COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Parecer n.º 67/2017

I. Pedido

A Ministra da Presidência e da Modernização Administrativa remeteu à Comissão Nacional de Protecção de Dados (CNPD), para parecer, o Projeto de Portaria Chave Móvel Digital, que visa regulamentar o desenvolvimento deste meio de autenticação dos cidadãos em sistemas, portais e sítios na internet e de assinatura eletrónica qualificada à distância, nos termos dos art.º 14.º e 15.º da Lei n.º 37/2014, de 26 de junho, alterada pela Lei n.º 32/2017, de 1 de junho.

O pedido formulado decorre das atribuições conferidas à CNPD pelo n.º 2 do artigo 22.º da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto – Lei de Proteção de Dados Pessoais (doravante, LPDP) –, e o parecer é emitido no uso da competência fixada na alínea a) do n.º 1 do artigo 23.º do mesmo diploma legal, restringindo-se aos aspetos relativos à proteção de dados pessoais.

II. Apreciação

1. Questão prévia

A alteração da Lei n.º 37/2014, de 26 de junho, que estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública denominado Chave Móvel Digital, levada a cabo pela Lei n.º 32/2017, de 1 de junho, foi, em momento próprio, analisada pela CNPD, então a propósito da Proposta de Lei n.º 22/XIII/1.ª (GOV), daí decorrendo a emissão do parecer n.º 20/2016, de 15 de junho[1].

Nesse parecer, a Comissão sintetizou as suas notas críticas em três pontos fundamentais, tendo considerado:

[1] Disponível em https://www.cnpd.pt/bin/decisoes/Par/40_20_2016.pdf.

i. «Te[r] fortes reservas quanto à utilização da Chave Móvel Digital como mecanismo de assinatura digital de documentos, na medida em que não é garantida a sua autenticidade na forma como está desenhada;

ii. Quanto às formas de autenticação ou aposição da assinatura eletrónica qualificada, recomenda que seja removida a possibilidade de o titular apenas se identificar pelo número de telemóvel; deve ainda neste âmbito garantir-se a segurança e confidencialidade das comunicações e dos dados armazenados pela aplicação móvel;

iii. Por último, [...] que o envio de códigos por correio eletrónico não cifrado não é um meio de comunicação que possa garantir a confidencialidade e a autenticidade, pelo que estando em causa o acesso à identificação pessoal dos cidadãos, deve ser encontrado um meio alternativo e seguro para a mesma finalidade.»

Assinala-se, a título prévio e genérico, que o presente projeto de portaria em nada permite ultrapassar as reservas supracitadas, mantendo-se a total pertinência das críticas então apontadas. De resto, e tal como notado à altura, no dito parecer, a discordância da CNPD quanto à opção de remeter aspetos essenciais dos tratamentos de dados pessoais para portaria, em nada se vê contraditada pelas soluções agora encontradas pelo Governo. Com efeito, pelas omissões que seguidamente se apontarão, a promessa de regulamentação constante de instrumento jurídico hierarquicamente superior não só desqualifica algumas das matérias que poderiam e deveriam (vide a determinação constitucional do art.º 35.º, n.º 2, da CRP) estar inscritas em lei, como acaba por nem sequer garantir que tal remissão venha a resultar na previsão expressa (ainda que formalmente desqualificada) dessas matérias.

2. Apreciação do articulado

No que concerne às específicas provisões do projeto de portaria, há a assinalar vários aspetos que parecem colidir com a proteção de dados pessoais.

- Aleatoriedade e segurança das palavras-passe

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Em primeiro lugar, atente-se nos artigos 3.º e 5.º do Projeto de Portaria, onde se descrevem os procedimentos para solicitação de uma Chave Móvel Digital (CMD), de forma presencial e através do envio de carta para a morada do titular, respetivamente. Ambas as modalidades preveem que seja gerada automaticamente uma palavra-passe temporária aleatória, contudo desconhece-se por que via técnica se virá a atingir tal desiderato. Ora, considerando a relevância que a aleatoriedade do mecanismo que gera as palavras-passe tem para a segurança do sistema da CMD, não pode a CNPD deixar de alertar para o risco de utilização de algoritmos pseudoaleatórios que permitam a dedução de palavras-passe e que, dessa forma, coloquem em risco a segurança do meio utilizado.

