COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

PARECER N.º 83 /2012

I. Do Pedido

O ICP - Autoridade Nacional de Comunicações remeteu a esta Comissão uma proposta de Regulamento da Comissão Europeia sobre as medidas a aplicar às notificações relativas às quebras de dados pessoais, previstas no artigo 3.º-A da Lei n.º 46/2012, de 29 de agosto.

De acordo com o pedido, a referida proposta será submetida a procedimento de exame em reunião do Comité das Comunicações (COCOM), solicitando aquela Autoridade o envio de parecer sobre o sentido de voto a adotar por Portugal (positivo, negativo ou abstenção).

II. Da Apreciação

De acordo com o artigo 3.º, n.º 5 da Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009, a «*Comissão poderá (...) aprovar medidas técnicas de execução respeitantes às circunstâncias, ao formato e aos procedimentos aplicáveis aos requisitos de informação e notificação das violações de dados pessoais*».

É, ainda, dito na mesma Diretiva que «*Na aprovação dessas medidas, a Comissão deve envolver todos os interessados, de modo, designadamente, a ser informada sobre os melhores meios técnicos e económicos disponíveis par a aplicação do presente artigo*».

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

É neste contexto, e na qualidade de autoridade nacional competente em matéria de proteção de dados pessoais, que a Comissão Nacional de Proteção de Dados (CNPD) se pronuncia sobre a referida proposta, emitindo o competente parecer.

O objetivo principal do Regulamento em apreço é o de harmonizar e de assegurar coerência na aplicação das medidas técnicas de execução respeitantes às circunstâncias, ao formato e aos procedimentos aplicáveis aos requisitos de informação e notificação em situação de violação de dados pessoais.

Analisado o texto da proposta, assumem particular destaque as questões que infra se referem.

A primeira que importa abordar é a relativa ao momento a partir do qual se considera que ocorreu uma deteção de uma violação de dados pessoais, matéria regulada no 2º parágrafo do n.º 2 do artigo 2.º da Proposta.

De acordo com o texto proposto, considera-se que ocorreu uma deteção de uma violação de dados pessoais quando o fornecedor de serviços «*adquiriu, deveria ter adquirido, suficiente tomada de consciência de que um incidente tenha ocorrido (...)*».

Ora, consideramos que o momento relevante deverá ser o da tomada de conhecimento e não o da tomada de consciência, na linha do que é defendido no considerando 61) da Diretiva 2002/58/CE, e que a proposta de Regulamento em apreço deve respeitar.

Aliás, nem se pode aceitar que seja de outro modo. A tomada de conhecimento do incidente constitui um fato suscetível de ser verificado, ou verificável, algo que já não acontece com a tomada de consciência. Quando esta está em causa, está-se no plano

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

do pensamento, logo, perante factos insuscetíveis de verificação, logo, insuscetíveis de demonstração ou comprovação.

A segunda questão tem que ver com o prazo dado aos fornecedores de serviços de comunicações eletrónicas para comunicar à autoridade de proteção de dados a existência de uma violação de dados pessoais.

O artigo 3.º, n.º 3, 1.º parágrafo, da Diretiva 2002/58/CE, de 12 de julho, alterada pela Diretiva 2009/136/CE, de 25 de novembro, determina que as violações de dados pessoais sejam comunicados à autoridade nacional competente «sem atraso injustificado».

A proposta de Regulamento em análise prevê, para os referidos efeitos, três prazos de comunicação diferentes, a saber: até 24 horas, até três dias, e superior a três dias, em função da existência, disponibilidade e suficiência de um conjunto de informação que deve ser comunicada pelos fornecedores de serviços à autoridade de proteção de dados e que constam no Anexo 1.

Ainda que se reconheça que a fixação de prazo torna mais transparente o procedimento de notificação, a verdade é que as autoridades de proteção de dados não podem ser condicionadas na sua atuação, atentas as suas atribuições e competências em matéria de incumprimento dos princípios e regras em proteção de dados. No caso de Portugal, a CNPD possui, designadamente, poderes de autoridade, de investigação e inquérito e, ainda, poderes sancionatórios, quando está em causa a violação de princípios e regras em matéria de proteção de dados pessoais.

