Sexta-feira, 21 de maio de 2021

P9_TA(2021)0262

Proteção adequada de dados pessoais pelo Reino Unido

Resolução do Parlamento Europeu, de 21 de maio de 2021, sobre a proteção adequada dos dados pessoais pelo Reino Unido (2021/2594(RSP))

(2022/C 15/23)

O Parlamento Europeu,

— Tendo em conta a Carta dos Direitos Fundamentais da União Europeia (a «Carta»), nomeadamente os artigos 7.º, 8.º, 16.º, 47.º e 52.º,

— Tendo em conta o acórdão do Tribunal de Justiça da União Europeia (TJUE), de 16 de julho de 2020, no processo C-311/18, *Data Protection Commissioner* contra *Facebook Ireland Ltd* e *Maximillian Schrems* (acórdão Schrems II) ([1]),

— Tendo em conta o acórdão do TJUE, de 6 de outubro de 2015, no processo C-362/14, *Maximillian Schrems* contra *Data Protection Commissioner* (acórdão Schrems I) ([2]),

— Tendo em conta o acórdão do TJUE, de 6 de outubro de 2020, no processo C-623/17, *Privacy International* contra *Secretary of State for Foreign and Commonwealth Affairs* ([3]),

— Tendo em conta a sua Resolução, de 12 de março de 2014, sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos ([4]),

— Tendo em conta a sua Resolução, de 5 de julho de 2018, sobre o nível de proteção adequado assegurado pelo escudo de proteção da privacidade UE-EUA ([5]),

— Tendo em conta a sua Resolução, de 25 de outubro de 2018, sobre a utilização pela Cambridge Analytica de dados dos utilizadores do Facebook e o impacto na proteção de dados ([6]),

— Tendo em conta a sua Resolução, de 20 de maio de 2021, sobre o acórdão do TJUE de 16 de julho de 2020 — *Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems* («Schrems II») — Processo C-311/18 ([7]),

— Tendo em conta a sua resolução, de 26 de novembro de 2020, sobre a revisão da política comercial da UE ([8]),

— Tendo em conta o Acordo de Comércio e Cooperação, de 31 de dezembro de 2020, entre a União Europeia e a Comunidade Europeia da Energia Atómica, por um lado, e o Reino Unido da Grã-Bretanha e da Irlanda do Norte, por outro ([9]),

— Tendo em conta a sua Resolução, de 28 de abril de 2021, sobre o resultado das negociações entre a UE e o Reino Unido ([10]),

— Tendo em conta o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados ([11]) (RGPD),

---

([1]) ECLI:EU:C:2020:559.
([2]) ECLI:EU:C:2015:650.
([3]) ECLI:EU:C:2020:790.
([4]) JO C 378 de 9.11.2017, p. 104.
([5]) JO C 118 de 8.4.2020, p. 133.
([6]) JO C 345 de 16.10.2020, p. 58.
([7]) Textos Aprovados, P9_TA(2021)0256.
([8]) Textos Aprovados, P9_TA(2020)0337.
([9]) JO L 444 de 31.12.2020, p. 14.
([10]) Textos Aprovados, P9_TA(2021)0141.
([11]) JO L 119 de 4.5.2016, p. 1.

— Tendo em conta a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados ([12]) (Diretiva sobre a Proteção de Dados na Aplicação da Lei),

— Tendo em conta a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas ([13]),

— Tendo em conta a proposta da Comissão de um regulamento do Parlamento Europeu e do Conselho, de 10 de janeiro de 2017, relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas COM(2017)0010), bem como a posição do Parlamento Europeu sobre esta matéria, aprovada em 20 de outubro de 2017 ([14]),

— Tendo em conta as recomendações do Comité Europeu para a Proteção de Dados (CEPD), incluindo a sua declaração de 9 de março de 2021 sobre o Regulamento Privacidade Eletrónica e as suas recomendações 01/2020, de 10 de novembro de 2020, sobre as medidas que complementam os instrumentos de transferência a fim de assegurar o cumprimento do nível de proteção da UE dos dados pessoais,

— Tendo em conta o referencial de adequação adotado pelo Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, em 6 de fevereiro de 2018, e aprovado pelo CEPD,

— Tendo em conta as recomendações 01/2021 do CEPD, de 2 de fevereiro de 2021, sobre o referencial de adequação ao abrigo da Diretiva sobre a Proteção de Dados na Aplicação da Lei,

— Tendo em conta os projetos de decisão de adequação publicados pela Comissão em 19 de fevereiro de 2021, um nos termos do RGPD ([15]) e o outro nos termos da Diretiva sobre a Proteção de Dados na Aplicação da Lei ([16]),

— Tendo em conta os pareceres 14/2021 e 15/2021 do CEPD, de 13 de abril de 2021, sobre o projeto de decisão de execução da Comissão Europeia nos termos da Diretiva (UE) 2016/680 quanto à adequação do nível de proteção de dados pessoais no Reino Unido,

— Tendo em conta a Convenção Europeia dos Direitos Humanos (CEDH) e a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal do Conselho da Europa, bem como o respetivo protocolo adicional («Convenção 108 +»), de que o Reino Unido é parte,

