COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

PARECER N.º 37 /2014

I. Pedido

A Comissão do Orçamento, Finanças e Administração Pública solicitou a emissão de parecer sobre o Projeto de Lei 214/XII, que *"estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública denominado Chave Móvel Digital"*.

O pedido formulado decorre das atribuições conferidas à Comissão Nacional de Protecção de Dados (doravante, CNPD) por via do disposto no n.º 2 do artigo 22.º da Lei n.º 67/98, de 26 de outubro, e é emitido no uso da competência prevista na alínea *a)* do n.º 1 do artigo 23.º do mesmo diploma legal.

II. Apreciação

A proposta de lei tem por objeto um tratamento de dados pessoais que foi já apreciado pela CNPD no Parecer n.º 73/2013.

A proposta cria uma nova forma de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública, funcionando através da associação da identidade do cidadão a um número de telemóvel que permite que o cidadão se identifique na Internet com o seu nome de utilizador, palavra-chave por si escolhida e introdução de um código temporário enviado para o número telemóvel associado e ou endereço de correio eletrónico – a Chave Móvel Digital, doravante apenas mencionada por CMD.

Trata-se de um *"mecanismo voluntário e alternativo de autenticação perante serviços públicos digitalizados para todo o utilizador, nacional ou não nacional"*.

Este mecanismo vem agora acrescer aos mecanismos de autenticação possíveis, para

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

a mesma finalidade, disponibilizados pela tecnologia associada ao cartão de cidadão.

Note-se que a CMD pressupõe o tratamento dos seguintes dados pessoais: n.º de identificação civil ou passaporte, consoante se tratar de cidadão nacional ou estrangeiro, n.º de telemóvel e/ou endereço de correio eletrónico.

A associação dos dados pessoais referidos destina-se a gerar a CMD através de um sistema multifator composto por uma *palavra-chave* permanente escolhida, e alterável, pelo cidadão, e por um código numérico de utilização única e temporária por cada autenticação, automaticamente gerado aquando da introdução da identificação do cidadão e da *palavra-chave* a ela associada, e enviado por *SMS* ou correio eletrónico para o respetivo número de telemóvel ou endereço de correio eletrónico registados pelo cidadão.

Como se mencionou no anterior parecer, trata-se de uma tecnologia em tudo semelhante à tecnologia *Token*. Com a utilização do *Token*, a senha memorizada pode ser substituída por uma senha gerada de forma aleatória randomizada por um algoritmo protegido. Dependendo do método utilizado, essa senha gerada tem um período de validade que normalmente é muito curto, com apenas segundos e não pode ser reutilizada, como se encontra também previsto no projeto.

Com esta tecnologia reduz-se o risco da senha ser capturada e utilizada indevidamente. O *Token* tem vindo a ser utilizado como um dispositivo de segurança adicional, uma vez que permite que os utilizadores continuem a ter as suas senhas e os seus dados pessoais utilizados no processo de autenticação e, como mecanismo adicional, o *Token* para complementar a autenticação.

Em relação às objeções então suscitadas pela CNPD no referido parecer, caem com esta proposta as que respeitavam à desconformidade formal e orgânica do projeto de diploma com a Constituição da República Portuguesa (CRP), uma vez que a mesma assume agora a forma de lei, em cumprimento do disposto na alínea b) do n.º 1 do artigo 165.º da CRP.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Resta, pois, apreciar a nova proposta na perspetiva da sua conformidade material com o quadro constitucional vigente. Vejamos.

1. Em anterior parecer, a CNPD manifestou como uma das principais preocupações em relação à solução legislativa encontrada a circunstância de a entidade responsável pela gestão e segurança da infraestrutura tecnológica que suporta a CMD, nomeadamente o sistema de geração e envio dos códigos de utilização única e temporária, ser a Agência para a Modernização Administrativa, I.P. (AMA, I.P.).

E isto porque a AMA, I.P., por força das competências que lhe são atribuídas, teria a possibilidade de conhecer todas as interações dos cidadãos que utilizem a CMD na sua relação com a Administração Pública, o que, conjugado com o acesso a outra informação pessoal na posse dos serviços da Administração Pública que no projeto de diploma então em apreço se previa (*v.g.,* acesso às reclamações apresentadas e respetivas respostas), não podia deixar de levantar reservas.

Com efeito, a geração e o envio das CMDs solicitadas implica que a AMA, I.P., tenha acesso a dados de identificação civil e ao n.º de telemóvel ou endereço de correio eletrónico. Ora, estando na posse das CMDs e dos dados que lhe estão associados, é possível à AMA, I.P., efetuar o total rastreamento das operações efetuadas pelo cidadão utilizador, sabendo, em concreto, que serviços utilizou e que operações efetuou.

Propunha-se, por isso, que fossem encontradas soluções tecnológicas que diminuíssem o risco de rastreio da interação do cidadão com a Administração Pública, e se consagrasse expressamente a proibição de acesso a dados pessoais dos cidadãos, para além dos necessários à ativação da CMD.