A manterem-se os prazos como proposto – até 24 horas, até 3 dias e, em alguns casos, superior a 3 dias –, é deixado, desde logo, ao prestador de serviços margem de discricionariedade de atuação, que a existir, deverá estar do lado da autoridade que controla e fiscaliza o cumprimento da lei e não do lado do fornecedor de serviços que

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

poderá estar em situação de incumprimento. Há que reduzir a margem de manobra do fornecedor de serviço, tendo em conta o risco de, por razões económicas (a imagem e, consequentemente a reputação da empresa em termos de mercado pode ser posta em causa) aquele tentar manipular provas de situações de incumprimento da sua parte.

O proposto prazo de notificação de 24 horas afigura-se razoável, mas, em algumas situações, pode mostrar-se excessivo. Tudo depende do caso em concreto. Por outro lado, prazos demasiado longos, como é o caso de prazo de 3 ou mais dias, dificultam e, em algumas situações, podem tornar inútil qualquer intervenção da autoridade de proteção de dados, designadamente por inexistência de provas.

Neste sentido, e por forma a assegurar uma efetiva e útil intervenção da autoridade de proteção de dados nesta matéria, bem como para evitar que possa haver manipulação das provas por parte dos fornecedores de serviços, entende-se que o prazo de 24 horas deve ser o prazo mantido. No entanto, por forma a assegurar a eficácia da intervenção da autoridade de proteção de dados, deve ser acrescentada cláusula de salvaguarda no seguinte sentido: «*sem prejuízo de a Autoridade de Proteção de Dados poder fixar prazo inferior, ou, ainda, face ao caso concreto, poder considerar que o prazo para cumprimento da notificação se mostrou excessivo, por inexistência de razão justificável por parte do prestador de serviços*».

A nossa posição não só está em linha com o papel ativo que as autoridades de proteção de dados pessoais devem ter nesta matéria, como é coincidente, no essencial, com o regime de violação de dados pessoais constante da proposta de Regulamento de Proteção de Dados que se encontra neste momento em fase de discussão nas instâncias europeias.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Outra questão que assume relevância nesta sede é a da inexistência de prazo para o fornecedor de serviços comunicar aos assinantes ou pessoas afetadas as violações de dados pessoais.

Na proposta em análise não se avança com qualquer prazo determinado, mantendo-se nesta matéria a expressão adotada no 2.º parágrafo do n.º 3 do artigo 3.º da Diretiva 2002/58/CE, que estabelece que a comunicação aos assinantes ou pessoas afetadas deve de ocorrer «*sem atraso injustificado*».

Não se percebe a razão de ser da distinção entre a notificação aos assinantes e pessoas que possam ter sido afetadas e a notificação às autoridades de proteção de dados, pelo que se considera que razões de segurança, transparência e objetividade impõem, quanto aquelas que seja estabelecido um prazo fixo, sem prejuízo da situação prevista no n.º 5 do artigo 3.º, caso em que a notificação está dependente de uma autorização da autoridade de proteção de dados, pelo que será em sede de autorização que tal prazo deverá ser fixado.

O fornecedor de serviços encontra-se em condições de, no mesmo prazo que lhe é imposto para comunicar à autoridade de proteção de dados, notificar os assinantes e pessoas que possam ter sido afetadas da violação de dados pessoais. Na verdade, as informações constantes do Anexo 2 estão relacionadas com as informações que deverão ser prestadas pelo fornecedor à autoridade de proteção de dados.

Pelas razões referidas, não se compreende e nem se aceita que, num primeiro momento, seja deixado ao critério do fornecedor de serviços o preenchimento do conceito vago e indeterminado «sem atraso injustificado», ficando os assinantes e pessoas que possam ter sido afetadas impedidas de tomar as precauções necessárias para evitar ou minimizar danos resultantes das violações.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Ainda sobre o artigo 3.º da proposta, mas agora no que toca ao seu n.º 7, existe um outro aspeto que merece destaque, que tem que ver com os meios de comunicação que os fornecedores de serviços devem utilizar quando precisam de notificar as pessoas afetadas pela violação de dados pessoais e não estão na posse da sua identificação e/ou dos seus contatos.

Nesta matéria, a proposta de Regulamento avança com a seguinte solução: « *(...) o fornecedor poderá notificar essas pessoas através de publicidade nos principais meios de comunicação nacionais e regionais (...)*».

