COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Parecer n.º 16/2017

I. Pedido

O Gabinete da Ministra da Presidência e da Modernização Administrativa solicitou à Comissão Nacional de Protecção de Dados (CNPD) parecer sobre o Projeto de Decreto-Lei que cria o serviço público de notificações eletrónicas associado à morada única digital, bem como regula os termos e as condições de envio e receção de notificações eletrónicas.

O pedido de parecer deu entrada nos serviços da CNPD no dia 8 de fevereiro de 2017.

O presente Projeto assume a forma de decreto-lei autorizado, emitido ao abrigo do diploma aprovado pela Assembleia da República[1] e que teve por base a Proposta de Lei n.º 41/XIII/2.ª GOV, em relação à qual, apesar de legalmente prevista a obrigação de consulta, não foi solicitado parecer à CNPD – cf. no 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 (LPDP).

A CNPD emite agora o presente parecer, ao abrigo da competência prevista na alínea a) do n.º 1 do artigo 23.º da LPDP, o qual se cinge às normas relativas a tratamentos de dados pessoais.

II. Apreciação

1. Considerações prévias

De acordo com o preâmbulo do presente Projeto de decreto-lei, pretende-se a criação de uma morada digital fidelizada que permita o envio de notificações com eficácia jurídica.

Para o efeito, cria-se um contacto único (morada única digital) para a interação com a Administração Pública (potencialmente com toda a Administração Pública) aplicável a todas as pessoas singulares e coletivas, nacionais e estrangeiras, na forma de um único endereço eletrónico, e que passa a ser equivalente ao domicílio das pessoas singulares ou sede das pessoas coletivas.

[1] Publicado no Diário da Assembleia da República, de 23 de janeiro de 2017, como Decreto n.º 62/XIII.

a. Na verdade, parece resultar do presente Projeto, bem como da autorização legislativa em que o mesmo assenta, que a adesão à morada única digital e à adesão ao serviço público de notificações eletrónicas têm objetos distintos, ainda que o segundo dependa do primeiro. A ser assim, a morada única digital vai funcionar como endereço único para todas as interações entre a Administração Pública (entidades aderentes) e o cidadão, seja para efeito de notificações eletrónicas, seja para quaisquer outras comunicações *de* e *para* a Administração Pública – portanto, a sua relevância jurídica não se esgota nas notificações eletrónicas.

b. Importa, antes do mais, explicitar que o endereço eletrónico de pessoas singulares é um dado pessoal, por constituir informação relativa a uma pessoa singular identificada ou identificável, nos termos definidos na alínea a) do artigo 3.º da LPDP. Pelo que o Projeto prevê a criação de um dado pessoal e cria um sistema de informação onde o mesmo vai ser utilizado: o sistema público de notificações eletrónicas. Nessa medida, o Projeto regula um tratamento de dados complexo que envolve várias operações sobre dados pessoais – *rectius*, um conjunto de tratamentos de dados pessoais, com funcionalidades interligadas.

   Na verdade, o endereço eletrónico não é o único dado pessoal cujo tratamento vem previsto no projeto. O sistema público de notificações eletrónicas envolve ainda, pelo menos, o tratamento dos dados relativos a data e hora da comunicação e eventualmente o respetivo assunto[2] – e, estando em causa uma entidade pública que disponibiliza tal sistema, a informação de que se está a enviar uma notificação sobre um determinado assunto com um serviço da Administração Pública identificado. Ora, o conjunto desta informação – sobre a interação com determinados serviços da Administração (*v.g.,* departamento responsável pelas contraordenações, serviço responsável pelas adoções) e o momento e frequência dessa interação – é revelador de aspetos da vida privada das pessoas, e, sendo suscetível de relacionamento, permite a centralização de informação sobre os cidadãos por parte do poder público e até a criação de um perfil de cada cidadão. Nesta medida, os tratamentos de dados sobre que incide o Projeto assumem a natureza de sensíveis, de acordo com o

[2] Na hipótese de a mesma entidade querer efetuar duas notificações distintas (*v.g.,* para pagamento de uma coima e de uma taxa), é necessário conseguir identificá-las. O que pode ser feito através do assunto ou de um qualquer outro elemento que permita distingui-las e rastreá-las.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

estatuído no n.º 1 do artigo 7.º da LPDP e em conformidade com o disposto no n.º 3 do artigo 35.º e no artigo 34.º da Constituição da República Portuguesa (CRP).

A intrusão na vida privada é significativamente potenciada se o sistema de notificações eletrónicas permitir dar a conhecer, à entidade responsável pela sua gestão, o conteúdo das comunicações – o que não resulta claro do presente Projeto.

c. Cabe também destacar que, para atingir a finalidade de criação de uma morada digital fidelizada que permita o envio de notificações com eficácia jurídica, o Projeto encerra uma opção sem a correspondente justificação, quando, em rigor, existem outras soluções adequadas à prossecução do mesmo fim e com menores riscos. Na verdade, não decorre do preâmbulo do Projeto de diploma que tenha sido realizado o imprescindível estudo sobre o impacto das medidas aqui propostas, sobretudo quanto aos riscos que a solução escolhida importa para a privacidade dos cidadãos, o que terá prejudicado a ponderação de outras soluções, seja como alternativa à morada única digital, seja para mitigar os riscos que decorrem desta opção. A estes pontos se voltará na apreciação do articulado do Projeto[3].

d. Assinale-se ainda que o Projeto prevê a criação de um sistema de informação sem que o mesmo esteja descrito de modo detalhado, o que dificulta a apreciação técnica e, consequentemente, a apreciação jurídica sobre a sua conformidade com os princípios e regras de proteção de dados. Donde, na análise subsequente, a CNPD se ver por vezes obrigada a admitir diferentes cenários para cada um dos componentes do sistema.