— Tendo em conta o Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão,

— Tendo em conta o artigo 132.º, n.º 2, do Regimento,

— Tendo em conta a proposta de resolução da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos,

A. Considerando que a capacidade de transferir dados pessoais através das fronteiras pode ser um fator essencial de inovação, produtividade e competitividade económica, revestindo-se de importância crucial para uma cooperação eficaz na luta contra a criminalidade organizada e grave transfronteiriça, bem como para a luta contra o terrorismo, que depende cada vez mais do intercâmbio de dados pessoais;

B. Considerando que, no seu acórdão Schrems I, o TJUE salientou que o acesso indiscriminado dos serviços de informação ao conteúdo de comunicações eletrónicas viola o conteúdo essencial do direito à confidencialidade das comunicações, tal como previsto no artigo 7.º da Carta e que os Estados Unidos não preveem vias de recurso suficientes para cidadãos estrangeiros contra a vigilância em larga escala, em violação do artigo 47.º da Carta;

([12]) JO L 119 de 4.5.2016, p. 89.
([13]) JO L 201 de 31.7.2002, p. 37.
([14]) A8-0324/2017.
([15]) Projeto de decisão de execução da Comissão ao abrigo do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido.
([16]) Projeto de decisão de execução da Comissão ao abrigo da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido.

Sexta-feira, 21 de maio de 2021

C. Considerando que o Reino Unido tem sido tradicionalmente um importante parceiro comercial de muitos Estados-Membros da UE, bem como um aliado próximo no domínio da segurança; que a UE e o Reino Unido devem manter esta estreita cooperação apesar da saída do Reino Unido da UE, tendo em conta as vantagens para ambas as partes;

D. Considerando que as empresas europeias necessitam de clareza e segurança jurídicas, uma vez que a capacidade para transferir dados pessoais além fronteiras se tornou cada vez mais importante para todos os tipos de empresas que fornecem bens e prestam serviços à escala internacional; que uma decisão de adequação relativa ao Reino Unido ao abrigo do RGPD é de extrema importância, uma vez que muitas empresas europeias têm trocas comerciais através do Canal da Mancha, especialmente tendo em conta o facto de o Brexit ser ainda muito recente e os fluxos de dados dentro da União não estarem sujeitos a restrições; que a não adoção de um quadro de adequação sólido implicaria o risco de perturbações nas transferências comerciais transfronteiras de dados pessoais entre a UE e o Reino Unido, bem como elevados custos de conformidade;

E. Considerando que o Acordo de Comércio e Cooperação inclui um conjunto de salvaguardas e condições para o intercâmbio de dados pessoais pertinentes no contexto da aplicação da lei; que as negociações sobre os fluxos de dados pessoais decorreram em paralelo com as negociações sobre o Acordo de Comércio e Cooperação, mas não estavam concluídas no final do período de transição em 31 de dezembro de 2020; que foi incluída uma «cláusula-ponte» no Acordo de Comércio e Cooperação a título de solução provisória, subordinada ao compromisso do Reino Unido de não alterar o seu atual regime de proteção de dados, para garantir a continuação dos fluxos de dados pessoais entre o Reino Unido e a UE até à adoção de uma decisão de adequação; que o período inicial de quatro meses foi prorrogado e expirará no final de junho de 2021;

F. Salienta que a avaliação efetuada pela Comissão antes de apresentar o seu projeto de decisão de execução estava incompleta e era incompatível com os requisitos do TJUE para avaliações da adequação, o que foi destacado pelo CEPD nos seus pareceres de adequação, com a recomendação de que a Comissão deve avaliar mais aprofundadamente aspetos específicos da legislação ou da prática do Reino Unido relacionados com a recolha em larga escala, a divulgação no estrangeiro e os acordos internacionais no domínio da partilha de informações, da utilização adicional das informações recolhidas para fins de aplicação da lei e da independência dos comissários judiciais;

G. Considerando que alguns aspetos da legislação e/ou da prática do Reino Unido não foram considerados pela Comissão, o que se traduziu em projetos de decisões de execução que não são conformes com o direito da UE; considerando que o artigo 45.º do RGPD estipula que, ao avaliar a adequação do nível de proteção, a Comissão deve, em particular, ter em conta «(…) a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência (…)», e «(…) os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais», que inclui acordos internacionais noutras áreas envolvendo o acesso a dados ou a partilha de informações e, por conseguinte, requer uma avaliação de tais acordos internacionais;

H. Considerando que o TJUE afirmou claramente no acórdão Schrems I que «(…) ao examinar o nível de proteção oferecido por um país terceiro, a Comissão está obrigada a apreciar o conteúdo das regras aplicáveis nesse país que resultam da legislação interna ou dos seus compromissos internacionais, bem como a prática destinada a assegurar o respeito de tais regras, devendo, em conformidade com o artigo 25.º, n.º 2, da Diretiva 95/46/CE, tomar em conta todas as circunstâncias relativas a uma transferência de dados pessoais para um país terceiro» (n.º 75);

