CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2023/12

I. Pedido

1. A Direção-Geral da Política de Justiça submeteu à Comissão Nacional de Proteção de Dados (doravante CNPD), para parecer, a Proposta de Regulamento do Parlamento Europeu e do Conselho COM (2022)209 final, que estabelece regras para prevenir e combater o abuso sexual de crianças[1] (doravante Proposta).

2. A CNPD emite parecer no âmbito das suas atribuições e competências enquanto autoridade nacional de controlo dos tratamentos de dados pessoais, conferidas 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, de 27 de abril – Regulamento Geral sobre a Proteção de Dados (RGPD), em conjugação com o disposto no artigo 3.º e na alínea *a)* do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto, e com o disposto no n.º 2 do artigo 30.º e na alínea *c)* do n.º 1 do artigo 44.º, ambos da Lei n.º 59/2019, de 8 de agosto .

II. Análise

i. Descrição do regime proposto

3. A Proposta de Regulamento submetida à análise da CNPD visa dar cumprimento aos compromissos assumidos pela União Europeia no âmbito da prevenção e repressão dos abusos sexuais em linha[2].

4. E na sequência do Regulamento (UE) 2021/1232, de 14 de julho de 2021, que estabelece uma derrogação temporária de determinadas disposições da Diretiva 2022/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas que protege a confidencialidade das comunicações e dos dados de tráfego[3] (Diretiva da Privacidade nas Comunicações Eletrónicas), no que respeita

---

[1] Proposta de Regulamento acessível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209.

[2] Nomeadamente, a Estratégia da UE para uma luta mais eficaz contra o abuso sexual de crianças, COM (2020) 607, de 24 de julho de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0607&from=ES e Proposta de Declaração Europeia sobre os direitos e princípios digitais para a década digital, COM (2022)28 de 26 de janeiro https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration; a Estratégia da EU para uma luta mais eficaz contra o abuso sexual de crianças, COM (2020) 607, de 24 de julho de 2020, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0607&from=ES e a Estratégia Global da UE sobre os Direitos da Criança, da Comissão Europeia de 24 de julho de 2021, na qual esta instituição insta as empresas a prosseguirem ações adequadas a detetar, denunciar e remover das suas plataformas e serviços os conteúdos ilegais, designadamente material relativo a abusos sexuais de crianças, acessível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:4540916

[3] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO

à utilização de tecnologias por prestadores de serviços de comunicações interpessoais independentes do número para o tratamento de dados pessoais e outros para efeitos de combate ao abuso sexual de crianças em linha.

5. Aquele Regulamento provisório não exige que os prestadores de serviços detetem ou eliminem os materiais, mas permite-lhes fazê-lo voluntariamente, estabelecendo para tal uma derrogação temporária das disposições previstas no n.º 1 do artigo 5.º e n.º 1 do artigo 6.º da Diretiva da Privacidade nas Comunicações Eletrónicas, que protegem a confidencialidade das comunicações e dos dados de tráfego, quando estejam em causa ações voluntárias dos prestadores de serviços, na medida do que entendam necessário para a deteção e eliminação de material relativo a abusos sexuais de crianças. Ainda, estabelece salvaguardas que os prestadores de serviços devem respeitar quanto ao tratamento de dados pessoais no âmbito daquele Regulamento.

6. A respeito da relação entre a presente Proposta e a Diretiva da Privacidade nas Comunicações Eletrónicas, deixam-se, desde já, duas notas.

7. A primeira, por consideração do regime agora proposto, prende-se com a conveniência em explicitar, no texto do novo Regulamento, a revogação do Regulamento Provisório na parte em que se admite a intervenção voluntária dos operadores de serviços naquela matéria, e, por conseguinte, a plena vigência da Diretiva da Privacidade nas Comunicações Eletrónicas sem as derrogações introduzidas por aquele Regulamento.

8. A segunda, para recomendar a revisão da previsão de aplicação, por analogia, do n.º 1 do artigo 15.º da Diretiva da Privacidade nas Comunicações Eletrónicas. Na verdade, prevê-se que seja aplicada analogicamente uma norma que permite que os Estados-Membros adotem medidas legislativas restritivas do âmbito de determinados direitos e obrigações sempre que estas restrições constituam uma medida necessária, adequada e proporcional, numa sociedade democrática, para salvaguardar a segurança nacional, a defesa, a segurança pública, a prevenção, investigação, deteção e repressão das infrações penais ou a utilização não autorizada de sistemas de comunicações eletrónicas. Ora, essa previsão de aplicação analógica daquela norma contraria a jurisprudência do Tribunal de Justiça da União Europeia (doravante, TJUE) – acórdão *Tele2 Sverige e Watson*[4]–, que decidiu que o n.º 1 do artigo 15.º da Diretiva, na medida em que permite uma restrição da confidencialidade das comunicações, constitui uma disposição excecional e, por conseguinte, insuscetível de aplicação analógica.

2002, L 201, p. 37), alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO 2009, L 337).

[4] Acórdão de 21 de dezembro de 2016, *Tele2 Sverige e Watson e o.*, C-203/15 e C-698/15, n.º 120.

9. Prosseguindo na análise da Proposta, a mesma visa uniformizar as regras da União em matéria de deteção, denúncia e supressão de material referente a abusos sexuais de crianças na Internet, de forma a limitar a circulação de material que represente os abusos, a complementar o Regulamento de Serviços Digitais e a evitar a fragmentação jurídica e os obstáculos ao mercado único digital.

10. Simultaneamente, visa "proporcionar segurança jurídica aos prestadores de serviços quanto às suas responsabilidades de avaliação e atenuação de riscos e [...] deteção, denúncia e supressão de tais abusos", de uma forma consentânea com a Carta dos Direitos Fundamentais da União Europeia (CDFUE) e em consonância com o quadro legal previsto no Regulamento dos Serviços Digitais, que constitui o seu referente.