[3] De todo o modo, sempre se dirá não perceber o que se pretende dizer no preâmbulo com a referência a *no sentido de evitar que os cidadãos e as empresas tenham de aceder a diversas caixas de correio disponibilizadas por múltiplas plataformas e portais dos diferentes serviços do Estado*. Com efeito, a CNPD desconhece quais as *múltiplas plataformas* dos serviços do Estado que disponibilizam caixas do correio, não se afigurando poder considerar este argumento como determinante (ou codeterminante) para a criação da referida morada única digital. A única realidade com que os cidadãos se deparam é a de aceder a portais dos diferentes serviços do Estado e, porventura, ter de interagir com alguns serviços por correio eletrónico. Nesta perspetiva, a morada única digital não parece simplificar nenhum ato do cidadão, não se alcançando a vantagem da solução vertida no Projeto.

2. Análise do teor do Projeto de Lei

2.1. No **artigo 2.º** do Projeto determina-se a natureza voluntária da adesão à morada única digital e ao serviço público de notificações eletrónicas.

Se se reconhece ser esta uma forma de contornar os obstáculos decorrentes de um sistema de vinculação a um único endereço e a uma forma (eletrónica) de interação com a Administração Pública, não pode deixar de se alertar para o que, com elevadíssima probabilidade, vai ocorrer num futuro próximo. Como a história recente tem demonstrado, medidas intrusivas na autonomia privada dos cidadãos são frequentemente introduzidas com carácter facultativo e, ulteriormente, transformadas em regras impositivas, com argumentos de eficiência, necessidade ou, simplesmente, de que se trata tão-somente de "oficializar" um mecanismo que já está implementado e a que adere alegadamente a generalidade da população[4]. A CNPD, num juízo de prognose, antecipa por isso a hipótese de a morada única digital depressa perder o seu cariz voluntário. Também em face desta probabilidade (mas a mera possibilidade, que ninguém está em condições de afastar, seria já por si suficiente), entende a CNPD justificar-se que na criação deste sistema se proceda a uma cuidadosa ponderação dos riscos envolvidos e se adotem soluções capazes de os minimizar.

2.2. No **artigo 3.º** prevê-se o direito a fidelizar um único endereço eletrónico.

2.2.1. A este propósito, importa começar por sublinhar que a fidelização de um único endereço eletrónico equivale a um identificador único do cidadão perante a Administração Pública, que é equiparado ao domicílio das pessoas singulares.

É evidente que se pretende que o endereço funcione como identificador único do cidadão perante toda a Administração Pública (cf. n.º 5 do artigo 3.º) e que todas as comunicações entre esta e o cidadão se processem exclusivamente por este meio.

Embora não seja explicitado neste artigo, nem nos restantes preceitos do Projeto, se este identificador será do conhecimento de todas as entidades públicas intervenientes ou apenas da entidade pública que disponibiliza o serviço público de notificações eletrónicas, ainda

---

[4] Tome-se o exemplo do e-fatura, que começou por ser um sistema de adesão voluntária e apresentado como mero meio para obter um prémio (um veículo automóvel, no âmbito de um sorteio), e hoje é condição legal para que os cidadãos usufruam das deduções que a lei reconhecia até aí em sede de IRS.

assim, mesmo nesta segunda hipótese (de as entidades públicas intervenientes não conhecerem o identificador), o identificador único permite um cruzamento de informação pessoal sem precedentes.

Além da maior facilidade de relacionamento da informação quando esta é transmitida por via eletrónica – por comparação com uma carta fechada –, há que atender ao facto de que, ao contrário do que sucede com o domicílio (que é o mesmo pelo menos para todo o agregado familiar), o endereço eletrónico será individual. O que permite a associação da informação à pessoa identificada e o relacionamento da informação entre si, acentuando consideravelmente a exposição da vida privada de cada cidadão perante o Estado.

Poderá, porventura, alegar-se que o risco é diminuto, por haver possibilidade de relacionamento de toda a informação.

Na realidade, o Projeto é omisso quanto à natureza da informação que é necessariamente transmitida à entidade pública que disponibiliza o serviço público de notificações eletrónicas para efeito de assegurar tal serviço. Todavia, mesmo admitindo que esta entidade pública não tenha acesso aos conteúdos das mensagens notificadas, parece ter sempre acesso à seguinte informação: com que entidade pública e respetivo serviço está o cidadão a interagir, bem como o momento, a frequência e o assunto da comunicação. Ora, esta informação, se disponível no seu conjunto e conservada durante um determinado período de tempo, é suscetível de revelar aspetos significativos da vida privada do cidadão de modo desnecessário. É que o facto de o endereço eletrónico corresponder a um identificador único dos cidadãos, e não estar afastada a hipótese de o mesmo ser potencialmente chave comum a todos os organismos da Administração Pública, oferece as condições para a criação de perfis dos cidadãos (*profiling*) a partir de informação pessoal em massa (*Big Data*).

