GRUPO DE TRABALHO PARA A PROTEÇÃO DE DADOS INSTITUÍDO PELO ARTIGO 29.º

01037/12/PT
GT 196

Parecer 05/2012 relativo a computação em nuvem

Adotado em 1 de julho de 2012

Resumo

No presente parecer, o Grupo de Trabalho instituído ao abrigo do Artigo 29.º analisa todas as questões relevantes relativas aos prestadores de serviços de computação em nuvem que desenvolvem atividades no Espaço Económico Europeu (EEE) e aos seus clientes, especificando todos os princípios aplicáveis da Diretiva Proteção de Dados (95/46/CE) e da Diretiva Privacidade das Comunicações Eletrónicas (2002/58/CE) (com a redação que lhe foi dada pela Diretiva 2009/136/CE) da UE sempre que relevante.

Apesar das vantagens reconhecidas da computação em nuvem (*cloud computing)*, tanto em termos económicos como societais, o presente parecer descreve o modo como a implantação em grande escala de serviços de computação em nuvem pode desencadear uma série de riscos no que diz respeito à proteção de dados, nomeadamente uma falta de controlo sobre os dados pessoais, bem como informação insuficiente sobre como, quando e por quem estão os dados a ser objeto de tratamento/subtratamento. Estes riscos devem ser cuidadosamente avaliados pelos organismos públicos e empresas privadas quando estudam a hipótese de contratar um prestador de serviços de computação em nuvem. O presente parecer examina as questões associadas à partilha de recursos com outras partes, à falta de transparência de uma cadeia de externalização constituída por múltiplos subcontratantes e subcontratantes ulteriores, à inexistência de um enquadramento comum global em matéria de portabilidade dos dados e à incerteza quanto à admissibilidade da transferência de dados pessoais para prestadores de serviços de computação em nuvem estabelecidos fora do EEE. Do mesmo modo, no presente parecer é salientada, como uma grande preocupação, a falta de transparência em termos das informações que um responsável pelo tratamento de dados é capaz de fornecer à pessoa em causa sobre o modo como os seus dados pessoais são tratados. As pessoas em causa devem[1] ser informadas sobre quem procede ao tratamento dos seus dados e para que finalidades de modo a terem a possibilidade de exercer os seus direitos nesta matéria.

Uma conclusão fundamental do presente parecer é que as empresas e as administrações que desejem utilizar a computação em nuvem devem proceder, numa primeira fase, a uma análise dos riscos aprofundada e abrangente. Todos os prestadores de serviços de computação em nuvem que oferecem os seus serviços no EEE devem facultar aos seus clientes todas as informações necessárias para avaliar corretamente as vantagens e desvantagens da contratação de um tal serviço. A segurança, a transparência e a segurança jurídica para os clientes devem ser fatores fundamentais subjacentes à oferta de serviços de computação em nuvem.

No que diz respeito às recomendações constantes do presente parecer, salientam-se as responsabilidades do cliente de um serviço de computação em nuvem enquanto responsável pelo tratamento de dados, pelo que se recomenda que o cliente selecione um prestador de serviços de computação em nuvem que garanta o cumprimento da legislação da UE em matéria de proteção de dados. O presente parecer aborda a questão da adequação das cláusulas contratuais de salvaguarda estabelecendo o requisito de que

[1] As palavras-chave «DEVE», «NÃO DEVE», «OBRIGATÓRIO», «DEVERÁ», «NÃO DEVERÁ», «DEVERIA», «NÃO DEVERIA», «RECOMENDADO», «PODE» e «FACULTATIVO» devem ser interpretadas tal como descritas no Pedido de Observações RFC 2119. O documento está disponível no seguinte endereço http://www.ietf.org/rfc/rfc2119.txt. No entanto, por uma questão de legibilidade, estas palavras não são todas apresentadas em maiúsculas nesta especificação.

qualquer contrato celebrado entre o cliente e prestador de serviços de computação em nuvem deve proporcionar garantias suficientes em termos de medidas técnicas e organizativas. Também importante é a recomendação de que o cliente de um serviço de computação em nuvem verifique se o prestador do serviço pode garantir a licitude de todas as transferências internacionais de dados.

Como qualquer processo evolutivo, a ascensão da computação em nuvem como um paradigma tecnológico mundial constitui um desafio. O presente parecer, na sua forma atual, pode ser considerado um passo importante na definição das tarefas a assumir nesta matéria pela comunidade responsável pela proteção de dados nos próximos anos.

Índice

1. Introdução

Para alguns, a computação em nuvem constitui uma das maiores revoluções tecnológicas dos últimos tempos. Para outros, é apenas a evolução natural de um conjunto de tecnologias que visa realizar o grande sonho que é a computação de utilidade pública. Em qualquer caso, um grande número de partes interessadas deu importância à computação em nuvem no desenvolvimento das suas estratégias tecnológicas.

A computação em nuvem consiste num conjunto de tecnologias e modelos de serviços centrados na utilização e fornecimento via Internet de aplicações informáticas, de capacidade de tratamento e armazenamento e de espaço de memória. A computação em nuvem pode gerar importantes benefícios económicos, uma vez que os recursos a pedido podem ser com bastante facilidade configurados, alargados e acedidos via Internet . Para além dos benefícios económicos, a computação em nuvem pode também ter vantagens em termos de segurança, uma vez que as empresas, em especial as pequenas e médias empresas, podem adquirir, a um custo marginal, tecnologias de primeira classe que de outra forma poderiam estar fora do seu orçamento.

Há uma vasta gama de serviços oferecidos pelos prestadores de serviços de computação em nuvem, desde sistemas de tratamento virtual (que substituem e/ou funcionam em paralelo com os servidores convencionais sob o controlo direto do responsável pelo tratamento dos dados), passando por serviços de apoio ao desenvolvimento de aplicações e serviços avançados de alojamento, até soluções de *software* com base na *web* que podem substituir aplicações instaladas de forma convencional nos computadores pessoais dos utilizadores finais. Estes incluem aplicações de processamento de texto, agendas e calendários, sistemas de arquivo para armazenamento de documentos em linha e soluções de correio eletrónico externalizadas. Algumas das definições mais frequentemente utilizadas para estes diferentes tipos de serviços constam do anexo ao presente parecer.

No presente parecer, o Grupo de Trabalho criado ao abrigo do artigo 29.º (a seguir designado GT 29) analisa o direito e as obrigações aplicáveis aos responsáveis pelo tratamento de dados no Espaço Económico Europeu (a seguir designado EEE) e aos prestadores de serviços de computação em nuvem que tenham clientes no EEE. O presente parecer incide na situação em que se presume que a relação se processa entre um responsável pelo tratamento de dados e um subcontratante, em que o cliente atua na qualidade de responsável pelo tratamento dos dados e o prestador de serviços de computação em nuvem atua na qualidade de subcontratante. Nos casos em que o prestador de serviços de computação em nuvem atua também na qualidade de responsável pelo tratamento de dados, é necessário que satisfaça requisitos adicionais. Em consequência, uma condição prévia para utilizar modalidades de computação em nuvem é que o responsável pelo tratamento dos dados proceda a uma avaliação dos riscos adequada, incluindo a localização dos servidores onde os dados são tratados e a análise dos riscos e benefícios de um ponto de vista da proteção dos dados, em conformidade com os critérios definidos nos parágrafos infra.

O presente parecer especifica os princípios aplicáveis tanto aos responsáveis pelo tratamento de dados como aos subcontratantes constantes da Diretiva 95/46/CE (Diretiva Geral sobre Proteção de Dados), tais como a especificação e limitação da finalidade, o apagamento de dados e as medidas técnicas e organizativas. O parecer formula orientações sobre os requisitos em matéria de segurança como uma salvaguarda simultaneamente de caráter estrutural e processual. É dado especial destaque às modalidades contratuais que devem reger a relação entre um responsável pelo tratamento de dados e um subcontratante neste contexto. Os

objetivos clássicos relativos à segurança dos dados são a disponibilidade, a integridade e a confidencialidade. No entanto, a questão de proteção dos dados não se limita à segurança dos mesmos, pelo que estas metas são complementadas com metas específicas de proteção dos dados no que diz respeito à transparência, isolamento, capacidade de intervenção e portabilidade, a fim de garantir o respeito do direito à proteção dos dados pessoais conforme consagrado no artigo 8.º da Carta dos Direitos Fundamentais da UE.

No que se refere às transferências de dados pessoais para fora do EEE, são analisados instrumentos como as cláusulas contratuais-tipo adotadas pela Comissão Europeia, a fundamentação da adequação e possíveis futuras regras vinculativas para empresas (*Binding Corporate Rules* - BCR) aplicáveis aos subcontratantes, bem como os riscos relativos à proteção de dados decorrentes de pedidos de controlo do cumprimento da legislação ao abrigo do direito internacional.

O presente parecer encerra com recomendações dirigidas aos clientes de serviços de computação em nuvem na qualidade de responsáveis pelo tratamento de dados, aos prestadores de serviços de computação em nuvem na qualidade de subcontratantes e à Comissão Europeia no que se refere a futuras alterações ao quadro europeu em matéria de proteção de dados.

O Grupo de Trabalho Internacional relativo à Proteção de Dados nas Telecomunicações (Grupo de Berlim) adotou o *Memorando Sopot*[2] em abril de 2012. O referido memorando analisa as questões relativas à proteção dos dados e da vida privada no contexto da computação em nuvem e salienta que a respetiva utilização não deve resultar numa redução dos níveis de proteção dos dados em comparação com o tratamento tradicional de dados.

2. Riscos em matéria de proteção de dados decorrentes da computação em nuvem

Uma vez que o presente parecer incide nas operações de tratamento de dados que utilizam serviços de computação em nuvem, apenas são considerados os riscos neste contexto[3]. A maioria destes riscos inscreve-se em duas categorias gerais de riscos, nomeadamente a falta de controlo sobre os dados e a insuficiência de informação sobre as operações de tratamento em si mesmas (ausência de transparência). Entre os riscos específicos decorrentes da computação em nuvem considerados no presente parecer incluem-se:

Falta de controlo

Ao confiar dados pessoais aos sistemas geridos por um prestador de serviços de computação em nuvem, os respetivos clientes perdem o controlo exclusivo desses dados e não podem implementar as medidas técnicas e organizativas necessárias para assegurar a disponibilidade, integridade, confidencialidade, transparência, isolamento[4], capacidade de intervenção e portabilidade dos dados. Esta falta de controlo pode manifestar-se da seguinte forma:

---

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

3 Para além dos riscos associados aos dados pessoais tratados no âmbito da computação em nuvem explicitamente mencionados no presente parecer, devem também ser tidos em consideração todos os riscos relacionados com a externalização do tratamento de dados pessoais.

4 Na Alemanha, foi introduzido o conceito mais lato de «inviabilidade de ligação» (*unlinkability*). Ver nota de pé de página 24 infra.