11. De forma a concretizar aquelas finalidades, prevê-se a criação de uma nova agência descentralizada da União Europeia com a finalidade de prevenir e combater o abuso sexual de crianças e de facilitar a aplicação do Regulamento em causa, designada Centro da União sobre o Abuso Sexual de Crianças (Centro da UE), cabendo aos Estados-Membros designar uma ou mais autoridades competentes responsáveis pela aplicação e execução coerciva do Regulamento (autoridades competentes) – cf. artigo 25.º.

12. Ainda, impõem-se determinadas obrigações a todos os prestadores de serviços de armazenagem em servidor ou de comunicações interpessoais (prestadores de serviços) que operem no espaço europeu, independentemente da tecnologia utilizada nos contactos, em especial quanto à deteção e eliminação de conteúdos e quanto ao bloqueio de acesso em matéria de abusos sexuais, regulando-se o processo de avaliação das circunstâncias que fundamentam a emissão de uma ordem de deteção e eliminação de conteúdos ou de bloqueio e acesso e a emissão das mesmas. Estabelece-se, ainda, que os prestadores de serviços criem um ponto de contacto único para o estabelecimento de comunicação direta com as autoridades de coordenação e outras autoridades dos Estados-Membros, a Comissão e o Centro da UE, para efeitos de execução do Regulamento (n.º 1 do artigo 23.º). Quanto a este aspeto, por uma questão de certeza na aplicação normativa, conviria que fosse concretizado o conceito de "prestador de serviços relevante", de forma a clarificar sobre quem recaem tais obrigações.

13. E impõe-se a todos os prestadores de serviços que operem no espaço europeu a obrigação de procederem a uma avaliação do risco de utilização abusiva dos seus serviços para a difusão de material relativo a abusos sexuais conhecido ou novo, bem como a obrigação de adotarem medidas de mitigação desses riscos, independentemente da tecnologia utilizada nos contactos, e para todos os serviços que ofereçam (artigo 3.º).

14. A pedido dos prestadores de serviços, o Centro da UE pode realizar uma análise de amostras de dados representativos e anonimizados, para identificação de potenciais riscos.

15. Pretende-se ainda que os prestadores de serviços detetem, tanto material "já conhecido" relativo a abusos sexuais, como material "novo", sendo este definido como "material potencialmente referente a abusos sexuais de crianças detetado, utilizando indicadores constantes da base de dados de indicadores definidos no artigo 44.º da Proposta (alínea n) do artigo 2.º) ou seja, "material suscetível de constituir material referente a abusos sexuais de crianças, mas ainda não confirmado por nenhuma autoridade como tal" e, ainda, que detetem situações de aliciamento das crianças, tanto conhecido como novo, de forma de prevenir os abusos.

16. A Proposta prevê, ainda, que possa ser emitida uma ordem de supressão, para que o operador elimine ou desative o acesso a um ou mais elementos específicos de material que tenha sido identificado como material de abusos sexuais de crianças (artigo 14.º), bem como uma ordem de bloqueio exigindo que um prestador de serviços de acesso à Internet tome medidas razoáveis para impedir o acesso dos utilizadores a material referente a abusos sexuais de crianças conhecido(artigo 16.º).

17. Estas ordens são solicitadas pela autoridade de coordenação à autoridade judicial competente ou pela autoridade administrativa independente do Estado-Membro que designou a autoridade de coordenação, após um processo prévio de avaliação pela autoridade de coordenação ou por um tribunal, de forma a garantir que se verificam os requisitos legalmente previstos.

18. Também sobre os operadores de lojas de aplicações informáticas recaem obrigações de informação, neste caso, obrigação de disponibilizarem ao público informações que descrevem o processo e os critérios para avaliar o risco, bem como as medidas técnicas e operacionais adotadas pelos prestadores de serviço e os sistemas de moderação de conteúdos (n.º 2 do artigo 6.º).

ii. Apreciação geral

19. Sem prejuízo de observações mais incisivas que se apresentam infra, destaca-se que o regime proposto, com a intenção de proteger as crianças no ambiente em linha, constitui uma ingerência grave nos direitos e liberdades fundamentais dos utilizadores de serviços de comunicações eletrónicas, em especial, os das próprias crianças que aqui se pretende proteger. A restrição aos direitos fundamentais à inviolabilidade dos conteúdos das comunicações, ao respeito pela vida privada e, consequentemente, à liberdade de expressão e à autodeterminação informativa (ou à proteção dos dados pessoais) é, pois, evidente.

20. O caráter geral, sistemático e automatizado da análise dos conteúdos das comunicações eletrónicas e do tratamento de dados pessoais nesse âmbito impacta com tal intensidade nos direitos dos utilizadores destes serviços, em especial sobre as crianças, que, com a intenção de as proteger quanto a abusos sexuais no ambiente em linha, elimina-se qualquer espaço de privacidade seu nesse mesmo ambiente, condicionando a sua

liberdade de expressão, mas sobretudo o desenvolvimento da sua personalidade, quando é certo que hoje uma parte significativa da sua interação com outras crianças se desenvolve nesse contexto.

21. Aplica-se aqui, com propriedade, a jurisprudência do TJUE proferida a propósito de tratamentos de dados pessoais no contexto das comunicações eletrónicas, máxime o acórdão *Digital Rights Ireland*, de 8 de abril de 2014 (procs. C-293/12 e C-594/12), onde o Tribunal afirma que «[*a] necessidade de dispor de tais garantias é ainda mais importante quando [...] os dados pessoais são sujeitos a tratamento automático e existe um risco significativo de acesso ilícito aos mesmos* [...]» (ponto 55), especialmente se, como sucede no presente caso, «[...] *abrange de maneira geral todas as pessoas, todos os meios de comunicação eletrónica*[...]» (ponto 57). É que, paralelamente ao apurado pelo Tribunal naquele acórdão (ponto 58), também esta Proposta «[...] *abrange, em geral, todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que, no entanto, [...] se encontrem, ainda que indiretamente, numa situação suscetível de dar lugar a ações penais. Assim, aplica-se mesmo a pessoas em relação às quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com infrações graves. Além disso, não prevê nenhuma exceção, pelo que é aplicável mesmo a pessoas cujas comunicações estão sujeitas ao segredo profissional, segundo as regras do direito nacional.*»

22. Ora, estando em causa a ingerência nos direitos, inclusive das crianças, consagrados nos artigos 7.º, 8.º e 11.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE) e no artigo 7.º e 10.º da Convenção Europeia dos Direitos Humanos – direitos igualmente consagrados nos artigos 26.º, 34.º, 35.º e 37.º da Constituição da República Portuguesa (CRP) – imperioso será que o articulado do regime assegure que a ingerência se limita ao mínimo indispensável para a prevenção dos crimes de abuso sexual contra crianças e que, ainda assim, não se revele excessivo – em conformidade com o princípio da proporcionalidade consagrado no artigo 52.º da CDFUE e no n.º 2 do artigo 18.º da CRP. Razão por que a respetiva regulação legal tem de ser clara e precisa na determinação do alcance e aplicação das medidas por ela previstas, devendo, «[...] *em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida que preveja o tratamento desses dados, garantindo, assim, que a ingerência se limita ao estritamente necessário*» – cf. ponto 117 do acórdão do TJUE de 21 de junho de 2022, proferido no processo C-817/19, *Ligue des droits humains* c. *Conseil des ministres* – prevendo para os titulares dos dados «[...] *garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos* [...]» (cf. ponto 54 do acórdão *Digital Rights Ireland*).

23. Todavia, a Proposta faz prevalecer o objetivo de prevenção de crimes de natureza sexual contras as crianças no ambiente em linha sem acompanhar o regime de garantias adequadas à salvaguarda da privacidade das

próprias crianças e sem prever orientações precisas e claras quanto aos termos do tratamento de dados pessoais, em clara contradição com as exigências de previsibilidade e segurança jurídicas na restrição de direitos, liberdades e garantias.

24. A Proposta, na exposição de motivos, assume como prioridade "a necessidade de garantir os direitos fundamentais das crianças aos cuidados e à proteção do seu bem-estar, saúde mental e interesse superior» e o «interesse público geral em adotar meios eficazes de prevenção, investigação e exercício da ação penal relativamente ao grave crime de abuso sexual de crianças" e reconhece que "as medidas previstas na proposta afetam, em primeiro lugar, o exercício dos direitos fundamentais dos utilizadores dos serviços", em especial o respeito pela vida privada e familiar, incluindo a confidencialidade das comunicações, concluindo que "nenhum destes direitos fundamentais é absoluto, pelo que devem ser considerados à luz da função que desempenham na sociedade".

25. Ora, a possibilidade de constrangimento de direitos e liberdades fundamentais não se mede pela *função que desempenham na sociedade*, sob pena de se permitir, em nome do interesse da sociedade, uma restrição insuportável de alguns dos direitos fundamentais que, pela sua própria natureza, conformam a dignidade da pessoa humana. Tal significaria funcionalizar os direitos fundamentais a um qualquer desígnio que os Estados pretendessem prosseguir, esquecendo que, nas sociedades democráticas, a dignidade do ser humano não é funcionalizável e que, a estabelecer-se alguma funcionalização, ela há de ter o sentido inverso: do Estado de Direito Democrático em relação ao princípio da dignidade da pessoa humana.

26. Com isto não se pretende negar a necessidade, e a premência, de proteger as crianças e jovens em qualquer contexto e que a utilização da Internet coloca as crianças e jovens face a perigos acrescidos, nomeadamente expondo-os mais facilmente a práticas abusivas de terceiros.

27. A CNPD está ciente de que o combate aos abusos sexuais tem de constituir preocupação de todas as comunidades e dos Estados, partilhando a preocupação da União Europeia de proteção da criança, tutela dos seus direitos, na consideração do seu superior interesse, assumida, nomeadamente, através da Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, da Estratégia da UE para uma luta mais eficaz contra o abuso sexual das crianças, COM (2020)607, de 24 de julho de 2020 e da Estratégia Global da UE sobre os Direitos da Criança. E reconhece a necessidade de dotar o sistema de instituições e meios eficazes para essa finalidade,

28. Mas, num Estado de Direito Democrático, não se pode descurar a harmonização daqueles relevantíssimos interesses e direitos fundamentais com o respeito pelos demais direitos e liberdades fundamentais,

nomeadamente dos direitos ao respeito pela vida privada e familiar, ao sigilo das comunicações, à liberdade de expressão, bem como à autodeterminação informativa e à proteção de dados pessoais dos cidadãos e especialmente das crianças e jovens, sem esquecer o princípio da presunção da inocência. Como, aliás, a CDFUE e a CRP exigem.

29. Impõe-se, pois, garantir a compatibilização entre os direitos das potenciais vítimas e os direitos de todos os utilizadores da Internet, incluindo as crianças.

30. Todavia, o regime estabelecido na Proposta prevê uma potencial intrusão na esfera jurídica da generalidade dos cidadãos, desde logo por estabelecer a obrigação de detetar abusos na Internet tanto nos serviços destinados ao público, como nos serviços privados, incluindo comunicações interpessoais, reforçada pela possibilidade de supressão de material dos utilizadores, a qual pode ser injustificada e, por essa via, contender com a liberdade de expressão e de informação.

31. Apesar da reiterada afirmação, na Proposta, de que se pretende alcançar o equilíbrio entre a proteção das crianças e os direitos dos demais envolvidos, certo é que tal equilíbrio não parece ser alcançado.