Só não será assim se estiverem previstos e forem implementados mecanismos adequados que previnam a possibilidade de relacionamento da informação. No entanto, este Projeto não regula o sistema de informação que cria.

Importa, a este propósito, recordar que o sentido e extensão da autorização legislativa é o de o serviço público de notificações eletrónicas ser regulado por via legislativa – e não por via de um mero ato regulamentar da Administração Pública.

Assim, face à atual redação do Projeto, a CNPD só pode concluir estar a ser desrespeitada a *ratio* subjacente à norma do n.º 5 do artigo 35.º da CRP e com isso o disposto no n.º 3 do mesmo artigo. Efetivamente, se a proibição constitucional do número nacional único do cidadão surge num contexto histórico específico, a verdade é que a razão de ser da proibição mantém hoje toda a pertinência: como ensinam Gomes Canotilho e Vital Moreira, «a proibição do número nacional único (n.º 5) funciona como garantia daqueles direitos [previstos nos n.ºs 1, 3 e 4 do artigo 35.º da CRP], dificultando o tratamento informático de dados pessoais e a sua interconexão, que seria facilitada com um identificador numérico comum»[5]. E o que se diz quanto a um identificador numérico não pode deixar de se afirmar quanto a um identificador comum (mesmo que não numérico), como o é a morada única digital.

Por outras palavras, a morada única digital vai tendencialmente constituir-se no identificador universal de cada cidadão perante a Administração Pública. E a sua utilização para a interação entre esta e os cidadãos, arquivada num repositório de informação – cf. alínea c) do artigo 16.º do Projeto –, vai permitir atingir o resultado que se pretende proibir no n.º 5 do artigo 35.º da CRP.

Um eventual contra-argumento de que este sistema não integra por ora a totalidade dos organismos públicos, mas que apenas se restringe às entidades públicas aderentes é frágil. A intenção legislativa aqui subjacente é claramente a de estender esta solução a toda a Administração Pública e ainda, sublinhe-se, a todas as entidades privadas que exercem poderes públicos de autoridade (*v.g.,* empresas fiscalizadoras do parqueamento de veículos no espaço público) ou prestem serviços públicos essenciais (empresas de fornecimento de energia, de serviços de telecomunicações, etc.) – cf. artigo 7.º do Projeto.

Poderá ainda ser invocado que a morada única digital tem cariz voluntário, argumento que, no entanto, não colhe. A adesão voluntária à morada única digital não afasta os riscos de relacionamento da informação pessoal dos cidadãos que a referida opção comporta e, portanto, recai sobre o legislador a específica obrigação de, por aplicação do princípio da proporcionalidade, afastar ou reduzir ao mínimo indispensável a restrição dos direitos fundamentais aqui afetados (cf. artigo 18.º, n.º 2 , da CRP).

---

[5] Cf. Gomes Canotilho/ Vital Moreira, *Constituição da República Portuguesa Anotada*, 4.ª ed., Vol. I, Coimbra Editora, p. 551.

É que ao remeter para a vontade do cidadão a decisão de fidelizar um único endereço eletrónico (cf. n.º 1 do artigo 3.º do Projeto), tem a lei de garantir que essa vontade é manifestada com o conhecimento de todas as consequências que daí advêm, o que este Projeto de diploma claramente não faz.

Por tudo isto, entende a CNPD que a criação da morada única digital, nos termos pouco precisos em que vem concretizada no presente Projeto, põe em causa a proibição constitucional de relacionamento da informação sobre o cidadão pelo Estado e o poder público (e ainda por outras entidades privadas potencialmente aderentes). Sendo de censurar o facto de o Projeto não prever medidas para acautelar tal resultado, quando cada vez mais se acentua no domínio da criação de sistemas de informação a necessidade de serem adotadas de raiz soluções que minimizem o impacto sobre a proteção de dados pessoais e se exige à lei a consagração desse princípio da precaução[6].

2.2.2. Uma via possível para prevenir os riscos de relacionamento da informação de cada cidadão a partir de uma base de dados de informação massiva seria a de admitir a indicação de mais do que um endereço eletrónico para o efeito do serviço público de notificações eletrónicas.

Na realidade, não se vislumbram razões para se afastar a possibilidade de utilizar o mesmo sistema de notificações através de vários endereços eletrónicos por pessoa. Solução que traz a inegável vantagem de prevenir o efeito negativo da morada única digital – reduz substancialmente os riscos de relacionamento da informação pessoal, mitigando assim o impacto na vida privada e sobre outras dimensões humanas tidas por sensíveis e especialmente protegidas no ordenamento jurídico português, Como facilmente se compreende, se uma pessoa utilizar um endereço eletrónico para interagir com a Autoridade Tributária e Aduaneira (AT), um outro para interagir com a Segurança Social, outro ainda para o Serviço Nacional de Saúde e outro para a comunicação com os restantes serviços públicos, serão maiores as dificuldades de relacionamento da informação e de controlo dessa

[6] Neste sentido, pode ver-se, apesar de ainda não aplicável, o artigo 25.º do Regulamento Geral sobre a Proteção de Dados – Regulamento (UE) 679/2016.

informação por parte do Estado. Obviamente, desde que tais endereços não sejam direta e imediatamente relacionáveis com o mesmo número de identificação do cidadão.

