

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

Síntese do parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Restabelecer a confiança nos fluxos de dados entre a UE e os EUA» e sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na EU

(O texto integral do presente parecer está disponível em alemão, francês e inglês no sítio web da AEPD em www.edps.europa.eu)

(2014/C 116/04)

I. Introdução

I.1. Consulta da AEPD

1. Em 27 de novembro de 2013, a Comissão adotou a Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Restabelecer a confiança nos fluxos de dados entre a UE e os EUA»⁽¹⁾ (a seguir «a Comunicação sobre o restabelecimento da confiança»). Esta Comunicação é acompanhada por um relatório sobre as conclusões dos copresidentes da UE do grupo de trabalho *ad hoc* UE-EUA sobre proteção de dados (a seguir, «o Relatório» e «o Grupo de Trabalho»).
2. Na mesma data, a Comissão adotou a Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE⁽²⁾ (a seguir, «a Comunicação sobre o sistema “porto seguro”»).
3. A AEPD congratula-se com o facto de lhe ter sido dada a oportunidade de apresentar observações informais à Comissão antes da adoção dos documentos supramencionados. Estes documentos foram adotados no rescaldo das revelações sobre os programas de vigilância executados pelos serviços de informação dos EUA. Tendo em conta o impacto destes programas de vigilância nos direitos das pessoas ao respeito pela vida privada e à proteção dos seus dados pessoais na UE, a AEPD decidiu adotar o presente parecer por iniciativa própria.

I.2. Objetivo e âmbito dos documentos da Comissão

a) A Comunicação sobre o restabelecimento da confiança e o Relatório

4. A Comunicação propõe o caminho a seguir após as revelações sobre os programas norte-americanos de recolha de informações em grande escala (a seguir, «os programas» ou «os programas revelados») e o seu impacto na confiança entre a UE e os EUA. Este documento não diz respeito a revelações sobre a condução de atividades semelhantes por Estados-Membros da UE ou por outros países terceiros e/ou sobre a colaboração destes com os EUA.
5. O Relatório reúne as conclusões dos copresidentes da UE do grupo de trabalho *ad hoc* UE-EUA sobre proteção de dados que foi criado no seguimento da reunião do Coreper de 18 de julho de 2013 com vista a apurar os factos sobre os programas e o seu impacto nos direitos fundamentais da UE e nos dados pessoais dos cidadãos da UE. Analisa o quadro jurídico norte-americano⁽³⁾, o modo de recolha e tratamento posterior dos dados⁽⁴⁾ e os atuais mecanismos de fiscalização e reparação.

⁽¹⁾ COM(2013) 846 final.

⁽²⁾ COM(2013) 847 final.

⁽³⁾ Em especial, a Constituição, tal como interpretada pelo Supremo Tribunal de Justiça; o artigo 702.º do *Foreign Intelligence Surveillance Act*, de 1978 (FISA) (com a redação que lhe foi dada pelo *2008 FISA Amendments Act*, 50 U.S.C. § 1881a); e o artigo 215.º do *USA PATRIOT Act*, de 2001 (que também alterou o FISA, 50 U.S.C. 1861) e o Decreto Executivo n.º 12333.

⁽⁴⁾ Com base nas informações prestadas pelos EUA no Grupo de Trabalho e em documentos desclassificados, incluindo pareceres do *Foreign Intelligence Surveillance Court* (a seguir, «FISC») e documentos publicamente disponíveis, tais como as diretrizes do Advogado-Geral sobre as operações internas do FBI (*Attorney's Guidelines for Domestic FBI Operations*).