Ainda relativamente à segurança da palavra-passe, o projeto de portaria refere a obrigatoriedade de alteração daquela logo no primeiro acesso, no entanto, omite quais as regras mínimas de segurança para a definição da nova palavra-passe por parte do utilizador. Como é sabido, a definição de palavras-passe facilmente dedutíveis (fracas) pode contribuir para a fragilização do sistema e facilitar o acesso ilegítimo aos dados do titular. Devem, por isso, ser definidas regras mínimas de formato de palavra-passe (e.g. dimensão mínima de número de carateres, obrigatoriedade de inclusão de carateres especiais, não repetição da palavra-passe original).

- Fragilidades da autenticação

Já o artigo 5.º descreve a *solicitação eletrónica da CMD através de envio de carta para a morada*, feita a partir de portais externos à AMA, I.P. A CNPD alerta para o facto desta modalidade de solicitação da CMD ser aquela que assenta no mecanismo de autenticação mais fraco. Mais concretamente, a forma de autenticação exigida corresponderá ao mecanismo existente *no sítio na Internet do portal das finanças ou de outros sítios, aplicações ou terminais eletrónicos que celebrem protocolo com a AMA, I. P.*, o que pode traduzir-se numa disparidade dos níveis de segurança. No caso específico do Portal das Finanças, por exemplo, a autenticação resume-se à indicação do número de contribuinte (um identificador facilmente acessível) e palavra-passe. A autenticação com nome de utilizador e palavra-passe é comummente considerada "fraca".

Deve ter-se presente que à AMA I.P., não só compete a qualidade de responsável pelo tratamento de dados da CMD e pela segurança do sistema, como também lhe cabe a responsabilidade pelos mecanismos de autenticação que permitem aceder aos serviços da CMD, como é o da solicitação de CMD. Ainda que esse acesso seja feito através dos mecanismos de autenticação de outras entidades, cabe à AMA I.P. assegurar-se que esses mecanismos proporcionam as corretas salvaguardas de segurança e privacidade para o sistema.

- Insuficiências da caracterização da aplicação e dos outros meios eletrónicos que permitam o envio do código numérico de segurança

O artigo 6.º, n.º 2, alínea c) prevê que o código numérico de segurança (*token*) seja remetido para a *aplicação móvel disponibilizada para o efeito (app) instalada no telemóvel*. A Portaria não descreve as caraterísticas técnicas nem as medidas de segurança associadas a esta aplicação, omitindo novamente aspetos críticos que permitam avaliar a conformidade da solução com os preceitos de proteção de dados pessoais. O mesmo ocorrendo com o n.º 2, alínea d), deste artigo, onde se prevê que o código numérico de segurança (*token*) seja remetido por *outros meios eletrónicos que permitam o envio de mensagens privadas*. Considerando a miríade de sistemas que atualmente permitem o envio de mensagens privadas, onde podem incluir-se sistemas *Over-The-Top* (OTT) e *instant messaging* (onde se incluem as redes sociais), a CNPD entende que esta alínea é demasiado vaga quanto à natureza das tecnologias envolvidas, o que impossibilita uma análise concreta das consequências para a privacidade dos dados.

Qualquer destas omissões resulta agravada no contexto da aplicação (a partir de 25 de maio de 2018) do Regulamento Geral sobre a Proteção de Dados Pessoais (RGPD), que prevê e providencia orientações muito claras em matéria de soluções promotoras da proteção de dados desde a conceção e por defeito (art.º 25.º do RGPD), as quais permitiriam mitigar alguns dos riscos assinalados quando não mesmo eliminá-los, o que aqui não acontece.