Recomenda, por isso, a CNPD que o Projeto reconheça aos cidadãos o direito de utilização de endereços diversificados no serviço público de notificações eletrónicas, ao contrário do que se estatui no n.º 5 do artigo 3.º.

2.2.3. Ainda no mesmo artigo 3.º, no n.º 2, faz-se referência a um *fornecedor admissível de correio eletrónico*, mas o Projeto é omisso quanto à definição de fornecedor admissível, bem como quanto aos critérios da admissibilidade, remetendo para regulamentação ulterior a sua explicitação. Em todo o caso, em sede de regulamentação importa assegurar que não haja discriminação injustificada dos titulares de dados quanto ao fornecedor de correio eletrónico selecionado. A discriminação dos titulares de dados com base no fornecedor de correio eletrónico só pode ser considerada legítima quando existirem razões fundamentadas para acreditar que esse fornecedor não providencia as exigências mínimas de segurança e não respeita o regime de proteção de dados da União Europeia.

2.3. O **artigo 4.º** do Projeto pretende regular o procedimento de fidelização do endereço eletrónico.

2.3.1. A primeira observação que este artigo merece é a de que pouco adianta quanto ao referido procedimento, remetendo a definição dos seus termos para regulamentação administrativa.

Importa, em todo o caso, advertir aqui para as fragilidades da chave móvel digital, já identificadas pela CNPD no Parecer n.º 20/2016[7], recomendando-se a sua correção antes da sua utilização para os efeitos aqui mencionados.

2.3.2. No n.º 3 do mesmo artigo prevê-se que, após a fidelização, o endereço eletrónico fique associado, no caso das pessoas singulares, à identificação civil (e, no caso das pessoas singulares estrangeiras, à identificação fiscal). Não é contudo evidente o que se quer dizer com a expressão «ficar associado» à identificação civil e fiscal: se o endereço fica associado

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

ao números de identificação civil ou fiscal, ou se aquele dado pessoal fica registado na base de dados de identificação civil ou na base de dados da AT.

Não se alcançado o sentido da norma, não se pode ajuizar se de tal associação decorre a diminuição da informação residente no serviço público de notificações eletrónicas e, com isso, uma minimização dos riscos para a privacidade dos cidadãos. Por razões de certeza jurídica, recomenda-se a clarificação deste preceito.

2.4. Cabe ao **artigo 5.º** a regulação do serviço público de notificações eletrónicas associado à morada única digital.

Aí se indica que a gestão desse serviço fica a cargo de uma entidade pública, cuja identificação se remete para regulamento administrativo, sobre a qual recai o dever de garantir a existência de um sistema informático de suporte que permita comprovar e registar a morada única digital. Fixa-se ainda que tal sistema tem de garantir a comprovação da data e hora da disponibilização efetiva das notificações nessa morada, pouco mais desenvolvendo em relação ao teor do mandato que o Parlamento nacional atribuiu ao Governo na alínea g) do artigo 2.º da autorização legislativa, o que não pode deixar de se estranhar.

2.4.1. Em primeiro lugar, importa recordar que do direito fundamental à inviolabilidade das comunicações, consagrado no artigo 34.º da CRP, decorre que o conteúdo das comunicações não pode ser do conhecimento de outrem que não seja o respetivo destinatário. Por essa razão, deve estar previsto, no próprio Projeto, um mecanismo adequado a assegurar a confidencialidade das comunicações, constituindo o meio mais apto para o efeito a criptografia do conteúdo das mensagens objeto de notificação.

Esta é uma das exigências básicas decorrente dos princípios da proporcionalidade e da minimização dos dados pessoais no âmbito de comunicações eletrónicas entre cidadãos e a Administração Pública (cf. alínea c) do n.º 1 do artigo 5.º da LPDP; v. ainda o artigo 4.º da Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto), como forma de garantia de que a entidade que disponibiliza o serviço público de comunicações eletrónicas, bem como o fornecedor de correio eletrónico, não conheça o conteúdo das mensagens e

anexos objeto de comunicação quando, em rigor, não tem necessidade de o conhecer para o cumprimento do serviço que disponibiliza.

Sendo em sede legislativa que os direitos, liberdades e garantias devem ser regulados (cf. alínea b) do n.º 1 do artigo 165.º da CRP), não pode deixar de se recomendar que no próprio Projeto de Decreto-Lei autorizado se imponha que o sistema de suporte ao serviço público de comunicações garanta que a entidade que o gere não pode conhecer do conteúdo das comunicações[8]. De outra forma estar-se-á a criar e a regular um sistema de informação que não assegura o respeito pelos direitos à reserva da intimidade da vida privada, à inviolabilidade das comunicações e à proteção dos dados pessoais (cf. artigos 26.º, n.º 1, 34.º e 35.º da CRP).

Acrescenta-se que, na hipótese de se prever a obrigação de cifrar os conteúdos das mensagens notificadas, é necessário equacionar uma solução que permita à entidade remetente trocar mensagens confidenciais com o cidadão, sem depender de uma chave criptográfica definida previamente. Uma solução possível passa pela utilização de certificados digitais (criptografia assimétrica), aproveitando porventura os certificados já existentes em cada cartão de cidadão. Este cenário implicaria o acesso das entidades às chaves públicas dos certificados digitais dos cidadãos, sem risco para a privacidade, já que a aplicação deste modelo criptográfico se baseia no conhecimento público destas chaves.