6. O Relatório menciona uma «segunda via», igualmente estabelecida durante a reunião do Coreper de 18 de julho de 2013, esclarecendo que, ao abrigo desta «segunda via», as instituições da UE podem suscitar junto das autoridades norte-americanas questões relacionadas com a alegada vigilância de instituições e missões diplomáticas da UE, ao passo que os Estados-Membros podem discutir com as autoridades norte-americanas, num formato bilateral, assuntos relacionados com a sua segurança nacional.
 7. O Relatório refere ainda que esta divisão impõe alguns limites ao debate no seio do Grupo de Trabalho e às informações nele fornecidas. A AEPD não recebeu quaisquer informações sobre a «segunda via» nem sobre a criação de um grupo de trabalho paralelo sobre esta matéria. Por conseguinte, a Comissão é convidada a informar a AEPD sobre as conclusões da «segunda via», sobretudo no que respeita à alegada vigilância de instituições e missões diplomáticas da UE.
- b) A Comunicação sobre o sistema «porto seguro»
8. A Comunicação sobre o sistema «porto seguro» analisa o funcionamento do sistema «porto seguro», identifica deficiências e propõe possíveis melhorias. Reconhece o aumento do volume de dados transferidos entre a UE e os EUA e o crescente número de empresas que aderiram aos princípios de «porto seguro». Depois de recordar a estrutura e o funcionamento do sistema «porto seguro», a Comissão reitera a necessidade de melhorar a fiscalização do cumprimento daqueles princípios pelas empresas participantes e pelos respetivos subcontratantes. Segundo a Comissão, tal exigiria que os princípios de «porto seguro» fossem incorporados de forma mais eficaz nas políticas de proteção da vida privada das empresas participantes e que estas políticas fossem disponibilizadas ao público. A Comissão Federal do Comércio deveria adotar uma abordagem mais proativa na fiscalização do seu cumprimento. Por outro lado, as autoridades responsáveis pela proteção de dados deveriam participar na sensibilização para o sistema «porto seguro» na UE e, em especial, para a existência do painel de proteção dos dados da UE. A Comissão também propõe soluções para melhorar os mecanismos de resolução alternativa de litígios.
 9. No que respeita ao acesso a dados transferidos no quadro do sistema «porto seguro» e tratados posteriormente por autoridades norte-americanas, a Comissão reafirma que se deve limitar ao que for estritamente necessário e proporcional. Exige ainda que o recurso a derrogações às políticas de proteção da vida privada para satisfazer requisitos de segurança nacional, interesse público ou execução legal seja cuidadosamente controlado para não comprometer a proteção conferida. Incentiva igualmente as empresas participantes a serem transparentes em relação a estas derrogações e ao seu efeito sobre a confidencialidade das comunicações a fim de sensibilizar os cidadãos.

I.3. *Âmbito e objetivo do presente parecer*

10. O presente parecer tem por objeto a Comunicação sobre o restabelecimento da confiança e, nesse contexto, também a Comunicação sobre o sistema «porto seguro». Consequentemente, não tece diretamente quaisquer comentários sobre revelações respeitantes à atuação dos Estados-Membros, seja em colaboração com os EUA ou isoladamente, nem sobre as atividades de vigilância realizadas por países terceiros diferentes dos EUA.
11. O parecer começa por comentar a abordagem geral da Comunicação sobre o restabelecimento da confiança. Na parte II, é apresentada uma análise sucinta da aplicabilidade do quadro jurídico relevante e das suas consequências, incluindo observações sobre a Comunicação sobre o sistema «porto seguro». Uma vez que o Grupo de Trabalho do artigo 29.º⁽¹⁾ está atualmente a analisar o quadro jurídico europeu e internacional aplicável, o presente parecer não se debruçará, em pormenor, sobre esta matéria. A parte III diz respeito às recomendações da Comissão sobre as medidas a adotar no futuro.

I.4. *Observações sobre a abordagem da Comunicação sobre o restabelecimento da confiança*

12. A Comunicação centra-se no facto de a confiança entre a UE e os EUA, enquanto parceiros estratégicos, ter sido abalada pelas revelações sobre os programas e de ser necessário restabelecê-la. A AEPD congratula-se com o reconhecimento deste facto.

(1) O Grupo de Trabalho do artigo 29.º sobre a proteção de dados, criado ao abrigo da Diretiva 95/46/CE, tem natureza consultiva e é independente no desempenho das suas funções. É composto por representantes das autoridades nacionais para a proteção de dados da UE, pela AEPD e pela Comissão.