I. Considerando que, nos termos dos Tratados, as atividades dos serviços de informação e a partilha de dados com países terceiros estão excluídas do âmbito de aplicação do direito da UE no que diz respeito aos Estados-Membros, uma vez que são abrangidas pelo âmbito da avaliação da adequação necessária do nível de dados pessoais oferecido por países terceiros, como confirmado pelo TJUE nos acórdãos Schrems I e II;

J. Considerando que as normas de proteção de dados se baseiam não só na legislação em vigor, mas também na aplicação dessas leis na prática, e que a Comissão, ao preparar a sua decisão, apenas avaliou a legislação, e não a sua aplicação efetiva na prática;

K. Considerando que a Comissão reconhece atualmente 12 países terceiros que proporcionam proteção adequada ao abrigo do RGPD e que concluiu recentemente negociações com a República da Coreia a este respeito; que o Reino Unido é o primeiro país ao qual a Comissão propôs conceder a adequação ao abrigo da Diretiva sobre a proteção de dados na aplicação da lei;

L. Considerando que o caso do Reino Unido é distinto de todas as avaliações da adequação anteriores, pois diz respeito a um antigo Estado-Membro da UE que incorporou as disposições do RGPD no seu direito interno e que, além disso, previu que toda a «legislação nacional derivada da UE», incluindo a legislação que transpõe a Diretiva sobre a proteção de dados na aplicação da lei, continuará a ser aplicável após o final do período de transição;

I. **REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS**

Observações gerais

1. Observa que o Reino Unido é signatário da CEDH e da Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal; espera que o Reino Unido assegure o mesmo quadro mínimo de proteção de dados, apesar de ter saído da União Europeia;

2. Congratula-se com o compromisso do Reino Unido de respeitar a democracia e o Estado de direito, bem como de proteger e defender os direitos fundamentais a nível nacional, nomeadamente os consagrados na CEDH, incluindo um nível elevado de proteção de dados; recorda que se trata de uma condição prévia necessária para a cooperação da UE com o Reino Unido; relembra que, apesar de o artigo 8.º da CEDH sobre o direito à privacidade fazer parte do direito nacional do Reino Unido, mediante a Lei dos Direitos Humanos de 1998, e do direito consuetudinário, mediante o novo delito de utilização indevida de informações privadas, o governo votou contra os esforços destinados a incluir o direito fundamental à proteção de dados;

3. Salienta que a UE optou por uma abordagem centrada nos direitos humanos para a governação de dados ao desenvolver regras robustas em matéria de proteção de dados no RGPD e, por conseguinte, manifesta profunda preocupação face às declarações públicas do primeiro-ministro britânico, que afirmou que o Reino Unido irá procurar divergir das regras da UE em matéria de proteção de dados e estabelecer os seus próprios controlos «soberanos» nesse domínio; considera que a estratégia nacional de dados do Reino Unido de 2020 representa uma mudança da proteção dos dados pessoais para uma utilização e partilha mais abrangente dos dados, que é incompatível com os princípios da equidade, da minimização de dados e da limitação da finalidade ao abrigo do RGPD; observa que, nos seus pareceres de adequação, o CEPD realçou que tal pode conduzir a possíveis riscos no que respeita à proteção dos dados pessoais transferidos da UE;

4. Salienta que as decisões de adequação válidas contribuem significativamente para a proteção dos direitos fundamentais dos cidadãos e a segurança jurídica das empresas; frisa, no entanto, que as decisões de adequação baseadas em avaliações incompletas e sem a devida execução por parte da Comissão podem ter o efeito contrário quando contestadas em tribunal;

5. Sublinha que a avaliação efetuada pela Comissão antes de apresentar o seu projeto de decisão de execução estava incompleta e era incompatível com os requisitos do TJUE para avaliações da adequação, o que foi destacado pelo CEPD nos seus pareceres de adequação, com a recomendação de que a Comissão deve avaliar mais aprofundadamente aspetos específicos da legislação ou da prática do Reino Unido relacionados com a recolha em larga escala, a divulgação no estrangeiro e os acordos internacionais no domínio da partilha de informações, da utilização adicional das informações recolhidas para fins de aplicação da lei e da independência dos comissários judiciais;

Aplicação do RGPD

6. Manifesta preocupação relativamente à aplicação deficiente, e muitas vezes à não aplicação, do RGPD pelo Reino Unido, quando o país ainda era membro da UE; chama a atenção, em particular, para a falta de uma aplicação adequada da legislação em vigor pela autoridade britânica para a proteção de dados no passado; destaca como exemplo o facto de a autoridade britânica para a proteção de dados ter arquivado uma queixa relacionada com a tecnologia de publicidade após realizar dois eventos com as partes interessadas e de ter elaborado um relatório (o «Update Report on Adtech») e declarado que «o setor da tecnologia de publicidade revela imaturidade na sua compreensão dos requisitos de proteção de dados»,

embora sem recorrer a nenhum dos seus poderes de execução ([17]); está preocupado com o facto de a não aplicação ser um problema estrutural, tal como previsto na política de ação regulamentar da autoridade britânica para a proteção de dados, que declara explicitamente que «na maioria dos casos, reservaremos os nossos poderes para os casos mais graves, que representem as violações mais graves das obrigações em matéria de direitos de informação. Estas situações envolvem, normalmente, atos intencionais, deliberados ou negligentes, ou violações repetidas das obrigações em matéria de direitos de informação, que causem danos ou prejuízos aos cidadãos»; sublinha que, na prática, tal significa que um número significativo de situações de violação da legislação em matéria de proteção de dados não foram corrigidas;

7. Toma nota da estratégia nacional do Reino Unido em matéria de dados, atualizada em 9 de dezembro de 2020, que sugere que haverá uma transição da proteção dos dados pessoais para uma maior e mais ampla utilização e partilha de dados; salienta que uma posição segundo a qual a retenção de dados pode ter um impacto negativo na sociedade, conforme referido na estratégia, não é compatível com os princípios de minimização de dados e limitação da finalidade ao abrigo do RGPD e do direito primário;

8. Regista que a Comissão dos Assuntos Constitucionais, em 2004 ([18]), e a Comissão dos Assuntos Públicos do Parlamento do Reino Unido, em 2014 ([19]), recomendaram que se garantisse a independência da autoridade britânica para a proteção de dados concedendo-lhe o estatuto de oficial do Parlamento, perante o qual passaria a responder, em vez de continuar a ser nomeada pelo Ministro das Tecnologias Digitais e do Desporto; lamenta que esta recomendação não tenha sido seguida;

Tratamento de dados para fins de controlo da imigração

9. Assinala que a legislação do Reino Unido em matéria de proteção de dados contém uma derrogação a certos aspetos dos direitos e princípios fundamentais da proteção de dados, como o direito de acesso e o direito de o titular dos dados saber com quem os seus dados foram partilhados, caso essa proteção prejudique o controlo efetivo da imigração; salienta que o acompanhamento e o cumprimento da utilização da isenção devem ser efetuados em consonância com as normas exigidas no referencial de adequação, que requerem a consideração tanto da prática como dos princípios, salientando que «é necessário considerar não só o conteúdo das regras aplicáveis aos dados pessoais transferidos para um país terceiro […] como também o sistema em vigor para garantir a eficácia de tais regras»; reconhece que esta isenção, que é acessível a todos os responsáveis pelo tratamento de dados no Reino Unido, foi aprovada pela autoridade britânica para a proteção de dados e por um tribunal, podendo apenas ser invocada caso a caso e aplicada de forma necessária e proporcionada; recorda as informações recentemente reveladas, segundo as quais foram apresentados 17 780 pedidos de acesso em relação a dados tratados pelo Ministério da Administração Interna, entre 1 de abril de 2018 e 31 de março de 2019, relativos a 146,75 milhões de titulares de dados e que a isenção relativa à imigração foi utilizada em mais de 70 % dos pedidos dos titulares de dados junto do Ministério da Administração Interna do Reino Unido em 2020 ([20]); salienta que, mesmo nos casos em que o Ministério da Administração Interna do Reino Unido fez uso da derrogação, o acesso à informação não foi totalmente negado, mas foi limitado a documentos em versões rasuradas;

10. Observa que essa isenção já se aplica aos cidadãos da UE que residem ou pretendam residir no Reino Unido; manifesta profunda preocupação com o facto de a isenção eliminar as principais possibilidades de responsabilização e vias de recurso e salienta que este não constitui um nível de proteção adequado;

([17]) Lomas, N., *UK's ICO faces legal action after closing adtech complaint with nothing to show for it* [A autoridade britânica para a proteção de dados enfrenta uma ação judicial após ter encerrado o processo relativo a uma queixa sobre a tecnologia de publicidade sem apresentar quaisquer elementos justificativos], TechCrunch, San Francisco, 2020.

([18]) Sétimo Relatório da Comissão dos Assuntos Constitucionais, publicado pela Câmara dos Comuns, em 13 de junho de 2006. No ponto 108 pode ler-se o seguinte: «Consideramos que a possibilidade de a autoridade britânica para a proteção de dados passar a responder diretamente ao Parlamento e ser por este financiada apresenta um mérito considerável e recomendamos que tal seja tido em consideração quando surgir uma oportunidade para alterar a legislação».

([19]) Relatório da Comissão da Administração Pública intitulado «Who's accountable? Relationships between Government and arm's-length bodies» [Quem é responsável? Relações entre o governo e os órgãos independentes], publicado pela Câmara dos Comuns em 4 de novembro de 2014. No ponto 64 pode ler-se o seguinte: «A autoridade britânica para a proteção de dados e o HM Inspectorate of Prisons (órgão de inspeção) devem tornar-se mais independentes do Governo e responder perante o Parlamento. A autoridade para a proteção de dados (Information Commissioner), a autoridade para nomeações públicas (Commissioner for Public Appointments) e o presidente do Comité de Normas na Vida Pública (Committee on Standards in Public Life) devem tornar-se oficiais do Parlamento, como já o são o Provedor de Justiça Parlamentar e dos Serviços de Saúde (Parliamentary and Health Service Ombudsman) e o Supervisor e Presidente do Tribunal de Contas (Comptroller and Auditor General)».