32. É o que em seguida se procurar demonstrar, considerando-se os aspetos de regime especialmente pertinentes na perspetiva do regime jurídico de proteção de dados.

iii. Avaliação, pelos prestadores de serviços, do risco de abusos

33. Começa-se por considerar o tratamento de dados pessoais a realizar pelos prestadores de serviços que operem no espaço europeu. Como se referiu, sobre eles impende a obrigação de proceder a uma avaliação do risco de utilização abusiva dos seus serviços para a difusão de material relativo a abusos sexuais conhecido ou novo, bem como a obrigação de adotar medidas de mitigação desses riscos, independentemente da tecnologia utilizada nos contactos, e para todos os serviços que ofereçam (artigo 3.º da Proposta).

34. Estabelece-se, entre outros aspetos, que a avaliação de risco deve considerar os casos anteriormente detetados, a existência de funcionalidades que permitam a verificação da idade ou de ferramentas que permitam, de forma ágil, assinalar os abusos sexuais e dá-los a conhecer aos prestadores de serviços, bem como o risco de aliciamento das crianças, tendo em consideração, neste caso, a possibilidade de o serviço ser utilizado por crianças e, sendo-o, quais os grupos etários das crianças e o risco em relação a cada um desse grupos.

35. Os critérios a considerar para a determinação do risco vêm indicados no n.º 2 do artigo 3.º.

36. No entanto, os critérios estão elencados em termos demasiado genéricos, entregando os prestadores de serviços a um amplo espaço de discricionariedade, sem efetiva orientação quanto a um tratamento de dados

que se revela altamente intrusivo da privacidade e das liberdades individuais dos utilizadores, inclusive das crianças. Senão, vejamos: é referido que na avaliação do risco deve atender-se "[à] forma como os utilizadores usam o serviço", sem que, todavia, seja explicitada qualquer situação que permita compreender com efetividade a concretização deste critério e a existência de fatores que criem ou potenciem o risco de aliciamento de crianças (como seja a possibilidade de contacto direto entre utilizadores e, nomeadamente, de adultos em relação a crianças, e a possibilidade de partilha de vídeos, nomeadamente através de comunicações privadas).

37. Insiste-se: a garantia de que a ingerência nos direitos fundamentais respeita o princípio da proporcionalidade pressupõe, no mínimo, que se indiquem as circunstâncias e as condições em que se pode adotar a medida restritiva, no caso, o tratamento dos dados pessoais no âmbito de comunicações eletrónicas.

38. Nestes termos, a CNPD recomenda a densificação, nesta sede, dos fatores ou critérios relevantes para efeito de avaliação do risco.

39. Demais, vem estabelecido na Proposta o momento em que deve ser efetuada aquela avaliação (no terceiro mês após a aplicação do Regulamento ou do início da prestação de serviços na União) e o dever de proceder a uma atualização periódica, como regra a cada três anos, bem como nos casos em que o serviço seja objeto de uma ordem de deteção ou em que a autoridade de coordenação do local do estabelecimento o exija, por existirem indícios de uma possível alteração substancial do risco de utilização abusiva do serviço (n.º 4 do artigo 3.º).

40. Atendendo ao ritmo da evolução tecnológica, a manter-se a intenção de impor esta obrigação, então para que ela seja ainda adequada a alcançar a finalidade visada, a CNPD recomenda que se pondere estreitar a regularidade dessa reavaliação, fixando uma obrigação de avaliação de riscos mais frequente.

41. Acresce que, embora os prestadores de serviços consigam aceder ao URL do conteúdo quando este se encontre desencriptado, o mesmo não ocorre quando o conteúdo circule via HTTPS, que impossibilitará o acesso, pelos prestadores de serviços, ao URL concreto. Ora, na medida em que, como parece decorrer da Proposta, se imponha a obrigação de fazer estes rastreios dos conteúdos das comunicações, tal implica a desencriptação das comunicações pelos prestadores de serviços. Isto quando a cifragem das comunicações ponta a ponta é e tem sido defendida como meio fundamental para a garantir a confidencialidade das comunicações, a liberdade de expressão e o respeito pela vida privada.

42. Por outro lado, tendo em consideração que o alvo da deteção de aliciamento são as conversas mantidas com crianças, há que ter especial cuidado para que o propósito da proteção de crianças contra eventual aliciamento e abusos não redunde, na prática, na intrusão desnecessária na sua privacidade, com consequências ao nível da utilização destes meios por pessoas daquela faixa etária.

43. Com este impacto, tendo especialmente em conta o caráter geral, sistemático e automatizado da análise dos conteúdos das comunicações, a CNPD entende que o regime previsto na Proposta é suscetível de afetar o conteúdo essencial daqueles direitos fundamentais,. Insiste-se que os titulares destes direitos são também as crianças, cuja proteção aqui se tem em vista. Só que, com a intenção de proteção das crianças quanto a abusos sexuais em linha, elimina-se qualquer espaço de privacidade destas nesse mesmo ambiente, quando é certo que hoje uma parte significativa da sua interação com outras crianças se desenvolve nesse contexto.

44. Afigura-se, assim, imprescindível a reponderação do regime aqui proposto, à luz do princípio da proporcionalidade, consagrado no artigo 52.º da CDFUE e no artigo 18.º da CRP, devendo ser especialmente ponderado o universo de pessoas potencialmente afetadas com a interferência nas comunicações (e garantindo a delimitação de tal universo ao efetivamente necessário), a extensão e duração da medida, bem como o grau de intrusividade, considerando, em especial, a tipologia de dados afetados, nomeadamente a possibilidade de afetação de categorias especiais de dados. Imprescindível é ainda garantir que os prestadores de serviços não venham a reduzir o grau de proteção da privacidade no contexto dos serviços a prestar, nomeadamente, prescindindo da cifragem das comunicações.

45. Há ainda que garantir que a tecnologia utilizada, seja para a identificação de material relativo a abusos sexuais, novo ou conhecido, seja de aliciamento, reduz a um mínimo suportável a margem de erro e potencie a identificação de falsos positivos, tendo em consideração as repercussões negativas de tal identificação na esfera jurídico-fundamental dos utilizadores e titulares de dados.

iv. Em especial, a verificação da idade dos utilizadores

46. A deteção de aliciamento apenas pode ocorrer quando estejam em causa conversas em que um dos interlocutores seja uma criança. O considerando 16 da Proposta prevê que os prestadores de serviços de armazenagem em servidor, bem como os prestadores de serviços de comunicações interpessoais acessíveis ao público, adotem as medidas razoáveis para atenuar os riscos de utilização abusiva dos serviços, nomeadamente, através de ferramentas de verificação de idade e de controlo parental.