Para obstar a que tal aconteça, poderá a base de dados agora criada abster-se de incluir quaisquer dados relativos às operações efetuadas pelos cidadãos para lá do tempo (segundos) estritamente necessário. Isto é, poderá conter os dados exatamente

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

necessários à ativação da CMD, sendo que toda a restante informação – dados provenientes da interação do cidadão com a Administração Pública – deverá continuar nas bases de dados dos respetivos serviços.

Os próprios *logs* (registos dos acessos) poderão permanecer descentralizados por serviço, devendo, nessa medida, ser adotada uma arquitetura da base de dados central que permita a descentralização.

Na proposta agora em análise, introduzem-se algumas alterações que interessa considerar.

Desde logo, no n.º 3 do artigo 2.º, salvaguarda-se que os dados pessoais obtidos por via da associação do número de identificação civil (ou passaporte) a um único número de telemóvel ou a um único endereço de correio eletrónico apenas podem ser utilizados com a finalidade de obtenção da CMD, vedando por isso à AMA, I.P., enquanto entidade gestora deste processo, a possibilidade de utilização da informação pessoal assim obtida para outras finalidades.

Esta previsão, louvável em si mesma, não é, todavia, garantia de que a tecnologia utilizada impeça a entidade gestora de, na posse das CMDs e dos dados que lhe estão associados, efetuar o total rastreamento das operações efetuadas pelo cidadão utilizador, sabendo em concreto que serviços da Administração Pública utilizou e que operações efetuou.

Admitindo-se que não caiba a um diploma legal a descrição da tecnologia utilizada que garanta a efetiva segregação entre o mecanismo de autenticação e as operações efetuadas no sítio da Administração Pública, e independentemente de à CNPD caber pronunciar-se em concreto sobre o tratamento de dados inerente à criação das CMDs, quer este venha a ser consubstanciado em regulamento ou seja notificado pelo responsável, o projeto deveria expressamente prever que está vedada a possibilidade de rastreamento das relações dos cidadãos com a administração pública.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

2. Outra objeção suscitada pela CNPD prendia-se com a criação da CMD para cumprir a mesma finalidade para que também foi criado o cartão de cidadão e com a necessidade (imposta pelo artigo 18.º da CRP) de justificação específica da criação deste mecanismo alternativo do qual decorre uma compressão de um direito, liberdade e garantia, por implicar o acesso a dados pessoais por uma única entidade pública – e que *prima facie* permitirá o rastreio da interação com a Administração Pública.

A presente proposta de lei vem, na exposição de motivos, fundamentar tal opção legislativa na circunstância de a reduzida taxa de utilização de serviços públicos *online* estar associada, entre outros «constrangimentos identificados», «às dificuldades práticas sentidas pelos cidadãos ao nível dos processos de autenticação», aí se apresentando este novo mecanismo como garante de um acesso mais simples e promotor da massificação da utilização daqueles serviços.

Na perspetiva da CNPD, a duplicação de meios de acesso aos serviços públicos *online* não é a solução mais razoável, por implicar a multiplicação de "chaves de acesso" a informação pessoal comunicada nas interações com a Administração Pública e, com isso, poder tornar mais vulnerável tal informação. Sobretudo, porque o novo mecanismo, tal como vem descrito na proposta, é suscetível de dar à entidade gestora mais informação do que aquela que existe na gestão da autenticação do cartão de cidadão.

Entende a CNPD as razões apresentadas. Contudo, não pode deixar de afirmar que o cartão de cidadão, objeto de soluções tecnológicas para autenticação com segurança reforçada, que importou em custos acrescidos justificados por essa mesma segurança, deveria ser o modo privilegiado para relação dos cidadãos com a Administração Pública. A criação de meios alternativos, que suscitam reservas de privacidade, não será seguramente o melhor incentivo para a progressiva utilização do cartão do cidadão.

De todo o modo, os motivos subjacentes à solução proposta, de simplificação e generalização da utilização de serviços públicos *online*, que se reconduzem em boa

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

parte aos princípios da eficiência administrativa e de boa administração e de aproximação da Administração Pública dos cidadãos, são valores que podem justificar a compressão do direito fundamental à proteção dos dados pessoais e que, no caso, não afeta o conteúdo essencial deste. Isto no pressuposto de que, de facto, o mecanismo de autenticação do cartão do cidadão não esteja a revelar-se uma solução adequada à finalidade pretendida.

3. Por último, a CNPD mantém que os regulamentos e acordos previstos nos n.ºs 10 a 12 do artigo 2.º da proposta, na medida em que incidem sobre matéria de proteção de dados pessoais, devem ser submetidos à sua apreciação prévia – o que se admite poder resultar da proposta em apreço, quando, no artigo 2.º, se determina a aplicação de todas as garantias em matéria de proteção de dados pessoais previstas na Lei n.º 67/98, de 26 de outubro.

É este o Parecer da CNPD.

Lisboa, 12 de maio de 2014

Luís Paiva de Andrade (Relator)