- Falta de disponibilidade devido à falta de interoperabilidade (dependência em relação a um único fornecedor): Se o prestador de serviços de computação em nuvem dispõe de uma tecnologia patenteada, o cliente desse serviço poderá ter dificuldade na transferência de dados e documentos entre diferentes sistemas baseados em serviços de computação em nuvem (portabilidade dos dados) ou no intercâmbio de informações com entidades que utilizam serviços de computação em nuvem geridos por diferentes fornecedores (interoperabilidade).
- Falta de integridade decorrente da partilha de recursos: Um serviço de computação em nuvem é composto por infraestruturas e sistemas partilhados. Os prestadores de serviços de computação em nuvem procedem ao tratamento dos dados pessoais provenientes de uma vasta gama de fontes em termos de organizações e pessoas em causa, pelo que há a possibilidade de surgirem conflitos de interesses e/ou objetivos diferentes.
- Falta de confidencialidade em termos de pedidos de controlo da aplicação da legislação diretamente a um prestador de serviços de computação em nuvem: Os dados pessoais em tratamento no âmbito de serviços de computação em nuvem podem ser objeto de pedidos de controlo da aplicação da legislação provenientes de autoridades encarregadas de aplicar a lei dos Estados-Membros da UE e de países terceiros. Existe o risco de os dados pessoais poderem ser divulgados a autoridades encarregadas de aplicar a lei (estrangeiras) sem uma base jurídica válida na UE e, por conseguinte, de uma violação da legislação da UE em matéria de proteção dos dados.
- Falta de capacidade de intervenção devido à complexidade e dinâmica da cadeia de externalização: O serviço de computação em nuvem oferecido por um fornecedor poderia ser prestado com uma combinação de serviços entre uma série de outros fornecedores, que podem ser dinamicamente incluídos ou excluídos durante a vigência do contrato com o cliente.
- Falta de capacidade de intervenção (direitos das pessoas em causa): Um prestador de serviços de computação em nuvem pode não proporcionar as medidas e ferramentas necessárias para assistir o responsável pelo tratamento de dados na gestão dos mesmos em termos, por exemplo, de acesso, apagamento ou correção dos dados.
- Falta de isolamento: O prestador de serviços de computação em nuvem pode utilizar o seu controlo físico sobre os dados de diferentes clientes para estabelecer ligações entre dados pessoais. Se dispuserem de direitos de acesso privilegiado suficientes (perfis de alto risco), os administradores poderiam estabelecer ligações entre informações de diferentes clientes.

Falta de informação sobre o tratamento dos dados (transparência)

A insuficiência de informações sobre as operações de tratamento do prestador de serviços de computação em nuvem comporta riscos para os responsáveis pelo tratamento de dados, bem como para as pessoas em causa, uma vez que estes podem não estar conscientes de potenciais ameaças e riscos, não podendo, por conseguinte, tomar as medidas que considerem adequadas.

Algumas potenciais ameaças podem decorrer do facto de o responsável pelo tratamento de dados não saber que:

- Está em curso um tratamento em cadeia que envolve múltiplos subcontratantes e subcontratantes ulteriores.

- Os dados pessoais são tratados em locais geográficos diferentes no interior do EEE. Este facto tem repercussões diretas no direito aplicável a quaisquer litígios em matéria de proteção de dados que possam surgir entre o utilizador e o prestador do serviço.
- Os dados pessoais são transferidos para países terceiros fora do EEE. Os países terceiros podem não proporcionar um nível adequado de proteção dos dados e as transferências podem não estar salvaguardadas por medidas adequadas (por exemplo, cláusulas contratuais-tipo ou regras vinculativas para empresas), pelo que podem ser ilícitas.

Um requisito em vigor é que as pessoas em causa cujos dados pessoais são tratados no âmbito da computação em nuvem sejam informadas da identidade do responsável pelo tratamento dos dados e da finalidade desse tratamento (um requisito em vigor aplicável a todos os responsáveis pelo tratamento de dados ao abrigo da Diretiva Proteção dos Dados (95/46/CE)). Tendo em conta a potencial complexidade das cadeias de tratamento de dados num ambiente de computação em nuvem, e com vista a garantir um tratamento leal dos dados no respeito dos direitos da pessoa em causa (artigo 10.° da Diretiva 95/46/CE), os responsáveis pelo tratamento de dados devem também, por uma questão de boas práticas, facultar informações complementares sobre os subcontratantes (ou subcontratantes ulteriores) que prestam os serviços de computação em nuvem.

3. Quadro jurídico

3.1 Quadro relativo à proteção de dados

O quadro jurídico relevante é a Diretiva Proteção de Dados (95/46/CE). A referida diretiva aplica-se em todos os casos em que são tratados dados pessoais em resultado da utilização de serviços de computação em nuvem. A Diretiva Privacidade das Comunicações Eletrónicas (2002/58/CE) (com a redação que lhe foi dada pela Diretiva 2009/136/CE) é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas publicamente disponíveis em redes de comunicações públicas (operadores de telecomunicações) e, por conseguinte, é relevante se tais serviços forem prestados numa modalidade de computação em nuvem[5].

3.2 Direito aplicável

Os critérios relativos à aplicabilidade da legislação constam do artigo 4.° da Diretiva 95/46/CE que se refere ao direito aplicável aos responsáveis pelo tratamento[6] com um ou mais estabelecimentos no território do EEE e também ao direito aplicável aos responsáveis pelo tratamento estabelecidos fora do EEE mas que utilizam equipamentos localizados no EEE para o tratamento de dados pessoais. O Grupo de Trabalho instituído pelo artigo 29.º analisou esta questão no seu Parecer 8/2010 sobre a lei aplicável[7].

---

5 Diretiva Privacidade e Comunicações Eletrónicas (2002/58/CE) (com a redação que lhe foi dada pela Diretiva 2009/136/CE): A Diretiva 2002/58/CE relativa à privacidade nas telecomunicações é aplicável aos prestadores de serviços de comunicações eletrónicas acessíveis ao público e exige que estes assegurem o cumprimento das obrigações relativas ao sigilo das comunicações e à proteção dos dados pessoais, bem como os direitos e obrigações em matéria de redes e serviços de comunicações eletrónicas. Nos casos em que atuem na qualidade de prestadores de um serviço de comunicações eletrónicas disponível ao público, os prestadores de serviços de computação em nuvem estão sujeitos a esta diretiva.

6 O conceito de responsável pelo tratamento está definido no artigo 2.º, alínea h), da diretiva e foi analisado pelo GT 29 no seu Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante».

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_pt.pdf

No primeiro caso, o fator que determina a aplicação da legislação da UE ao responsável pelo tratamento de dados é o seu local de estabelecimento e as atividades que desenvolve, em conformidade com o disposto no artigo 4.º, n.º 1, alínea a), da diretiva, sendo o tipo de serviço de computação em nuvem irrelevante. A legislação aplicável é o direito do país em que está estabelecido o responsável pelo tratamento de dados que contrata os serviços de computação em nuvem e não o do local em que os respetivos prestadores de serviços estão localizados.

Caso o responsável pelo tratamento dos dados esteja estabelecido em vários Estados-Membros e proceda ao tratamento dos dados como parte das suas atividades nesses países, o direito aplicável deve ser o de cada um dos Estados-Membros em que é efetuado esse tratamento.

O artigo 4.º, n.º 1, alínea c)[8], refere-se ao modo como a legislação em matéria de proteção de dados é aplicável aos responsáveis pelo tratamento de dados não estabelecidos no território do EEE mas que utilizam equipamentos automatizados ou não automatizados localizados no território do Estado-Membro, exceto quando estes são utilizados apenas para fins de trânsito. Isso significa que, se o cliente de um serviço de computação em nuvem estiver estabelecido fora do EEE, mas contratar um prestador de serviços estabelecido no EEE, então o prestador de serviços «exporta» a legislação em matéria de proteção de dados para o seu cliente.

3.3 Deveres e responsabilidades dos diferentes intervenientes

Conforme anteriormente referido, a computação em nuvem envolve uma grande variedade de intervenientes. É importante avaliar e clarificar o papel de cada um desses intervenientes a fim de estabelecer as suas obrigações específicas face à legislação em vigor em matéria de proteção de dados.

Recorda-se que o GT 29 salientou, no seu Parecer 1/2010 relativo aos conceitos de «responsável pelo tratamento» e de «subcontratante», «*que a principal e primeira função no conceito de responsável pelo tratamento é, antes de mais, determinar quem será o responsável pelo cumprimento das normas sobre proteção de dados e o modo como as pessoas em causa podem exercer na prática os seus direitos. Por outras palavras: atribuir a responsabilidade*». Estes dois critérios gerais relativos ao cumprimento e atribuição de responsabilidade devem ser tidos em consideração pelas partes envolvidas na análise em causa.

3.3.1 Cliente do serviço de computação em nuvem e prestador do serviço de computação em nuvem

O cliente do serviço de computação em nuvem determina a finalidade última do tratamento, decide sobre a externalização desse tratamento e a delegação da totalidade ou de parte das atividades de tratamento numa organização externa. Por conseguinte, o cliente do serviço de computação em nuvem atua como responsável pelo tratamento dos dados. A diretiva define como responsável pelo tratamento «*a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais*». O cliente do serviço

[8] O artigo 4.º, n.º 1, alínea c), estabelece que é aplicável a legislação de um Estado-Membro quando «*o responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território desse Estado-Membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade*».

de computação em nuvem, na sua qualidade de responsável pelo tratamento dos dados, deve aceitar a responsabilidade de respeitar a legislação em matéria de proteção de dados, está sujeito a todas as obrigações jurídicas estabelecidas na Diretiva 95/46/CE e é responsável pelo respetivo cumprimento. O cliente do serviço de computação em nuvem pode encarregar o respetivo prestador de serviços de escolher os métodos e as medidas de caráter técnico ou organizativo a utilizar para atingir as finalidades do responsável pelo tratamento de dados.

O prestador de serviços de computação em nuvem é a entidade que presta esses serviços nas diferentes modalidades supramencionadas. Quando o prestador de serviços de computação em nuvem fornece os meios e a plataforma, agindo em nome do seu cliente, o prestador de serviços é considerado um subcontratante, ou seja, nos termos da Diretiva 95/46/CE «*a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trata os dados pessoais por conta do responsável pelo tratamento*».[9, 10]

Tal como referido no Parecer 1/2010, podem ser utilizados alguns critérios[11] para determinar quem é o responsável pelo tratamento dos dados. De facto, pode haver situações em que o prestador de serviços de computação em nuvem pode ser considerado um responsável conjunto pelo tratamento ou um responsável pelo tratamento de pleno direito, dependendo das circunstâncias concretas. Por exemplo, pode ser esse o caso se o prestador de serviços proceder ao tratamento dos dados para as suas próprias finalidades.

É de salientar que, até mesmo em situações complexas de tratamento de dados, em que diferentes responsáveis pelo tratamento desempenham um papel no tratamento dos dados pessoais, o cumprimento das normas sobre proteção de dados e a responsabilidade por eventuais violações das mesmas devem estar claramente atribuídos, a fim de evitar uma redução do grau de proteção dos dados pessoais ou a ocorrência de um «conflito negativo de competências» e lacunas, em que algumas obrigações ou direitos decorrentes da diretiva não sejam assegurados por nenhuma das partes.

No atual cenário de computação em nuvem, os clientes destes serviços podem não ter margem de manobra na negociação das condições contratuais da respetiva utilização uma vez que uma característica de muitos serviços de computação em nuvem é oferecerem condições normalizadas. No entanto, é em última análise o cliente que decide sobre a atribuição de parte ou da totalidade das operações de tratamento a serviços de computação em nuvem para finalidades específicas, pelo que o papel do prestador desses serviços será o de um contratante perante o cliente, o que constitui o ponto essencial no presente caso. Conforme consta do Parecer do Grupo de Trabalho instituído pelo artigo 29.º[12] sobre os conceitos de responsável pelo tratamento e subcontratante, «*o desequilíbrio na relação contratual entre um pequeno responsável pelo tratamento de dados e uma grande empresa de prestação de serviços não pode ser invocado como justificação para a aceitação de cláusulas e condições incompatíveis com a legislação sobre proteção de dados por parte do responsável pelo tratamento*». Por esta razão, o responsável pelo tratamento de dados deve escolher um prestador de serviços de computação em nuvem que garanta o cumprimento da legislação em matéria de proteção de

---

9 O presente parecer incide apenas na relação normal entre o responsável pelo tratamento e o subcontratante.

10 O ambiente de computação em nuvem também pode ser utilizado por pessoas singulares (utilizadores) para a realização de atividades exclusivamente pessoais ou domésticas. Nesse caso, deve analisar-se cuidadosamente se é aplicável a chamada exceção doméstica que isenta os utilizadores da qualificação de responsáveis pelo tratamento de dados. Contudo, esta questão está fora do âmbito do presente parecer.