- Consequências da suspensão da CMD

O n.º 2 do artigo 9.º (Validade e suspensão temporária) refere que a *findo o prazo de validade previsto na alínea a) do número anterior a CMD é suspensa até à renovação do mesmo documento*. Não são, no entanto, descritas na Portaria as consequências da suspensão de uma CMD, o que importaria conhecer, desde logo por inadmissibilidade da conservação dos dados pessoais em causa por períodos irrestritos, sendo manifesta a desproporcionalidade da manutenção dessa informação quando decorra um período de tempo considerável, e aqui não fixado, desde o acontecimento que espoletou a suspensão. Dir-se-á que a renovação do documento de identificação civil português é uma obrigação legal[2] donde, só por tal facto, se comprovaria a desadequação do cancelamento, sem mais, de uma CMD que se encontrasse suspensa. Contudo, e quanto a cidadãos nacionais, importaria, no momento da renovação desse documento, renovar igualmente a "autorização" ou consentimento para o tratamento de dados pessoais relativo à manutenção ou reativação da CMD, requisito dificilmente enquadrável como supérfluo ou burocratizante. O mesmo se dirá, *mutatis mutandis*, quanto aos cidadãos estrangeiros, isto é, relativamente àqueles que possam e entendam renovar o seu documento de identificação civil português ou o respetivo passaporte.

- Outros aspetos procedimentais ligados à gestão da CMD

No art.º 10.º, o n.º 2 (Comunicação de dados) informa que, nos casos de *solicitação eletrónica da CMD através de envio de carta para a morada* através do Portal das Finanças, é *comunicada e validada a respetiva morada* à AMA, I.P. Por seu lado, o n.º 1 do artigo 5.º refere que a palavra-passe temporária gerada automaticamente e de forma aleatória é remetida por carta *para a morada do titular do Cartão de Cidadão*. Não é claro, por isso, se a morada para a qual é enviada a palavra-passe temporária corresponde à que está associada ao Cartão de Cidadão ou se o utilizador tem a possibilidade de indicar diferente morada no Portal das Finanças (o que justificaria a referida validação).

[2] De acordo com o disposto no n.º 1 do art.º 3.º, da Lei n.º 7/2007, de 5 de fevereiro, alterada, em último, pela Lei n.º 32/2017, de 1 de junho.

A Portaria deve esclarecer esta questão tendo em conta que a indicação de uma morada diferente daquela que está associada ao Cartão de Cidadão pode resultar em maior risco para a privacidade (e.g. risco da conta do Portal das Finanças ser acedida por um utilizador ilegítimo[3] e deste encaminhar a palavra-passe para uma morada indicada por si).

Ainda neste mesmo artigo, o n.º 9 refere que, para efeitos de cancelamento da mesma e da respetiva assinatura qualificada, são comunicados à AMA, I. P., mediante protocolo a celebrar com o Instituto dos Registos e Notariado, I. P. (IRN), a morte do titular da CMD ou a sua incapacidade superveniente. Não se antevê que o detalhe da informação aqui previsto seja indispensável ao regular cumprimento das obrigações por parte da AMA, I.P. no que respeita à administração das CMD e das assinaturas eletrónicas. Do que se apreende da forma como o sistema vem descrito, não se alcança que a morte do titular tenha implicações diferentes de uma situação de incapacidade superveniente. Ora, salvo quando, a nível aplicacional, tal diferenciação decorra diretamente de uma dessas situações (o que, sublinha-se, não resulta nem do texto do projeto sob análise, nem da lei que este visa regulamentar), só se pode concluir que o IRN deve limitar-se a remeter à AMA, I.P. a informação de que aquela CMD deve ser cancelada, registando-o internamente.

