Parecer conjunto 4/2022 do CEPD e da AEPD

sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual de crianças

Adotado em 28 de julho de 2022

ÍNDICE

Síntese

Em 11 de maio de 2022, a Comissão Europeia publicou uma proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual de crianças.

A proposta imporia aos prestadores de serviços de armazenagem em servidor, de serviços de comunicações interpessoais e de outros serviços obrigações qualificadas em matéria de deteção, denúncia, supressão e bloqueio de material referente a abusos sexuais de crianças em linha, conhecido ou novo, bem como de aliciamento de crianças. A proposta também prevê a criação de uma nova agência descentralizada da UE («Centro da UE») e de uma rede de autoridades de coordenação nacionais para questões relacionadas com o abuso sexual de crianças, a fim de facilitar a aplicação do regulamento proposto. Tal como reconhecido na exposição de motivos da proposta, as medidas nela contidas afetariam o exercício dos direitos fundamentais dos utilizadores dos serviços em causa.

O abuso sexual de crianças é um crime particularmente grave e hediondo e o objetivo de permitir uma ação eficaz para o combater constitui um objetivo de interesse geral reconhecido pela União, com vista a proteger os direitos e as liberdades das vítimas. Simultaneamente, o CEPD e a AEPD recordam que quaisquer limitações dos direitos fundamentais, tais como as previstas na proposta, devem cumprir os requisitos estabelecidos no artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia.

O CEPD e a AEPD salientam que a proposta suscita sérias preocupações no que diz respeito à proporcionalidade da interferência prevista e às limitações da proteção dos direitos fundamentais à privacidade e à proteção dos dados pessoais. A este respeito, o CEPD e a AEPD salientam que as garantias processuais nunca podem substituir totalmente as garantias substantivas. Um sistema progressivo complexo, desde medidas de avaliação e atenuação dos riscos até uma ordem de deteção, não pode substituir a clareza necessária das obrigações substantivas.

O CEPD e a AEPD consideram que a proposta carece de clareza em elementos essenciais, como os conceitos de «risco significativo». Além disso, as entidades responsáveis pela aplicação dessas garantias, desde os operadores privados até às autoridades administrativas e/ou judiciais, gozam de uma margem de apreciação muito ampla, o que gera incerteza jurídica quanto à forma de equilibrar os direitos em causa em cada caso individual. O CEPD e a AEPD salientam que o legislador, ao permitir ingerências particularmente graves nos direitos fundamentais, deve proporcionar clareza jurídica sobre quando e onde as permite. Embora reconhecendo que a legislação não pode ser demasiado prescritiva e deve permitir alguma flexibilidade na sua aplicação prática, o CEPD e a AEPD consideram que a proposta deixa demasiada margem para possíveis abusos devido à ausência de normas substantivas claras.

No que diz respeito à necessidade e à proporcionalidade das medidas de deteção previstas, o CEPD e a AEPD estão particularmente preocupados com as medidas previstas para a deteção de material referente a abusos sexuais de crianças desconhecido e do aliciamento de crianças em serviços de comunicações interpessoais. Tendo em conta o caráter intrusivo e a natureza probabilística destas tecnologias e as taxas de erro que lhes estão associadas, o CEPD e a AEPD consideram que a ingerência criada por estas medidas vai além do que é necessário e proporcionado. Além disso, as medidas que permitem às autoridades públicas ter acesso generalizado ao conteúdo de uma comunicação para detetar o aliciamento de crianças são mais suscetíveis de afetar o conteúdo essencial dos direitos garantidos pelos artigos 7.º e 8.º da Carta. Por conseguinte, as disposições pertinentes relacionadas com o aliciamento de crianças devem ser suprimidas da proposta. Além disso, a proposta não exclui do seu âmbito de aplicação a análise de comunicações áudio. O CEPD e a AEPD

consideram que a análise de comunicações áudio é particularmente intrusiva e, como tal, deve permanecer fora do âmbito das obrigações de deteção estabelecidas no regulamento proposto, tanto no que diz respeito às mensagens de voz como às comunicações em direto.

O CEPD e a AEPD também manifestam dúvidas quanto à eficiência das medidas de bloqueio e consideram que seria desproporcionado exigir aos fornecedores de serviços Internet que decifrassem comunicações em linha para bloquear as que contêm material referente a abusos sexuais de crianças.

Além disso, o CEPD e a AEPD salientam que as tecnologias de cifragem contribuem de modo fundamental para o respeito pela vida privada e pela confidencialidade das comunicações, para a liberdade de expressão, bem como para a inovação e o crescimento da economia digital, que depende do elevado nível de confiança e segurança proporcionado por essas tecnologias. O considerando 26 da proposta adverte que a escolha quer das tecnologias de deteção, quer das medidas técnicas para proteger a confidencialidade das comunicações, como a cifragem, deve cumprir os requisitos do regulamento proposto, ou seja, deve permitir a deteção. Tal reforça a ideia decorrente do artigo 8.º, n.º 3, e do artigo 10.º, n.º 2, da proposta segundo a qual um prestador de serviços não pode recusar a execução de uma ordem de deteção com base na impossibilidade técnica. O CEPD e a AEPD consideram que deve existir um melhor equilíbrio entre a necessidade social de dispor de canais de comunicação seguros e privados e de combater a sua utilização abusiva. A proposta deve indicar claramente que nenhuma das disposições do regulamento proposto pode ser interpretada como uma proibição ou enfraquecimento da cifragem.