11 Por exemplo, nível das instruções, fiscalização por parte do cliente do serviço de computação em nuvem, competências especializadas das partes

12 Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_pt.pdf

dados. Deve ser colocada especial ênfase nas modalidades dos contratos aplicáveis — devendo estas incluir um conjunto de salvaguardas normalizadas em matéria de proteção de dados, nomeadamente as definidas pelo GT nos pontos 3.4.3 (Medidas técnicas e organizativas) e 3.5 (Transferências internacionais) — bem como de eventuais mecanismos adicionais que se possam revelar adequados para facilitar a devida diligência e a responsabilização (tais como auditorias de terceiros independentes e certificação dos serviços de um prestador de serviços — ver ponto 4.2).

Os prestadores de serviços de computação em nuvem (na sua qualidade de subcontratantes) têm o dever de assegurar a confidencialidade. A Diretiva 95/46/CE estabelece que: «*Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais, não procederá ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais*». O acesso aos dados por parte do prestador de serviços de computação em nuvem durante o período em que presta esses serviços é também fundamentalmente regido pelos requisitos de cumprimento das disposições do artigo 17.º da diretiva - ver ponto 3.4.2.

Os subcontratantes devem ter em conta o tipo de computação em nuvem em causa (pública, privada, comunitária ou híbrida/IaaS, SaaS ou PaaS [ver anexo a) Modelos de implantação - b) Modelos de prestação de serviços]) e o tipo de serviço contratado pelo cliente. Os subcontratantes são responsáveis pela adoção de medidas de segurança consentâneas com a legislação da UE conforme aplicadas nas jurisdições do responsável pelo tratamento dos dados e do subcontratante. Os subcontratantes devem também apoiar e assistir o responsável pelo tratamento de dados no respeito dos direitos (exercidos) das pessoas em causa.

3.3.2 Subcontratantes

Os serviços de computação em nuvem podem implicar a participação de várias partes contratantes que atuam na qualidade de subcontratantes. É também comum os subcontratantes contratarem subcontratantes ulteriores adicionais, os quais obtêm assim acesso a dados pessoais. Se subcontratarem serviços a subcontratantes ulteriores, os subcontratantes são obrigados a disponibilizar essa informação ao cliente, especificando o tipo de serviço objeto de subcontratação, as características dos atuais ou potenciais subcontratantes ulteriores e as garantias que essas entidades oferecem ao prestador de serviços de computação em nuvem para fins de cumprimento do disposto na Diretiva 95/46/CE.

Por conseguinte, todas as obrigações relevantes devem também ser aplicáveis aos subcontratantes ulteriores mediante contratos celebrados entre o prestador de serviços de computação em nuvem e o subcontratante ulterior que transponham as disposições do contrato celebrado entre o cliente e o prestador desses mesmos serviços. No seu Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante», o Grupo de Trabalho instituído pelo artigo 29.º refere a multiplicidade de subcontratantes em casos em que estes podem ter uma relação direta com o responsável pelo tratamento dos dados ou atuam na qualidade de subcontratantes ulteriores quando os subcontratantes externalizam parte do trabalho de tratamento de dados de que foram incumbidos. «*A diretiva não impede que, devido a requisitos organizativos, várias entidades possam ser designadas como subcontratantes (diretos ou indiretos), subdividindo as tarefas em causa. No entanto, todas elas devem cumprir as instruções emitidas pelo responsável pelo tratamento na realização das atividades de tratamento*»[13].

[13] Ver GT 169, Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

Nesses cenários, as obrigações e responsabilidades decorrentes da legislação em matéria de proteção de dados deve ser claramente definidas e não ser dispersas ao longo de toda a cadeia da externalização ou de subcontratação, a fim de assegurar o controlo efetivo das atividades de tratamento e a atribuição de responsabilidades claras.

Um modelo possível de garantias que pode ser utilizado para clarificar os direitos e obrigações dos subcontratantes quando subcontratam atividades de tratamento foi introduzido pela primeira vez pela Decisão da Comissão de 5 de fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros[14]. Nesse modelo, é permitida a subcontratação ulterior apenas com o consentimento prévio escrito do responsável pelo tratamento e com um acordo escrito que imponha ao subcontratante ulterior obrigações idênticas àquelas a que está sujeito o subcontratante. Em caso de incumprimento pelo subcontratante ulterior das obrigações em matéria de proteção de dados que lhe incumbem nos termos do referido acordo escrito, o subcontratante continua a ser plenamente responsável perante o responsável pelo tratamento de dados pelo cumprimento das obrigações do subcontratante ulterior ao abrigo do referido acordo. Uma disposição deste tipo pode ser utilizada em quaisquer cláusulas contratuais entre um responsável pelo tratamento de dados e um prestador de serviços de computação em nuvem, quando este último tenciona prestar serviços recorrendo a subcontratação, a fim de assegurar as garantias necessárias na subcontratação ulterior.

A Comissão propôs recentemente uma solução similar em matéria de garantias aplicáveis a subcontratação ulterior na proposta relativa ao Regulamento Geral sobre Proteção de Dados[15]. Os atos do subcontratante devem ser regidos por um contrato ou outro ato jurídico que o vincule ao responsável pelo tratamento de dados e que estipule, designadamente, que, entre outros requisitos, o subcontratante apenas recorrerá a outro subcontratante com a autorização prévia do responsável pelo tratamento (artigo 26.º, n.º 2, da proposta).

Na opinião do GT 29, o subcontratante só pode subcontratar as suas atividades com o consentimento do responsável pelo tratamento, que pode, de modo geral, ser dado no início do serviço[16] com a obrigação clara de o subcontratante informar o responsável pelo tratamento de quaisquer alterações previstas relativas à adição ou substituição de subcontratantes ulteriores, mantendo o responsável pelo tratamento permanentemente a possibilidade de apresentar objeções a essas alterações ou de rescindir o contrato. Deve existir uma obrigação clara de o prestador de serviços de computação em nuvem facultar o nome de todos os subcontratantes utilizados. Além disso, devia ser assinado um contrato entre o prestador de serviços de computação em nuvem e o subcontratante que transponha as disposições do contrato celebrado entre o cliente e o prestador de serviços de computação em nuvem. O responsável pelo tratamento deve poder utilizar as possibilidades contratuais de recurso em caso de violações do contrato causadas por subcontratantes ulteriores. Para esse fim, poder-se-ia garantir que o subcontratante seja diretamente responsável perante o responsável pelo tratamento de dados por quaisquer violações causadas por subcontratantes ulteriores por ele contratados ou poder-se-ia criar um direito de terceiro beneficiário em benefício do responsável pelo tratamento de dados nos contratos assinados entre o subcontratante e os subcontratantes ulteriores ou prever que esses contratos sejam assinados

[14] Ver FAQ, ponto II.5 do GT 176.

[15] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares relativamente ao tratamento de dados pessoais pelas instituições e organismos comunitários e sobre a livre circulação desses dados, 25.1.2012.

[16] Ver FAQ II, 1) do GT 176, adotadas em 12 de julho de 2010.

em nome do responsável pelo tratamento de dados, o que faz deste último uma parte no contrato.

3.4 Requisitos em matéria de proteção de dados na relação entre o cliente e o prestador de serviços

3.4.1 Cumprimento dos princípios básicos

A licitude do tratamento de dados pessoais no âmbito dos serviços de computação em nuvem depende da adesão aos princípios básicos da legislação da UE em matéria de proteção de dados. Deve, nomeadamente, ser garantida a transparência face à pessoa em causa e ser respeitado o princípio da especificação e limitação da finalidade e os dados pessoais devem ser apagados logo que a sua conservação já não seja necessária. Além disso, devem ser implementadas medidas técnicas e organizativas adequadas a fim de garantir um nível adequado de proteção e segurança dos dados.

3.4.1.1 Transparência

A transparência é de importância crucial para um tratamento justo e legítimo dos dados pessoais. A Diretiva 95/46/CE obriga o cliente de serviços de computação em nuvem a facultar à pessoa em causa, junto da qual recolha dados que lhe digam respeito, informações sobre a sua identidade e a finalidade do tratamento. O cliente dos serviços de computação em nuvem deve também facultar quaisquer informações, nomeadamente relativas aos destinatários ou categorias de destinatários dos dados, que podem também incluir subcontratantes e subcontratantes ulteriores na medida em que essas outras informações sejam necessárias para garantir um tratamento leal dos dados face à pessoa em causa (ver o artigo 10.º da diretiva)[17].

Deve igualmente ser assegurada a transparência na relação entre o cliente do serviço de computação em nuvem, o prestador desses serviços e os subcontratantes (caso existam). O cliente de serviços de computação em nuvem só pode avaliar a licitude do tratamento de dados pessoais no âmbito da computação em nuvem se o prestador de serviços o informar de todas as questões relevantes. Um responsável pelo tratamento de dados que considere a possibilidade de contratar um prestador de serviços de computação em nuvem deve verificar cuidadosamente os termos e condições do prestador desses serviços e avaliá-los numa perspetiva de proteção de dados.

A transparência no âmbito da computação em nuvem significa que é necessário que o cliente desses serviços seja informado de todos os subcontratantes que contribuem para a prestação do respetivo serviço de computação em nuvem, bem como da localização de todos os centros de dados em que os dados pessoais podem ser tratados.[18]

Caso a prestação do serviço exija a instalação de *software* nos sistemas do cliente de serviços de computação em nuvem (por exemplo, módulos de expansão (*plug-ins*) para o programa de navegação), o prestador desses serviços deve, por questão de boas práticas, informar o cliente dessa circunstância e, em particular, das suas implicações do ponto de vista da proteção e segurança dos dados. E vice-versa, o cliente de serviços de computação em nuvem deve

---

[17] O correspondente dever de informação da pessoa em causa existe quando os dados que não tenham sido recolhidos junto da pessoa em causa, mas a partir de diferentes fontes, são registados ou comunicados a terceiros (ver artigo 11.º)

[18] Só então poderá decidir se os dados pessoais podem ser transferidos para um chamado país terceiro fora do Espaço Económico Europeu (EEE) que não assegure um nível adequado de proteção na aceção da Diretiva 95/46/CE. Ver também a secção 3.4.6 infra.

apresentar essa questão *ex ante*, caso esta não seja abordada de forma suficiente pelo prestador desses serviços.

3.4.1.2 Especificação e limitação da finalidade

O princípio da especificação e limitação da finalidade determina que os dados pessoais devem ser recolhidos para finalidades especificadas, explícitas e legítimas e que não serão posteriormente tratados de forma incompatível com essas finalidades (ver artigo 6.º, n.º 1, alínea b), da Diretiva 95/46/CE). O cliente de serviços de computação em nuvem deve determinar a(s) finalidade(s) do tratamento antes da recolha dos dados pessoais da pessoa em causa e informá-la do facto. O cliente de serviços de computação em nuvem não deve proceder ao tratamento de dados pessoais para outras finalidades que não sejam compatíveis com as finalidades originais.

Além disso, há que assegurar que os dados pessoais não sejam tratados (ilicitamente) para outras finalidades pelo prestador de serviços de computação em nuvem ou por um dos seus subcontratantes. Uma vez que um cenário típico da computação em nuvem pode facilmente envolver um maior número de subcontratantes, o risco de tratamento de dados pessoais para outras finalidades incompatíveis deve, por conseguinte, ser avaliado como bastante elevado. A fim de minimizar este risco, o contrato celebrado entre o prestador de serviços de computação em nuvem e o respetivo cliente deve incluir medidas técnicas e organizativas para atenuar esse risco e proporcionar garantias sobre o registo e auditoria das operações de tratamento relevantes relativas a dados pessoas que sejam efetuadas por empregados do prestador de serviços de computação em nuvem ou por subcontratantes[19]. Devem ser impostas no contrato sanções aplicáveis ao prestador de serviços ou ao subcontratante em caso de violação da legislação em matéria de proteção de dados.

3.4.1.3 Apagamento de dados

Nos termos do artigo 6.º, n.º 1, alínea e), da Diretiva 95/46/CE, os dados pessoais devem ser conservados de forma a permitir a identificação das pessoas em causa apenas durante o tempo necessário para a prossecução das finalidades para que foram recolhidos os dados ou para o seu tratamento posterior. Os dados pessoais que já não sejam necessários devem ser apagados ou verdadeiramente anonimizados. Se estes dados não puderem ser apagados devido a disposições jurídicas em matéria de conservação (por exemplo, regulamentação fiscal), o acesso a esse dados pessoais deve ser bloqueado. Cabe ao cliente dos serviços de computação em nuvem a responsabilidade de assegurar que os dados pessoais sejam apagados logo que já não sejam necessários no sentido supramencionado[20].

O princípio de apagamento dos dados é aplicável aos dados pessoais, independentemente de estes estarem armazenados em discos rígidos ou noutros suportes de armazenamento de dados (por exemplo, bandas magnéticas de salvaguarda). Uma vez que os dados pessoais podem ser mantidos de forma redundante em diferentes servidores e em diferentes locais, deve garantir-se que todas as ocorrências desses dados sejam apagadas sem possibilidade de recuperação (ou seja, devem ser também apagadas versões anteriores, ficheiros temporários e mesmo fragmentos de ficheiros).

---

19 Ver também a secção 3.4.3 infra.

20 O apagamento de dados é uma questão que se coloca tanto ao longo de todo o período de duração de um contrato de serviços de computação em nuvem como após o seu termo. É igualmente pertinente no caso da substituição ou retirada de um subcontratante.

Os clientes de serviços de computação em nuvem devem estar cientes de que os dados de registo[21] que facilitam a realização de auditorias, por exemplo, sobre o armazenamento, alterações ou apagamento de dados, podem também ser considerados dados pessoais relativos à pessoa que iniciou o respetivo tratamento[22].

Para garantir o apagamento dos dados pessoais é necessário proceder à destruição ou desmagnetização dos meios de armazenamento ou à supressão efetiva dos dados pessoais armazenados mediante a reescrita de dados. Para fins de reescrita de dados pessoais, deverão ser utilizadas ferramentas informáticas especiais que reescrevem dados múltiplas vezes em conformidade com uma especificação reconhecida.

O cliente de serviços de computação em nuvem deve certificar-se que o prestador desses serviços garante o apagamento seguro dos dados na aceção supramencionada e que o contrato entre o prestador de serviços e o cliente contém disposições claras relativas ao apagamento de dados pessoais[23]. O mesmo se aplica aos contratos celebrados entre os prestadores de serviços de computação em nuvem e os subcontratantes.

3.4.2 Salvaguardas contratuais da(s) relação(ões) entre o «responsável pelo tratamento» e o «subcontratante»

Quando decidem contratar serviços de computação em nuvem, os responsáveis pelo tratamento de dados são obrigados a escolher um subcontratante que ofereça garantias suficientes no que se refere às medidas de segurança técnica e de organização do tratamento a efetuar e devem zelar pelo cumprimento dessas medidas (artigo 17.º, n.º 2, da Diretiva 95/46/CE). Além disso, têm a obrigação legal de assinar um contrato formal com o prestador de serviços de computação em nuvem, tal como estabelecido no artigo 17.º, n.º 3, da Diretiva 95/46/CE. O referido artigo estabelece que a relação entre o responsável pelo tratamento e o subcontratante deverá ser regida por um contrato ou outro ato jurídico vinculativo. Para efeitos de conservação de provas, os elementos do contrato ou do ato jurídico relativos à proteção dos dados, bem como o requisitos relativos às medidas técnicas e organizativas, devem ser consignados por escrito ou sob forma equivalente.

O contrato deve, no mínimo, estabelecer o facto de, em especial, o subcontratante dever seguir as instruções do responsável pelo tratamento dos dados e aplicar medidas técnicas e organizativas para a proteção adequada dos dados pessoais.

A fim de garantir a segurança jurídica, o contrato deve igualmente conter os seguintes elementos:

1. Informações pormenorizadas sobre (o âmbito e as modalidades de) instruções do cliente a fornecer ao prestador de serviços, em especial no que diz respeito aos acordos sobre o nível de serviço aplicáveis (que devem ser objetivos e mensuráveis) e às sanções relevantes (financeiras ou outras, incluindo a capacidade de processar o prestador de serviços em caso de incumprimento).
2. Especificação das medidas de segurança que o prestador de serviços de computação em nuvem deve aplicar, em função dos riscos inerentes ao tratamento e à natureza dos dados a proteger. É de grande importância que sejam especificadas medidas técnicas e organizativas concretas, tais como as referidas no ponto 3.4.3 infra. Estas em nada

[21] No ponto 4.3.4.2 são apresentadas observações sobre os requisitos relativos a registo de dados.

[22] Isto significa que devem ser definidos períodos razoáveis para a conservação de ficheiros de registo e que devem estar criados processos que salvaguardem o apagamento ou anonimização atempados desses dados.

[23] Ver também a secção 3.4.3 infra.

prejudicam a aplicação de disposições mais rigorosas, caso existam, que possam ser consideradas ao abrigo do direito nacional do cliente.

3. Objeto e escala temporal do serviço de computação em nuvem a fornecer pelo prestador de serviços, extensão, forma e finalidade do tratamento de dados pessoais pelo prestador desses serviços, bem como tipos de dados pessoais tratados.
4. Especificação das condições para a devolução dos dados (pessoais) ou a destruição dos dados uma vez concluído o serviço. Além disso, há que assegurar que os dados pessoais sejam apagados em condições de segurança a pedido do cliente dos serviços de computação em nuvem.
5. Inclusão de uma cláusula de confidencialidade vinculativa tanto para o prestador de serviços de computação em nuvem como para todos os seus empregados que possam ter acesso aos dados. Apenas as pessoas autorizadas podem ter acesso aos dados.
6. Obrigação por parte do prestador de serviços de apoiar o cliente na facilitação do exercício dos direitos das pessoas em causa de acederem aos seus dados e de os corrigirem ou suprimirem.
7. O contrato deve estabelecer expressamente que o prestador de serviços de computação em nuvem não pode comunicar os dados a terceiros, mesmo para fins de conservação, exceto se estiver previsto no contrato que haverá subcontratantes. O contrato deve especificar que os subcontratantes ulteriores só podem ser contratados com consentimento que pode, em geral, ser dado pelo responsável pelo tratamento dos dados em consonância com o dever claro de o subcontratante informar o responsável pelo tratamento de dados de quaisquer alterações previstas a este respeito, mantendo o responsável pelo tratamento permanentemente a possibilidade de se opor a essas alterações ou de rescindir o contrato. Deve haver uma obrigação clara por parte do prestador de serviços de computação em nuvem de indicar o nome de todos os subcontratantes contratados (por exemplo, num registo digital público). Deve ser assegurado que os contratos celebrados entre o prestador de serviços de computação em nuvem e o subcontratante transponham as disposições do contrato celebrado entre o cliente dos serviços de computação em nuvem e o prestador desses serviços (ou seja, que os subcontratantes ulteriores estejam sujeitos a deveres contratuais idênticos aos do prestador de serviços de computação em nuvem). Em particular, deve garantir-se que tanto o prestador de serviços de computação em nuvem como todos os subcontratantes apenas atuarão de acordo com instruções dadas pelo cliente dos referidos serviços. Conforme explicado no capítulo relativo a subcontratação ulterior, a cadeia de responsabilidades deve ser claramente indicada no contrato. Deve estabelecer-se que o subcontratante tem a obrigação de enquadrar as transferências internacionais mediante, por exemplo, a assinatura de contratos com subcontratantes ulteriores, com base nas cláusulas contratuais-tipo estabelecidas na Decisão 2010/87/UE.
8. Clarificação da obrigação do prestador de serviços de computação em nuvem de notificar o cliente dos referidos serviços em caso de violação de dados que afete os dados do cliente desses mesmos serviços.
9. Obrigação do prestador de serviços de computação em nuvem de facultar uma lista dos locais em que os dados podem ser tratados.
10. Direito do responsável pelo tratamento de fiscalizar e correspondente obrigação do prestador de serviços de computação em nuvem de cooperar.

11. Deve ser estabelecido contratualmente que o prestador de serviços de computação em nuvem deve informar o cliente sobre alterações relevantes referentes ao respetivo serviço, tais como a implementação de funções adicionais.
12. O contrato deve prever o registo e a auditoria das operações de tratamento de dados pessoais relevantes que sejam efetuadas pelo prestador de serviços de computação em nuvem ou pelos subcontratantes.
13. Notificação do cliente de serviços de computação em nuvem sobre qualquer pedido juridicamente vinculativo de divulgação de dados pessoais por parte de uma autoridade competente para a aplicação da lei, a não ser que exista uma proibição em contrário como, por exemplo, uma proibição prevista no direito penal para preservar a confidencialidade de uma investigação policial.
14. Obrigação geral de o prestador de serviços garantir que a sua organização interna e as modalidades de tratamento de dados (e os dos seus subcontratantes ulteriores, se for o caso) estão conformes com as normas e requisitos jurídicos nacionais e internacionais aplicáveis.

Em caso de violação por parte do responsável pelo tratamento de dados, qualquer pessoa que tenha sofrido danos decorrentes de tratamento ilícito de dados tem o direito de obter desse responsável a reparação pelos prejuízos causados. Caso utilizem os dados para quaisquer outras finalidades ou os comuniquem ou utilizem de uma forma que viole o contrato, os subcontratantes serão igualmente considerados responsáveis pelo tratamento dos dados e serão responsabilizados pelas violações em que estejam pessoalmente envolvidos.

É de salientar que, em muitos casos, os prestadores de serviços de computação em nuvem propõem serviços e contratos normalizados a assinar pelos responsáveis pelo tratamento dos dados, que estabelecem um formato normalizado para o tratamento de dados pessoais. O desequilíbrio na relação contratual entre um pequeno responsável pelo tratamento de dados e uma grande empresa de prestação de serviços não pode ser invocado pelo primeiro como justificação para a aceitação de cláusulas e condições incompatíveis com a legislação sobre proteção de dados.

3.4.3 Medidas técnicas e organizativas relativas à proteção e segurança dos dados

O artigo 17.º, n.º 2, da Diretiva 95/46/CE atribui plena responsabilidade aos clientes dos serviços de computação em nuvem (que atuem na qualidade de responsáveis pelo tratamento) pela escolha de prestadores desses serviços que apliquem medidas de segurança técnica e organizativa adequadas para proteger os dados pessoais e que possam demonstrar o seu sentido de responsabilidade.

Para além dos objetivos de segurança de base relativos à disponibilidade, confidencialidade e integridade, deve também chamar-se a atenção para as metas complementares de proteção de dados relativas a transparência (ver ponto 3.4.1.1 supra), isolamento[24], capacidade de intervenção, responsabilidade e portabilidade. A presente secção destaca estas metas centrais de proteção de dados, sem prejuízo de outras análises de risco complementares orientadas para questões de segurança[25].

[24] Na Alemanha, foi introduzido o conceito mais lato de «inviabilidade de ligação» (*unlinkability)* que é promovido pela Conferência dos Comissários para a Proteção de Dados.