47. Uma vez que, nos termos da Proposta, apenas é possível emitir uma ordem de deteção quando esteja em causa uma conversa mantida entre um adulto e uma criança, não se vê como pode o processo decorrer sem que seja determinada essa idade. E, no entanto, a Proposta é omissa quanto ao meio para aquela determinação.

48. Tal constitui, na verdade, tarefa de difícil prossecução, tendo em consideração, por um lado, a constante evolução das soluções tecnológicas e, por outro, o facto de a utilização de mecanismos de identificação com mais precisão poder constituir uma intrusão excessiva e constituir obstáculo à fluidez das comunicações e, por

essa via, um fator que dificulta a comunicação e a utilização livre dos meios de comunicação digitais. E isto, mesmo que, para maior fidedignidade, a identificação se fizesse por recurso a um meio digital oficial, o que se mostra improvável uma vez que estes meios não estão disponíveis em todo o espaço da União Europeia. No entanto, esta dificuldade pode redundar, na prática, num acesso desproporcionado às comunicações.

49. A CNPD recomenda, por isso, que se regule na Proposta, com um mínimo de orientação normativa, o tratamento de dados a realizar para a finalidade de verificação da idade dos utilizadores.

v. O tratamento de dados pessoais pelas autoridades de coordenação

50. Às autoridades de coordenação cabe o poder de solicitar à autoridade judiciária ou à autoridade administrativa independente que emitam as ordens de deteção dirigidas aos prestadores de serviços para que estes tomem medidas para deteção dos abusos, quando tenham provas de existência de perigos significativos – conceito que vem especificado consoante se trate de ordem de deteção de material conhecido ou novo, ou uma ordem de deteção de aliciamento de crianças – ou que suprimam material referente a abusos ou, ainda, que os obriguem a desativar o acesso a determinado serviço em todos os Estados-Membros (artigos 7.º a 14.º).

51. Todavia, tal como sucede noutros pontos da Proposta, a caracterização das circunstâncias que justifica a emissão de tal ordem é feita por recurso a conceitos imprecisos, como "risco significativo" ou "extensão apreciável", que, por imprimirem um grau de discricionariedade no âmbito de um regime legal restritivo de direitos e liberdades, tem de ser evitado, em conformidade, aliás, com a jurisprudência do TJUE já citada (cf. supra, ponto 21). Na verdade, tendo em consideração que a confidencialidade das comunicações, a liberdade de expressão e a reserva da vida privada são garantidas pela CDFUE e pelo Direito Internacional, qualquer interferência nas comunicações, muito particularmente nas comunicações privadas, tem de garantir o respeito pelos princípios da necessidade, da adequação e da proporcionalidade, o que apenas se alcançará, desde logo, através do estabelecimento de regras substantivas e processuais muito claras.

52. De resto, é a própria Proposta, no respetivo preâmbulo ou exposição de motivos, a reconhecer que o processo de deteção de aliciamento é "o mais intrusivo para os utilizadores", que "exige o escrutínio automático de textos constantes de comunicações interpessoais" e que embora "a tecnologia utilizada não compreenda o conteúdo das comunicações, procurando antes padrões conhecidos e previamente identificados que indicam uma potencial situação de aliciamento, reconhecendo-se que, não obstante, "as ingerências em causa continuam a ser altamente sensíveis".

53. A tecnologia utilizada para o cumprimento de cada uma das ordens previstas é, naturalmente, diversa e deve ser apta a garantir o cumprimento da finalidade visada com a maior eficiência, através de um nível significativo

de precisão na identificação de falsos positivos, permitindo que o Centro da UE possa descartar os falsos positivos que não serão transmitidos às autoridades policiais competentes.

54. Assim, no que respeita ao material conhecido de abusos sexuais, tais tecnologias compreendem a comparação com materiais constantes de uma base de dados existente. Já para a deteção de material novo prevê-se que seja utilizada, nomeadamente, tecnologia que compreenda inteligência artificial. Quanto ao aliciamento, no que respeita às mensagens escritas, a deteção far-se-á através de meios que permitam reconhecer padrões e apenas em relação a mensagens em que seja interveniente uma criança. Nada é dito, no entanto, quanto à deteção de aliciamento através de mensagens áudio, que a presente Proposta não exclui, ao contrário do que ocorre com o Regulamento provisório.

55. É de notar que a avaliação de mensagens em texto para identificação de potenciais abusos – ainda que automatizada – constitui, com alto grau de probabilidade, maior intrusão na vida dos utilizadores do que a identificação de imagens, pelo que, caso venha a estabelecer-se esse regime, é necessário impor medidas eficazes que garantam a menor intrusão possível na vida privada, bem como na liberdade de expressão e na confidencialidade das comunicações.

56. O mesmo se diga – e por maioria de razão – quanto à possibilidade de detetar aliciamento em conversas áudio, uma vez que, para que tal ocorra, se exige uma monitorização de comunicação enquanto esta ocorre, o que se traduz num grau acrescido de intromissão nas comunicações, na vida privada e contende com o direito à palavra, igualmente tutelado pela CDFUE (artigos 7.º e 8.º).

57. A estas, há que acrescer salvaguardas reforçadas quando se trate de deteção de material novo relativo a abusos sexuais ou suspeita de aliciamento, pela possibilidade de intrusão generalizada nas comunicações pessoais e eventual condicionamento da liberdade de expressão, por receio de que as mensagens venham a ser objeto de acesso por terceiros.