Discordamos desta solução, na medida em que a mesma é contrária ao texto da Diretiva 2002/58/CE. Com efeito, o que nos diz esta Diretiva é que o fornecedor está obrigado a comunicar aos seus assinantes e pessoas que possam ter sido afetadas da violação dos dados pessoais quando estas possam afetar negativamente os dados pessoais e a privacidade daqueles. Ora, não está em causa uma faculdade, mas sim uma obrigação legal que recai sobre o fornecedor de serviços.

O que verdadeiramente importa é que as pessoas afetadas tenham conhecimento da sua existência para poderem tomar as precauções necessárias para evitar ou minimizar danos resultantes das violações.

Neste sentido, nas situações em que o fornecedor de serviços tenha desenvolvido esforços, no prazo previsto, para identificar as pessoas que possam ter sido afetadas e não tenha tido sucesso, fica, ainda assim, obrigado a notificar esse universo de pessoas. O fornecedor de serviços tem iguais obrigações quer relativamente aos seus assinantes quer relativamente às pessoas que possam ter sido afetadas, uma vez que ambos são utilizadores dos serviços que presta e, nessa medida, os seus dados podem ser violados.

Por outro lado, nestas situações, importa que os fornecedores utilizem meios de comunicação eficazes que assegurem que a informação sobre a existência de violação de dados pessoais chega ao conhecimento das pessoas afetadas.

De acordo com o proposto, a publicidade deve ser feita com recurso a meios de comunicação nacionais e regionais. A solução proposta não pode ser acolhida, sob pena de deixar de fora os assinantes e as pessoas afetadas de um Estado Membro diferente do Estado Membro onde o fornecedor de serviços se encontra estabelecido, situação prevista no n.º 5 do artigo 2.º da proposta.

Neste sentido, devem constar no texto da proposta de Regulamento outros meios de comunicação que permitam, nas situações previstas no artigo 2.º, n.º 5, que as pessoas que possam ter sido afetadas tenham efetivo conhecimento da violação de dados.

Em conformidade com o exposto, a CNPD propõe, desde logo, a substituição do termo «pode» por «deve», por este último ser conforme ao texto da Diretiva 2002/58/CE, ao mesmo tempo que propõe a seguinte redação para a parte final da primeira frase do artigo 3.º, n.º 7: «(...) *o fornecedor de serviços deve notificar as pessoas que possam ter sido afetadas através de publicidade com recurso a meios idóneos que permitam a tomada de conhecimento das violações por parte daquelas*».

Outro dos aspetos que merece ser comentado respeita à «utilização de terceiro», prevista no artigo 5.º da proposta e que também é referido no ponto 8) da secção 1 do Anexo I.

Para evitar equívocos, dificuldades de interpretação e aplicação das regras previstas na proposta de Regulamento, a terminologia de proteção de dados usada na presente proposta de Regulamento deve ser coincidente com a constante da Diretiva 2002/58/CE, a que aquela está subordinada, e com a prevista na Diretiva 95/46/CE, de

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

24 de outubro (Diretiva da Privacidade e dos Dados Pessoais), que é subsidiariamente aplicável à primeira.

A expressão «*Third party*» significa, em proteção de dados «Terceiro», tendo o seguinte significado: «*pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que não a pessoa em causa, o responsável pelo tratamento, o subcontratante e as pessoas que sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão habilitadas a tratar os dados*».

Ora, quando o fornecedor de serviços de comunicações eletrónicas recorre a outras entidades para que estas lhe prestem parte dos seus serviços, estas assumem necessariamente a qualidade de «*Processor*», que significa «Subcontratante». O fornecedor de serviços é o responsável pelo tratamento, porque é quem define as finalidades do tratamento e, nessa medida, é o responsável pela adoção das medidas técnicas e organizativas para proteger os dados pessoais, pelo que outra qualquer entidade que intervenha no tratamento fá-lo em nome e por conta do responsável. Existe uma relação de dependência e subordinação do «prestador de serviços» ao «fornecedor de serviços». Tudo se passa como se de uma única entidade se tratasse.

Nos termos da lei, esta relação contratual deve estar suportada num ato jurídico que estabeleça os deveres e as obrigações de cada um dos intervenientes em matéria de tratamento de dados.