13. Porém, os programas, cuja existência é, em alguns casos, claramente confirmada pelo Relatório,⁽¹⁾ afetam não apenas a confiança, como também os direitos consagrados no direito primário e secundário da UE e do Conselho da Europa, em especial os direitos ao respeito pela vida privada e à proteção de dados. Revelam igualmente a recolha de informações estrangeiras em grande escala atualmente em curso ao abrigo do quadro jurídico norte-americano⁽²⁾, conforme interpretado pelo Supremo Tribunal de Justiça dos EUA⁽³⁾. O Relatório confirma ainda o facto de o quadro norte-americano não contemplar garantias, proteção, direitos, supervisão e mecanismos de reparação para os cidadãos da UE⁽⁴⁾.
14. Tal como tem sido repetidamente sublinhado pela Comissão, a confiança dos cidadãos e das empresas nas comunicações através da Internet depende da existência de ferramentas técnicas eficazes de proteção da privacidade e, mais concretamente, da confidencialidade das informações. Esta necessidade também foi reconhecida no Grupo de Análise sobre Tecnologias da Informação e Comunicação dos EUA,⁽⁵⁾ que emitiu várias recomendações para restabelecer a confiança em *software* comercial e ferramentas de encriptação, bem como no funcionamento de mecanismos rápidos de correção de vulnerabilidades do *software*. A deterioração da confiança nestes sistemas tem sido considerada um dos efeitos mais nefastos do recente debate sobre as chamadas operações de *signal intelligence* (que abrangem informações eletrónicas e informações sobre transmissões) por alguns dos mais conceituados peritos em segurança⁽⁶⁾. Tendo em conta a importância de uma cibersegurança eficaz para Europa, importa formular uma resposta a este desafio técnico e político ao nível da UE com base numa iniciativa da Comissão.
15. Na secção 3 da Comunicação, a Comissão aborda as medidas que será necessário adotar no futuro para restabelecer a confiança nas transferências de dados entre a UE e os EUA. A AEPD congratula-se com esta secção, dado que incide sobre a melhoria do quadro jurídico em vigor e propõe novos instrumentos. Contudo, a Comissão não refere o modo como os instrumentos nacionais, da UE e do Conselho da Europa aplicáveis foram afetados pelos programas. A AEPD considera que o impacto sobre os instrumentos jurídicos existentes deveria ter recebido mais atenção na Comunicação.

IV. Observações finais

79. A AEPD congratula-se com as medidas ponderadas pela Comissão, mas salienta que as atividades de vigilância dos serviços de informação norte-americanos em causa não afetam apenas a confiança nos fluxos de dados entre a UE e os EUA. Estas atividades também têm repercussões sobre os atuais direitos dos cidadãos da UE ao respeito pela vida privada e à proteção dos seus dados pessoais, direitos esses que são suscetíveis de aplicação coerciva. Estes direitos estão consagrados no direito primário e secundário da UE e do Conselho da Europa. Por conseguinte, a AEPD lamenta que a Comunicação sobre o restabelecimento da confiança não tenha dedicado mais atenção ao impacto sobre os instrumentos jurídicos em vigor.
80. A AEPD acolheria com satisfação, em vários aspetos, uma abordagem mais ambiciosa por parte Comissão na definição das próximas medidas a adotar e considera que:
- a correta aplicação e fiscalização do cumprimento do quadro jurídico europeu em matéria de proteção de dados, para além de ser um imperativo legal, seria também um contributo essencial para o restabelecimento da confiança. O mesmo é válido para os instrumentos que regulam as transferências internacionais entre a UE e os EUA, incluindo os atuais princípios de «porto seguro»,
 - a Comissão deveria recordar que as derrogações ou restrições a direitos fundamentais para fins de defesa da segurança nacional só são justificadas e admissíveis se forem estritamente necessárias, proporcionais e conformes com a jurisprudência do TEDH e do Tribunal de Justiça,

(1) Ver p. 5, 10 e 26 do Relatório, que, com base nos pareceres desclassificados do *Foreign Intelligence Surveillance Court*, confirma que os serviços de informação norte-americanos têm recurso a métodos de recolha com grande alcance ao abrigo do artigo 702.º, tais como a recolha de dados junto de prestadores de serviços de Internet através do PRISM ou a «recolha a montante» de dados em trânsito pelos EUA.

(2) Os EUA confirmaram que existem outras bases legais para a recolha de informações que permitem a aquisição de dados de cidadãos de países terceiros, mas não forneceram informações concretas sobre as autoridades competentes e os procedimentos jurídicos aplicáveis. Nem todas as bases legais relevantes foram comunicadas ao GT (ver p. 13 do Relatório).

(3) Ver p. 4-12 do Relatório.

(4) Ver p. 26-27 do Relatório.