Embora acolham favoravelmente a declaração da proposta segundo a qual esta não afeta os poderes e competências das autoridades de proteção de dados ao abrigo do RGPD, o CEPD e a AEPD consideram que é importante enquadrar melhor a relação entre as atribuições das autoridades de coordenação e as atribuições das autoridades de proteção de dados. A este respeito, o CEPD e a AEPD valorizam o papel que a proposta atribui ao CEPD ao exigir a sua participação na aplicação prática do regulamento, em especial a necessidade de o CEPD emitir um parecer sobre as tecnologias que o Centro da UE disponibilizaria para executar as ordens de deteção. No entanto, importa clarificar qual seria a finalidade do parecer no processo e de que forma atuaria o Centro da UE depois de receber um parecer do CEPD.

Por último, o CEPD e a AEPD observam que a proposta prevê uma estreita cooperação entre o Centro da UE e a Europol, que devem facultar um ao outro «o mais amplo acesso possível às informações e aos sistemas de informação pertinentes». Embora apoiem, em princípio, a cooperação entre as duas agências, o CEPD e a AEPD formulam várias recomendações para melhorar as disposições pertinentes, tendo em conta que o Centro da UE não é uma autoridade policial, propondo nomeadamente que a transmissão de dados pessoais entre o Centro da UE e a Europol só se possa realizar caso a caso, na sequência de um pedido devidamente avaliado e através de uma ferramenta de intercâmbio seguro de comunicações, como a rede SIENA.

O Comité Europeu para a Proteção de Dados e a Autoridade Europeia para a Proteção de Dados

Tendo em conta o artigo 42.º, n.º 2, do Regulamento (UE) 2018/1725, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (RPDUE)[1],

Tendo em conta o Acordo EEE e, nomeadamente, o seu anexo XI e o seu Protocolo n.º 37, com a redação que lhe foi dada pela Decisão n.º 154/2018 do Comité Misto do EEE, de 6 de julho de 2018[2],

Tendo em conta o pedido de parecer conjunto apresentado pela Comissão Europeia ao Comité Europeu para a Proteção de Dados e à Autoridade Europeia para a Proteção de Dados, de 12 de maio de 2022, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual de crianças[3],

ADOTARAM O PRESENTE PARECER CONJUNTO

1. CONTEXTO

1. Em 11 de maio de 2022, a Comissão Europeia («Comissão») publicou uma proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual de crianças («proposta» ou «regulamento proposto»)[4].

2. A proposta foi apresentada no seguimento da adoção do Regulamento (UE) 2021/1232 relativo a uma derrogação temporária de determinadas disposições da Diretiva 2002/58/CE no que respeita 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 («regulamento provisório») [5]. O regulamento provisório não exige que os prestadores de serviços em causa adotem medidas para detetar material referente a abusos sexuais de crianças (por exemplo, imagens, vídeos, etc.) ou aliciamento de crianças nos seus serviços, mas

[1] JO L 295 de 21.11.2018, p. 39.
[2] As referências a «Estados-Membros» no presente documento devem ser entendidas como referências a «Estados-Membros do EEE».
[3] Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual de crianças (COM(2022) 209 final).
[4] *Ibid*.
[5] Regulamento (UE) 2021/1232 do Parlamento Europeu e do Conselho, de 14 de julho de 2021, relativo a uma derrogação temporária de determinadas disposições da Diretiva 2002/58/CE no que respeita 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 (JO L 274 de 30.7.2021, p. 41).

permite-lhes fazê-lo voluntariamente, em conformidade com as condições estabelecidas nesse regulamento[6].

3. A proposta é constituída por dois elementos principais. Em primeiro lugar, impõe aos prestadores de serviços de armazenagem em servidor, de serviços de comunicações interpessoais e de outros serviços obrigações qualificadas em matéria de deteção, denúncia, supressão e bloqueio de material referente a abusos sexuais de crianças em linha, conhecido ou novo, bem como de aliciamento de crianças. Em segundo lugar, a proposta prevê a criação de uma nova agência descentralizada da UE («Centro da UE sobre o Abuso Sexual de Crianças» ou «Centro da UE») e de uma rede de autoridades de coordenação nacionais para questões relacionadas com o abuso sexual de crianças, a fim de facilitar a aplicação do regulamento proposto[7].

