

PARECER/2026/56

I. Objeto

1. A Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República solicitou à Comissão Nacional de Proteção de Dados (CNPD) que se pronunciasse sobre o Projeto de Lei 697/XVII/1 (CH) - *Criminaliza a conduta «usurpação de identidade digital», procedendo à alteração à Lei n.º 109/2009, de 15 de setembro, que consagra a Lei do Cibercrime.*
2. A presente pronúncia é emitida ao abrigo do disposto no artigo 43.º, n.º 1, e no artigo 44.º, n.º 1, alíneas a) e c), da Lei n.º 59/2019, de 8 de agosto, enquanto autoridade nacional de controlo competente no domínio da proteção de dados pessoais tratados para fins de prevenção, investigação, deteção e repressão de infrações penais.

II. Enquadramento geral

3. O Projeto de Lei visa a alteração da Lei n.º 109/2009, de 15 de setembro, nomeadamente a ***alteração do Artigo 2.º, por introdução da alínea i) com o seguinte teor:***

«Para efeitos da presente lei, considera-se:

[...]

i) «*Identidade digital*» o conjunto de elementos de identificação ou representação digitais de uma pessoa singular ou coletiva, incluindo, v.g., o nome, a imagem, a voz, os dados pessoais, o endereço de correio eletrónico, a conta, o perfil, a página, o nome de utilizador, as credenciais de acesso e o identificador digital ou qualquer outro elemento idóneo a permitir a sua identificação, representação ou associação perante terceiros».

4. É ainda **aditado o artigo 7.º-A** à Lei n.º 109/2009, de 15 de setembro, que passa a ter a seguinte redação:

Artigo 7.º-A

Usurpação de identidade digital

1 - Quem, sem consentimento do titular, de modo idóneo e com o intuito de atuar em seu nome, sob a sua identidade e sem a sua autorização, utilizar, assumir, controlar, manter ou disponibilizar conta, perfil, página, endereço eletrónico, nome de utilizador, credenciais de acesso ou qualquer outro elemento de

identidade digital de pessoa singular ou coletiva, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2 - A pena é de prisão até 2 anos ou multa até 240 dias se o agente que, por qualquer meio informático, utilizar elementos de identidade digital de terceiro com intenção de causar prejuízo, lograr obter vantagem ilegítima.

3 - A pena é de prisão de 1 a 5 anos quando:

a) O agente, por qualquer meio informático, utilizar elementos de identidade digital de terceiro com intenção de causar prejuízo, lograr obter vantagem ilegítima;

c) A conduta envolva a divulgação, ameaça de divulgação ou utilização de dados pessoais sensíveis, imagens íntimas, comunicações privadas ou informações relativas à vida familiar, profissional, financeira ou clínica da vítima;

d) A conduta for praticada através de rede criminal organizada ou atinja uma pluralidade de contas, perfis ou identidades digitais;

e) A conduta for praticada por funcionário no exercício das suas funções ou com abuso das mesmas.

4 - A tentativa é punível.

5 - O procedimento criminal depende de queixa, salvo nos casos previstos no n.º 3, ou quando a vítima seja menor ou especialmente vulnerável.

7 - Não é punível a utilização manifestamente satírica, paródica, artística, académica, jornalística ou de crítica política ou social, desde que não seja idónea a induzir terceiros em erro quanto à identidade do titular, nem seja praticada com intenção de causar prejuízo, obter vantagem ilegítima ou facilitar a prática de um crime.