58. De notar que a Proposta não consagra expressamente o princípio da proteção de dados desde a conceção e por defeito. Não obstante, deve observar-se o disposto no artigo 25.º do RGPD. Neste âmbito, recomenda-se que se imponha que a tecnologia utilizada não seja capaz de extrair o conteúdo das comunicações, exceto as estritamente necessárias para a deteção de material de abusos sexuais de criança, nem de deduzir esse conteúdo a partir de informação conhecida, integrando tal previsão no âmbito das salvaguardas indicadas no artigo 10.º.

59. Acresce a previsão de que, se a ordem que o prestador de serviços receba disser respeito à deteção de aliciamento, o prestador de serviços elabore um plano de execução com as medidas que tenciona adotar para executar a ordem e que, caso se trate de ordem nova, isto é, que não constitua renovação de ordem anterior ou,

sendo-a, introduza alterações substanciais nessa ordem, seja efetuada uma avaliação de impacto sobre a proteção de dados e um procedimento de consulta prévia à autoridade de proteção de dados nos termos dos artigos 35.º e 36.º do RGPD, relativamente às medidas estabelecidas no plano de execução, submetida (cf. alínea b) do n.º 3 do artigo 7.º da Proposta).

60. A este respeito justifica-se convocar o considerando 54 da Proposta na parte em que consagra que "as regras do presente regulamento em matéria de supervisão e cumprimento não devem ser entendidas como afetando os poderes e competências das autoridades de proteção de dados ao abrigo do Regulamento (UE)2016/679". No entanto, a proposta é praticamente omissa a este respeito.

61. Ora, considerando que o RGPD também se aplica ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas por prestadores de serviços e que a atual proposta não exclui a intervenção das autoridades de proteção de dados deste âmbito, conviria que a presente Proposta refletisse aquele regime.

62. Isto porque a concorrência de intervenção de ambas as entidades (autoridade nacional de proteção de dados e autoridade competente para efeito da Proposta) pode conduzir a situações de conflitos entre a decisão proferida por uma autoridade de proteção de dados e a autoridade competente no âmbito do novo Regulamento, sendo que a Proposta em análise deixa claro que a autoridade de coordenação pode não atender ao parecer emitido pela autoridade nacional de proteção de dados e tendo em consideração o conflito que poderá surgir da circunstância de a autoridade competente em matéria de proteção de dados pessoais manter todos os poderes corretivos que lhe são conferidos pelo RGPD, incluindo o poder de ordenar a proibição de determinado tratamento de dados.

63. Por outro lado, seria desejável que a pronúncia da autoridade nacional de proteção de dados competente não fosse exigida apenas quando a ordem a emitir seja de aliciamento, mas, também, quando seja ordem de deteção de outro tipo de material relativo a abusos sexuais de crianças.

vi. O tratamento de dados pessoais pelo Centro da UE

64. Através do Regulamento em análise pretende-se criar um centro europeu para prevenir e combater o abuso sexual de crianças, designado "Centro da UE", enquanto agência descentralizada da União, que funciona como ligação entre os operadores de serviços, as autoridades policiais e judiciais e as vítimas (artigos 41.º e 42.º).

65. Nomeadamente, cabe-lhe receber as denúncias dos prestadores de serviços, proceder à verificação dos factos de forma a reduzir o número de falsos positivos e a prevenir denúncias infundadas e, havendo fundamento, transmiti-las às autoridades policiais competentes do Estado-Membro e à Europol (n.º 1 do artigo

48.º), bem como propor ordens de deteção e de supressão de materiais referentes a abusos sexuais, bem como ordens de bloqueio de acesso e prestar apoio aos operadores de serviços através da disponibilização der tecnologias que lhes permitam executar as ordens.

66. Estabelece-se, ainda, que o Centro da UE facilita o acesso dos prestadores de serviços a tecnologias de deteção confiáveis e seguras e fornece indicadores criados com base no abuso sexual de crianças em linha conhecido e verificado pelas autoridades judiciais ou autoridades administrativas independentes, que sirvam de base à deteção por parte dos fornecedores de serviços, e apoia na comunicação entre as várias autoridades nacionais competentes nesta matéria.

67. Prevê-se a criação de canais de cooperação entre o Centro da UE e as autoridades de cooperação, por um lado (artigo 52.º) com a Europol (artigo 53.º) e com redes parceiras, como a *International Association of Internet Hotlines* (INHOPE).

68. No exercício das suas funções, o Centro da UE é responsável pela criação, manutenção e gestão de "bases de dados de indicadores" referente a abusos sexuais de material anteriormente detetado, de material não anteriormente detetado e de aliciamento de crianças e, ainda, uma base de dados de denúncias que lhe sejam comunicadas pelos prestadores de serviços de armazenagem em servidores, pelos prestadores de serviços de comunicações interpessoais, bem como pela verificação da completude, precisão e atualidade dos dados constantes nessas bases de dados (artigos 44.º e 45.º e n.º 7 do artigo 46.º).

69. Vêm elencadas, no artigo 51.º, as situações em que, para o desempenho das suas atribuições, o Centro da UE trata dados pessoais, os quais são conservados *pelo tempo estritamente necessário para o cumprimento das finalidades previstas* na Proposta. E estabelece-se que o Centro da UE verifique "regularmente se os dados constantes das bases de dados se mantêm completos, precisos e atuais e se continuam a ser necessários para efeitos de denúncia, deteção e bloqueio em conformidade com o presente regulamento" (n.º 7 do artigo 48.º).

70. A este respeito, importa assinalar que as normas não fixam prazos precisos, limitando-se a repetir os princípios da limitação da conservação e da exatidão, previstos, respetivamente, na alínea *e)* e *d)* do n.º 1 do artigo 4.º e ainda no artigo 5.º da Diretiva 2016/680, não cumprindo assim a função de orientação sobre os tratamentos de dados pessoais que as mesmas disposições do Direito da União exigem às normas de direito dos Estados-Membros que funcionem como fundamento de licitude dos tratamentos, não podendo, certamente, idêntico padrão de exigência deixar de se aplicar a um regulamento da União.