([20]) Comunicado de imprensa do Open Rights Group, de 3 de março de 2021, intitulado «Documents reveal controversial Immigration Exemption used in 70 % of access requests to Home Office» (Documentos revelam isenção controversa relativa à imigração em 70 % dos pedidos de acesso enviados ao Ministério da Administração Interna do Reino Unido).

11. Reitera a sua grande preocupação relativamente a uma exceção aos direitos dos titulares de dados na política de imigração do Reino Unido; reitera a sua posição de que a isenção para o processamento de dados pessoais para fins de imigração da Lei de Proteção de Dados do Reino Unido necessita de ser alterada antes que uma decisão de adequação válida possa ser emitida, conforme repetidamente expresso, nomeadamente na sua resolução, de 12 de fevereiro de 2020, sobre a nova parceria com o Reino Unido da Grã-Bretanha e da Irlanda do Norte ([21]) e no parecer da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos, de 5 de fevereiro de 2021 ([22]); exorta a Comissão a tomar medidas com vista à eliminação da isenção relativa à imigração ou a assegurar que seja reformada de modo que a isenção e a sua utilização proporcionem salvaguardas suficientes para os titulares dos dados e não violem as normas esperadas de um país terceiro;

Vigilância em larga escala

12. Recorda as revelações do denunciante Edward Snowden sobre a vigilância em larga escala por parte dos EUA e do Reino Unido; relembra que o programa «Tempora» do Reino Unido, gerido pelo Government Communications Headquarters (GCHQ), interceta comunicações em tempo real através de cabos de fibra ótica da infraestrutura de base da Internet e grava os dados, para que possam ser tratados e analisados posteriormente; recorda que esta vigilância em larga escala dos conteúdos e metadados das comunicações tem lugar independentemente da existência de suspeitas específicas ou de quaisquer dados alvo;

13. Recorda que, nos acórdãos Schrems I e Schrems II, o TJUE considerou que o acesso em larga escala ao conteúdo das comunicações privadas afeta a essência do direito à privacidade e que, em tais casos, um teste de necessidade e proporcionalidade deixa de ser necessário; sublinha que estes princípios se aplicam às transferências de dados para outros países terceiros que não os EUA, incluindo o Reino Unido;

14. Recorda a sua resolução, de 12 de março de 2014, que considerou que os programas de vigilância em larga escala, de forma indiscriminada e sem base em suspeitas, executados pelos serviços de informação GCHQ, são incompatíveis com os princípios da necessidade e da proporcionalidade numa sociedade democrática e não são adequados ao abrigo da legislação da UE em matéria de proteção de dados; reconhece que, desde então, o Reino Unido reformou, significativamente, a sua legislação em matéria de vigilância e introduziu salvaguardas que vão além das condições definidas pelo Tribunal de Justiça da União Europeia (TJUE) no seu Acórdão Schrems II ([23]) e das salvaguardas previstas na legislação em matéria de vigilância da maioria dos Estados-Membros; congratula-se, em particular, com a disposição que prevê o pleno acesso a vias de recurso judicial eficazes; recorda que o Relator Especial das Nações Unidas sobre o Direito à Privacidade saudou as salvaguardas sólidas introduzidas pelo «Investigatory Powers Act (IPA)2016» (Lei de 2016 relativa à regulamentação das competências de investigação) em termos de necessidade, proporcionalidade e autorização independente por um órgão judicial;

15. Recorda que, em setembro de 2018, o Tribunal Europeu dos Direitos Humanos confirmou que os programas do Reino Unido de interceção e conservação de dados em larga escala, nomeadamente o programa Tempora, eram «ilegais e incompatíveis com as condições necessárias para uma sociedade democrática» ([24]);

16. Considera inaceitável o facto de os projetos de decisões de adequação não terem em conta a falta de limitações à utilização das capacidades do Reino Unido em matéria de dados em larga escala ou a utilização efetiva das operações de vigilância do Reino Unido e dos EUA, tal como divulgado por Edward Snowden, incluindo os seguintes factos;

a) não existe supervisão substantiva efetiva por parte da autoridade para a proteção de dados ou dos tribunais relativamente à utilização da isenção de segurança nacional na legislação em matéria de proteção de dados do Reino Unido;

b) as limitações sobre a utilização de «competências em larga escala» do Reino Unido não estão estabelecidas na própria lei, conforme exigido pelo TJUE (ao invés, são deixadas ao arbítrio executivo, sujeitas a um controlo judicial «respeitoso»);

([21]) Textos Aprovados, P9_TA(2020)0033.

([22]) Parecer da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos sobre a celebração, em nome da União Europeia, do Acordo de Comércio e Cooperação entre a União Europeia e a Comunidade Europeia da Energia Atómica, por um lado, e o Reino Unido da Grã-Bretanha e da Irlanda do Norte, por outro, e do Acordo entre a União Europeia e o Reino Unido da Grã-Bretanha e da Irlanda do Norte sobre os Procedimentos de Segurança para o Intercâmbio e a Proteção de Informações Classificadas, LIBE_AL (2021)680848.

([23]) Acórdão de 16 de julho de 2020, *Data Protection Commissioner* contra *Facebook Ireland Limited* e *Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559.

([24]) Acórdão do Tribunal Europeu dos Direitos Humanos, de 13 de setembro de 2018, *Big Brother Watch e o.* contra o Reino Unido, processos n.os 58170/13, 62322/14 e 24960/15.

c) a descrição de «dados secundários» (metadados) nos projetos de decisão é gravemente enganosa e não refere que tais dados podem ser altamente reveladores e intrusivos e que estão sujeitos a análises automatizadas sofisticadas (conforme o TJUE apurou no caso da *Digital Rights Ireland* ([25])); no entanto, de acordo com a legislação do Reino Unido, os metadados não são significativamente protegidos contra o acesso indevido, a recolha em larga escala e a análise baseada em IA pelos serviços de informação do Reino Unido;

d) que as agências «Five Eyes», nomeadamente o GCHQ e a Agência de Segurança Nacional (NSA), na prática, partilham todos os dados confidenciais;

assinala, além disso, que, em relação aos EUA, os cidadãos do Reino Unido estão sujeitos a algumas salvaguardas informais entre o GCHQ e a NSA; manifesta profunda preocupação com o facto de essas salvaguardas não protegerem os cidadãos ou residentes da UE cujos dados possam ser objeto de transferências ulteriores e partilha com a NSA;

17. Exorta os Estados-Membros a celebrarem acordos de não espionagem com o Reino Unido e insta a Comissão a utilizar os seus intercâmbios com os seus homólogos do Reino Unido para transmitir a mensagem de que, se as leis e as práticas de vigilância do Reino Unido não forem alteradas, a única opção viável para facilitar as decisões de adequação seria a celebração de acordos de «não espionagem» com os Estados-Membros;

Transferências ulteriores

18. Realça com firmeza o facto de a Lei de 2018 sobre a (Retirada da) União Europeia (European Union (Withdrawal) Act 2018) prever que a jurisprudência do TJUE criada antes do termo do período de transição ser mantida no direito interno e, por conseguinte, ser juridicamente vinculativa para o Reino Unido; salienta que o Reino Unido está vinculado pelos princípios e condições definidos nos acórdãos Schrems I e Schrems II do TJUE quando avalia a adequação de outros países terceiros; manifesta preocupação com o facto de os tribunais do Reino Unido deixarem de aplicar a Carta; chama a atenção para o facto de o Reino Unido já não estar sob a jurisdição do TJUE, a instância máxima que pode interpretar a Carta;

19. Assinala que as regras do Reino Unido relativas à partilha de dados pessoais ao abrigo da Lei da Economia Digital de 2017 e às transferências ulteriores de dados de investigação claramente não são «essencialmente equivalentes» às regras estabelecidas no RGPD, segundo a interpretação do TJUE;

20. Manifesta preocupação com facto de o Reino Unido se ter concedido o direito de declarar que outros países terceiros ou territórios proporcionam uma proteção de dados adequada, independentemente de a UE ter determinado se os países terceiros ou territórios em causa proporcionam ou não uma proteção de dados adequada; relembra que o Reino Unido já declarou que Gibraltar oferece essa proteção, embora a UE não o tenha feito; manifesta profunda preocupação com o facto de o estatuto de adequação do Reino Unido permitir, por conseguinte, contornar as regras da UE em matéria de transferências para países ou territórios que não são considerados adequados ao abrigo da legislação da UE;

21. Regista que, em 1 de fevereiro de 2021, o Reino Unido enviou um pedido de adesão ao Acordo Global e Progressivo de Parceria Transpacífico (CPTTP), em particular «para tirar partido das regras modernas de comércio digital que permitem a livre circulação de dados entre os membros e eliminam os obstáculos desnecessários às empresas [etc.]»; observa com preocupação que o CPTTP tem onze membros e que oito deles não dispõem de uma decisão de adequação da UE; manifesta profunda preocupação face às potenciais transferências ulteriores de dados pessoais de cidadãos e residentes da UE para esses países, caso seja concedida uma decisão de adequação ao Reino Unido ([26]);

([25]) Acórdão do Tribunal de Justiça de 8 de abril de 2014, *Digital Rights Ireland Ltd* contra *Minister for Communications, Marine and Natural Resources e o.* e *Kärntner Landesregierung* e o., C-293/12 e C-594/12, ECLI:EU:C:2014:238.

([26]) Comunicado de imprensa do Ministério do Comércio Internacional do Reino Unido, de 30 de janeiro de 2021, intitulado «UK applies to join huge Pacific free trade area CPTPP» [Reino Unido solicita a adesão à grande zona de comércio livre do Pacífico CPTPP].

