AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

Resumo do parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão «Explorar plenamente o potencial da computação em nuvem na Europa»

(O texto integral do presente parecer está disponível em EN, FR e DE no sítio web da AEPD em http://www.edps.europa.eu)

(2013/C 253/03)

I. **Introdução**

I.1. *Objetivo do parecer*

1. Tendo em conta a importância da computação em nuvem na sociedade da informação em evolução e o debate político em curso no seio da União Europeia sobre a computação em nuvem, a AEPD decidiu emitir este parecer por iniciativa própria.

2. O presente parecer responde à Comunicação da Comissão «Explorar plenamente o potencial da computação em nuvem na Europa» de 27 de setembro de 2012 (a seguir designada «a Comunicação») ([1]), que estabelece as ações-chave e as medidas políticas necessárias para acelerar a utilização dos serviços de computação em nuvem na Europa. Tendo sido consultada a título informal antes da adoção da Comunicação, a AEPD formulou observações informais, e congratula-se pelo facto de algumas dessas observações terem sido tomadas em conta na Comunicação.

3. Contudo, atendendo ao âmbito e à importância do debate em curso sobre a relação entre a computação em nuvem e o quadro jurídico para a proteção de dados, o presente parecer não se limita às questões abordadas na Comunicação.

4. O parecer incide especialmente sobre os desafios que a computação em nuvem representa para a proteção de dados e a forma como o regulamento proposto relativo à proteção de dados (a seguir designado «regulamento proposto») ([2]) os poderá superar. Apresenta igualmente observações sobre outras áreas de ação identificadas na Comunicação.

I.2. *Contexto*

5. No quadro do debate político geral realizado na União Europeia (UE) sobre a computação em nuvem, as atividades e documentos seguintes assumem uma importância específica:

— Na sequência da sua Comunicação datada de 2010 e intitulada «Uma Agenda Digital para a Europa» ([3]) a Comissão lançou, entre 16 de maio e 31 de agosto de 2011, uma consulta pública sobre a computação em nuvem na Europa e publicou os resultados em 5 de dezembro de 2011 ([4]);

— Em 1 de julho de 2012, o grupo de trabalho para a proteção de dados instituído pelo artigo 29.º ([5]) aprovou um parecer sobre a Computação em Nuvem (a seguir designado o «Parecer do GT29») ([6]) que analisa a aplicação das atuais regras relativas à proteção de dados estabelecidas na Diretiva 95/46/CE aos prestadores de serviços de computação em nuvem que operam no Espaço Económico Europeu (EEE) e seus clientes ([7]);

— Em 26 de outubro de 2012, os Comissários para a Proteção de Dados e da Vida Privada adotaram na sua 34.ª Conferência Internacional uma resolução sobre a computação em nuvem ([8]).

([1]) COM(2012) 529 final.
([2]) COM(2012) 11 final.
([3]) COM(2010) 245 final.
([4]) http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf
([5]) O Grupo de Trabalho 29 é um organismo consultivo criado ao abrigo do artigo 29.º da Diretiva 95/46/CE. É composto por representantes das autoridades de controlo nacionais e da AEPD e por um representante da Comissão.
([6]) Parecer 05/2012 do GT29 relativo a computação em nuvem, disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_pt.pdf
([7]) Além disso, a nível nacional, as Autoridades para a Proteção de Dados de diversos Estados-Membros, nomeadamente Itália, Suécia, Dinamarca, Alemanha, França e Reino Unido, emitiram as suas próprias orientações em matéria de computação em nuvem.
([8]) Resolução sobre computação em nuvem aprovada na 34.ª Conferência Internacional dos Comissários para a Proteção de Dados e da Vida Privada, Uruguai, 26 de outubro de 2012.

I.3. *Comunicação sobre a Computação em Nuvem*

6. A AEPD acolhe favoravelmente a Comunicação. Esta identifica três ações-chave necessárias a nível da UE para acompanhar e promover a utilização da computação em nuvem na Europa, da seguinte forma:

— Ação-chave 1: Pôr fim à selva de normas

— Ação-chave 2: Estabelecer condições contratuais seguras e justas

— Ação-chave 3: Criar uma parceria europeia para a nuvem destinada a impulsionar a inovação e o crescimento com base no setor público.