[25] Ver, por exemplo,. ENISA em: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

3.4.3.1 Disponibilidade

Por disponibilização entende-se garantir o acesso atempado e fiável aos dados pessoais.

Uma ameaça grave à disponibilidade nos serviços de computação em nuvem é a quebra acidental de ligação à rede entre o cliente e o prestador de serviços ou de desempenho do servidor devido a ações maliciosas, tais como ataques de recusa de serviços (distribuídos) (*Distributed Denial of Service* -DoS)[26]. Entre outros riscos relativos à disponibilidade contam-se falhas acidentais dos equipamentos, quer na rede quer nos sistemas de computação em nuvem para armazenamento e tratamento de dados, falhas de energia elétrica e outros problemas com infraestruturas.

Os responsáveis pelo tratamento de dados devem verificar se o prestador de serviços de computação em nuvem adotou medidas razoáveis para fazer face aos riscos de perturbações, tais como ligações alternativas à internet e mecanismos redundantes e eficazes de armazenamento e salvaguarda de dados.

3.4.3.2 Integridade

A integridade pode ser definida como a propriedade que garante que os dados são autênticos e não foram alterados acidental ou intencionalmente durante o tratamento, armazenamento ou transmissão. O conceito de integridade pode ser alargado a sistemas informáticos e exige que o tratamento de dados pessoais nesses sistemas permaneça inalterado.

A deteção de alterações aos dados pessoais pode obter-se mediante mecanismos de autenticação criptográfica, tais como códigos ou assinaturas de autenticação de mensagens.

A interferência com a integridade dos sistemas informáticos no serviço de computação em nuvem pode ser evitada ou detetada por meio de sistemas de deteção/prevenção de intrusão (*intrusion prevention/detection systems* - IPS/IDS). Este aspeto é particularmente importante no tipo de ambientes de rede aberta em que geralmente operam os serviços de computação em nuvem.

3.4.3.3 Confidencialidade

Num ambiente de computação em nuvem, a cifragem pode contribuir de forma significativa para garantir a confidencialidade dos dados pessoais se for aplicada corretamente, embora não torne os dados pessoais irreversivelmente anónimos[27]. A cifragem de dados pessoais deve ser utilizada em todos os casos para dados «em trânsito» e sempre que disponível para dados «em repouso»[28]. Em alguns casos (por exemplo, serviços de armazenamento IaaS), o cliente do serviço de computação em nuvem pode não confiar na solução de cifragem oferecida pelo prestador de serviços, optando por cifrar os dados pessoais antes do seu envio para o serviço de computação em nuvem. A cifragem de dados em repouso exige uma especial atenção

---

[26] Um ataque sob a forma de negação de serviço («*DoS attack*») é uma tentativa coordenada para tornar indisponível um recurso de um computador ou de uma rede relativamente aos seus utilizadores autorizados, quer temporariamente quer por um período indeterminado (por exemplo, por meio de um grande número de sistemas de ataque que paralisam o seu alvo com uma multitude de pedidos de comunicação externa).

[27] Diretiva 95/46/CE - Considerando 26: «(...) *considerando que os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável; (...)*». Na mesma linha, os processos técnicos de fragmentação de dados que podem ser utilizados no âmbito da prestação de serviços de computação em nuvem não permitirão uma anonimização irreversível, pelo que não implicam a não-aplicação das obrigações em matéria de proteção dos dados.

[28] É o caso, nomeadamente, dos responsáveis pelo tratamento de dados que desejam transferir dados sensíveis na aceção do artigo 8.º da Diretiva 95/46/CE (por exemplo, dados no domínio da saúde) para os serviços de computação em nuvem ou que estão sujeitos a obrigações legais específicas de sigilo profissional.

quanto à gestão da chave criptográfica, uma vez que a segurança dos dados depende então, em última análise, da confidencialidade das chaves de cifragem.

As comunicações entre o prestador de serviços de computação em nuvem e o cliente, bem como entre os centros de dados, devem ser cifradas. A administração à distância da plataforma de computação em nuvem só deve fazer-se através de um canal de comunicação seguro. Se um cliente desejar não só armazenar, mas também proceder ao tratamento dos dados pessoais no âmbito do serviço de computação em nuvem (por exemplo, para a pesquisa de registos em bases de dados), deve ter em conta que a cifragem não pode ser mantida durante o tratamento dos dados (exceto em processos de tratamento muito específicos).

Entre outras medidas técnicas que visam garantir a confidencialidade contam-se os mecanismos de autorização e de autenticação profunda (por exemplo, autenticação bi-fatorial). As cláusulas contratuais devem também impor obrigações de confidencialidade aos empregados de clientes de serviços de computação em nuvem e respetivos prestadores de serviços e subcontratantes.

3.4.3.4 Transparência

As medidas técnicas e organizativas devem promover a transparência a fim de permitir a sua análise (ver ponto 3.4.1.1).

3.4.3.5 Isolamento (limitação da finalidade)

No âmbito dos serviços de computação em nuvem, as infraestruturas, os recursos como o armazenamento, a memória e as redes são partilhados entre muitos clientes. Esta situação gera novos riscos de divulgação e tratamento de dados para fins ilegítimos. A meta de proteção relativa ao «isolamento» incide nesta questão e contribui para garantir que os dados sejam utilizados apenas para a sua finalidade inicial (artigo 6.º, n.º 1, alínea b), da Diretiva 95/46/CE) e para manter a sua confidencialidade e integridade[29].

Para fins de isolamento, é primeiro necessária uma governação adequada dos direitos e perfis de acesso aos dados pessoais, que seja revista periodicamente. Deve ser evitada a utilização de perfis com privilégios excessivos (por exemplo, nenhum utilizador ou administrador deve ser autorizado a aceder a toda a plataforma de computação em nuvem). De um modo mais geral, os administradores e os utilizadores devem ter apenas acesso à informação que seja necessária para os seus fins legítimos (princípio do menor privilégio).

Em segundo lugar, o isolamento depende igualmente de medidas técnicas, tais como o endurecimento de hipervisores e a boa gestão dos recursos partilhados se forem utilizadas máquinas virtuais para partilhar recursos físicos entre diferentes clientes de serviços de computação em nuvem.

3.4.3.5 Capacidade de intervenção

A Diretiva 95/46/CE confere à pessoa em causa os direitos de acesso, retificação, apagamento, bloqueio e oposição (ver artigos 12.º e 14.º). O cliente de serviços de computação em nuvem deve verificar que o prestador desses serviços não impõe obstáculos técnicos e organizativos a estes requisitos, inclusive nos casos em que os dados são objeto de tratamento complementar por parte de subcontratantes.

[29] Ver ponto 3.4.1.2.

O contrato entre o cliente e o prestador de serviços deve estipular que o prestador de serviços de computação em nuvem está obrigado a dar apoio ao cliente a fim de facilitar o exercício dos direitos das pessoas em causa e de garantir que o mesmo acontece na sua relação com qualquer subcontratante[30].

3.4.3.6 Portabilidade

Atualmente, a maior parte dos prestadores de serviços de computação em nuvem não utiliza formatos de dados normalizados e interfaces de serviços que facilitem a interoperabilidade e a portabilidade entre diferentes prestadores desses serviços. Se o cliente de um serviço de computação em nuvem decidir migrar de um prestador de serviços para outro, esta falta de interoperabilidade pode resultar na impossibilidade ou, pelo menos, em dificuldades de transferência dos dados (pessoais) do cliente para o novo prestador de serviços (dependência em relação a um único vendedor). O mesmo se aplica aos serviços que o cliente tenha desenvolvido numa plataforma oferecida pelo prestador de serviços de computação em nuvem inicial (PaaS). O cliente de serviços de computação em nuvem deve verificar se e de que modo o prestador de serviços garante a portabilidade dos dados e serviços antes de contratar um serviço de computação em nuvem[31].

3.4.4.7 Responsabilidade

No domínio das tecnologias da informação, a responsabilidade pode ser definida como a capacidade para determinar o que uma entidade fez num determinado momento no passado e o modo como o fez. Em matéria de proteção de dados, adquire frequentemente uma aceção mais lata e descreve a capacidade das partes para demonstrar que tomaram as medidas adequadas para garantir que foram aplicados os princípios relativos à proteção de dados.

A responsabilidade no domínio das tecnologias da informação é particularmente importante para investigar violações de dados pessoais, em que os clientes de serviços de computação em nuvem, os prestadores desses serviços e os subcontratantes ulteriores podem cada um deles ter um certo grau de responsabilidade operacional. Quanto a este aspeto, é de importância primordial a capacidade da plataforma de computação em nuvem de proporcionar mecanismos de fiscalização fiáveis e mecanismos de registo exaustivo.

Além disso, os prestadores de serviços de computação em nuvem devem apresentar provas documentais da implementação de medidas adequadas e eficazes que permitam obter os resultados visados nos princípios de proteção de dados enunciados nas secções anteriores. Exemplos dessas medidas são procedimentos para assegurar a identificação de todas as operações de tratamento de dados, a resposta a todos os pedidos de acesso, a atribuição de recursos, incluindo a designação de pessoas responsáveis pela proteção de dados que sejam responsáveis pela organização do cumprimento das disposições relativas à proteção de dados, ou procedimentos de certificação independentes. Além disso, os responsáveis pelo tratamento de dados devem garantir que estão preparados para demonstrar à autoridade supervisora competente, a pedido desta[32], que foram adotadas as medidas necessárias.

---

30 Ver ponto 3.4.2, n.º 6 supra. O prestador de serviços pode mesmo ser instruído para responder a pedidos em nome do cliente.

31 De preferência, o prestador de serviços deve utilizar interfaces e formatos de dados normalizados ou abertos. Em qualquer caso, devem ser acordadas cláusulas contratuais que estipulem formatos assegurados, a preservação de relações lógicas e quaisquer custos decorrentes da migração para um outro prestador de serviços de computação em nuvem.

32 O Grupo de Trabalho apresentou observações pormenorizadas sobre a questão da responsabilidade no seu Parecer 3/2010 sobre o princípio da responsabilidade: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_pt.pdf.

3.5 Transferências internacionais

Os artigos 25.º e 26.º da Diretiva 95/46/CE preveem a livre circulação de dados pessoais para países situados fora do EEE apenas se esse país ou destinatário proporcionar um nível adequado de proteção de dados. Caso contrário, o responsável pelo tratamento de dados e os seus corresponsáveis e/ou subcontratantes devem estabelecer salvaguardas específicas. No entanto, a computação em nuvem caracteriza-se mais frequentemente por uma completa ausência de localização estável dentro da rede do prestador desses serviços. Os dados podem encontrar-se num centro de dados às 2 horas da tarde e encontrar-se no outro lado do mundo às 4 horas da tarde. Por conseguinte, o cliente de serviços de computação em nuvem encontra-se raramente em posição de saber, em tempo real, onde os dados estão localizados, armazenados ou em trânsito. Neste contexto, verificam-se limitações nos instrumentos jurídicos tradicionais que proporcionam um quadro regulamentar aplicável às transferências de dados para países terceiros não membros da UE que não proporcionem uma proteção adequada.

3.5.1 Porto seguro e países adequados

A fundamentação da adequação, nomeadamente de «porto seguro» (*Safe Harbor*), é limitada no que se refere ao âmbito geográfico, pelo que não abrange todas as transferências no âmbito de serviços de computação em nuvem.
As transferências para organizações dos EUA que aderem aos princípios podem processar-se licitamente ao abrigo da legislação da UE, uma vez que se considera que os organismos destinatários proporcionam um nível adequado de proteção dos dados transferidos.