5. Nos termos do artigo 4.º do Projeto de Lei, «A presente lei entra em vigor 30 dias após a sua publicação».

III. Análise

6. Na ótica específica da proteção de dados pessoais, o projeto suscita várias questões de qualidade legislativa, determinabilidade e proporcionalidade, bem como de articulação com o RGPD, com a Lei n.º 59/2019, de 8 de agosto, e com o quadro penal existente. A identidade pessoal e a proteção dos dados pessoais constituem direitos fundamentais constitucionalmente tutelados, designadamente pelos artigos 26.º e 35.º da Constituição. Não se confundem, porém, entre si, nem esgotam os diferentes bens e interesses que podem ser afetados pela utilização da identidade de terceiro

em ambiente digital, designadamente o bom nome e a reputação, a imagem, a palavra, a reserva da intimidade da vida privada ou a segurança e confiança nas relações digitais. A própria exposição de motivos convoca alguns destes diferentes planos de tutela. Assim, a criação de uma incriminação destinada à proteção da identidade em ambiente digital deve permitir identificar com suficiente precisão o bem ou bens jurídicos tutelados e, em particular, a relação entre a tutela da identidade pessoal e a proteção dos dados pessoais.

III.1. Definição excessivamente ampla de «identidade digital»

7. A «*Identidade digital*» aparece definida como «*o conjunto de elementos de identificação ou representação digitais de uma pessoa singular ou coletiva, incluindo, v.g., o nome, a imagem, a voz, os dados pessoais, o endereço de correio eletrónico, a conta, o perfil, a página, o nome de utilizador, as credenciais de acesso e o identificador digital ou qualquer outro elemento idóneo a permitir a sua identificação, representação ou associação perante terceiros*».
8. A expressão «identidade digital» não apresenta, contudo, um significado jurídico unívoco. No direito da União, designadamente no quadro instituído pelo Regulamento (UE) 2024/1183, de 11 de abril de 2024, que alterou o Regulamento (UE) n.º 910/2014¹ no respeitante à criação do Regime Europeu para a Identidade Digital, a identidade digital é tratada essencialmente num contexto funcional de identificação eletrónica, autenticação e partilha de atributos relacionados com a identidade. Por seu turno, o artigo 12.º da Lei n.º 27/2021, de 17 de maio, ao reconhecer o direito à identidade pessoal, ao bom nome, à reputação, à imagem e à palavra em ambiente digital e ao incumbir o Estado de combater a usurpação de identidade, inscreve-se numa perspetiva mais ampla de proteção da pessoa no ambiente digital.
9. Importa, neste contexto, distinguir a identidade pessoal da mera identificação da pessoa. O direito à identidade pessoal, constitucionalmente reconhecido no artigo 26.º, n.º 1, da Constituição, não se esgota nos elementos que permitem proceder à identificação civil do respetivo titular. A identificação constitui antes uma operação funcional de individualização ou reconhecimento da pessoa através de determinados atributos ou identificadores, não se confundindo com a identidade pessoal que através deles se pretende estabelecer ou representar.

¹ Cf., ainda, a Declaração Europeia sobre os Direitos e Princípios Digitais para a Década Digital (2023/C 23/01), que se refere à identidade digital numa perspetiva funcional, associando-a ao acesso a serviços em linha e ao controlo pelo utilizador dos dados que pretende partilhar.

10. A mesma distinção deve ser preservada no ambiente digital. O quadro europeu da identidade digital não permite reconduzir esta, em termos gerais, à simples transposição da identificação civil para meios eletrónicos. Nele coexistem funções distintas de identificação eletrónica, autenticação e utilização ou partilha de atributos relacionados com a identidade. Também fora desse contexto, uma pessoa pode projetar ou representar a sua identidade no ambiente digital através de uma conta ou perfil sem que estes constituam, por esse facto, meios de identificação civil ou de autenticação.
11. Deste modo, devem distinguir-se, designadamente, a identidade da pessoa, os atributos ou dados que permitem identificá-la, os meios através dos quais essa identidade é representada perante terceiros e os mecanismos técnicos destinados a autenticar uma pessoa ou a permitir o acesso a determinado sistema. A inclusão indiferenciada de todas estas realidades num conceito unitário de «identidade digital» é suscetível de tornar incerto o próprio objeto da conduta criminalizada.
12. Esta diversidade de planos torna particularmente importante que uma norma de natureza penal delimite autonomamente o sentido em que utiliza a expressão «identidade digital». Não basta, para esse efeito, agregar num mesmo conceito atributos pessoais, dados pessoais, formas de representação da pessoa, contas e perfis digitais e mecanismos técnicos de autenticação ou controlo de acesso, por se tratar de realidades que desempenham funções distintas e cuja utilização por terceiro não apresenta necessariamente o mesmo significado nem a mesma relevância jurídico-penal.
13. Esta distinção permite ainda identificar com maior precisão o eventual espaço próprio de uma tutela da identidade em ambiente digital. A utilização de um dado pessoal, de um identificador ou de uma credencial de terceiro não equivale, por si só, à assunção da sua identidade. Diferente poderá ser a criação ou utilização de uma representação digital através da qual o agente se apresenta perante terceiros como sendo determinada pessoa, de modo objetivamente idóneo a induzi-los em erro quanto à identidade de quem atua. Neste caso, o núcleo da conduta não reside na natureza dos elementos digitais utilizados, que constituem apenas os meios através dos quais a atuação é realizada, mas na falsa assunção ou representação da identidade de terceiro perante outrem.
14. Se for esta a realidade que a iniciativa legislativa pretende autonomamente tutelar, a construção do tipo em torno da «utilização» de uma enumeração aberta de «elementos de identidade digital» apresenta-se excessivamente ampla. A delimitação poderia antes atender à assunção ou representação da identidade de pessoa determinada perante terceiros e à idoneidade da conduta para os induzir em erro quanto à identidade de quem atua, sem prejuízo da necessária demonstração

da existência de uma lacuna de tutela e da dignidade e necessidade penal das condutas que permaneçam fora dos tipos legais vigentes.

15. A definição proposta para o artigo 2.º, alínea i), inclui *"nome, imagem, voz, dados pessoais, endereço de correio eletrónico, conta, perfil, página, nome de utilizador, credenciais de acesso e identificador digital ou qualquer outro elemento de identidade digital de pessoa singular ou coletiva..."*
16. O conceito de dados pessoais não aparece densificado para este efeito. A referência autónoma a 'dados pessoais' torna-se redundante face aos demais elementos já enunciados e introduz um conceito de extensão potencialmente indeterminada.
17. O perfil como elemento da identidade digital não aparece densificado.
18. A página como elemento de identidade digital é um conceito muito vago, carecendo de densificação.
19. A noção proposta de identidade digital agrega realidades de natureza e função distintas, incluindo atributos diretamente identificativos ou representativos, contas e perfis digitais, bem como elementos técnicos destinados à autenticação ou ao controlo de acesso. A cláusula aberta «qualquer outro elemento idóneo» amplia ainda o âmbito do conceito, podendo suscitar dificuldades de previsibilidade na aplicação de uma norma de natureza penal.
20. Em particular, embora as credenciais de acesso possam constituir dados pessoais quando respeitem a pessoa singular identificada ou identificável, a sua função primordial enquanto mecanismos de autenticação ou de segurança não se confunde necessariamente com a função identificativa ou representativa dos demais elementos enumerados, recomendando-se uma delimitação conceptual mais rigorosa. Sendo uma incriminação, é especialmente relevante o princípio da determinabilidade e da tipicidade penal, exigindo conceitos suficientemente precisos.
21. A definição proposta aproxima-se mais de uma enumeração aberta e heterogénea de elementos digitais do que de um conceito jurídico suficientemente determinado de identidade digital.

III.2. Risco de sobreposição com ilícitos já existentes

22. A CNPD recomenda que se demonstre uma efetiva necessidade de uma circunscrição objetiva de tutela penal.
23. O crime de falsidade informática (artigo 3.º da Lei do Cibercrime), por exemplo, pune o comportamento de quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que

- estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias (n.º 1).
24. Quando as ações descritas no número anterior incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão (n.º 2).
25. Pune ainda quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente (n.º 3).
26. Finalmente, pune também quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados à prática das ações previstas no n.º 2, é punido com pena de prisão de 1 a 5 anos (n.º 4).
27. Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos (n.º 5).
28. O bem jurídico tutelado pelo crime de falsidade informática é «a integridade dos sistemas de informação, que visa impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas de redes e dados, abrangendo o tipo objetivo as ações de introdução, modificação, apagamento ou supressão de dados informáticos ou qualquer outra forma de interferência num tratamento informático de dados, de que resulte a produção de dados ou documentos não genuínos, e exigindo o tipo subjetivo, para além do dolo, a intenção de provocar engano nas relações jurídicas, com o propósito de produzir dados ou documentos não genuínos para que sejam utilizados nas finalidades pretendidas pelo agente, como se fossem genuínos» (cf. Ac. da Relação de Coimbra, de 20-11-2024, Processo nº 716/21.8PCCBR.C1, disponível em www.dgsi.pt).
29. O projeto cria um novo tipo legal de crime sem explicar por que razão a tutela penal atualmente existente é insuficiente, o que suscita dúvidas de necessidade e proporcionalidade da intervenção legislativa.
30. A criação de um novo crime autónomo de «usurpação de identidade digital» pressupõe a demonstração de uma efetiva tutela penal. Todavia, a exposição de motivos não identifica de forma suficientemente precisa quais as situações que permanecem atualmente desprovidas de tutela penal nem explica por que razão os tipos legais vigentes se revelam inadequados para a sua repressão.

31. Uma análise comparativa evidencia que uma parte muito significativa das condutas descritas no proposto artigo 7.º-A já encontra enquadramento em diversos ilícitos penais. Assim, e a título exemplificativo, a jurisprudência tem enquadrado situações semelhantes nos seguintes tipos legais:

– Falsidade informática:

- Criação de perfil falso utilizando dados de terceiro: falsidade informática (artigo 3.º da Lei do Cibercrime), quando exista produção de dados informáticos não genuínos destinados a produzir efeitos juridicamente relevantes – ex.: Ac. Relação de Lisboa, de 18.12.2025, Processo 400/21.2GDALM.L1-3, e Ac. Relação do Porto, de 24-04-2013, CJ, 2013, T2, pág.223, disponíveis em www.dgsi.pt ;
- Utilização do nome ou de parte do nome de outrem no nome de utilizador e/ou endereço eletrónico, por parte de quem criou conta de correio eletrónico: falsidade informática – ex.: Ac. Relação de Évora, de 19-05-2015, Processo 238/12.8PBPTG.E1, disponível em www.dgsi.pt ;
- Indicação a operadora de telecomunicações em conversação telefónica do nome de filho menor, que estava à guarda do pai, como titular do contrato de prestação de serviços de fornecimento de internet e de telefone que estava a realizar: falsidade informática – ex.: Ac. Relação de Coimbra, de 11-10-2023, Processo n.º 1158/19.0T9CTB.C1, disponível em www.dgsi.pt ;
- Manipulação deliberadamente de plataforma informática de empresa, mediante a introdução de dados informáticos falsos, cujo tratamento pelo sistema produziu um resultado não genuíno: falsidade informática – ex.: Ac. da Relação de Guimarães de 11-11-2025, Processo n.º 1536/19.2PIPRT.G1, disponível em www.dgsi.pt ;
- Utilização fraudulenta de documentos eletrónicos: falsidade informática e falsificação documental (cf. Ac. Relação do Porto, de 13-11-2024, Processo n.º 4225/17.1T9MTS.P1, disponível em www.dgsi.pt), consoante os casos;

– Burla informática:

- Utilização da identidade para obtenção de vantagem patrimonial: burla informática (artigo 221.º do Código Penal), frequentemente em concurso com acesso ilegítimo e falsidade informática – ex.: Ac. Relação de Évora, de 14-01-2025, Processo n.º 248/20.1GDSRP.E1, disponível em www.dgsi.pt ;

- Phishing, smishing e vishing: acesso ilegítimo, falsidade informática e burla (clássica ou informática) — ex.: Ac. Relação de Lisboa, de 15-07-2024, Processo n.º 670/20.3JGLSB.L1-3, disponível em www.dgsi.pt (cf. para além do mais, criação de páginas na Internet imitadas ou copiadas das dos sites oficiais de certas empresas, instituições, organizações ou outra entidades ou pessoas coletivas legítimas como sejam os Bancos, fazendo-o com a finalidade de obter informações sensíveis de natureza bancária, financeira ou outra que seja pessoal ou deva ser considerada confidencial através da indução da vítima em erro);
- Burla realizada mediante a introdução de dados incorretos/falsos no sistema informático da Segurança Social: existe concurso efetivo de burla e falsidade informática — ex.: Ac. Relação do Porto, de 30-04-2008, Processo n.º 0745386, disponível em www.dgsi.pt.
- Crimes da Lei do Cibercrime:
 - Apropriação de credenciais de acesso: acesso ilegítimo, interceção ilegítima, dispositivos ilícitos e demais crimes previstos na Lei do Cibercrime;
- Crimes contra a reserva da vida privada:
 - Divulgação de imagens íntimas ou dados relativos à vida privada: devassa da vida privada, gravações e fotografias ilícitas, divulgação não consentida de conteúdos íntimos e demais ilícitos aplicáveis — ex.: Ac. Relação de Coimbra, de 12.03.2025, Processo 69/22.7JAGRD.C1, disponível em www.dgsi.pt ;
- Crimes previstos na Lei n.º 58/2019:
 - Tratamento ilícito de dados pessoais: crimes previstos na Lei n.º 58/2019, de 08.08, quando estejam preenchidos os respetivos pressupostos;

32. A casuística jurisprudencial exposta evidencia que uma parte significativa das condutas que o projeto pretende autonomizar já encontra enquadramento em tipos legais vigentes, designadamente nos crimes de falsidade informática, burla informática, acesso ilegítimo, devassa da vida privada e tratamento ilícito de dados pessoais, o que suscita dúvidas quanto à necessidade da criação de um novo tipo legal autónomo.

33. Não se exclui que possa conceber-se situações de utilização da identidade digital de terceiro que não preencham os elementos típicos dos ilícitos atualmente existentes. A eventual existência dessa zona residual não demonstra, porém, por si só, a necessidade de uma nova incriminação, nem dispensa a identificação das condutas concretamente carecidas de tutela penal autónoma.

34. Caberia precisamente à iniciativa legislativa identificar essa eventual zona residual, determinar o bem jurídico cuja proteção penal adicional se mostra necessária e demonstrar que tais condutas apresentam dignidade e necessidade penal suficientes para justificar uma nova incriminação. O Projeto não procede a essa delimitação.
35. Ao invés, o próprio artigo 7.º-A reproduz parcialmente elementos típicos já constantes de outros crimes. A intenção de causar prejuízo ou de obter vantagem ilegítima prevista nos n.ºs 2 e 3 aproxima-se da estrutura típica da burla informática, enquanto a utilização de elementos de identidade digital de terceiro através de meios informáticos pode, em numerosas situações, preencher simultaneamente o crime de falsidade informática.
36. Deste modo, o projeto suscita dúvidas quanto à delimitação das relações entre os diversos tipos legais. Não resulta claro se o legislador pretende estabelecer uma relação de especialidade, subsidiariedade ou concurso efetivo entre a nova incriminação e os crimes já existentes, circunstância suscetível de gerar dificuldades interpretativas e problemas de aplicação prática.
37. A jurisprudência existente relativamente ao crime de falsidade informática demonstra, aliás, que os tribunais têm vindo a integrar naquele tipo legal, por vezes em concurso efetivo com outros ilícitos, situações de criação de perfis ou contas falsas e de utilização de elementos identificativos de terceiros quando delas resulte a produção de dados ou documentos informáticos não genuínos, verificados os demais elementos do tipo, designadamente a intenção de provocar engano nas relações jurídicas e a finalidade de utilização daqueles dados ou documentos para finalidades juridicamente relevantes.
38. Nestas circunstâncias, seria desejável que a iniciativa legislativa explicitasse quais as condutas concretas que pretende autonomizar, distinguindo aquelas que já encontram resposta nos tipos legais vigentes das que eventualmente permaneçam fora do respetivo âmbito, e demonstrasse, quanto a estas últimas, a existência de uma necessidade de tutela penal autónoma, à luz dos princípios da necessidade, proporcionalidade e subsidiariedade da intervenção penal.
39. A criação de tipos penais parcialmente coincidentes pode comprometer a previsibilidade do sistema sancionatório e gerar dificuldades na delimitação do concurso de infrações, aumentando a incerteza interpretativa sem correspondente acréscimo da tutela material dos direitos fundamentais. Sempre que o ordenamento jurídico já disponha de instrumentos aptos a reprimir as condutas em causa, a introdução de novas incriminações deve ser especialmente fundamentada quanto à respetiva necessidade e valor acrescentado.
40. A criação de um novo tipo legal autónomo deve assentar na identificação suficientemente precisa de uma lacuna de tutela e na demonstração de que os mecanismos jurídicos atualmente vigentes

não asseguram, de forma adequada, a proteção dos direitos fundamentais dos titulares dos dados.

41. Esta exigência assume particular intensidade em matéria penal, atenta a natureza de *ultima ratio* da intervenção criminal, não bastando a relevância social ou a frequência de determinado fenómeno para justificar, por si só, a criação de uma nova incriminação quando as condutas materialmente lesivas já encontrem resposta no ordenamento vigente.

III.3. Inconsistências de redação e articulação interna do tipo legal

42. Consta do artigo 7.º-A, 2, do Projeto de Lei que «A pena é de prisão até 2 anos ou multa até 240 dias se o agente que, por qualquer meio informático, utilizar elementos de identidade digital de terceiro com intenção de causar prejuízo, lograr obter vantagem ilegítima».
43. E do n.º 3 que «A pena é de prisão de 1 a 5 anos quando: a) O agente, por qualquer meio informático, utilizar elementos de identidade digital de terceiro com intenção de causar prejuízo, lograr obter vantagem ilegítima;».
44. A redação do n.º 2 tem a palavra “*que*” a mais.
45. Por outro lado, verifica-se uma sobreposição entre o n.º 2 e a alínea a) do n.º 3 do artigo 7.º-A, sem que se compreenda qual o elemento diferenciador justificativo do distinto enquadramento sancionatório.
46. Assinala-se ainda que a numeração proposta apresenta descontinuidades, inexistindo a alínea b) do n.º 3 e o n.º 6 do artigo 7.º-A, aspetos que deverão ser corrigidos.

III.4. Utilização da expressão «dados pessoais sensíveis»

47. O artigo 7.º-A, n.º 3, alínea c), refere “dados pessoais sensíveis”.
48. A expressão «dados pessoais sensíveis» não corresponde à terminologia adotada pelo RGPD, que utiliza o conceito de «categorias especiais de dados pessoais» no seu artigo 9.º. Acresce que a enumeração subsequente da própria alínea c) abrange informações que não integram necessariamente aquelas categorias especiais, pelo que não é possível determinar com segurança o sentido e alcance autónomos que o Projeto pretende atribuir àquela expressão.
49. Tratando-se de elemento de um tipo penal agravado, esta indeterminação assume especial relevância, recomendando-se a sua substituição por categorias normativamente delimitadas ou a definição expressa dos dados abrangidos.

III.5. Proporcionalidade da tutela penal

50. A incriminação prevista no n.º 1 do artigo 7.º-A pune a mera utilização ou assunção de elementos de identidade digital: "utilizar, assumir, controlar, manter ou disponibilizar".
51. "*Manter elementos de identidade digital de outrem*" carece de densificação no contexto pretendido.

III.6. Credenciais de acesso

52. Como já dissemos, a inclusão de "credenciais de acesso" na definição de identidade digital merece atenção.
53. As credenciais são simultaneamente:
- elemento de identificação;
 - mecanismo de segurança.
54. A mera posse ou obtenção de credenciais já encontra enquadramento em outros tipos legais da Lei do Cibercrime.

III.7. Pessoas coletivas

55. A incriminação protege igualmente a identidade digital de "pessoa singular ou coletiva".
56. Nos termos do artigo 3.º, n.º 1, al.ª c), da Lei n.º 59/2019, de 08.08 (cf. estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, transpondo para a ordem jurídica interna a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016), «Dados pessoais», são «informações relativas a uma pessoa singular identificada ou identificável («titular dos dados»)».
57. A CNPD salienta que a proteção de dados pessoais ao abrigo da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e ainda do artigo 4.º(1) do Regulamento (UE) n.º 679/2016, de 27 de Abril (RGPD) não se aplica às pessoas coletivas, pelo que a fundamentação do diploma não deveria assentar exclusivamente em argumentos de proteção de dados quando uma parte significativa do âmbito proposto ultrapassa esse domínio.

58. A identidade digital de pessoas coletivas pode justificar tutela jurídica própria, mas essa tutela não se confunde com a proteção de dados pessoais nem integra o âmbito material de competência da CNPD.

III.8. Estudo de impacto sobre a proteção de dados pessoais

59. Assinala-se, por último, que o pedido de parecer não foi acompanhado do estudo de impacto sobre a proteção de dados pessoais previsto no artigo 18.º, n.º 4, da Lei n.º 43/2004, de 18 de agosto, nos termos do qual os pedidos de parecer relativos a disposições legais e regulamentares em preparação devem ser remetidos à CNPD instruídos com o respetivo estudo de impacto. A ausência daquele elemento não permite à CNPD dispor da avaliação que o legislador considerou necessária para instruir a consulta, designadamente quanto aos impactos concretos da iniciativa no domínio da proteção de dados pessoais.

IV. Conclusão

60. A CNPD recomenda uma revisão da redação proposta, por forma a assegurar maior precisão concetual e conformidade com os princípios da determinabilidade penal, bem como a adequada articulação com o RGPD, a Lei n.º 59/2019, de 08.08 e os ilícitos já previstos na Lei do Cibercrime e demais legislação penal.

61. Em particular, sugere-se:

- a) A delimitação dos elementos abrangidos pelo conceito de «identidade digital» e, em particular, do alcance da referência genérica a «dados pessoais»;
- b) A densificação do próprio conceito de «identidade digital» à luz das exigências de determinabilidade da lei penal;
- c) A substituição ou delimitação da expressão «dados pessoais sensíveis»;
- d) A identificação suficientemente precisa do bem jurídico cuja tutela se pretende assegurar através da nova incriminação e da sua relação com a proteção dos dados pessoais;
- e) A identificação das concretas situações eventualmente não abrangidas pelos tipos legais vigentes e a demonstração, quanto a estas, da necessidade, proporcionalidade e subsidiariedade de uma tutela penal autónoma;

- f) A clarificação da articulação do novo crime com os tipos legais já vigentes, designadamente quanto às relações de especialidade, subsidiariedade e concurso.

Aprovado na reunião de 1 de setembro de 2026.

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2026.09.01 20:11:39+01'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

