul, China, Índia, Jordânia, México, Rússia, Singapura)

24. Como se descreveu supra, nos pontos 5 e 11, os dados pessoais dos cidadãos residentes em Portugal são enviados para servidores da Cloudflare situados em diferentes países não identificados, nem identificáveis pelo INE ou pelos titulares dos dados. Acresce que a chave de cifragem e de decifragem é propriedade da Cloudflare.

25. Ora, o contrato celebrado pelo INE e a Cloudflare prevê o trânsito dos dados pessoais para qualquer um dos 200 servidores por esta utilizados, bem como a transferência de dados pessoais para os EUA.

26. Com efeito, nos termos da *Data Processing Addendum* versão 3.0 (doravante, DPA), que, recorda-se, integra o contrato, são transferidos dados pessoais do cliente (exportador de dados) para a Cloudflare (importador de dados), nos Estados Unidos da América, utilizando como mecanismo de transferência internacional as cláusulas contratuais-tipo baseadas na Decisão da Comissão 2010/87/UE, de 5 de fevereiro de 2010, aplicáveis



às transferências de dados pessoais para subcontratantes estabelecidos em países terceiros⁶, as quais fazem parte integrante da adenda e são, nessa medida, subscritas pelo cliente (cf. alínea *m*) da cláusula 1.1 da DPA)⁷.

27. A DPA aplica-se na medida em que a Cloudflare trata dados pessoais submetidos pelo cliente à Cloudflare ou, como é o caso do INE, recolhidos e tratados pelo cliente utilizador do serviço, quando esses dados pessoais estão sujeitos à legislação de proteção de dados aplicável.

28. Assim, ao (sub)contratar os serviços da Cloudflare, o INE, na sua qualidade de responsável pelo tratamento e simultaneamente de cliente, aceitou as condições de utilização do serviço, incluindo a adenda aos termos de tratamento de dados pessoais, a qual contém um contrato entre o responsável pelo tratamento (INE) e a subcontratante (Cloudflare) para a transferência de dados pessoais para os Estados Unidos da América.

29. Ainda de acordo com os termos da DPA, o INE concedeu uma autorização geral à Cloudflare para que esta possa recorrer a outros (sub-)subcontratantes, sejam empresas dentro ou fora do Grupo (cláusula 4.2), reconhecendo e aceitando que pudesse ser necessário para a prestação do serviço o recurso a (sub-)subcontratantes estabelecidos em países terceiros (cláusula 6.4).

30. Se as cláusulas contratuais-tipo são, em geral, um instrumento legal para a transferência de dados pessoais para países terceiros, ao abrigo das disposições conjugadas do artigo 46.º, n.º 2, alínea c), e n.º 5, do RGPD, é necessário verificar, todavia, se a legislação do Estado terceiro, que se sobrepõe obviamente a um instrumento de natureza contratual, não diminui ou esvazia as garantias oferecidas por essas cláusulas, as quais têm precisamente como objetivo compensar a falta de um nível de proteção adequado no país de destino dos dados (cf. artigo 44.º e 46.º do RGPD)⁸.

31. De acordo com o Tribunal de Justiça da União Europeia (TJUE), é ao exportador de dados que compete, caso-a-caso, com a colaboração do importador de dados, verificar se o país de destino em concreto assegura um nível de proteção de dados essencialmente equivalente ao garantido pela UE, devendo, se possível, adotar salvaguardas adicionais que permitam ultrapassar os obstáculos e garantir que a proteção dos dados se mantém⁹. Esta obrigação decorre igualmente do cumprimento do princípio da responsabilidade, consagrado no artigo 5.º, n.º 2, do RGPD.

⁶ Conforme consta do *website* da Cloudflare, a política de privacidade foi revista em 27 de outubro de 2020, para «refletir» uma alteração do instrumento legal em que assenta a transferência de dados pessoais da União Europeia (UE) para os Estados Unidos da América (EUA), que deixou de ser a decisão de adequação do Escudo de Proteção da Privacidade (*Privacy Shield*), invalidada pelo Tribunal de Justiça da União Europeia (TJUE), em julho de 2020, no caso *Schrems II*, para passarem a ser as cláusulas contratuais-tipo.

⁷ https://www.cloudflare.com/cloudflare_customer_SCCs.pdf

⁸ Ver n.ºs 92 e 93 do Acórdão *Schrems II*, em que o Tribunal salientou que a avaliação da existência de um nível de proteção essencialmente equivalente ao garantido na UE no país de destino dos dados deve ser feita independentemente de ser utilizado um mecanismo de transferência previsto no Capítulo V do RGPD.

⁹ Ver n.º 134 do Acórdão *Schrems II*.

32. De acordo com a análise do TJUE no caso *Schrems II*, a legislação dos EUA – que é o país de destino das transferências internacionais da Cloudflare ao abrigo das cláusulas contratuais-tipo – possibilita ingerências nos direitos fundamentais das pessoas, baseadas em requisitos relativos à segurança nacional e ao interesse público, que podem resultar no acesso a dados pessoais transferidos da UE para os EUA e da utilização desses dados no âmbito de programas de vigilância, com base na Secção 702 da FISA (*Foreign Intelligence Surveillance Act*) e no Decreto Executivo 12333¹⁰.