71. Assim, a CNPD recomenda a definição de prazos de conservação dos dados pessoais, bem como a especificação do prazo para a verificação da exatidão e atualização dos dados, sem embargo da identificação de situações em que essa revisão possa ter de ocorrer antes do prazo estabelecido.

72. Por outro lado, prevê-se que o Centro da UE fique instalado no mesmo local da Europol, uma vez que desempenha as suas funções em estreita colaboração com esta entidade, estabelecendo-se que cada uma destas entidades deve permitir o "mais amplo acesso possível" às informações detidas pela outra, sempre que tal seja necessário ao desempenho das respetivas funções, ficando as condições e cooperação e os métodos de trabalho para tal cooperação relegadas para um futuro memorando de entendimento (n.º 3 do artigo 53.º).

73. Tendo em consideração que as competências da Europol se encontram determinadas pelo Regulamento (UE)2016/794, que cria a Agência Europeia para a Cooperação Policial (Europol), e que o acesso a dados pessoais por parte da Europol no âmbito da transmissão de dados por outras entidades deve cingir-se ao necessário ao cumprimento dessas finalidades, a CNPD não pode deixar de estranhar o caráter vago das normas relativas a esta colaboração numa matéria como a que aqui está em causa, considerando que a segurança jurídica quanto ao grau de ingerência e de restrição de direitos e liberdades aqui em crise reclama uma maior especificação ao nível do texto do próprio Regulamento.

74. Ademais, prevê-se o acesso da Europol à base de dados de denúncias (n.º 5 do artigo 46.º), que as denúncias sejam comunicadas pelo Centro da UE à Europol e que, quando este não conseguir identificar a autoridade ou autoridades policiais competentes, aquela comunicação seja acompanhada das informações consideradas pertinentes para que a Europol determine a autoridade competente e lhes reencaminhe a denúncia, devendo consagrar-se que este reencaminhamento por parte da Europol deve ser comunicado ao Centro da UE.

75. No entanto, deve enfatizar-se que os dados pessoais a transmitir devem ser, não apenas pertinentes, mas limitados ao estritamente necessário ao cumprimento das finalidades.

76. A este respeito refira-se que não se mostra evidente a razão que fundamenta a transmissão das denúncias à Europol, quando sejam conhecidas as autoridades competentes, ademais tendo em consideração o mandato da Europol.

77. Deste modo, a norma que prevê a transmissão de dados pessoais à Europol no caso de ser conhecida a autoridade policial competente deve especificar em que circunstâncias podem os dados pessoais ser objeto de transmissão, com que finalidades e os respetivos limites, de acordo com o Regulamento Europol. Do mesmo modo, não é evidente a razão pela qual o Centro da UE encaminha todas as denúncias que "não sejam manifestamente infundadas" às autoridades policiais nacionais e à Europol. Esta determinação é excessiva, especialmente tendo em conta que o Centro da UE é um "centro especializado" que deveria realizar uma avaliação completa de modo a limitar o risco de dados de pessoas inocentes serem transmitidos às autoridades policiais.

78. Por outro lado, uma vez que o Centro da UE não tem natureza policial, nem tem competência para investigar crimes, também não se compreende a razão para o Centro da UE ter acesso aos sistemas de informação da

Europol, para mais tratando-se, como é o caso, de dados pessoais relativos à vida privada dos cidadãos e dados que integram categorias especiais de dados, o que restringe o acesso a outras entidades (n.º 3 do artigo 30.º do Regulamento Europol). Assim, por não corresponder a um tratamento de dados pessoais necessário à prossecução das respetivas atribuições, deve a Proposta refletir o regime jurídico de proteção de dados, também previsto no Regulamento da Europol, e eliminar a previsão da legitimidade de acesso aos dados pessoais constantes dos sistemas de informação da Europol pelo Centro da UE.

vii. Direitos das vítimas e dos utilizadores dos serviços quanto ao tratamento dos seus dados pessoais

79. A proposta padece ainda de várias fragilidades quanto à garantia de exercício dos direitos reconhecidos pelo RGPD e pela Diretiva n.º 2016/680 aos titulares dos dados.

80. De facto, vem referido que os fornecedores de serviços devem informar os utilizadores quando seja emitida uma ordem de deteção dos materiais de abuso sexual de crianças (n.º 6 do artigo 10.º), que a informação não será transmitida de imediato quando a Europol ou uma autoridade policial competente solicitar que tal informação não seja prestada, para evitar interferir com as atividades de prevenção, deteção, investigação e ação penal (n.º 6 do artigo 48.º da Proposta), prevendo, ainda, o direito de apresentar reclamação a uma autoridade coordenadora.

81. A Proposta não refere, porém, como podem os titulares dos dados exercer os seus direitos nem, tendo em consideração a quantidade de entidades que podem aceder a esses dados, junto de quem deve exercê-los.

82. Assim, a CNPD recomenda a previsão expressa, no texto da Proposta, junto de que entidades e de que forma podem os titulares exercer os direitos reconhecidos pelo regime jurídico de proteção de dados pessoais.

83. Ademais, tendo em consideração que, no âmbito do processo para emissão de uma ordem, os dados são comunicados a várias entidades, deve prever-se o direito de o titular ser informado, também, das entidades às quais esses dados foram transmitidos (Europol, autoridades policiais, Centro da UE, autoridades de coordenação, entre outras.).

84. Apenas se encontra especificamente previsto, no n.º 1 do artigo 20.º da Proposta, o direito de "as pessoas residentes na União" apresentarem à autoridade de coordenação designada pelo Estado um pedido para serem informadas sobre os casos de difusão de material referente a abusos sexuais de crianças conhecidos em que estejam representadas e que tenham sido denunciados ao Centro da UE. E, na segunda frase do n.º 1, que "as pessoas com deficiências têm direito de solicitar e receber essas informações de forma acessível".