No entanto, no entender do Grupo de Trabalho, a autocertificação apenas com base em «porto seguro» pode não ser considerada suficiente na ausência de um sólido controlo da aplicação dos princípios de proteção de dados no ambiente de computação em nuvem. Além disso, o artigo 17.º da diretiva da UE exige a assinatura de um contrato entre o responsável pelo tratamento de dados e o subcontratante para fins de tratamento de dados, o que é confirmado no ponto 10 das FAQ dos documentos-quadro da UE-EUA relativos a «porto seguro». O referido contrato não está sujeito a autorização prévia das autoridades europeias responsáveis pela proteção de dados. O contrato especifica o tratamento a efetuar e quaisquer outras medidas necessárias para garantir que esses dados sejam mantidos em condições de segurança. As diversas legislações e autoridades nacionais responsáveis pela proteção de dados podem exigir requisitos adicionais.

O Grupo de Trabalho considera que as empresas que exportam dados não devem confiar apenas na declaração do importador de dados que afirma ter uma certificação de «porto seguro». Pelo contrário, a empresa que exporta dados deve obter provas de que a autocertificação de «porto seguro» existe e solicitar elementos de prova que demonstrem que os seus princípios são respeitados. Isto é importante sobretudo no que diz respeito às informações fornecidas às pessoas em causa afetadas pelo tratamento de dados[33, 34].

O Grupo de Trabalho considera igualmente que o cliente de serviços de computação em nuvem deve verificar se os contratos-tipo elaborados pelos prestadores destes serviços estão em conformidade com os requisitos nacionais no que diz respeito a cláusulas relativas a

---

[33] Ver Autoridade responsável pela Proteção de Dados (APD) da Alemanha: http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

[34] Relativamente a requisitos para a contratação de subcontratantes ulteriores, ver ponto 3.3.2.

tratamento de dados. A legislação nacional pode exigir que a subcontratação ulterior seja definida no contrato, o que inclui as localizações e outros dados relativos aos subcontratantes ulteriores, bem como a rastreabilidade dos dados. Normalmente, os prestadores de serviços de computação em nuvem não facultam ao cliente essas informações – mas a sua adesão aos princípios de «porto seguro» não pode compensar a ausência das garantias supramencionadas quando exigidas pela legislação nacional. Nestes casos, o exportador é encorajado a utilizar outros instrumentos jurídicos disponíveis, como as cláusulas contratuais-tipo ou as regras vinculativas para empresas.

Por último, o Grupo de Trabalho considera que os princípios de «porto seguro» por si só podem também não garantir ao exportador de dados os meios necessários para assegurar que o prestador de serviços de computação em nuvem nos EUA tenha aplicado as medidas de segurança adequadas que possam ser exigidas pelas legislações nacionais ao abrigo da Diretiva 95/46/CE[35]. Em termos de segurança dos dados, a computação em nuvem suscita vários riscos que lhe são específicos, como a perda de governação, o apagamento incompleto dos dados ou sem a devida segurança, pistas de auditoria insuficientes ou deficiências de isolamento[36], que não são suficientemente abordados nos atuais princípios de «porto seguro» relativos à segurança dos dados[37]. Por conseguinte, pode recorrer-se a salvaguardas adicionais para garantir a segurança dos dados, tais como integrar as competências e os recursos de terceiros que sejam capazes de avaliar a adequação dos prestadores de serviços de computação em nuvem mediante diferentes regimes de auditoria, normalização e certificação [38]. Por estas razões, poderá ser aconselhável complementar a adesão do importador de dados aos princípios de «porto seguro» com salvaguardas adicionais que tenham em conta a natureza específica da computação em nuvem.

3.5.2 Isenções

As isenções previstas no artigo 26.º da Diretiva 95/46 da UE permitem aos exportadores de dados transferir dados para fora da UE sem fornecer garantias suplementares. Contudo, o GT 29 emitiu um parecer em que considerou que as isenções só serão aplicáveis quando as transferências não têm caráter recorrente, maciço ou estrutural[39].

Com base nas referidas interpretações, é praticamente impossível invocar isenções no âmbito da computação em nuvem.

3.5.3 Cláusulas contratuais-tipo

As cláusulas contratuais-tipo conforme adotadas pela Comissão da UE para fins de enquadramento das transferências internacionais de dados entre dois responsáveis pelo tratamento de dados ou entre um responsável pelo tratamento de dados e um subcontratante baseiam-se numa abordagem bilateral. Quando o prestador de serviços de computação em nuvem é equiparado a subcontratante, as cláusulas-tipo conformes com a Decisão 2010/87/CE da Comissão são um instrumento que pode ser utilizado entre o subcontratante e o

---

35 Ver o parecer da APD da Dinamarca: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Descrição pormenorizada no documento da ENISA «C*loud Computing: Benefits, Risks and Recommendations for Information Security*» em: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 «As organizações devem tomar precauções razoáveis para evitar a perda, utilização indevida e acesso, revelação, alteração ou destruição não autorizados de informações pessoais».

38 Ver ponto 4.2 infra.

39 Documento de Trabalho 12/1998: Transferência de dados pessoais para países terceiros: Aplicação dos artigos 25.º e 26.º da Diretiva da UE relativa à proteção dos dados. Adotado pelo Grupo de Trabalho em 24 de julho de 1998 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_pt.pdf).

responsável pelo tratamento de dados como base para que a plataforma de computação em nuvem possa oferecer garantias adequadas no contexto das transferências internacionais.

Para além das cláusulas contratuais-tipo, o Grupo de Trabalho considera que os prestadores de serviços de computação em nuvem podem propor aos clientes disposições baseadas na sua experiência prática desde que as mesmas não contrariem, direta ou indiretamente, as cláusulas contratuais-tipo aprovadas pela Comissão nem prejudiquem os direitos ou liberdades fundamentais das pessoas em causa[40]. No entanto, as empresas não podem emendar ou alterar as cláusulas contratuais-tipo sem indicar que essas cláusulas já não são «cláusulas-tipo»[41].

Quando o prestador de serviços de computação em nuvem que atua na qualidade de subcontratante está estabelecido na UE, a situação poderá ser mais complexa, uma vez que as cláusulas-tipo apenas são aplicáveis, em geral, à transferência de dados de um responsável pelo tratamento de dados da UE para um subcontratante fora da UE (ver considerando 23 da Decisão 2010/87/UE da Comissão relativa a cláusulas-tipo e GT 176).

No que diz respeito à relação contratual entre o subcontratante fora da UE e os subcontratantes ulteriores, deve ser celebrado um acordo escrito que imponha obrigações ao subcontratante ulterior idênticas às impostas ao subcontratante nas cláusulas-tipo.

3.5.4 Regras vinculativas para empresas (BCR): para uma abordagem global

As regras vinculativas para empresas (*Binding Corporate Rules* - BCR) constituem um código de conduta aplicável às empresas que transferem dados no interior do seu grupo. Esse tipo de solução será também proporcionada no contexto da computação em nuvem quando o prestador de serviços é um subcontratante. Com efeito, o GT 29 está a trabalhar na elaboração de regras vinculativas para empresas aplicáveis a subcontratantes que permitirão a transferência no âmbito do grupo em benefício dos responsáveis pelo tratamento de dados sem que seja necessária a assinatura de contratos entre o subcontratante e os subcontratantes ulteriores, por cliente[42].

As referidas regras vinculativas para empresas aplicáveis a subcontratantes permitiriam ao cliente do prestador de serviços confiar os seus dados pessoais ao subcontratante com a garantia de que os dados transferidos no âmbito das atividades comerciais do prestador de serviços beneficiariam de um nível adequado de proteção.

4. Conclusões e recomendações

As empresas e as administrações que desejem utilizar a computação em nuvem devem proceder, numa primeira fase, a uma análise de risco aprofundada e exaustiva. A análise deve abordar os riscos relacionados com o tratamento de dados no âmbito da computação em nuvem (falta de controlo e informação insuficiente - ver ponto 2 supra) tendo em conta o tipo

---

40 Ver FAQ IV, B1.9 9: Podem as empresas incluir cláusulas contratuais-tipo num contrato mais vasto e adicionar cláusulas específicas?, publicado pela CE em: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

41 Ver FAQ IV B1.10: As empresas podem emendar e alterar as cláusulas contratuais-tipo aprovadas pela Comissão?

42 Ver Documento de Trabalho 02/2012 que estabelece uma tabela com os elementos e princípios constantes das regras vinculativas para empresas, adotado em 6 de junho de 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

de dados tratados nesse âmbito[43]. Deve também ser prestada especial atenção à avaliação dos riscos jurídicos em matéria de proteção de dados, que dizem principalmente respeito às obrigações de segurança e às transferências internacionais. O tratamento de dados sensíveis por via da computação em nuvem suscita ainda outras preocupações. Por conseguinte, sem prejuízo do disposto nas legislações nacionais, o referido tipo de tratamento exige salvaguardas adicionais[44]. As conclusões infra visam proporcionar uma lista de verificação para fins de conformidade em matéria de proteção de dados por parte dos clientes de serviços de computação em nuvem e dos respetivos prestadores de serviços com base no atual quadro jurídico. São também formuladas algumas recomendações com vista a uma evolução futura do quadro regulamentar a nível da UE e não só.

4.1 Orientações destinadas aos clientes e prestadores de serviços de computação em nuvem

- Relação entre o responsável pelo tratamento de dados e o subcontratante: O presente parecer incide na relação entre o cliente e o prestador de serviços como um relação entre um responsável pelo tratamento de dados e um subcontratante (ver ponto 3.3.1). No entanto, com base em circunstâncias concretas, podem verificar-se situações em que o prestador de serviços de computação em nuvem atue também como responsável pelo tratamento de dados, por exemplo, quando o prestador de serviços procede ao retratamento de alguns dados pessoais para os seus próprios fins. Nesse caso, o prestador de serviços de computação em nuvem tem plena responsabilidade (conjunta) pelo tratamento e deve cumprir todas as obrigações jurídicas estabelecidas nas Diretivas 95/46/CE e 2002/58/CE (se aplicável);

- Responsabilidade do cliente de serviços de computação em nuvem na qualidade de responsável pelo tratamento de dados: O cliente que é responsável pelo tratamento de dados deve aceitar a responsabilidade de respeitar a legislação relativa à proteção dos dados e está sujeito a todas as obrigações jurídicas referidas nas Diretivas 95/46/CE e 2002/58/CE, quando aplicável, particularmente perante as pessoas em causa (ver ponto 3.3.1). O cliente deve selecionar um prestador de serviços de computação em nuvem que garanta o cumprimento da legislação da UE em matéria de proteção de dados, tal como refletido nas cláusulas de salvaguarda adequadas a seguir resumidas;

- Salvaguardas aplicáveis à subcontratação: As disposições aplicáveis aos subcontratantes devem ser definidas em todos os contratos celebrados entre o prestador de serviços de computação em nuvens e os respetivos clientes. O contrato deve especificar que os subcontratantes ulteriores só podem ser contratados com base num consentimento que pode ser em geral dado pelo responsável pelo tratamento dos dados em consonância com um dever claro do subcontratante de informar o responsável pelo tratamento de dados de quaisquer alterações previstas a este respeito, mantendo o responsável pelo tratamento permanentemente a possibilidade de se opor a essas alterações ou de rescindir o contrato a qualquer momento. Deve haver uma obrigação clara por parte do prestador de serviços de computação em nuvem de indicar o nome de todos os subcontratantes contratados. O prestador de serviços de computação em nuvem deve assinar um contrato com cada subcontratante que transponha as disposições do seu contrato celebrado com o respetivo cliente; o cliente deve assegurar que goza de possibilidades contratuais de recurso em caso de violações do contrato por parte dos subcontratantes do prestador de serviços (ver ponto 3.3.2);

---

[43] A ENISA disponibiliza uma lista dos riscos que devem ser tomados em consideração: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[44] Ver o Memorando Sopot, nota de-pé-de-página 2 supra.