7. São igualmente previstas medidas políticas adicionais, nomeadamente medidas destinadas a incentivar a utilização da computação em nuvem, promovendo a investigação e desenvolvimento ou a sensibilização para o tema, bem como a necessidade de abordar temas essenciais relacionados com os serviços em nuvem — incluindo, entre outros, a proteção de dados, o acesso dos organismos judiciais/policiais aos dados, segurança, responsabilidade dos fornecedores intermediários de serviços — mediante um maior diálogo internacional.

8. A proteção de dados é mencionada na Comunicação como um elemento essencial para garantir o sucesso da implantação da computação em nuvem na Europa. A Comunicação faz notar ([1]) que o regulamento proposto dá resposta a muitas das questões suscitadas pelos prestadores de serviços de computação em nuvem e pelos clientes desses serviços ([2]).

I.4. *Objetivos e estrutura do parecer AEPD*

9. O presente parecer visa três objetivos.

10. O primeiro objetivo consiste em realçar a importância da proteção de dados e da privacidade nos debates atualmente em curso sobre computação em nuvem. Mais especificamente, sublinha que o nível de proteção de dados num ambiente de computação em nuvem não deve ser inferior ao exigido em qualquer outro contexto de tratamento de dados. As práticas relativas à computação em nuvem só podem ser desenvolvidas e aplicadas legalmente se garantirem que este nível de proteção de dados é respeitado (ver capítulo III.3). O parecer leva em conta as orientações formuladas no parecer do GT29.

11. O segundo objetivo consiste em analisar mais aprofundadamente os principais desafios que a computação em nuvem representa para a proteção de dados no quadro do regulamento proposto relativo à proteção de dados, em particular a dificuldade de definir de forma inequívoca as responsabilidades dos diferentes atores e as noções de responsável pelo tratamento dos dados e subcontratante. O parecer (em particular no capítulo IV) analisa de que forma o regulamento proposto, na sua versão atual ([3]), contribui para garantir um elevado nível de proteção dos dados nos serviços de computação em nuvem. Por conseguinte, toma por base os pontos de vista desenvolvidos pela AEPD no seu Parecer sobre o Pacote de Reforma Legislativa sobre a Proteção de Dados (a seguir designado «o Parecer da AEPD sobre o Pacote de Reforma Legislativa sobre a Proteção de Dados») ([4]) e completa-o analisando especificamente o ambiente de computação em nuvem. A AEPD sublinha que o seu Parecer sobre o Pacote de Reforma Legislativa sobre a Proteção de Dados se aplica na íntegra aos serviços de computação em nuvem e deve ser considerado como base do presente parecer. Além do mais, algumas das questões mencionadas no referido documento — como a sua análise das novas disposições relativas aos direitos dos titulares de dados ([5]) — são apresentadas com suficiente clareza e, por conseguinte, não serão desenvolvidas no presente parecer.

12. O terceiro objetivo consiste em identificar as áreas que requerem novas ações a nível da UE numa perspetiva de proteção de dados e privacidade, tendo em vista a estratégia para a computação em nuvem apresentada pela Comissão na sua Comunicação. Estas áreas incluem, entre outras, a formulação de orientações suplementares, o desenvolvimento de esforços de normalização, a realização de novas avaliações dos riscos para setores específicos (como o setor público), a definição de condições contratuais-tipo, o estabelecimento de um diálogo internacional sobre as questões relacionadas com a computação em nuvem e a garantia de meios eficazes para estabelecer uma cooperação internacional (a desenvolver no capítulo V).

([1]) Ver p. 9 da Comunicação, secção «Ações da Agenda Digital para criar confiança nas tecnologias digitais».
([2]) O termo «clientes de serviços de computação em nuvem» é genericamente utilizado no presente parecer para designar os clientes, que atuam na qualidade de empresas, e os consumidores, que atuam na qualidade de utilizadores finais individuais.
([3]) Cumpre ter em conta que a proposta de regulamento está atualmente em discussão no Conselho e Parlamento Europeu de acordo com o processo legislativo ordinário.
([4]) O Parecer está disponível em http://www.edps.europa.eu
([5]) Ver Parecer da AEPD, em particular os n.os 140 a 158.

13. O parecer está estruturado da seguinte forma: a secção II fornece uma visão geral das principais características da computação em nuvem e dos desafios conexos em matéria de proteção de dados. A secção III analisa os elementos mais relevantes do atual quadro jurídico da UE e do regulamento proposto. A secção IV analisa de que forma o regulamento proposto contribuirá para responder aos desafios relativos à proteção de dados colocados pela utilização de serviços de computação em nuvem. A secção V analisa as sugestões da Comissão com vista a desenvolvimentos políticos futuros e identifica as áreas que poderão necessitar de mais atenção. A secção VI apresenta as conclusões.

14. Embora muitas das suas considerações se apliquem a todos os ambientes em que a computação em nuvem é utilizada, o presente parecer mesmo não aborda a utilização dos serviços de computação em nuvem especificamente por instituições e órgãos da UE sujeitos à supervisão da AEPD ao abrigo do Regulamento (CE) n.º 45/2001. A AEPD formulará em separado orientações sobre a matéria, destinadas a estas instituições e órgãos.

VI. **Conclusões**

121. Conforme descrito na Comunicação, a computação em nuvem oferece várias novas oportunidades a empresas, consumidores e setor público no que respeita à gestão de dados através da utilização de recursos externos de TI de suporte remoto. Paralelamente, apresenta muitos desafios, em particular no que toca ao nível adequado de proteção de dados que é oferecido aos dados tratados nestes moldes.

122. A utilização de serviços de computação em nuvem comporta um importante risco de ver dissipada a responsabilidade respeitante às operações de tratamento realizadas pelos prestadores de serviços de computação em nuvem, no caso de os critérios de aplicabilidade da legislação da UE relativa à proteção de dados não serem suficientemente claros e de a função e responsabilidade do prestador de serviços de computação em nuvem serem definidas ou entendidas em termos demasiado restritos, ou não serem eficazmente implementadas. A AEPD salienta que a utilização dos serviços de computação em linha não pode justificar uma redução do nível de proteção de dados, comparativamente ao aplicável às convencionais operações de tratamento de dados.

123. A este respeito, o regulamento proposto relativo à proteção de dados, na versão apresentada, proporcionará várias clarificações e instrumentos suscetíveis de garantir a consecução de um nível satisfatório de proteção de dados por parte dos prestadores de serviços de computação em nuvem que disponibilizam os seus serviços a clientes estabelecidos na Europa, em especial:

— o artigo 3.º clarificará o âmbito de aplicação territorial das normas da UE relativas à proteção de dados e alargará o seu âmbito por forma a abranger os serviços de computação em nuvem;

— o artigo 4.º, n.º 5, introduzirá um novo elemento na questão relativa ao controlo, ou seja, «condições». Isto será consentâneo com a tendência emergente segundo a qual, tendo em conta a complexidade técnica das TI subjacente à prestação de serviços de computação em nuvem, se impõe alargar as circunstâncias em que um prestador de serviços de computação em nuvem pode estar habilitado a ser o responsável pelo tratamento de dados. Isto refletirá melhor o verdadeiro nível de influência nas operações de tratamento;

— o regulamento proposto aumentará a responsabilidade e a responsabilização dos responsáveis pelo tratamento dos dados e dos subcontratantes, graças à introdução de obrigações específicas, tais como a proteção dos dados, desde a conceção e por defeito (artigo 23.º), a notificação de violações da segurança dos dados (artigos 31.º e 32.º), e a avaliação de impacto sobre a proteção de dados (artigo 33.º). Além disso, obrigará os responsáveis pelo tratamento dos dados e os subcontratantes a aplicar mecanismos para verificação da eficácia das medidas de proteção de dados implementadas (artigo 22.º);

— os artigos 42.º e 43.º do regulamento proposto permitirão uma utilização mais flexível dos mecanismos de transferência de dados a nível internacional, por forma a ajudar os clientes dos serviços de computação em nuvem e os prestadores de serviços de computação em nuvem a apresentarem garantias adequadas de proteção de dados no que se refere às transferências de dados pessoais para centros de dados ou servidores localizados em países terceiros;

— os artigos 30.º, 31.º e 32.º do regulamento proposto definirão melhor as obrigações dos responsáveis pelo tratamento dos dados e subcontratantes no que respeita à segurança do tratamento e aos requisitos de informação em caso de violações de dados, estabelecendo a base para uma abordagem abrangente e cooperativa da gestão da segurança entre os diferentes atores num ambiente de computação em nuvem;

— os artigos 55.º a 63.º do regulamento proposto reforçarão a cooperação entre as autoridades de controlo e a sua supervisão coordenada no que se refere às operações de tratamento transfronteiriças, o que assume particular importância num ambiente como o da computação em nuvem.

124. Não obstante, a AEPD sugere que, depois de ter tido em conta as especificidades dos serviços de computação em nuvem, sejam incluídas clarificações adicionais no regulamento proposto relativamente aos seguintes aspetos:

— no que respeita ao âmbito de aplicação territorial do regulamento proposto, alterar o artigo 3.º, n.º 2, alínea a), da seguinte forma «A oferta de bens ou serviços *que envolvam o tratamento de dados pessoais desses* titulares de dados na União», ou em alternativa aditar um novo considerando que refira especificamente que o tratamento de dados pessoais de titulares de dados na União por responsáveis pelo tratamento de dados estabelecidos fora da União que ofereçam os seus serviços a pessoas legalmente estabelecidas na UE, também se inscreve no âmbito de aplicação territorial do regulamento;

— aditar uma definição clara da noção de «transferência», como consta no seu Parecer sobre o Pacote de Reforma Legislativa sobre a Proteção de Dados;

— aditar uma disposição específica para clarificar as condições em que poderá ser permitido o acesso aos dados armazenados, no âmbito dos serviços de computação em nuvem, por parte de organismos judiciais/policiais de países não pertencentes ao EEE. Essa disposição poderá incluir também a obrigação do destinatário do pedido de informar e consultar a autoridade de controlo competente na UE em casos específicos.

125. A AEPD salienta igualmente que haverá necessidade de a Comissão e/ou autoridades de controlo (em particular através do futuro Comité Europeu para a Proteção de Dados) disponibilizarem mais orientações sobre os seguintes aspetos:

— clarificar que mecanismos devem ser criados por forma a garantir a verificação da eficácia das medidas de proteção de dados na prática;

— auxiliar os subcontratantes na aplicação das regras vinculativas para empresas (*Binding Corporate Rules — BCR*) e no cumprimento dos requisitos aplicáveis;

— providenciar melhores práticas relativamente a questões como a responsabilidade do responsável pelo tratamento dos dados/subcontratante, a conservação adequada de dados no ambiente de computação em nuvem, a portabilidade de dados e o exercício dos direitos dos titulares de dados.

126. Além disso, a AEPD reconhece que os códigos de conduta elaborados pela indústria e aprovados pelas autoridades de controlo competentes poderão constituir uma ferramenta útil para reforçar o cumprimento, bem como a confiança entre os diversos atores.

127. A AEPD apoia o desenvolvimento por parte da Comissão, em concertação com as autoridades de controlo, de condições contratuais-tipo para a prestação de serviços de computação em nuvem que respeitem os requisitos de proteção de dados, tendo especialmente em vista:

— definir condições contratuais modelo a incluir nas condições comerciais da oferta de serviços de computação em nuvem;

— definir condições e requisitos comuns no domínio da contratação pública para o setor público, tendo em conta a sensibilidade dos dados tratados;

— adequar ainda mais os mecanismos internacionais de transferência de dados ao ambiente de computação em nuvem, em especial por meio da atualização das cláusulas contratuais-tipo vigentes e da apresentação de cláusulas contratuais-tipo aplicáveis à transferência de dados entre subcontratantes estabelecidos na UE e subcontratantes localizados fora da UE.

128. A AEPD sublinha que deve ser dada especial atenção aos requisitos de proteção de dados na elaboração de normas e sistemas de certificação, especialmente no sentido de:

— aplicar os princípios de privacidade desde a conceção e por defeito na elaboração das normas;

— integrar os requisitos de proteção de dados, como por exemplo, a limitação das finalidades e a limitação do armazenamento na conceção das normas;

— introduzir a obrigação de os prestadores do serviço disponibilizarem aos seus clientes a informação necessária para realizar uma avaliação de risco válida, bem como as medidas de segurança que implementaram e ainda alertas relativos aos incidentes no domínio da segurança.

129. Por último, a AEPD salienta a necessidade de dar resposta os desafios que a computação em nuvem coloca a nível internacional. Exorta a Comissão a entabular um diálogo internacional sobre as questões suscitadas pela computação em nuvem, incluindo a jurisdição e o acesso aos dados por parte dos organismos judiciais/policiais, e sugere que muitas dessas questões sejam contempladas nos diferentes acordos internacionais ou bilaterais, nomeadamente acordos de assistência mútua e acordos comerciais. Deverão ser elaboradas normas globais a nível internacional a fim de estabelecer condições e princípios mínimos respeitantes ao acesso aos dados por parte dos organismos judiciais/policiais. A AEPD apoia igualmente o desenvolvimento, por parte das autoridades de controlo, de mecanismos eficazes de cooperação internacional, em especial no que respeita a questões de computação em nuvem.

Feito em Bruxelas, em 16 de novembro de 2012.

Peter HUSTINX

Supervisor Europeu para a Proteção de Dados