- Verificação prévia dos Protocolos

Nota crítica, ainda, para a redação ambígua do n.º 10 do artigo em análise. Quando aí se refere que «Os protocolos previstos no presente artigo relativos à comunicação dos dados são notificados à Comissão Nacional de Proteção de Dados», fica a dúvida sobre se o legislador pretende que a CNPD seja meramente informada sobre o conteúdo desses protocolos, o que seria desadequadamente limitativo das funções que lhe cabem por lei, ou, se, pelo contrário, se pretende submetê-los ao crivo da Comissão, nos termos do art.º 27.º da LPDP. Caso seja esta última a opção do legislador, sugere-se a alteração da redação deste número nos seguintes termos: «Os protocolos previstos no presente

[3] Aqui reitera-se o risco associado a autenticação fraca do Portal das Finanças que foi enunciado anteriormente.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

artigo relativos à comunicação dos dados são sujeitos a verificação prévia da Comissão Nacional de Proteção de Dados, nos termos da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto.».

- Monitorização do histórico de autenticações por parte do utilizador

Finalmente, salienta-se que não é referido na portaria qualquer mecanismo que permita ao utilizador monitorizar o seu histórico de autenticações e/ou assinaturas. Esta funcionalidade, ainda que balizada por razoáveis limites temporais, permitiria ao titular ter um maior controlo sobre a utilização dos seus dados, contribuindo para um exercício pleno do direito à autodeterminação informacional a que se refere a Constituição da República Portuguesa (art.º 35.º, da CRP).

III. Conclusões

O Projeto de Portaria Chave Móvel Digital, que visa regulamentar o desenvolvimento deste meio de autenticação dos cidadãos em sistemas, portais e sítios na internet e de assinatura eletrónica qualificada à distância,

i. mesmo descurando as insuficiências constitucionais do ponto de vista formal e orgânico não resolve os aspetos críticos que a CNPD já tinha apontado no seu Parecer n.º 20/2016, à então Proposta de Lei n.º 22/XIII/1.ª (GOV), relativamente às alterações propugnadas à Lei n.º 37/2014, de 26 de junho;

ii. é omisso quanto
   a. ao risco de utilização de algoritmos pseudoaleatórios que permitam a dedução de palavras-passe e que, dessa forma, coloquem em risco a segurança da utilização da Chave Móvel Digital (CMD);
   b. à definição de regras mínimas de segurança para a definição da nova palavra-passe por parte do utilizador.

iii. coloca na AMA I.P. a responsabilidade pelos tratamentos de dados pessoais relativos à emissão da CMD, sendo esta a responsável pela segurança e garantias de privacidade dos mecanismos de autenticação

dos titulares dos dados, ainda quando tal mecanismo respeite a terceiros que celebrem protocolo com a AMA, I. P, o que pode traduzir-se numa disparidade nada recomendável dos níveis de segurança em causa, urgindo evitá-lo ;

iv. não descreve as caraterísticas técnicas nem as medidas de segurança associadas à aplicação móvel utilizável para receber o código que permite autenticar o utilizador, nem concretiza devidamente quais as tecnologias envolvidas nos outros meios eletrónicos admitidos para aquele efeito;

v. não define as consequências da suspensão de uma CMD, nem permite perceber o que acontece com a informação quando a condição da suspensão se prolonga indefinidamente;

vi. não é claro sobre qual a morada para onde é enviada a palavra-passe temporária, concretamente se é aquela que está associada ao Cartão de Cidadão ou se o utilizador tem a possibilidade de indicar diferente morada no Portal das Finanças;

vii. determina que a AMA, I.P. seja informada pelo IRN, I.P., da morte do titular da CMD ou da sua incapacidade superveniente para cancelamento da chave e da respetiva assinatura qualificada, quando se afigura suficiente que apenas seja comunicada a informação de que aquela CMD deve ser cancelada, sendo tal registado internamente;

viii. prevê que os protocolos relativos à comunicação dos dados sejam notificados à Comissão Nacional de Proteção de Dados. Contudo, para clarificação da redação, sugere-se que se especifique que esses protocolos dependam de notificação e autorização da CNPD, nos termos da LPDP;

ix. não estabelece qualquer mecanismo que permita ao utilizador monitorizar o seu histórico de autenticações e/ou assinaturas, o que importa corrigir.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

É este o parecer da CNPD.

Lisboa, 19 de dezembro de 2017

Filipa Calvão (Presidente)

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt