

PARECER/2019/41

I. Pedido

O Gabinete da Ministra do Mar remeteu à Comissão Nacional de Proteção de Dados (CNPD), para apreciação, o projeto de decreto-lei que cria a Janela Única Logística (JUL), estabelecendo as condições de funcionamento e acesso, da sua governação, gestão e operação e transpõe para a ordem jurídica interna a Diretiva n.º 2010/65/UE, do Parlamento Europeu e do Conselho, de 20 de outubro, relativa às formalidades de declaração exigidas aos navios à chegada e ou à partida dos portos dos Estados membros, e que revoga a Diretiva n.º 2002/6/CE, do Parlamento Europeu e do Conselho, de 18 de fevereiro.

O pedido formulado e o parecer ora emitido decorrem das atribuições e competências da CNPD, enquanto entidade administrativa independente com poderes de autoridade para o controlo dos tratamentos de dados pessoais, conferidos pela alínea c) do n.º 1 do artigo 57.º e pelo n.º 4 do artigo 36.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), em conjugação com o disposto no n.º 1 do artigo 21.º e no n.º 1 do artigo 22.º, ambos 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).

A apreciação da CNPD cinge-se às normas que preveem ou regulam tratamentos de dados pessoais.

II. Apreciação

O objetivo primordial deste projeto de decreto-lei é consagrar, no plano nacional, as soluções de facilitação declarativa por parte de quem utiliza os portos nacionais. A proposta de regulamento europeu nesta matéria, já votada pelo Parlamento Europeu¹, e que deverá ser publicado em breve, aponta justamente para a simplificação das obrigações declarativas neste âmbito². De resto, e para lá dessa facilitação, encontra-se inscrita no texto do futuro regulamento a necessidade de garantir a interoperabilidade dos sistemas de gestão do fluxo (de pessoas, carga e navios) dos portos europeus.

¹ Texto aprovado disponível em http://www.europarl.europa.eu/doceo/document/TA-8-2019-0434_PT.html#title2.

² Cfr. considerando 19 do citado futuro regulamento.



Sublinhe-se que, desde a Diretiva 2002/59/CE, no domínio do controlo do tráfego de navios na UE, se aponta para sistemas que promovam e efetivem a referida interoperabilidade.

No contexto português, a mais relevante das novidades trazida pelo presente projeto de diploma encontra-se no alargamento das facilidades declarativas e centralização da informação a outros meios de transporte, no caso, o rodoviário e ferroviário, procedendo-se à padronização dos modelos e obrigações de reporte de informação na chamada Janela Única Logística, plataforma que agora sucede à Janela Única Portuária, cujo enquadramento legal se iniciou com o Decreto-Lei n.º 370/2007, de 06 de novembro.

Esta nova plataforma *“é de utilização obrigatória para a apresentação das formalidades de declaração e para a gestão dos fluxos de informação associados ao planeamento, execução e monitorização da movimentação dos meios de transporte e das mercadorias entre os nós da cadeia de transporte que usem os portos nacionais para a importação, exportação ou transshipment, ou em qualquer circunstância pontual que requeira o uso de um porto nacional.”* (cfr. artigo 3.º, n.º 2). E a sua utilização abrange as atividades previstas nos n.ºs 3 e 4 do artigo 3.º do projeto: Transporte marítimo de pessoas e bens através dos portos nacionais; Transporte de mercadorias ao longo das cadeias logísticas que utilizem os portos nacionais; Transporte de passageiros pela via marítima ou fluvial; Tráfego de cruzeiros e gestão de marinas e portos de recreio; Atividades marítimo-turísticas, incluindo a gestão do tráfego fluvial; Serviços prestados nos portos de pesca, incluindo os relativos à exportação e importação de pescado; Execução das formalidades de declaração e dos procedimentos associados ao controlo de fronteira nas zonas internacionais inseridas nas áreas de jurisdição dos portos nacionais.

Prescreve-se, para todas *“As entidades públicas e privadas que intervenham na JUL [o dever de] atuar em estreita colaboração, desenvolvendo os melhores esforços no sentido da concertação de interesses, designadamente no âmbito da Comissão Nacional para a Simplificação e Digitalização do Transporte e Logística criada pelo presente decreto-lei, e no desenvolvimento de forma coordenada dos sistemas de informação da competência de cada uma das partes”* (cfr. artigo 4.º, n.º 5 do projeto). Sendo certo que *“Têm acesso à plataforma tecnológica as pessoas singulares e coletivas, públicas e privadas, às quais o presente decreto-lei se aplica.”* de acordo com o prescrito no artigo 11.º, n.º 1.

A. Nota prévia

O projeto de decreto-lei não é claro sobre a existência de interconexões de distintas bases de dados por forma a permitir a operacionalização das muitas capacidades descritas no artigo 9.º, n.º 2. No entanto, a necessidade de compatibilização desta plataforma com a “*componente nacional do sistema SafeSea Net respeitante à implementação da Diretiva n.º 2002/59/CE, do Parlamento Europeu e do Conselho, de 27 de junho, relativa à instituição de um sistema comunitário de acompanhamento e de informação do tráfego de navios, integrando a informação proveniente, nomeadamente, do posicionamento dos navios e dos atos declarativos efetuados nos portos através da JUP*” (cfr. preâmbulo do projeto de decreto-lei), indicia a existência de pelo menos algumas interconexões³ as quais, por se encontrarem omissas, não permitem à CNPD emitir qualquer juízo sobre a sua robustez técnica ou adequação legal.

Seria, pelo exposto supra, importante que o futuro decreto-lei possa discriminar essas interconexões (se existentes) e que as mesmas venham a ser objeto de regulamentação para garantir os imprescindíveis aspetos de segurança e resiliência das redes de comunicação em causa.

B. Notas sobre o regime de proteção de dados

Existe uma cláusula genérica no n.º 4 do artigo 5.º (Princípios gerais do funcionamento da JUL) que assim dispõe: “*Sem prejuízo do acesso aos dados pessoais facultados no âmbito da JUL às entidades competentes, é garantida a confidencialidade das informações comerciais e outras informações sensíveis partilhadas na JUL, sendo ainda assegurado o tratamento adequado desses dados pessoais para as finalidades previstas no presente decreto-lei*”. Em si mesma, a redação deste número não é obstáculo à concretização do regime de proteção de dados, mas a forma como se englobam dados pessoais e “dados comerciais e outras informações sensíveis” marca a tónica do projeto de decreto-lei, em que a matéria ligada ao direito fundamental, previsto no artigo 35.º da Constituição da República Portuguesa, parece ser abordada

³ Como, de resto, também resulta de outras passagens do preâmbulo: “*com vista à integração da informação marítima numa só plataforma, são interligados com a JUL todos os sistemas nacionais e internacionais cuja informação seja necessária para o funcionamento desta plataforma*”.



como uma dimensão acessória ou complementar da restante informação tratada no quadro da JUL.

Quanto ao ponto específico da proteção de dados pessoais, o projeto destina-lhe um artigo próprio (artigo 15.º), sendo que outros dois transportam dimensões relevantes ligadas à concretização de obrigações fundamentais inscritas no RGPD (artigo 16.º e 17.º).

- Responsáveis pelo tratamento

Nesse primeiro artigo dedicado a regulamentar os tratamentos de dados pessoais no contexto do presente projeto, assinala-se que os responsáveis pelo tratamento⁴ de dados inseridos na JUL são “A ACN [*Autoridade Competente Nacional – a Direção-Geral de Recurso naturais, Segurança e Serviços Marítimos*] e as ACL [*Autoridades Competentes Locais – administrações portuárias*], em conformidade com as responsabilidades definidas no artigo 8.º”. Percebe-se a designação destas entidades, se atentarmos no que dispõe o n.º 3 do artigo 9.º do projeto: “No sentido de assegurar o cumprimento integral da legislação, bem como dos procedimentos que visem aumentar a eficácia e eficiência dos meios de transporte e das cadeias logísticas associados ao setor marítimo-portuário, a governação, gestão e operação da JUL compete: a) À ACN no que concerne às políticas e decisões de âmbito nacional e às soluções tecnológicas que compõem a Camada Nacional da JUL; b) Às ACL no que concerne às restantes soluções tecnológicas da JUL”. Ao estarem incumbidas do cumprimento desta legislação e da operacionalização da JUL, a consequência natural dessa função seria justamente a atribuição da condição de responsáveis pelo tratamento, até porque, para lá da gestão funcional da plataforma, a efetivação dos direitos dos titulares dos dados não pode deixar de fazer corresponder a esse estatuto quem materialmente esteja capacitado para determinar e gerir o ciclo de vida das operações que ocorram sobre tais dados.

Apesar do acerto da opção pela designação daquelas entidades como responsáveis pelo tratamento, não pode esquecer-se que o alargamento muito sensível de entidades com acesso ao sistema, que ocorrerá sob a égide deste diploma, obrigará a preocupações reforçadas com a segurança da informação. A estratificação dos acessos e a garantia de integridade dos dados devem constituir objetivos prioritários dos

⁴ Conceito previsto no artigo 4.º, n.º 7, do RGPD.

responsáveis, os quais não podem deixar de se ligar à estrutural fiabilidade da rede que permitirá esses novos acessos. É bem-vinda, por isso, a previsão do n.º 2 do artigo 11.^º, onde se afirma que *“O acesso à informação e aos serviços disponibilizados na plataforma tecnológica são objeto de autenticação individual do utilizador, sendo estabelecidas proteções baseadas em ficheiros de controlo de acessos e de auditoria dos utilizadores, nos termos do sistema comum de gestão de utilizadores e de acessos estabelecido pela ACN e pelas ACL”*. Espera-se, todavia, que haja particular atenção, na regulamentação futura da JUL, aos requisitos essenciais que permitam concretizar de forma coerente as preocupações com a gestão de acessos e credenciação de utilizadores.

- Dados pessoais tratados

O n.º 3 do artigo 15.^º lista os dados pessoais tratados⁶ para os efeitos do n.º 2 do artigo 7.^º, sendo que este último se reporta ao modelo de referência nacional utilizado para garantir a interoperabilidade do sistema por parte de todos os utilizadores da JUL. Já o n.º 4 acrescenta à lista de dados citada *“as seguintes categorias especiais de dados, recolhidas para efeitos de apresentação das formalidades às autoridades e controlo de acessos: a) Dados relativos à saúde de tripulantes e passageiros; b) Dados biométricos”*. Estas listas de dados, se bem que úteis e promotoras da transparência na utilização da informação pessoal dos titulares dos dados, não permitem perceber, com clareza, a quem se referem (quais as categorias de titulares dos dados afetados). É imperscrutável o sentido da recolha de vídeos se não for especificado o universo de pessoas a quem tal recolha respeite, como é igualmente insondável a razão para a recolha de dados biométricos da generalidade dos titulares dos dados sujeitos a figurarem na JUL. Se no n.º 4 se denota um esforço para restringir esse universo, não se pode deixar de assinalar que a redação apresentada não logra limitar ao essencial as categorias de titulares de dados afetados. Desde logo, a mistura da recolha de dados

⁵ Como útil é também a redação do n.º 1 do artigo 14.^º quanto à obrigatoriedade de “A ACN e as ACL deve[r]em garantir a autenticidade da origem, a integridade do conteúdo e a legibilidade das formalidades e demais informações trocadas eletronicamente, desde o momento da sua emissão até ao final do período de arquivo, implementando controlos suscetíveis de auditoria ao fluxo de informação”.

⁶ São eles: Nome; Data de nascimento; Naturalidade; Nacionalidade; Género; Tipo e número de identificação civil e respetiva data de validade; Número de identificação fiscal; Função ou categoria profissional; Morada; Correio eletrónico; Contacto de telefone móvel; Fotografia e vídeo; Assinatura autografa e assinatura digital qualificada.



biométricos para “apresentação de formalidades às autoridades e controlo de acessos” funde num mesmo grupo, categorias de titulares seguramente distintas.

- Direitos dos titulares dos dados

Por seu turno, o n.º 5 deste mesmo artigo 15.º, determina quem tem acesso aos dados pessoais constantes da JUL: *“a) Qualquer utilizador da JUL, quanto aos seus dados pessoais; b) O utilizador indicado por cada entidade pública ou privada, para efeitos de manutenção das contas de acesso da sua entidade, limitado aos dados identificados no n.º 3; c) Os organismos e serviços do Estado e demais pessoas coletivas de direito público, utilizadores da JUL, para prossecução das respetivas competências; d) Quaisquer outras entidades cujo interesse seja fundamentado, mediante consentimento escrito dos titulares dos dados”*. De novo se assiste a uma confusão de universos, desta feita entre o que é um direito de acesso, na aceção do artigo 15.º do RGPD, e o que é ter acesso a informação de cariz pessoal por força de um privilégio ou credencial específicos. Com efeito, melhor se perceberia se o legislador optasse por consagrar um artigo ou uma secção do diploma à matéria dos tratamentos de dados pessoais, definindo aí os dados a tratar, as prerrogativas de atuação e confidencialidade, bem como os mecanismos de segurança, colocando num outro artigo ou secção a questão da definição dos acessos, aqui numa lógica mais operacional. Ao misturarem-se os conceitos num mesmo artigo, prejudica-se a coerência da disciplina legal que se pretende consagrar e diminui-se a certeza quanto aos regimes subsidiariamente aplicáveis.

- Confidencialidade e prazos de conservação

Finalmente, e quanto ao mesmo desencontro de conceitos e regimes, duas notas sintéticas. A primeira quanto ao artigo 16.º, que parece reservar as garantias de confidencialidade e integridade da informação àquelas que se classifiquem de comerciais ou sensíveis (cfr. artigo 16.º, n.º 1 do projeto). Ora, esta compartimentação das categorias de informação beneficiárias ou elegíveis para essas garantias, coloca este regime em clara colisão com o RGPD. Lembre-se que os dados pessoais, independentemente da sua especial sensibilidade (tal como vem prevista no artigo 9.º, n.º 1 do RGPD), merecem idênticas preocupações quanto à sua segurança, integridade e confidencialidade, como resulta de uma leitura rápida do artigo 32.º, n.º 1, corpo, do RGPD. E, como bem o insinua o n.º 2 do artigo a que acaba de se aludir, muitas são as vezes em que os riscos decorrem diretamente dos processos e operações de tratamento

e não meramente, como no projeto de decreto-lei se aparenta indicar, da natureza ou categoria dos dados tratados.

A segunda nota respeita ao artigo 19.º, que rege a matéria do arquivo e retenção de dados. A confusão de regimes em matéria de proteção de dados encontraria, logo na epígrafe, suficientes razões para sublinhados críticos, já que o conceito de retenção de dados nos remete para a disciplina da conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas⁷, mas o ponto principal é outro.

Tal como se encontra, o n.º 1 do artigo 19.º do projeto obriga à conservação dos dados tratados na JUL *“durante um período mínimo de 10 anos subsequentes à data em que foram recolhidos ou em que terminar a execução de sanções aplicadas em processos contraordenacionais ou judiciais e desde que a sua eliminação não ponha em risco a consistência de outros dados”*. Por sua vez, o n.º 2 do mesmo artigo exceciona desta obrigação *“os dados pessoais os quais são conservados durante cinco anos após a data do cancelamento da inscrição da JUL e em ficheiro histórico durante 10 anos contados da data da respetiva eliminação na base de dados.”*.

Para a CNPD torna-se extremamente difícil compatibilizar estes dois incisos. Áparentemente, a exceção do n.º 2 só opera quanto a dados recolhidos para efeitos de inscrição na JUL, o que limita fortemente o âmbito de proteção específico dos dados pessoais. Em boa verdade, só se poderá interpretar este artigo como autorizando a conservação de dados pessoais relativos à *“execução de sanções aplicadas em processos contraordenacionais ou judiciais”* durante o tal período mínimo de 10 anos, o qual poderá ser ultrapassado (sem qualquer limite previsto) quando a sua eliminação *“ponha em risco a consistência de outros dados”*. Ora, o princípio da limitação da conservação constante do artigo 5.º, n.º 1, al. f) do RGPD, é, por princípio, contrário à existência de períodos instáveis ou não fechados de conservação da informação, pelo que, apontar um período mínimo de 10 anos, sobretudo quando estão em causa categorias de dados relacionados com condenações penais e contraordenacionais, indicia, desde logo, excessividade⁸, e projeta uma indeterminabilidade incoerente com o regime de proteção de dados vigente. E mais incoerente se torna quando faz depender

⁷ Lei n.º 32/2008, de 17 de julho

⁸ Com o risco de se tornar uma sanção acessória, podendo, até, ultrapassar quaisquer prazos legais eventualmente invocáveis quanto à reincidência ou prescrição de processos.



a eliminação desses dados da inexistência de um risco para a consistência de outros dados.