85. Esta redação merece ser revista. Por um lado, convém explicitar com mais precisão quem tem legitimidade para exercer aquele direito. Isto é, saber se a referência a "pessoas residentes na União" enquadra os casos em que o pedido seja efetuado por uma criança - na aceção da alínea i) do artigo 2.º, isto é, uma pessoa singular com menos de 18 anos – através do seu representante, ou se se admite que o pedido seja efetuado pela própria criança e, em caso positivo, se se estabelece uma idade mínima. O teor da alínea b) do n.º 2 daquele artigo parece ir no sentido de que a criança poderá efetuar o pedido (por ser a pessoa representada no material), devendo indicar "a pessoa singular ou entidade que deve receber as informações em nome da pessoa que apresenta o pedido".

86. No entanto, esta solução parece incongruente por duas ordens de razões: porque, não sendo indicada uma idade mínima para que a criança materialize o pedido em nome próprio, pode, na realidade, ao contender com a legislação nacional, tornar inexequível o pedido pela própria criança; e porque se exige, tão só, a indicação da pessoa ou entidade que deve receber as informações, sem que seja exigido qualquer elemento que legitime o recebimento das mesmas.

III. Conclusão

87. Com os fundamentos acima expostos, a CNPD entende que a Proposta de Regulamento centra-se fundamentalmente na regulação de aspetos de cariz processual, esquecendo ou subalternizando a regulação dos tratamentos de dados pessoais dele decorrente e o impacto que o mesmo tem nos direitos e liberdades.

88. Com a intenção de assegurar a proteção das crianças contra abusos de cariz sexual no ambiente em linha, o regime proposto representa uma séria ingerência nos direitos e liberdades fundamentais dos utilizadores de serviços de comunicações eletrónicas, em especial, os das próprias crianças que aqui se pretende proteger.

89. A restrição aos direitos fundamentais à inviolabilidade dos conteúdos das comunicações, ao respeito pela vida privada e, consequentemente, à liberdade de expressão e à autodeterminação informativa (ou à proteção dos dados pessoais) está, ademais, prevista com caráter geral, sistemático e automatizado, decorrendo da análise dos conteúdos das comunicações eletrónicas e do tratamento dos dados pessoais nesse âmbito recolhidos, em especial quando os utilizadores sejam crianças e jovens, condicionando assim a sua liberdade de expressão, mas sobretudo o desenvolvimento da sua personalidade, quando é certo que hoje uma parte significativa da interação entre as crianças e jovens se desenvolve nesse contexto.

90. Atendendo à magnitude do impacto do regime proposto, os tratamentos de dados pessoais nele previstos carecem de uma regulação clara e precisa quanto ao seu alcance e pressupostos de aplicação, devendo especificar-se em que circunstâncias e sob que condições podem verificar-se, de modo a garantir-se que a

ingerência sobre aqueles direitos fundamentais se limita ao estritamente necessário, o que esta Proposta de Regulamento não contém nem garante. Não contém orientações precisas e claras quanto aos termos do tratamento de dados pessoais, como o revela o recurso a conceitos imprecisos para definir os critérios para a avaliação dos riscos, a ausência de definição de prazos certos para o tratamento dos dados, em especial, a sua conservação, a imprecisão na definição das condições de acesso por terceiros aos dados conservados, em clara contradição com as exigências de previsibilidade e segurança jurídicas na restrição de direitos, liberdades e garantias.

91. A CNPD recomenda, assim, a reponderação do regime aqui proposto, à luz do princípio proporcionalidade, previsto no artigo 52.º da CDFUE, devendo ser especialmente ponderado o universo de pessoas potencialmente afetadas com a interferência nas comunicações (e garantindo a delimitação de tal universo ao efetivamente necessário), a extensão e duração da medida, bem como o grau de intrusividade, considerando, em especial, a suscetibilidade de o tratamento incidir sobre categorias especiais de dados pessoais. E ainda que se garanta que os prestadores de serviços não venham a reduzir o grau de proteção da privacidade no contexto dos serviços a prestar, nomeadamente, prescindindo da cifragem das comunicações.

92. Em especial, a CNPD recomenda que no texto da Proposta de Regulamento se:

a. densifiquem os critérios de avaliação do risco e se intensifique a frequência da sua atualização (cf. supra, pontos 40 a 45);

b. preveja orientação quanto ao tratamento de dados a realizar para a finalidade de verificação da idade dos utilizadores (cf. supra, pontos 47 a 49);

c. densifiquem as circunstâncias que justificam a emissão da ordem de deteção dos abusos (cf. supra, ponto 51);

d. clarifiquem as competências da autoridade de coordenação competente para efeito do regime proposto face às competências da autoridade nacional de proteção de dados, assegurando a articulação dos seus poderes (cf. supra, pontos 61 a 63);

e. especifiquem os prazos de conservação dos dados e da regularidade de verificação da exatidão dos dados conservados (cf. supra, pontos 70 e 71);

f. identifique claramente as entidades junto das quais, bem como de que forma, os titulares dos dados podem exercer os direitos reconhecidos pelo regime jurídico de proteção de dados pessoais (cf. supra, pontos 81 a 83).

93. A CNPD recomenda também que a norma que prevê a transmissão de dados pessoais à Europol no caso de ser conhecida a autoridade policial competente especifique em que circunstâncias podem os dados pessoais ser objeto de transmissão, com que finalidades e os respetivos limites, em conformidade com o Regulamento Europol, restringindo-se aos casos em que tal seja solicitado pela Europol (cf. supra, pontos 73 a 77).

94. Demais, como o Centro da UE não tem natureza policial, nem competência para investigar crimes deve ser eliminada a norma que reconhece ao Centro da UE legitimidade para aceder aos sistemas de informação da Europol (cf. supra, ponto 78).

95. Recomenda-se ainda a revisão da articulação da presente Proposta com a Diretiva da Privacidade nas Comunicações Eletrónicas, nos termos expostos supra, nos pontos 7 e 8.

Aprovado na reunião de 9 fevereiro de 2023

Filipa Calvão (Presidente)