33. O TJUE concluiu que tais ingerências não são proporcionais, à luz do direito da União, na medida em que não é definido o alcance das limitações aos direitos das pessoas, não existem regras claras e precisas quanto à aplicação dessas medidas nem requisitos mínimos para proteção contra riscos de abuso, não se verifica um juízo de necessidade, e não são conferidos direitos oponíveis aos titulares dos dados nem vias de recurso jurisdicional, pelo que as limitações à proteção de dados que decorrem da legislação dos EUA não satisfazem os requisitos exigidos pela Carta dos Direitos Fundamentais da UE¹¹ (cf. artigos 7.º, 8.º, 47.º e 52.º, n.º 1).

34. Por conseguinte, só seria possível realizar uma transferência de dados pessoais para os EUA se a legislação aqui em causa, e expressamente referida pelo TJUE, não fosse direta ou indiretamente aplicável à Cloudflare ou aos seus (sub-)subcontratantes, e mesmo assim apenas mediante a adoção de medidas suplementares que pudessem demonstradamente comprovar que esta legislação não seria aplicável ou não teria efeito prático nas transferências de dados pessoais.

35. Contudo, os serviços prestados pela Cloudflare, designadamente aqueles contratados pelo INE quando subscreveu o *Business Plan*, colocam a empresa diretamente sob a alçada da legislação dos EUA que lhe impõe a obrigação de conceder acesso em massa aos dados pessoais por si tratados, desde logo enquanto prestador de serviços de comunicações eletrónicas¹², sem prejuízo de outro tipo de serviços ser abrangido igualmente por outras disposições da legislação norte-americana de vigilância.

36. A Cloudflare reconhece no ponto 7 da DPA que, no seu papel de subcontratante, poderá ser objeto de pedidos de acesso a dados pessoais, por parte de terceiros no âmbito de procedimentos legais, que possam ser «inconsistentes» com a lei aplicável ao seu cliente, ou seja, o RGPD. Nesse caso, existindo conflito de leis, a Cloudflare declara que informará de imediato o cliente, «a menos que tal notificação seja legalmente proibida» (cf. alínea a) cláusula 7.1).

¹⁰ Ver n.º 165 do acórdão citado, em que são citados os programas PRISM e UPSTREAM.

¹¹ Ver n.ºs 175-176, 180-185, 191 e 194 do acórdão citado.

¹² Cf. Secção 702 da FISA alterada pelo 50 USC § 1881^a.

37. Ora é precisamente o caso desta legislação dos EUA que impede as empresas norte-americanas de informarem os seus clientes do acesso realizado pelas autoridades norte-americanas para fins de recolha de informação sobre estrangeiros, no contexto da atividade de segurança nacional.

38. Verifica-se, pois, que não há qualquer garantia que os dados pessoais dos cidadãos residentes em Portugal, recolhidos pelo INE através do seu *website*, no âmbito do Censos 2021, não sejam acedidos pelas autoridades dos EUA, por intermédio da Cloudflare devido aos serviços por esta prestados ao INE e que implicam, conforme contrato firmado, a transferência desses dados pessoais para os EUA.

39. Nesse sentido, não podendo as cláusulas contratuais-tipo, ao abrigo das quais os dados pessoais são transferidos pelo INE para a Cloudflare, nos EUA, ser respeitadas no país terceiro de destino, na medida em que estas não vinculam as autoridades desse país, não oferecendo assim as garantias adequadas exigíveis pelo RGPD, está a CNPD obrigada a proibir essas transferências de dados, de acordo com o prescrito pelo TJUE.¹³

40. Acresce que, de acordo com a mesma jurisprudência¹⁴, ainda que o INE pudesse demonstrar que os dados pessoais não foram transferidos para os EUA, o trânsito dos dados sempre dependeria da adoção de medidas suplementares adequadas e suficientes, que aqui não se verificam.

41. Nos termos do n.º 2 do artigo 5.º e do artigo 24.º do RGPD, recai sobre o INE a obrigação de cumprir os princípios e regras de proteção de dados pessoais, bem como de demonstrar a conformidade dos tratamentos de dados pessoais da sua responsabilidade.

III. Conclusão

42. Face ao exposto e por não existir outra medida corretiva suscetível de acautelar os direitos dos titulares dos dados, a CNPD delibera, ao abrigo da alínea j) do n.º 2 do artigo 58.º do RGPD, ordenar ao Instituto Nacional de Estatística, I.P., a suspensão do envio de dados pessoais do Censos 2021 para os EUA e para outros países terceiros sem um nível de proteção adequado, seja através da Cloudflare, Inc., ou de outra empresa, no prazo máximo de 12 horas.

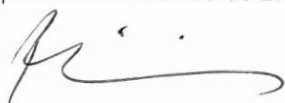
43. Deve ainda a mesma entidade garantir, no âmbito de eventuais subcontratações, que os subcontratantes não estejam obrigados a cumprir uma legislação que afaste a proteção conferida pelo RGPD.

¹³ Ver n.º 107 e 121 do acórdão citado.

¹⁴ Cf. n.ºs 63 e 183 do mesmo acórdão.

44. Dispensa-se a audiência, nos termos da alínea a) do n.º 1 do artigo 124.º do Código do Procedimento Administrativo, considerando a urgência da medida corretiva, tendo em conta o período temporal da recolha *online* do Censos e que, de outro modo, se manteria o risco para os direitos, liberdades e garantias dos cidadãos, potencialmente mais de quatro milhões, que ainda não cumpriram a obrigação legal de resposta à operação censitária.

Aprovado na reunião de 27 de abril de 2021



Filipa Calvão (Presidente)