PROTECÇÃO DE DADOS NA COMPUTAÇÃO EM NUVEM

1. INTRODUÇÃO

O desenvolvimento das tecnologias de computação e informação permite, nos dias de hoje, a melhoria da qualidade e da oferta de bens e serviços oferecidos, ao mesmo tempo que chamam a atenção para importantes problemas, nomeadamente, a protecção de dados pessoais e comerciais.

Com um desenvolvimento exponencial nos últimos anos, a computação em nuvem (*cloud computing*) oferece actualmente um conjunto de serviços cada vez mais abrangente, sendo por isso necessário reforçar alguns dos pilares essenciais na prestação destes serviços, designadamente ao nível da protecção e gestão dos dados que são armazenados na nuvem.

O recurso à computação em nuvem permite ao utilizador recorrer a um conjunto de serviços que pode ser prestado à distância, dado que as plataformas e infra-estruturas onde o serviço é prestado podem situar-se em qualquer parte do mundo.

Pode inclusivamente acontecer que os serviços sejam prestados por um provedor que não é titular da infra-estrutura física onde correm os programas e onde é feito o armazenamento de dados.

A quantidade e diversidade de particulares e empresas que utilizam actualmente a computação em nuvem é imensa, o que torna o tipo de dados que são carregados nestes sistemas ainda mais densos, estando muitas vezes em causa o tratamento e a transmissão de dados pessoais e comercias a uma pluralidade de intervenientes.

A presente informação é o segundo elemento de uma série dedicada à computação em nuvem, debruçando-se em particular sobre a protecção de dados pessoais na computação em nuvem.

A informação anterior, denominada *Cloud Computing*, pode ser encontrada em aqui.

2. TIPO DE NUVENS

De entre as várias classificações existentes quanto ao tipo de nuvens, optámos pela seguinte:

(a) *Private clouds*, ou seja, nuvens privadas que estão na titularidade do próprio beneficiário do serviço, sendo por ela geridas e assegurando este a sua protecção;

(b) *Public clouds*, ou nuvens públicas, onde existe uma partilha de infra-estruturas que fornecem os serviços prestados e armazenam a informação recebida dos utilizadores, passando a gestão e protecção pelo próprio provedor da nuvem.

(c) *Hybrid clouds* ou nuvens híbridas que, situadas a meio termo entre as *private* e as *public clouds*, permitem nomeadamente que a infra-estrutura em causa pertença ao utilizador mas a sua gestão fique a cargo de um provedor de uma nuvem pública.

Atendendo à diversidade de tipos é fácil de depreender que o nível de preocupações com a protecção de dados varia, entre outros factores, de acordo com o concreto tipo de nuvem que é escolhido pelo utilizador.

3. SERVIÇOS E PROGRAMAS DE PROTECÇÃO DE DADOS

Face aos receios sentidos pelos utilizadores desta tecnologia de informação, várias empresas passaram a oferecer uma gama de produtos que têm o objectivo de proteger os dados que são carregados pelos utilizadores na nuvem.

Salientaremos, de entre os diversos tipos que são oferecidos, os mais significativos.

De um lado temos os produtos que permitem ao provedor da nuvem utilizar programas de protecção de dados (nomeadamente da informação crítica), a gestão e partilha de documentos, a recuperação de diversos tipos de informações que sejam acidentalmente perdidas e o acesso remoto aos serviços e informações disponibilizadas na nuvem. Este tipo de programas destina-se, essencialmente, às *public clouds* e às *hybrid clouds.*

No outro lado, temos um conjunto de programas que apenas permitem a gestão de determinado tipo de informações, nomeadamente para efeitos estatísticos e de melhoramento dos programas e serviços disponibilizados, ficando a administração da nuvem a cargo, por exemplo, da equipa de tecnologias de informação do próprio utilizador. Este tipo de programas é particularmente direccionado para as *private clouds*.

A tipologia de programas oferecidos partilha muitas das preocupações e cautelas que são levantadas face à computação em nuvem que referiremos de seguida.

4. PRECAUÇÕES A TER NA PROTECÇÃO DE DADOS

Como já anteriormente referimos, os serviços de computação em nuvem podem estar a ser prestados nas mais diversas latitudes, desconhecendo-se muitas vezes a localização exacta das unidades físicas e quem são os seus verdadeiros proprietários. Ora, estes factores não podem deixar de estar previstos no contrato de prestação de serviços que é assinado.

A localização geográfica das infra-estruturas nos mais diversos países pode levantar dúvidas quanto ao nível de protecção de dados pessoais e comercias constantes da nuvem. Nestes termos a União Europeia tem, desde há largos anos, dedicado especial atenção a esta temática, garantido a harmonização de alguns elementos da protecção de dados ao nível dos diversos Estados Membros.

Igualmente a nível europeu, a Comissão Europeia tem competência para analisar a transmissão de dados pessoais para outros países fora da União, com o intuito de avaliar se os níveis de protecção que são concedidos nos países de destino se coadunam com os que estão previstos na legislação europeia.

É, desta forma, importante que o utilizador da computação em nuvem procure a informação relativa aos países que a União Europeia considera possuírem um adequado nível de protecção de dados e apenas aceite celebrar contratos de prestação de serviços onde esteja claramente prevista a localização física dos equipamentos e infra-estruturas, devendo por isso optar pelo provedor que lhe garanta que estes se encontram numa jurisdição que ofereça a protecção adequada aos dados armazenados.

Por outro lado, importa ainda ter em consideração outros factores relevantes, designadamente, os relativos à gestão dos dados e a responsabilidade pelo tratamento da informação..

Nestes termos é importante que o utilizador do serviço possa, a todo o momento, saber com exactidão quem é o responsável técnico pela gestão e quem é que pode ter acesso aos dados que são carregados para a nuvem. É por isso essencial que no contrato de prestação de serviços esteja claramente definida a necessidade de manter a protecção e a confidencialidade das informações a todos os elementos que possam ter acesso a elas, bem como a determinação da responsabilidade pela gestão.

É igualmente necessário garantir que, quando o utilizador seja uma empresa e os dados que são carregados sejam pessoais, os titulares desses dados dêem o seu consentimento ao tratamento dessa informação por terceiros, sendo este um requisito essencial, porquanto estamos a tratar de dados que podem inserir-se na reserva da intimidade da vida privada.

Igualmente, no caso de o utilizador optar por um produto que ofereça apenas a protecção dos dados, é necessário que esteja claramente definido no contrato de prestação de serviços quais as utilizações que podem ser dadas à informação, nomeadamente o tratamento estatístico e de melhoramento da oferta dos serviços da nuvem, criando desta forma uma vinculação à utilização dos dados que é limitativa da actuação do gestor de informação.

O utilizador deve garantir, ainda, que o prestador de serviços garanta o seu direito a ser esquecido, ou seja, o direito que assiste aos indivíduos de pôr cobro a qualquer tipo de recolha, análise, tratamento ou utilização dos seus dados pessoais e de os suprimir quando já não forem necessários para os fins legalmente previstos.

No seguimento dessa exigência, é aconselhável que exista uma clara vinculação contratual à utilização dos dados, deixando sempre claro que tipo de utilização lhes será dado, garantido a confidencialidade e a restrição no acesso à informação, e prevendo a necessidade de informar imediatamente o utilizador sempre que sejam detectadas quaisquer situações de violação das protecções oferecidas aos dados carregados.

5. CONCLUSÕES

Fizemos um levantamento sumário das questões que devem estar claramente previstas nos contratos de prestação de serviços que sejam celebrados entre os utilizadores e os provedores das nuvens.

Salientamos que, dada a delicadeza do tipo de informações podem estar em causa, é exigido sempre que o titular dos dados pessoais que serão carregados dê o seu consentimento expresso para que o tratamento desses dados seja feito por terceiro.

Para efeitos de responsabilização, deverá ficar sempre claro no contrato quem serão os responsáveis pela gestão da informação e da rede de segurança dos dados, permitido saber directamente quem poderá ser responsabilizado no caso de os dados serem divulgados a terceiros não autorizados ou no caso de estes serem utilizados para uma finalidade diversa da prevista.

É também necessário saber onde será feita a localização física dos equipamentos, que será relevante para a determinação, nomeadamente, do direito aplicável quer à protecção dos dados quer à responsabilização em caso de infracção.

Assiste-se, neste momento, a um preocupação cada vez mais elevada dos órgãos dos diversos países na protecção de dados e na regulação das actividades relacionadas com as tecnologias de informação. A própria União Europeia iniciou recentemente uma consulta pública particularmente dirigida à computação em nuvem, com o objectivo de recolher contributos para aprovação de uma legislação comunitária relativa a esta temática.