- Cumprimento dos princípios fundamentais de proteção de dados:
    - Transparência (ver ponto 3.4.1.1): Os prestadores de serviços de computação em nuvem devem informar os seus clientes de todos os aspetos relevantes (relativos a proteção de dados) dos seus serviços durante as negociações de contratos. Os clientes devem, em especial, ser informados sobre todos os subcontratantes que contribuem para a prestação dos serviços de computação em nuvem e sobre todos os locais em que os dados podem ser armazenados ou tratados pelo prestador de serviços e/ou pelos seus subcontratantes (nomeadamente, se alguns ou todos os locais se situarem fora do Espaço Económico Europeu (EEE)). Deve ser facultada ao cliente informação pertinente sobre as medidas técnicas e organizativas aplicadas pelo prestador de serviços; o cliente deve, por questão de boas práticas, informar as pessoas em causa sobre o prestador de serviços de computação em nuvem e todos os seus subcontratantes (se aplicável), bem como sobre os locais em que os dados podem ser armazenados ou tratados pelo prestador de serviços e/ou pelos seus subcontratantes;
    - Especificação e limitação da finalidade (ver ponto 3.4.1.2): O cliente deve assegurar o cumprimento dos princípios da especificação e limitação da finalidade e garantir que os dados não sejam tratados para outras finalidades pelo prestador de serviços ou por quaisquer subcontratantes. Os compromissos nesta matéria devem ser consagrados em disposições contratuais adequadas (incluindo garantias técnicas e organizativas);
    - Conservação de dados (ver ponto 3.4.1.3): O cliente é responsável por garantir que os dados pessoais sejam apagados (pelo prestador de serviços e quaisquer subcontratantes) onde quer que estejam armazenados logo que deixem de ser necessários para as finalidades específicas. Nas condições dos contratos devem ser previstos mecanismos de apagamento seguros (destruição, desmagnetização, reescrita);
- Garantias contratuais (ver pontos 3.4.2, 3.4.3 e 3.5.):
    - Em geral: O contrato celebrado com o prestador de serviços (e os contratos a celebrar entre o prestador de serviços e os subcontratantes) deve proporcionar garantias suficientes em termos de segurança técnica e de medidas organizativas (ao abrigo do artigo 17.º, n.º 2, da diretiva) que devem ser consignadas por escrito ou sob forma equivalente. O contrato deve especificar as instruções do cliente ao prestador de serviços, incluindo o objeto e a escala temporal do serviço, o objetivo e os níveis mensuráveis de serviço, bem como as sanções (financeiras ou outras) relevantes. Deve especificar as medidas de segurança a cumprir em função dos riscos do tratamento e da natureza dos dados, em conformidade com os requisitos apresentados infra e sob reserva de medidas mais rigorosas que possam estar previstas na legislação nacional do cliente. Se desejarem utilizar cláusulas contratuais-tipo, os prestadores de serviços de computação em nuvem devem garantir que essas condições estejam conformes com os requisitos de proteção de dados (ver ponto 3.4.2). Em especial, as medidas técnicas e organizativas implementadas pelo prestador de serviços devem ser especificadas nas respetivas condições;
    - Acesso a dados: Apenas as pessoas autorizadas devem ter acesso aos dados. Deve ser incluída no contrato uma cláusula de confidencialidade aplicável ao prestador de serviços e aos seus empregados;

- Divulgação de dados a terceiros: Esta questão deve ser regida apenas pelo contrato, que deve incluir a obrigação de o prestador de serviços indicar o nome todos os seus subcontratantes – por exemplo, num registo digital público – e assegurar o acesso do cliente a informações relativas a quaisquer alterações, a fim de lhe permitir opor-se a essas alterações ou rescindir o contrato. O contrato deve igualmente exigir que o prestador de serviços notifique qualquer pedido juridicamente vinculativo de divulgação dos dados pessoais por parte de uma autoridade competente para a aplicação da lei, a não ser que essa divulgação seja de outro modo proibida. O cliente deve garantir que o prestador de serviços rejeitará quaisquer pedidos de divulgação que não sejam juridicamente vinculativos;
- Obrigações de cooperação: O cliente deve assegurar que o prestador de serviços seja obrigado a cooperar no que diz respeito ao direito que assiste ao cliente de fiscalizar as operações de tratamento, a facilitar o exercício dos direitos das pessoas em causa relativas ao acesso/correção/apagamento dos seus dados e (quando aplicável) a notificar os clientes de serviços de computação em nuvem de qualquer violação de dados que afete os dados do cliente;
- Transferências transfronteiras de dados: O cliente de serviços de computação em nuvem deve verificar se o prestador desses serviços pode garantir a licitude das transferências transfronteiras de dados e limitar as transferências a países escolhidos pelo cliente, se possível. As transferências de dados para países terceiros não adequados exigem salvaguardas específicas mediante a utilização de modalidades de «porto seguro», de cláusulas contratuais-tipo (SCC) ou de regras vinculativas para empresas (BCR), conforme adequado. A utilização de cláusulas contratuais-tipo aplicáveis a subcontratantes (ao abrigo da Decisão 2010/87/CE da Comissão) exige determinadas adaptações ao ambiente da computação em nuvem (a fim de evitar que haja contratos separados para cada cliente celebrados entre um prestador de serviços e os seus subcontratantes ulteriores), que podem implicar a necessidade de autorização prévia da Autoridade responsável pela Proteção de Dados (APD) competente. A lista dos locais em que o serviço pode ser prestado deve ser incluída no contrato;
- Registo e auditoria do tratamento de dados: O cliente deve solicitar o registo das operações de tratamento efetuadas pelo prestador de serviços e pelos seus subcontratantes. O cliente deve estar habilitado a proceder à auditoria das referidas operações de tratamento, embora também possam ser aceitáveis a certificação e a auditoria por terceiros escolhidos pelo responsável pelo tratamento de dados, desde que seja garantida uma plena transparência (por exemplo, prevendo a possibilidade de obter uma cópia do certificado de auditoria de terceiros ou uma cópia do relatório de auditoria que verifica a certificação);
- Medidas técnicas e organizativas: Devem visar a correção dos riscos inerentes à falta de controlo e de informação que é a característica mais proeminente no ambiente da computação em nuvem. As primeiras incluem medidas destinadas a garantir a disponibilidade, integridade, confidencialidade, isolamento, capacidade de intervenção e portabilidade, conforme definido no documento, enquanto as últimas incidem na questão da transparência (ver ponto 3.4.3 para informações completas).

4.2 Certificações da proteção de dados por terceiros

- A verificação ou certificação independente por um terceiro reputado pode ser uma forma credível de os prestadores de serviços de computação em nuvem demonstrarem o cumprimento das suas obrigações, conforme especificado no presente parecer. A referida certificação indicaria, no mínimo, que os controlos relativos à proteção dos dados tinham sido sujeitos a auditoria ou exame por uma organização terceira reputada em função de uma norma reconhecida que satisfaça os requisitos definidos no presente parecer[45]. No contexto da computação em nuvem, os potenciais clientes devem procurar determinar se os prestadores de serviços de computação em nuvem podem facultar uma cópia do certificado de auditoria de terceiros ou uma cópia do relatório de auditoria que verifique a certificação, incluindo o respeito dos requisitos definidos no presente parecer.

- As auditorias individuais dos dados armazenados num ambiente de servidor virtualizado e com múltiplas partes podem ser impossíveis de um ponto de vista técnico, podendo em alguns casos aumentar os riscos inerentes aos controlos de segurança da rede física e lógica existentes. Nesses casos, pode considerar-se que uma auditoria relevante de terceiros escolhidos pelo responsável pelo tratamento de dados é adequada em lugar do direito de um responsável pelo tratamento de dados de proceder à auditoria.

- A adoção de normas e certificações especificamente relativas à privacidade é um aspeto essencial para o estabelecimento de uma relação de confiança entre os prestadores de serviços de computação em nuvem, os responsáveis pelo tratamento de dados e as pessoas em causa.

- Estas normas e certificações devem abordar medidas técnicas (como a localização ou a cifragem de dados), bem como os processos no âmbito da organização dos prestadores de serviços de computação em nuvem que garantam a proteção de dados (como as políticas de controlo do acesso, o controlo do acesso ou as cópias de segurança).

4.3 Recomendações: Evolução futura

O Grupo de Trabalho está plenamente consciente de que não é possível fazer face de modo pleno às complexidades da computação em nuvem com as salvaguardas e soluções descritas no presente parecer, o qual constitui, no entanto, uma base sólida para assegurar o tratamento dos dados pessoais que os clientes estabelecidos no EEE enviem a prestadores de serviços de computação em nuvem. A presente secção visa destacar algumas questões que é necessário abordar no curto a médio prazo a fim de reforçar as salvaguardas em vigor e assistir a indústria de computação em nuvem no que diz respeito às questões salientadas, assegurando simultaneamente o respeito dos direitos fundamentais de proteção da privacidade e dos dados.

- Melhor equilíbrio de responsabilidades entre o responsável pelo tratamento de dados e o subcontratante: O Grupo de Trabalho congratula-se com as disposições do artigo 26.º das propostas da Comissão (proposta de Regulamento Geral sobre Proteção de Dados da UE) que visam tornar os subcontratantes mais responsáveis perante os responsáveis pelo tratamento de dados, apoiando-os no sentido de assegurar o cumprimento, em especial, das obrigações de segurança e obrigações conexas. O artigo 30.° da proposta estabelece uma obrigação jurídica aplicável ao subcontratante de implementação de medidas técnicas

[45] As referidas normas incluiriam as publicadas pela Organização Internacional de Normalização, o *International Auditing and Assurance Standards Board* e o *Auditing Standards Board* do *American Institute of Certified Public Accountants* na medida em que estas organizações disponibilizam normas que satisfazem os requisitos estabelecidos no presente parecer.

e organizativas adequadas. Os projetos de propostas deixam claro que um subcontratante que não cumpra as instruções do responsável pelo tratamento de dados é equiparado a um responsável pelo tratamento de dados e está sujeito a regras específicas relativas a responsabilidade conjunta. O Grupo de Trabalho instituído pelo artigo 29.º considera que a referida proposta vai no bom sentido com vista a corrigir os desequilíbrios que são frequentes no ambiente de computação em nuvem, em que o cliente (especialmente se for uma PME) pode ter dificuldades em exercer o pleno controlo exigido pela legislação em matéria de proteção de dados sobre a forma como o prestador presta os serviços solicitados. Além disso, tendo em conta a situação jurídica assimétrica das pessoas em causa e das pequenas empresas utilizadoras face a grandes prestadores de serviços de computação em nuvem, recomenda-se às organizações de proteção dos consumidores e das empresas que tenham um papel mais proativo a fim de negociarem com essas empresas termos e condições gerais mais equilibrados.

- Acesso a dados pessoais para fins de segurança nacional e de controlo do cumprimento da lei: É da maior importância que seja introduzida no futuro regulamento a proibição de os responsáveis pelo tratamento de dados em operação na UE divulgarem dados pessoais a um país terceiro se tal for solicitado por uma autoridade judicial ou administrativa de um país terceiro, a menos que tal seja expressamente autorizado por um acordo internacional, esteja previsto em tratados de assistência jurídica mútua ou seja aprovado por uma autoridade de supervisão. O Regulamento (CE) n.º 2271/96 do Conselho é um bom exemplo de base jurídica nesta matéria[46]. Por essa razão, o Grupo de Trabalho está preocupado com esta lacuna na proposta da Comissão uma vez que implica uma perda considerável de segurança jurídica para as pessoas em causa, cujos dados pessoais estão armazenados em centros de dados espalhados por todo o mundo. O Grupo de Trabalho gostaria, pois, de sublinhar[47] a necessidade de incluir no regulamento a utilização obrigatória de tratados de auxílio judiciário mútuo nos casos de divulgação não autorizada pelo direito da União ou dos Estados-Membros.

- Precauções especiais por parte do setor público: Justifica-se uma advertência especial quanto à necessidade de os organismos públicos começarem por determinar se a comunicação, tratamento e armazenamento de dados fora do território nacional pode criar riscos inaceitáveis para a segurança e privacidade dos cidadãos e a segurança e economia nacionais - em especial se estiverem envolvidas bases de dados (por exemplo, dados de censos) e serviços (por exemplo, cuidados de saúde) com caráter sensível[48]. De qualquer forma, devem ser tomadas estas precauções especiais sempre que sejam tratados dados sensíveis no contexto da computação em nuvem. Deste ponto de vista, as administrações nacionais e as instituições da União Europeia poderão ter em consideração a necessidade de proceder a um estudo mais aprofundado do conceito de plataforma governamental

---

46 Regulamento (CE) n.º 2271/96 do Conselho, de 22 de novembro de 1996, relativo à proteção contra os efeitos da aplicação extraterritorial de legislação adotada por um país terceiro e das medidas nela baseadas ou dela resultantes, Jornal Oficial L 309 de 29.11.1996, p.1-6, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:PT:HTML

47 Ver GT 191 – Parecer 01/2012 sobre as propostas de reforma em matéria de proteção de dados, página 23.

48 Nesta matéria, a ENISA formula a seguinte recomendação no seu documento «*Security & Resilience in Governmental Clouds*» (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): «Em termos de arquitetura, no que diz respeito a aplicações sensíveis, as plataformas privadas e comunitárias de computação em nuvem parecem ser a solução que atualmente melhor se adapta às necessidades das administrações públicas, uma vez que oferecem o nível mais elevado de governação, controlo e visibilidade, embora, quando se planeia uma plataforma privada ou comunitária de computação em nuvem, se deva ter em especial consideração a escala da infraestrutura».

europeia de computação em nuvem como um espaço virtual supranacional em que poderia ser aplicado um conjunto de regras coerente e harmonizado.

- Parceria Europeia para a Computação em Nuvem: O Grupo de Trabalho apoia a estratégia relativa à Parceria Europeia para a Computação em Nuvem apresentada pela Vice-Presidente da Comissão Europeia Nelie Kroes, em janeiro de 2012, em Davos[49]. Esta estratégia envolve os concursos públicos para aquisição de produtos informáticos com vista a incentivar o mercado europeu de serviços de computação em nuvem. A transferência de dados pessoais para um prestador europeu de serviços de computação em nuvem, soberanamente regido pela legislação europeia em matéria de proteção de dados, pode ter grandes vantagens para os clientes em termos de proteção de dados, em especial ao promover a adoção de normas comuns (em particular, a nível da interoperabilidade e da portabilidade dos dados), bem como a segurança jurídica.

[49] Neelie Kroes, Vice-Presidente da Comissão Europeia e responsável pela Agenda Digital, «*Setting up the European Cloud Partnership*», Discurso no Fórum Económico Mundial, Davos, Suíça, 26 de janeiro de 2012, URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ANEXO

a) Modelos de implantação

O termo **«plataforma privada de computação em nuvem»**[50] designa uma infraestrutura informática dedicada a uma organização individual; está localizada nas instalações da organização, ou a sua gestão é externalizada a terceiros (normalmente mediante alojamento em servidor), e encontra-se sob o total controlo do responsável pelo tratamento de dados. Uma plataforma privada de computação em nuvem pode ser comparada a um centro de dados tradicional, residindo a diferença nas tecnologias aplicadas a fim de otimizar a utilização dos recursos disponíveis e reforçar esses recursos através de pequenos investimentos que são efetuados de uma forma gradual ao longo do tempo.

Uma **plataforma pública de computação em nuvem** é, em contrapartida, uma infraestrutura que é propriedade de um prestador de serviços especializado na prestação de serviços que disponibiliza - e por conseguinte partilha – os seus sistemas com/entre utilizadores, empresas e/ou os organismos da administração pública. Os serviços podem ser acedidos através da Internet, o que implica a transferência de operações de tratamento de dados e/ou de dados para os sistemas do prestador de serviços. Por conseguinte, o prestador de serviços assume um papel fundamental na proteção eficaz dos dados confiados aos seus sistemas. Juntamente com os dados, o utilizador é obrigado a transferir uma grande parte do seu controlo sobre esses dados.

Paralelamente às plataformas «públicas» e «privadas» de computação em nuvem, há as chamadas plataformas «intermédias» ou «híbridas» de computação em nuvem em que os serviços prestados por infraestruturas privadas coexistem com serviços adquiridos a plataformas públicas de computação em nuvem. Deve referir-se também as «plataformas comunitárias de computação em nuvem», em que a infraestrutura informática é partilhada por várias organizações em benefício de uma comunidade de utilizadores específica.

A flexibilidade e a simplicidade na configuração de sistemas de computação em nuvem permitem o seu dimensionamento «elástico», ou seja, estes sistemas podem ser adaptados a requisitos específicos em função de uma abordagem baseada na utilização. Os utilizadores não têm de gerir sistemas informáticos, os quais são utilizados com base em acordos de externalização, pelo que são plenamente geridos pelo terceiro em cuja plataforma de computação em nuvem estão armazenados os dados. Frequentemente, intervêm prestadores de serviços de grandes dimensões com infraestruturas complexas; é por essa razão que a

[50] O NIST (*National Institute of Standards and Technology*) nos EUA está há alguns anos a trabalhar na normalização das tecnologias baseadas na computação em nuvem e as suas definições são também referidas no documento da ENISA:
«Plataforma privada de computação em nuvem».
A infraestrutura de computação em nuvem é exclusivamente gerida para uma organização. Pode ser gerida pela organização ou por terceiros e pode estar situada dentro ou fora das respetivas instalações. É de salientar que uma «plataforma privada de computação em nuvem» assenta, pelo menos, em determinadas tecnologias que são também típicas das «plataformas públicas de computação em nuvem» – incluindo, em especial, as tecnologias de virtualização que promovem a reorganização (ou a remodelação) da arquitetura de tratamento de dados, conforme explicado supra.
Plataforma pública de computação em nuvem.
A infraestrutura de computação em nuvem é colocada à disposição do grande público ou de um grande grupo empresas e é propriedade de uma organização que vende serviços de computação em nuvem.

computação em nuvem se pode distribuir por vários locais e os utilizadores podem não saber exatamente onde estão a ser armazenados os seus dados.

b) Modelos de prestação de serviços

Em função dos requisitos dos utilizadores, há várias modalidades de serviços de computação em nuvem disponíveis no mercado que podem ser agrupadas em três categorias principais ou «modelos de serviços». Estes modelos são geralmente aplicáveis tanto a soluções privadas como públicas de computação em nuvem:

- **Infraestrutura de computação em nuvem como serviço (*Cloud Infrastructure as a Service - IaaS*):** Um prestador de serviços aluga uma infraestrutura tecnológica, ou seja, servidores virtuais à distância que o utilizador final pode utilizar de acordo com mecanismos e modalidades que permitam uma simplificação e maior eficácia, bem como a substituição de sistemas informáticos nas instalações das empresas e/ou a utilização da infraestrutura alugada em paralelo com os sistemas das empresas. Esses prestadores de serviços são geralmente operadores especializados no mercado e dispõem efetivamente de uma infraestrutura física complexa que está frequentemente distribuída por várias regiões geográficas.
- **Software de computação em nuvem como serviço (*Cloud Software as a Service* - SaaS):** Um prestador de serviços fornece, através da Web, serviços relativos a várias aplicações e disponibiliza-os aos utilizadores finais. Esses serviços destinam-se frequentemente a substituir aplicações tradicionais a instalar pelos utilizadores nos seus sistemas locais, pelo que os utilizadores acabam, em última instância, por externalizar os seus dados confiando-os a um determinado prestador de serviços. É este o caso, por exemplo, de aplicações típicas de escritório baseadas na Web, como folhas de cálculo, aplicações de tratamento de texto, registos e agendas informatizados, calendários partilhados, etc. Contudo, os serviços em questão também incluem aplicações de correio eletrónico baseadas em computação em nuvem.
- **Plataforma de computação em nuvem como serviço (*Cloud Platform as a Service* - PaaS):** Um prestador de serviços oferece soluções avançadas para o desenvolvimento e o alojamento virtual de aplicações. Esses serviços são normalmente dirigidos a intervenientes no mercado que os utilizam para o desenvolvimento e alojamento de soluções baseadas em aplicações patenteadas a fim de satisfazer requisitos internos e/ou de prestar serviços a terceiros. Mais uma vez, os serviços fornecidos por um prestador de serviços PaaS dispensam o utilizador de dispor de *hardware* ou *software* adicionais e/ou específicos a nível interno.

Uma transição plena para um sistema exclusivamente público de computação em nuvem não parece viável a curto prazo por diversas razões, em especial no que se refere às entidades de grandes dimensões, como grandes empresas ou organizações que têm de cumprir obrigações específicas – por exemplo, grandes bancos, organismos públicos, grandes municípios, etc.. Tal pode dever-se principalmente a dois motivos: em primeiro lugar, há um fator dinâmico relacionado com os investimentos necessários para proceder a essa transição; em segundo lugar, há que ter em conta as informações especialmente valiosas e/ou sensíveis a tratar em casos específicos.

Um outro fator a favor da escolha de plataformas privadas de computação em nuvem (pelo menos nos casos supramencionados) tem a ver com a circunstância de, muitas vezes, nenhum prestador de serviços públicos de computação em nuvem poder garantir a qualidade do serviço (com base em acordos sobre o nível dos serviços), a fim de acompanhar as exigências de natureza crítica do serviço que o responsável pelo tratamento de dados deve fornecer -

talvez pelo facto de a largura de banda e a fiabilidade da rede não serem suficientes ou adequadas numa determinada zona, ou no que respeita a determinadas ligações específicas utilizador-prestador de serviços. Por outro lado, é razoável pressupor que em alguns dos casos supramencionados podem ser alugadas plataformas privadas de computação em nuvem (dado que tal poderá revelar-se mais eficaz em termos de custos) ou ser implantados modelos híbridos de computação em nuvem (incluindo as componentes pública e privada). As respetivas implicações teriam de ser cuidadosamente consideradas em todos os casos.

Na ausência de normas acordadas a nível internacional, há o risco de serem adotadas soluções de computação em nuvem do tipo «faça você mesmo» ou soluções federadas de computação em nuvem, o que implica um aumento dos riscos de dependência em relação a um único vendedor (bem como o que foi designado um risco de «monoculturas de privacidade»)[51] e impede o pleno controlo sobre os dados sem garantia de interoperabilidade. A interoperabilidade e a portabilidade dos dados são efetivamente fatores-chave para desenvolver tecnologias baseadas na computação em nuvem, bem como para permitir o pleno exercício dos direitos de proteção de dados de que gozam as pessoas em causa (como o acesso ou a retificação).

Deste ponto de vista, o atual debate sobre as tecnologias de computação em nuvem constitui um exemplo significativo da tensão existente entre as abordagens orientadas para os custos e as orientadas para os direitos, conforme descrito sucintamente na secção 2 supra. Embora o recurso a serviços privados de computação em nuvem possa ser viável e até mesmo aconselhável numa perspetiva da proteção de dados, desde que se tenha em conta as circunstâncias específicas do tratamento dos dados, esta solução pode não ser viável a longo prazo para as organizações, principalmente numa perspetiva de custos. É necessária uma avaliação cuidadosa dos interesses em jogo, uma vez que, neste domínio, não é possível neste momento apontar para uma solução única que seja boa para todos.

[51] Ver o estudo do Parlamento Europeu «*Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy*», publicado em dezembro de 2011.