2.4.2. O artigo 5.º pouco mais adianta sobre o sistema de suporte ao serviço público de comunicações eletrónicas. Donde, ficam por regular aspetos importantes do seu funcionamento com diretas e relevantes repercussões na esfera jurídica fundamental dos cidadãos.

a. Desde logo, para além de não se descrever como opera a disponibilização efetiva das notificações, nem se fixarem parâmetros para a sua conceção, fica por esclarecer

---

[8] Deve ainda prever-se que o assunto da comunicação – em relação ao qual, para efeito de comprovação da sua disponibilização, se admite que a entidade que disponibiliza o serviço público de comunicações tenha acesso – seja identificado também de acordo com aqueles princípios, por forma a atenuar ao mínimo indispensável o impacto na privacidade dos cidadãos.

como se realiza a comprovação das notificações feitas, bem como do seu conteúdo integral.

O silêncio do Projeto nesta matéria parece apontar no sentido de que o sistema que suporta o serviço público das notificações eletrónicas conserva o conteúdo das mesmas. Mas se é isso que sucede, então a solução arquitetada suscita reservas não apenas quanto à inviolabilidade das comunicações – já referidas em 2.4.1. –, como também quanto à centralização da informação pessoal que a Administração Pública detém sobre um concreto cidadão num único sistema de informação, atenta a natureza sensível dos dados pessoais que podem ser objeto de notificação. Sem prejuízo de uma tal solução ser, na perspetiva da CNPD, inconstitucional, nos termos acima expostos, afigura-se crucial a explicitação no texto do Projeto da opção tomada quanto ao sistema de informação que suporta o serviço público de notificações. E caso seja esta, importa que o Projeto imponha a adoção de medidas de segurança especialmente reforçadas.

b. Outra questão que não encontra resposta no Projeto – nem no n.º 2 do artigo 5.º, nem no artigo 8.º –, prende-se com as situações em que a notificação não seja entregue por algum motivo ou venha devolvida, por exemplo, porque a caixa de correio do destinatário se encontra cheia ou a conta está bloqueada. O Projeto de diploma não resolve, e as presunções do artigo 8.º do mesmo Projeto e do artigo 113.º do Código do Procedimento Administrativo, também não têm nesta sede aplicação.

c. Um outro aspeto de regime que aqui está omisso, e com especial relevância prática, prende-se com a estatuição de que a notificação eletrónica dispensa a consulta de qualquer outra página ou portal na internet, vertida no n.º 3 do artigo 5.º.

   Embora se compreendam as razões de simplificação e desburocratização que tal previsão normativa tem subjacentes, não pode deixar de se assinalar que este sistema de notificações eletrónicas, tal como descrito no Projeto, aumenta consideravelmente o risco de ataques baseados na personificação de organismos públicos (*i.e., phishing*) com a intenção de levar os titulares dos dados a providenciarem informações pessoais ou diligenciarem esforços que lhes sejam prejudiciais (*v.g.,* pagamento de coimas inexistentes). Veja-se, aliás, o recente exemplo de ataques em que as vítimas eram

aparentemente contactadas pela AT no sentido de procederem à regularização da situação tributária, pelo pagamento de um valor em dívida[9].

Na verdade, não se prevendo um qualquer sistema de validação, seja quanto ao remetente, seja quanto à idoneidade do conteúdo da notificação, este sistema apresenta-se como o campo ideal para a proliferação de ataques deste tipo. Não se encontrando no texto do Projeto qualquer medida destinada a prevenir ou mitigar este risco, à CNPD resta apenas alertar para o mesmo e recomendar que se repense esta solução e se imponha a adoção das medidas adequadas.

d. Finalmente, uma outra medida que não se vê aqui prevista diz respeito à verificação da autenticidade das notificações, que se afigura imprescindível. O titular tem que ter à sua disposição mecanismos que lhe permitam verificar que as notificações que recebe correspondem, efetivamente, a comunicações de organismos legítimos. Uma solução possível passa por atribuir um código único e aleatório a cada notificação cuja autenticidade possa ser verificada numa página eletrónica do próprio serviço público de notificações eletrónicas. Pela indicação do código de notificação e endereço de correio eletrónico, por exemplo, a página eletrónica poderia indicar ao titular se se trata ou não de uma comunicação autêntica.

2.5. O disposto no **artigo 6.º**, que incide sobre a adesão ao serviço público de comunicações eletrónicas, suscita algumas questões, sobretudo quando lido em conjugação com o disposto no artigo 7.º do mesmo Projeto.

Com efeito, a adesão ao serviço público de comunicações eletrónicas é voluntária também para as entidades públicas, prevendo-se a sua adesão progressiva. Ora, uma pessoa singular que adira a este serviço está a aderir a um sistema de comunicação sem conhecer à partida que entidades públicas poderão no futuro comunicar consigo por esta via.

Na verdade, a lista de entidades que aderem ao serviço público, e que estará permanentemente disponível no Portal de Cidadão (cf. n.º 2 do artigo 7.º do Projeto), é uma lista aberta, suscetível de atualização, pelo que o consentimento manifestado num determinado momento apenas é informado e específico quanto às entidades então já

[9] Cf. notícia em https://www.dinheirovivo.pt/economia/portal-das-financas-esta-a-ser-alvo-de-ataque-de-phishing/

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

aderentes, não cobrindo as entidades que entretanto venham a aderir ao referido serviço, não servindo para o efeito de legitimar o tratamento de dados pessoais.