Assim, nas situações em que está em causa a prestação de parte dos serviços de comunicações eletrónicas por parte de outras entidades que não o fornecedor, como acontece nas situações em que há recursos a outra entidade para prestação do serviço de faturação (exemplo, aliás, mencionado no considerando 18) da proposta), estas entidades, apesar de externas ao fornecedor de serviços, assumem a qualidade de subcontratantes na aceção do artigo 2.º, alínea e), da Diretiva da privacidade e dos dados pessoais.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Pelas razões acima expostas, defendemos que a expressão «*Third party*» deve ser substituída pela expressão «*Processor*», uma vez que esta última está em sintonia com o regime de proteção de dados e com a realidade em análise.

Caso o legislador também pretenda abranger «Third Party», que significa «Terceiros» na aceção da alínea f) do artigo 2.º da Diretiva da privacidade e dos dados pessoais, deverá ser claro e inequívoco quanto a esta opção.

No artigo em análise, mostra-se ainda necessário clarificar a questão do prazo para comunicação das violações de dados pessoais quando o fornecedor recorre a outras entidades para prestar parte do serviço, seja na qualidade de «subcontratantes», seja na qualidade de «terceiros».

A responsabilidade de notificar a violação de dados pessoais é sempre do fornecedor de serviços, que é o responsável pelo tratamento, pelo que nas situações subcontratação deve o mesmo assegurar, designadamente no ato jurídico que for celebrado, que quando o subcontratante detete violação de dados pessoais, lhe comunica imediatamente a tomada de conhecimento dessa violação.

A inexistência de prazo para a comunicação de quebras de violação de dados pessoais entre o subcontratante e o fornecedor de serviços pode possibilitar um alargamento do prazo inicialmente fixado ao responsável para notificar as violações, caso a redação do texto do artigo 5.º se mantenha nos termos propostos.

Com efeito, a atual redação deste artigo pode permitir o entendimento segundo o qual, nas situações de subcontratação, o prazo inicial de 24 horas que o fornecedor de serviços tem para notificar as violações só começa a contar a partir do momento do recebimento da comunicação da violação de dados ao fornecedor por parte do subcontratante.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Na prática, da norma resulta que, quando recorra a outras entidades, o fornecedor de serviços passa não só a dispor de prazo superior ao fixado, como esse prazo passa a ser indeterminado.

Este entendimento não pode ser aceite, na medida em que cria uma diferenciação de regime, quanto ao prazo de notificação, entre os fornecedores de serviços que recorrem a outras entidades para lhe prestarem parte dos seus serviço e os que não recorrem, distinção que não tem fundamento.

O fornecedor de serviços é, perante a autoridade de proteção de dados, o responsável pela adoção das medidas de segurança e, consequentemente, por evitar a ocorrência de violação de dados pessoais.

Assim, o que tem de suceder é que o fornecedor de serviços deve estar sujeito ao cumprimento do mesmo prazo para proceder à notificação das violações, independentemente da existência ou não de operações de tratamento realizadas em regime de subcontratação.

Nesta conformidade, propõe-se a seguinte redação para o artigo 5º: «Nas situações em que existe recurso por parte dos fornecedores de serviços a entidades subcontratadas, o prazo previsto no artigo 2.º e 3.º começa a contar do momento da deteção do incidente [que em nosso entendimento deve ser o da tomada de conhecimento] por parte destas entidades.

Por último, no ponto 8) da secção 1 do Anexo 1 da proposta refere-se «*Relevant use of third party*».

Para além das questões acima referidas, a propósito do significado do conceito «*Third party*», a introdução da expressão «Relevant use» torna tudo, ainda, mais difícil de perceber, e consequentemente, de aplicar.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

O uso da expressão «*Relevant use of third party*» não tem qualquer paralelo quer no instrumento que habilita a proposta de Regulamento ora em análise, quer em qualquer outro instrumento comunitário (aprovado ou em preparação), quer, ainda, em legislação nacional relativa a matéria de proteção de dados pessoais.

Além do mais, introduz um conceito vago e indeterminado que é gerador de incerteza e insegurança no procedimento, cujo preenchimento é deixado ao critério de quem aplica.

Neste sentido, a informação relativa à existência de uma entidade externa aos fornecedores de serviços, independentemente da qualidade que a mesma assuma no tratamento, é a informação que releva e que deve constar no ponto 8) da secção 1 do Anexo 1, para efeitos de violações de dados pessoais.

*

Este é o nosso Parecer.

Lisboa, 06 de Dezembro de 2012

Luís Paiva de Andrade (relator)