(5) «Liberty and Security in a Changing World», Relatório e recomendações do Grupo de Análise sobre Tecnologias da Informação e Comunicação do Presidente, em especial as Recomendações 25, 29 e 30. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12-rg_final_report.pdf

(6) B Schneier, C Soghoian *in* artigo de 6 de setembro de 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>; B. Preneel: Intervenção de encerramento da ISSE 2013: «The Cryptographic Year in Review» http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf

- a AEPD concorda plenamente que a consolidação e a melhoria do quadro jurídico da UE em matéria de proteção de dados exigem a rápida adoção das propostas de reforma legislativa neste domínio com um conteúdo adequado, a fim de assegurar uma proteção mais sólida, eficaz e coerente dos dados pessoais e da privacidade em todas as áreas do direito da UE. Deveria também estar prevista uma proteção adequada dos dados no caso da sua utilização posterior para fins de aplicação coerciva da lei e de conflitos internacionais de competência,
- os princípios de «porto seguro» deveriam ser revistos e reforçados nos moldes sugeridos pela Comissão. A AEPD recomenda a fixação de prazos mais rigorosos para a adoção destas medidas, nomeadamente para um seguimento adequado caso ainda subsistam deficiências,
- as garantias em matéria de proteção de dados aplicáveis à cooperação policial e judicial entre a UE e os EUA têm de ser reforçadas. As negociações atualmente em curso sobre um «acordo-quadro» não deveriam legitimar transferências de grandes volumes de dados, respeitando antes o atual quadro jurídico em matéria de proteção de dados e o resultado do processo de revisão em curso. Em especial, todas as pessoas em causa deveriam ter acesso a mecanismos eficazes de reparação, independentemente da sua nacionalidade. Isto deveria ser também aplicável, a seu tempo, aos acordos internacionais em vigor, sempre que necessário com base em cláusulas de transição adequadas,
- a Comissão deveria apoiar os esforços desenvolvidos pela Administração norte-americana e o Congresso norte-americano para aprovar uma lei geral em matéria de privacidade que preveja garantias eficazes e mecanismos de supervisão adequados, especialmente em áreas onde não existe atualmente uma verdadeira proteção da privacidade,
- as negociações atualmente em curso com vista à adoção de uma Parceria Transatlântica de Comércio e Investimento (TTIP) não deveriam ter um impacto negativo na proteção dos dados pessoais dos cidadãos. Paralelamente, a Comissão deveria ponderar a definição de um objetivo comum de desenvolvimento gradual no sentido de uma maior interoperabilidade de quadros jurídicos em matéria de privacidade e de proteção de dados, objetivo para o qual os EUA poderiam contribuir nos moldes supramencionados,
- a promoção internacional de normas sobre a proteção da privacidade deveria incluir:
 - i) a promoção da plena coerência entre os novos instrumentos internacionais e o quadro jurídico europeu em matéria de proteção de dados;
 - ii) a promoção da adesão de países terceiros, em especial dos EUA, à Convenção n.º 108 do Conselho da Europa;
 - iii) o apoio à adoção de um instrumento internacional que exija o respeito das normas sobre proteção de dados pelos serviços de informação. Este instrumento poderia ser adotado ao nível das Nações Unidas com base no artigo 17.º do PIDCP,
- as atividades de vigilância deveriam ser obrigadas a respeitar, a todo o tempo, o Estado de direito e os princípios da necessidade e proporcionalidade numa sociedade democrática. Por conseguinte, os quadros jurídicos deveriam ser clarificados a todos os níveis relevantes e, quando necessário, complementados. Estes quadros deveriam abranger mecanismos de supervisão adequados e suficientemente fortes,
- as instituições da UE e todas as entidades relevantes nos Estados-Membros, enquanto responsáveis pelo tratamento de dados, também são diretamente responsáveis por assegurar uma segurança informática efetiva. Esta responsabilidade envolve a realização de uma avaliação do risco de segurança dos dados ao nível adequado. Implica igualmente a promoção da investigação sobre mecanismos de encriptação e a sensibilização dos responsáveis pelo tratamento de dados e dos cidadãos para os riscos que os produtos vendidos ou utilizados colocam em matéria de privacidade, bem como a exigência da utilização de métodos de conceção concretos por parte dos programadores para evitar ou, pelo menos, reduzir, estes riscos. A UE deveria liderar as iniciativas de educação sobre a segurança dos dados tratados na Internet.

Feito em Bruxelas, em 20 de fevereiro de 2014.

Peter HUSTINX

Autoridade Europeia para a Proteção de Dados