Ora, uma vez que a adesão ao serviço público de comunicações eletrónicas pelas pessoas singulares traduz o consentimento que legitima o tratamento de dados pessoais que este sistema de informação implica – e que não se resume ao tratamento do dado *endereço eletrónico* e aos *dados de identificação*, mas ainda abrange os *dados relativos à comunicação* (hora, data da comunicação, assunto, entidade pública e respetivo serviço), bem como, ainda que eventualmente cifrados, os dados pessoais integrados no texto da mensagem comunicada, documentos anexos, etc. –, tal consentimento tem, para ser juridicamente relevante, de preencher os requisitos previstos na alínea h) do artigo 3.º da LPDP: livre, específico e informado. E como tal consentimento incide sobre um tratamento de dados sensíveis, tem também de ser expresso – cf. n.º 2 do artigo 7.º da LPDP.

Sucede que tal consentimento é em rigor genérico e nalguns casos não plenamente informado. Senão, vejamos.

a. O n.º 1 do artigo 6.º veda a possibilidade de se excluir a receção das notificações enviadas pelas entidades aderentes ao serviço. Tal significa que ao aderir, o cidadão manifesta a vontade de consentir em toda e qualquer comunicação de dados pessoais, independentemente da natureza destes dados. Esta adesão constitui, pois, um consentimento genérico dos múltiplos e sucessivos atos de notificação que venham a ocorrer e que envolvem diferentes tipos de dados pessoais. Mas, então, não corresponde ao consentimento específico que a LPDP exige e que a Diretiva que esta transpõe e o novo Regulamento Geral sobre a Proteção de Dados – Regulamento (UE) 2016/679 (RGPD) – também impõem.

   A exigência legal de uma manifestação de vontade específica no que aos dados sensíveis diz respeito – que transpõe para o ordenamento jurídico nacional a exigência definida na Diretiva 95/46/CE e reiterada no RGPD – não é compatível com a previsão da adesão genérica a um sistema de comunicação que não permite a exclusão de certos dados ou das comunicações de certas entidades públicas. Essa adesão, como forma de manifestação de vontade e portanto de consentimento no tratamento de dados pessoais, não cumpre o requisito de especificidade. E não permite ao titular dos dados adequar o seu consentimento aos dados em causa, por exemplo para aderir a

tal forma de comunicação quanto aos dados pessoais que a AT trata e já não pretender essa forma de comunicação – leia-se essa forma de tratamento de dados pessoais – para os dados de saúde. A CNPD entende por isso que o Projeto deveria integrar nas suas disposições a possibilidade de a adesão não abranger a notificação por certas entidades públicas[10].

b. Recorda-se que em relação aos dados sensíveis o consentimento deve ser expresso, pelo que a operação que sobre eles incida tem necessariamente de assentar numa manifestação de vontade expressa que não pode corresponder à simples inatividade ou inércia. Nesse sentido, cada inclusão na lista de entidades aderentes deve ser comunicada a quem aderiu à notificação eletrónica, para que cada pessoa possa dar o seu consentimento informado sobre à manutenção do interesse em receber as notificações eletrónicas em face da nova lista de entidades aderentes. Repare-se que, embora ainda não aplicável, o novo RGPD alarga a exigência de consentimento explícito, já presente na Diretiva 95/46/CE para os dados sensíveis, a todos os tratamentos de dados qualquer que seja a natureza dos dados pessoais dele objeto (cf. n.º 11 do artigo 4.º do RGPD).

2.6. No que diz respeito ao n.º 4 do **artigo 7.º** do Projeto, embora se assinale como positiva a expressa limitação do acesso pelas entidades aderentes *aos dados necessários relativos às pessoas aderentes ao serviço público de notificações eletrónicas que lhes permitam realizar a notificação pela forma prevista* no diploma, não pode deixar de lamentar-se não haver uma clara enunciação das categorias de dados pessoais que são necessárias à realização da notificação. Na medida em que esta norma do Projeto não prevê um dos elementos essenciais desta operação de acesso aos dados pessoais das pessoas singulares – as categorias de

[10] Mesmo que o legislador, com esta disposição, pretendesse derrogar a disposição da alínea h) do artigo 3.º da LPDP, adverte-se para a circunstância de tal norma corresponder à alínea h) do artigo 2.º da Diretiva 95/46/CE, não constituindo este preceito e os artigos 7.º e 8.º, que definem as condições de legitimidade do tratamento de dados, disposições da diretiva que possam ser objeto de derrogações ou restrições por parte dos Estados-Membros (cf. artigo 13.º da Diretiva). E o RGPD, embora ainda não aplicável, exige as mesmas características ao consentimento para que seja relevante.

dados a que pode aceder (cf. alínea b) do n.º 1 do artigo 30.º da LPDP) – a mesma não serve como instrumento de regulação de tal operação.