Em suma, será aconselhável repensar todo este artigo e adequar a sua futura redação à legislação de proteção de dados.

C. Necessidade de Avaliação de Impacto sobre a Proteção de Dados

Como é evidente do objeto do presente projeto de decreto-lei, no futuro teremos uma reforçada centralização de informação proveniente de vários e distintos atores no setor do transporte de pessoas e mercadorias. Esta concentração de informação, também de ordem pessoal, gera maiores riscos quando se ponderam os potenciais perigos que enfrentam as bases de dados pessoais no tempo presente.

Atentas as distintas finalidades permitidas pela plataforma tecnológica que concretiza a JUL, onde se incluem controlos fronteiriços referentes à circulação de pessoas (artigo 9.º, n.º 2, al. c)), informações sobre pessoas transportadas (artigo 9.º, n.º 2, al. k)) e Controlos fronteiriços e de acesso de pessoas a instalações (artigo 9.º, n.º 2, al. l)), facilmente se percebe a amplitude dos tratamentos que aqui estão em causa. Adicionalmente, sendo certa a inscrição de uma quantidade superlativa de dados pessoais respeitantes a um número incomensurável de pessoas, a que se liga um conjunto elevado de potenciais pessoas singulares e coletivas com acesso à JUL, com o risco adicional de se proceder a tratamentos de categorias especiais de dados (dados biométricos e de saúde), a CNPD considera ser seriamente de ponderar a realização de uma Avaliação de Impacto sobre a Proteção de Dados, tal como ela vem configurada no artigo 35.º do RGPD, em momento prévio à operacionalização da JUL.

A este respeito, o n.º 3 do artigo do RGPD citado menciona a obrigatoriedade da realização de avaliações de impacto sempre que exista: *“a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º...”*.

Perante a quantidade e qualidade de dados, a profusão de intervenientes na plataforma e a legítima interpretação que liga a Janela Única Logística a um sistema com as características técnicas ideais para se enquadrar em ambas as alíneas do artigo 35.º, n.º 3 do RGPD⁹, resulta seriamente aconselhável a realização de uma tal avaliação prévia.

III. Conclusões

O presente projeto de decreto-lei representa um passo ambicioso em matéria de convergência de bases de dados, mormente na dimensão da interoperabilidade, notando-se alguns apontamentos de preocupação atenta e consistente com as matérias de proteção de dados pessoais. Ainda assim, a CNPD alerta para a necessidade de:

- a. Clarificar a existência de interconexões da JUL com outras bases de dados, positivando-as no texto do diploma e determinando a sua regulamentação convenientemente, devendo a CNPD ser chamada a pronunciar-se sobre essa regulamentação;
- b. Destacar as questões de proteção de dados pessoais daquelas relativas à gestão da informação que esteja expurgada dos referidos dados, potenciando a clareza das regras concretamente aplicáveis aos diferentes âmbitos que estejam em foco, sobretudo quanto à efetivação dos direitos dos titulares dos dados e ao respeito pelos princípios estruturantes da proteção de dados;
- c. Ponderar a realização de uma avaliação de impacto sobre a proteção de dados prévia à operacionalização da Janela Única Logística, por forma a antever, gerir e, se possível, eliminar os riscos potenciais para os direitos e liberdades das pessoas singulares ligados à concentração de informação de natureza pessoal, bem como aos múltiplos e distintos acessos que passam a ser possibilitados por esta plataforma.

Lisboa, 16 de julho de 2019



Filipa Calvão (Presidente)

⁹ E sem prejuízo de poder incluir-se os tratamentos previstos numa das situações em que é obrigatória a avaliação de impacto sobre a proteção de dados, elencados na lista aprovada pela CNPD e publicada no Regulamento n.º 1/2018, disponível em https://www.cnpd.pt/bin/decisoos/regulamentos/regulamento_1_2018.pdf.