22. Lamenta que a Comissão não tenha avaliado o impacto e os riscos potenciais do Acordo entre o Reino Unido da Grã-Bretanha e da Irlanda do Norte e o Japão para uma Parceria Económica Abrangente, que inclui disposições em matéria de dados pessoais e de nível da proteção de dados;

23. Receia que, caso o Reino Unido inclua disposições sobre transferências de dados em acordos comerciais futuros, nomeadamente com os EUA, o nível de proteção proporcionado pelo RGPD seja comprometido;

II. **DIRETIVA SOBRE A PROTEÇÃO DE DADOS NA APLICAÇÃO DA LEI**

24. Destaca que o Reino Unido é o primeiro país relativamente ao qual a Comissão sugeriu adotar uma decisão de adequação ao abrigo da Diretiva (UE) 2016/680;

25. Toma nota do acordo de acesso transfronteiriço a dados entre o Reino Unido e os EUA ([27]), ao abrigo da Lei CLOUD dos EUA, que facilita as transferências para fins de aplicação da lei; manifesta profunda preocupação com o facto de tal permitir o acesso indevido das autoridades dos EUA a dados pessoais dos cidadãos e residentes da UE; partilha a preocupação do CEPD quanto à possibilidade de as salvaguardas previstas no Acordo-Quadro UE-EUA ([28]), aplicadas numa base *mutatis mutandis*, não cumprirem os critérios de regras claras, precisas e acessíveis no que diz respeito ao acesso aos dados pessoais, ou não terem um estatuto jurídico que garanta a sua eficácia e exequibilidade ao abrigo da legislação do Reino Unido;

26. Recorda que o acórdão C-623/17 do TJUE deve ser interpretado como excluindo a legislação nacional que permite que uma autoridade estatal exija que os prestadores de serviços de comunicações eletrónicas procedam à transmissão geral e indiscriminada de dados de tráfego e de localização aos serviços de segurança e de informação do Estado com o objetivo de salvaguardar a segurança nacional;

27. Observa que, neste caso, o TJUE considerou ilegal a recolha de dados em larga escala realizada no Reino Unido nos termos da lei de 2000 relativa à regulamentação das competências de investigação (Regulation of Investigatory Powers Act 2000); refere que essa lei foi entretanto substituída pela IPA 2016, a lei relativa aos poderes de investigação (Investigatory Powers Act), a fim de reforçar os princípios da necessidade e da proporcionalidade; sublinha que a IPA 2016 subordina a interceção ao controlo judicial e habilita as pessoas a aceder aos seus dados e a apresentar queixas junto do tribunal competente em matéria de investigação; lamenta, no entanto, que a IPA 2016 continue a permitir a prática de conservação de dados em larga escala;

28. Manifesta preocupação relativamente aos recentes relatos de que um sistema de recolha e conservação de dados em larga escala fez parte de um teste realizado pelo Ministério da Administração Interna do Reino Unido ao abrigo da IPA 2016;

29. Recorda que, na sua resolução de 12 de fevereiro de 2020, o Parlamento Europeu salientou que «o Reino Unido não pode ter acesso direto aos dados dos sistemas de informação da UE ou participar nas estruturas de gestão das agências da UE no domínio da liberdade, segurança e justiça, ao passo que qualquer partilha de informações — incluindo dados pessoais com o Reino Unido — deve estar subordinada a condições rigorosas em matéria de salvaguardas, auditoria e de supervisão, incluindo um nível de proteção dos dados pessoais equivalente ao previsto no direito da UE»; constata as lacunas identificadas na forma como o Reino Unido aplicou a legislação em matéria de proteção de dados, quando ainda era membro da UE; recorda que o Reino Unido estava a gravar e a conservar uma cópia do Sistema de Informação Schengen (SIS); espera que os serviços responsáveis pela aplicação da lei do Reino Unido, no futuro, cumpram integralmente as normas aplicáveis no quadro do intercâmbio de dados pessoais; relembra que o Reino Unido mantém o acesso a algumas bases de dados dos serviços de aplicação da lei da UE apenas com base num sistema de respostas positivas/negativas e está legalmente impedido de aceder ao SIS;

([27]) Acordo entre o Governo do Reino Unido da Grã-Bretanha e da Irlanda do Norte e o Governo dos Estados Unidos da América, de 3 de outubro de 2019, sobre o acesso a dados eletrónicos para efeitos de combate à criminalidade grave.

([28]) Acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais (JO L 336 de 10.12.2016, p. 3).

30. Manifesta-se preocupado por se ter descoberto, em janeiro de 2021, que 400 000 registos criminais foram apagados acidentalmente da base de dados nacional da polícia do Reino Unido; salienta que tal não contribui para a confiança nos esforços do Reino Unido em matéria de proteção de dados para fins de aplicação da lei;

31. Observa que o projeto de decisão de adequação avalia exaustivamente os direitos de cada autoridade do Reino Unido habilitada pelo direito nacional a intercetar e a conservar dados pessoais para fins de segurança nacional; congratula-se, além disso, com o facto de os relatórios de supervisão detalhados relativos às autoridades responsáveis pela comunidade de informações de segurança fornecerem informações sobre as atuais práticas de vigilância do Reino Unido; exorta a Comissão a continuar a avaliar e a controlar os tipos de dados de comunicações abrangidos pelas capacidades de conservação e de interceção legal de dados do Reino Unido;