2.7. No **artigo 8.º** definem-se regras sobre o envio e receção de notificações eletrónicas.

Ora, neste artigo o direito de acesso pelo titular dos dados está consagrado em termos demasiado restritos, pelo menos quando em causa estão dados de pessoas singulares. Efetivamente, o n.º 2 do artigo 8.º admite que a presunção de receção da notificação prevista no n.º1 seja ilidida, mas não prevê o acesso direto pelo titular dos dados à informação sobre a data efetiva de receção de uma notificação eletrónica; prevê somente o acesso indireto, por via da entidade notificadora ou do tribunal, a requerimento do interessado.

Não se alcança a razão de ser de tal restrição, que na LPDP está prevista para um conjunto restrito de situações onde esta situação não se encaixa (cf. artigo 11.º da LPDP). No caso concreto, não há razão objetiva para limitar o exercício do direito de acesso previsto no n.º 1 do artigo 35.º da CRP, justificando-se o reconhecimento do direito do titular dos dados (destinatário da notificação) a solicitar a listagem de todas as comunicações a si dirigidas, bem como de toda a informação a si respeitante.

2.8. Finalmente, o **artigo 16.º** define as matérias que serão objeto de regulamento administrativo, demonstrando que os principais elementos do tratamento de dados que este novo sistema de informação implica não se encontra definido por ato legislativo – como deveria ocorrer, em cumprimento da autorização legislativa – antes se delegando tal poder no plano administrativo.

2.8.1. Em primeiro lugar, importa destacar que esta opção se afigura inconstitucional, uma vez que a Assembleia da República, na alínea g) do artigo 2.º da autorização legislativa, conferiu ao Governo poder para, por via de decreto-lei autorizado, «Estabelecer as regras de garantia, de segurança e de privacidade do sistema informático de suporte ao serviço público de notificações eletrónicas, nomeadamente garantindo a comprovação da data e hora de disponibilização efetiva das notificações e o sistema de arquivo de notificações, bem como as

regras aplicáveis à sua indisponibilidade»[11], e o diploma remete a definição dos *requisitos de segurança e privacidade da informação* para regulamento – apenas afirmando que o sistema garante a segurança e privacidade da informação, nos termos da LPDP.

Na verdade, com este Projeto não está a cumprir-se plenamente o mandato conferido pelo Parlamento, mas sobretudo remete-se o exercício dos poderes normativos conferidos pela lei de autorização, e que o Parlamento quer ver exercidos (como tem de ser nos termos da alínea b) do n.º 1 do artigo 165.º da CRP) por ato legislativo, para um regulamento do Governo no exercício da sua função administrativa. Ora, é evidente que o *reenvio para regulamento administrativo está também sujeito aos limites constitucionais da reserva de lei, não podendo a lei, no âmbito da reserva de lei, deixar de esgotar toda a regulamentação «primária» das matérias, só podendo remeter para regulamento os aspetos «secundários»*[12]. E este Projeto de diploma não esgota a regulamentação primária para que foi mandatado pela autorização legislativa, não estabelecendo «as regras de garantia de segurança e de privacidade do sistema informático de suporte ao serviço público de notificações eletrónicas». Especialmente, não define o regime aplicável ao tratamento de dados pessoais que o sistema de informação necessariamente envolve, sendo, como se explicará em seguida, omisso quanto aos elementos essenciais do mesmo, seja quanto à sua identificação, seja quanto a critérios ou parâmetros para a sua definição ulterior, não sendo suficiente, para esse efeito, a mera afirmação de que tal sistema cumprirá o disposto na LPDP. A ausência de fixação de parâmetros quanto ao sistema de informação no que à garantia de privacidade e de segurança diz respeito é, pois, evidente.

Assim, entende a CNPD que este Projeto desrespeita o sentido e extensão da autorização emitida nos termos do artigo 165.º da CRP e o disposto nos n.ºs 2 e 5 do artigo 112.º da CRP.

2.8.2. Por outro lado, a remissão da previsão específica dos vários elementos do tratamento de dados pessoais para regulamento administrativo não permite considerar o Projeto de Decreto-Lei como instrumento de regulação do tratamento de dados, nos termos do artigo 30.º da LPDP.

---

[11] Disponível em http://debates.parlamento.pt/catalogo/r3/dar/s2a/13/02/056/2017-01-23/2?pgs=2-3&org=PLC&plcdf=true

[12] Gomes Canotilho / Vital Moreira, ob. cit., pp. 70-71.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Na realidade, omite-se a identificação do responsável pelo sistema, e portanto, pelo conjunto do tratamento de dados pessoais; omite-se o elenco das categorias de dados pessoais tratados; não se prevê qualquer medida de segurança nem de garantia de autenticidade das notificações; não se explica como funciona o sistema, se há conservação dos dados pessoais, por quanto tempo e em que condições.

Acresce que apenas nas disposições finais do Projeto, mais especificamente na alínea c) deste artigo 16.º, se faz pela primeira vez referência a um arquivo – não se percebendo que tipo de informação é registada ou arquivada, nem se adivinhando a extensão dessa informação.

Recomenda-se assim que o Projeto de diploma preveja e regule nalgum ponto do seu articulado a existência de uma base de dados de notificações eletrónicas, identificando a entidade por ela responsável e definindo, pelo menos, os dados pessoais que a integram e o prazo de conservação dos mesmos.