32. Refere que o Acordo de Comércio e Cooperação UE-Reino Unido inclui títulos relativos ao intercâmbio de ADN, impressões digitais e dados de registo de veículos, à transferência e tratamento de dados do registo de identificação dos passageiros (PNR), à cooperação em matéria de informações operacionais e à cooperação com a Europol e a Eurojust, que serão aplicáveis independentemente da decisão de adequação; recorda, no entanto, as preocupações manifestadas no parecer da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos, de fevereiro de 2021, sobre o Acordo de Comércio e Cooperação no que diz respeito à utilização especial e ao prolongamento da conservação de dados pessoais concedidos ao Reino Unido ao abrigo dos títulos Prüm e PNR do Acordo, que não estão em conformidade com a utilização e conservação pelos Estados-Membros; relembra o direito de interpor uma ação perante o TJUE, a fim de solicitar a verificação da legalidade do acordo internacional proposto e, nomeadamente, da sua compatibilidade com a proteção de um direito fundamental ([29]);

Conclusões

33. Insta a Comissão a garantir às empresas da UE que a decisão de adequação irá proporcionar uma base jurídica sólida, suficiente e orientada para o futuro no que diz respeito às transferências de dados; sublinha a importância de assegurar que essa decisão de adequação seja considerada aceitável se for revista pelo TJUE e salienta que todas as recomendações formuladas no parecer do CEPD devem, por conseguinte, ser tidas em conta;

34. Congratula-se com o facto de as decisões de adequação se aplicarem apenas durante quatro anos, uma vez que o Reino Unido, agora que já não é um Estado-Membro da UE, pode optar por alterar a legislação sujeita à avaliação de adequação da Comissão; solicita à Comissão que, entretanto, continue a acompanhar o nível de proteção de dados no Reino Unido, tanto em termos de legislação, como de práticas, e que realize uma avaliação exaustiva antes de renovar a decisão de adequação em 2025;

35. Considera que, ao adotar as duas decisões de execução, as quais não são compatíveis com o direito da UE, sem ter abordado todas as preocupações expressas na presente resolução, a Comissão excede as competências de execução conferidas pelo Regulamento (UE) 2016/679 e pela Diretiva (UE) 2016/680; opõe-se, por conseguinte, aos dois atos de execução, por considerar que os projetos de decisão de execução não são compatíveis com o direito da UE;

36. Exorta a Comissão a alterar os dois projetos de decisões de execução, a fim de os tornar plenamente coerentes com o direito e a jurisprudência da UE;

37. Solicita que as autoridades nacionais de proteção de dados suspendam a transferência de dados pessoais que possam estar sujeitos a acesso indiscriminado pelos serviços de informação do Reino Unido, caso a Comissão adote as suas decisões de adequação em relação ao Reino Unido antes de este resolver as questões supracitadas;

38. Exorta a Comissão e as autoridades competentes do Reino Unido a elaborarem um plano de ação, a fim de corrigir o mais rapidamente possível as deficiências identificadas pelos pareceres do CEPD e outras questões pendentes na proteção de dados do Reino Unido, enquanto condição prévia para a decisão final de adequação;

39. Solicita à Comissão que continue a acompanhar de perto o nível de proteção de dados, bem como as leis e as práticas em matéria de vigilância em larga escala no Reino Unido; refere que existem outras possibilidades jurídicas de transferência de dados pessoais para o Reino Unido no Capítulo V do RGPD; recorda que, em consonância com as orientações do CEPD, as transferências baseadas em derrogações para situações específicas nos termos do artigo 49.º do RGPD devem ser excecionais;

([29]) Resolução do Parlamento Europeu sobre um projeto de Decisão da Comissão que verifica o nível de proteção adequado dos dados pessoais contidos nos dados do registo de identificação dos passageiros (PNR) transmitidos aos serviços das alfândegas e da proteção das fronteiras dos Estados Unidos (JO C 103 E de 29.4.2004, p. 665).

40. Lamenta que a Comissão tenha ignorado os apelos do Parlamento para suspender o Escudo de Proteção da Privacidade até que as autoridades dos EUA cumpram os seus termos, preferindo sempre, ao invés, «supervisionar a situação» sem qualquer resultado concreto em termos de proteção de dados para os cidadãos e de segurança jurídica para as empresas; insta a Comissão a aprender com os erros do passado, nomeadamente o facto de ter ignorado os apelos do Parlamento e de peritos no que respeita à execução e ao acompanhamento das decisões de adequação anteriores e o facto de não deixar a aplicação adequada da legislação da UE em matéria de proteção de dados a cargo do TJUE na sequência de queixas apresentadas por cidadãos;

41. Exorta a Comissão a acompanhar de perto a legislação e as práticas em matéria de proteção de dados no Reino Unido, a informar e consultar imediatamente o Parlamento sobre quaisquer alterações futuras ao regime de proteção de dados do Reino Unido e a conferir ao Parlamento um papel de controlo no novo quadro institucional, nomeadamente no que diz respeito a organismos relevantes, como o Comité Especializado da Aplicação da Lei e Cooperação Judiciária;

o

o o

42. Encarrega o seu Presidente de transmitir a presente resolução à Comissão, aos Estados-Membros e ao Governo do Reino Unido.