III. Conclusões

1. A morada única digital constitui um identificador único do cidadão, que servirá potencialmente para qualquer interação com a Administração Pública e com outras entidades privadas, e que permite a associação da informação a uma concreta pessoa singular e o relacionamento da informação entre si (quanto aos cidadãos que a ela adiram), permitindo inclusive a criação de perfis. Sob pena de se ter por violado o disposto no n.º 3 do artigo 35.º da Constituição e o n.º 5 do mesmo artigo, enquanto norma que serve de garantia da proibição de cruzamento e interconexão da informação sobre os cidadãos pelo Estado e o poder público, a CNPD entende que cabe ao legislador, no Projeto, prever as medidas adequadas a eliminar ou mitigar tais riscos, em cumprimento daqueles comandos constitucionais e do n.º 2 do artigo 18.º da Constituição.

2. A CNPD destaca também o facto de este risco ser potenciado pela previsão de um registo de notificações eletrónicas e de um arquivo (remetendo-se a respetiva regulação para regulamento administrativo), no âmbito do serviço público de notificações eletrónicas, que implica a conservação e recolha de informação pessoal suscetível de expor a vida privada dos cidadãos. Com efeito, a utilização da morada única digital para a interação entre a Administração Pública e os cidadãos, arquivada numa base de dados, vai permitir atingir o resultado que se pretende proibir no n.º 5 do artigo 35.º da CRP.

   Recomenda, por isso, a CNPD que o Projeto preveja medidas adequadas a eliminar ou mitigar os riscos de relacionamento ou cruzamento de informação relativa aos cidadãos que adiram à morada única digital, bem como ao serviço público de notificações eletrónicas; tais soluções podem passar pelo reconhecimento aos cidadãos do direito de utilização de endereços diversificados no serviço público de notificações eletrónicas, ao contrário do que se estatui no n.º 5 do artigo 3.º do Projeto.

3. Alerta ainda para a circunstância de no Projeto não se garantir a inviolabilidade das comunicações, através da previsão de medidas que previnam o conhecimento dos seus conteúdos pela entidade que disponibiliza o serviço público de notificações eletrónicas (porventura por meio de uma solução de cifragem das comunicações); o Projeto é omisso quanto ao tipo de informação a que tal entidade pode aceder, sem

que se possa concluir que respeita os direitos fundamentais previstos no artigo 34.º, no n.º 1 do artigo 26.º e nos n.ºs 1 e 3 do artigo 35.º da Constituição.

4. Uma vez que o Projeto não regula o essencial do sistema de informação que serve de suporte ao serviço público de comunicações eletrónicas, sendo omisso quanto a uma série de elementos fundamentais do tratamento de dados pessoais que o mesmo envolve, e remete o exercício do poder normativo conferido pela Assembleia da República para regulamento administrativo, a CNPD entende estar a ser desrespeitado o sentido e a extensão da autorização legislativa, tendo sérias dúvidas quanto à constitucionalidade de uma tal opção, em face do estatuído nos artigos 165.º, n.º 1, alínea b), e 112.º, n.ºs 2 e 5, da Constituição.

   A CNPD recomenda, assim, que o Projeto de diploma explicite a criação de uma base de dados de notificações eletrónicas, identificando a entidade por ela responsável e definindo, pelo menos, os dados pessoais que a integram e o prazo de conservação dos mesmos, sob pena de não ser apta a funcionar como instrumento de regulação do tratamento, nos termos do artigo 30.º da LPDP; além disso, recomenda a definição de regras claras sobre o funcionamento do serviço público de notificações, desde logo quanto ao modo de disponibilização das mesmas, o seu registo e alguns aspetos do regime da prova assinalados.

5. De entre outras observações expostas supra, no ponto II.2., a CNPD destaca ainda que:

   i. A dispensa de consulta de qualquer outra página ou portal na internet, vertida no n.º 3 do artigo 5.º do Projeto, operada pela notificação eletrónica aumenta o risco de *phishing*, pelo que recomenda que se equacione tal solução e se preveja um qualquer sistema de validação externo às notificações, seja quanto ao remetente, seja quanto à idoneidade do conteúdo da notificação, que previna ou atenue tal risco;

   ii. A adesão ao serviço público de comunicações eletrónicas, regulada no artigo 6.º do Projeto, para poder legitimar o subsequente tratamento de dados pessoais tem de traduzir uma manifestação de vontade livre, específica e informada (cf. artigo 3.º, alínea h), da LPDP), o que, tal como se encontra regulado no Projeto, não se verifica; isto porque, no momento em que tal

vontade é exteriorizada, os termos dos tratamentos de dados não estão cristalizados, podendo ainda surgir como entidades aderentes outras para além das que constam da lista publicada; e o consentimento para o tratamento dos dados pessoais decorrentes das notificações eletrónicas provenientes destas novas entidades não pode, de acordo com o n.º 2 do artigo 7.º da LPDP, corresponder à simples inatividade ou inércia;

iii. O artigo 8.º regula o direito de acesso pelo titular dos dados para efeito de ilidir uma presunção legal, mas restringindo-o a um acesso indireto, em violação do direito consagrado no n.º 1 do artigo 35.º da CRP e no artigo 11.º da LPDP (bem como no Direito da União Europeia);

iv. É conveniente a clarificação da redação de algumas normas, designadamente o n.º 2 do artigo 3.º e o n.º 3 do artigo 4.º do Projeto.

É este o Parecer da CNPD.

Lisboa, 2 de março de 2017

Helena Delgado António (Relatora)