4. Tal como reconhecido na exposição de motivos da proposta, as medidas nela contidas afetariam o exercício dos direitos fundamentais dos utilizadores dos serviços em causa. Esses direitos incluem, em especial, os direitos fundamentais ao respeito da privacidade (incluindo a confidencialidade das comunicações, como parte do direito mais amplo ao respeito pela vida privada e familiar), à proteção dos dados pessoais e à liberdade de expressão e de informação[8].

5. Além disso, as medidas propostas destinam-se a desenvolver e, em certa medida, complementar a legislação da UE em vigor em matéria de proteção de dados e privacidade. A este respeito, a exposição de motivos assinala o seguinte:

> «A proposta baseia-se no Regulamento Geral sobre a Proteção de Dados (RGPD). Na prática, os prestadores de serviços tendem a invocar vários motivos previstos no RGPD para efetuar o tratamento de dados pessoais inerente à deteção e denúncia voluntárias de abusos sexuais de crianças na Internet. A proposta estabelece um sistema de ordens de deteção específicas e define as condições de deteção, proporcionando maior segurança jurídica em relação a essas atividades. No que diz respeito às atividades de deteção obrigatória que envolvem o tratamento de dados pessoais, a proposta, em especial as ordens de deteção emitidas com base na mesma, estabelece assim o motivo para tratamento referido no artigo 6.º, n.º 1, alínea c), do RGPD, que prevê o tratamento de dados pessoais necessário para o cumprimento de uma obrigação jurídica ao abrigo do direito da União ou dos Estados-Membros a que o responsável pelo tratamento esteja sujeito.
>
> A proposta abrange, entre outros, os prestadores que oferecem serviços de comunicações eletrónicas interpessoais e que, por conseguinte, estão sujeitos às disposições nacionais que dão aplicação à Diretiva Privacidade Eletrónica e à sua proposta de revisão atualmente em fase de negociação. As medidas previstas na proposta restringem, em alguns aspetos, o âmbito dos direitos e obrigações previstos nas disposições pertinentes da referida diretiva, concretamente no que diz respeito às atividades estritamente necessárias para executar ordens de deteção. A este respeito, a proposta implica a aplicação, por analogia, do artigo 15.º, n.º 1, da referida diretiva»[9].

---

[6] Ver também o Parecer 7/2020 da AEPD sobre a proposta de derrogações temporárias à Diretiva 2002/58/CE para efeitos de luta contra o abuso sexual de crianças em linha (10 de novembro de 2020).
[7] COM(2022) 209 final, p. 17.
[8] COM(2022) 209 final, p. 14.
[9] COM(2022) 209 final, p. 5.

6. Dada a gravidade das ingerências previstas nos direitos fundamentais, a proposta reveste-se de especial importância para a proteção dos direitos e das liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais. Por conseguinte, em 12 de maio de 2022, a Comissão decidiu consultar o Comité Europeu para a Proteção de Dados (CEPD) e a Autoridade Europeia para a Proteção de Dados (AEPD), em conformidade com o artigo 42.º, n.º 2, do RPDUE.

2. ÂMBITO DO PARECER

7. O presente parecer conjunto apresenta as posições comuns do CEPD e da AEPD sobre a proposta, limitando-se aos aspetos da proposta relativos à proteção da privacidade e dos dados pessoais. Em especial, o parecer conjunto salienta os domínios em que a proposta não garante uma proteção suficiente dos direitos fundamentais à privacidade e à proteção de dados ou requer um maior alinhamento com o quadro jurídico da UE em matéria de proteção da privacidade e dos dados pessoais.

8. Tal como explicado mais pormenorizadamente no presente parecer conjunto, a proposta suscita sérias preocupações no que diz respeito à necessidade e à proporcionalidade da ingerência prevista e às limitações da proteção dos direitos fundamentais à privacidade e à proteção dos dados pessoais. Contudo, o objetivo do presente parecer conjunto não é fornecer uma lista exaustiva de todas as questões de privacidade e proteção de dados suscitadas pela proposta, nem apresentar sugestões específicas para melhorar a redação da proposta. Em vez disso, o presente parecer conjunto apresenta observações de alto nível sobre as principais questões suscitadas pela proposta identificadas pelo CEPD e pela AEPD. No entanto, o CEPD e a AEPD continuam disponíveis para apresentar outras observações e recomendações sobre a proposta aos colegisladores durante o processo legislativo.

3. OBSERVAÇÕES GERAIS SOBRE OS DIREITOS À CONFIDENCIALIDADE DAS COMUNICAÇÕES E À PROTEÇÃO DOS DADOS PESSOAIS

9. A confidencialidade das comunicações é um elemento essencial do direito fundamental ao respeito pela vida privada e familiar, consagrado no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia («Carta»)[10]. Além disso, o artigo 8.º da Carta reconhece o direito fundamental à proteção dos dados pessoais. O direito à confidencialidade das comunicações e o direito à vida privada e familiar são igualmente garantidos pelo artigo 8.º da Convenção Europeia dos Direitos Humanos (CEDH) e fazem parte das tradições constitucionais comuns aos Estados-Membros[11].

10. O CEPD e a AEPD recordam que os direitos consagrados nos artigos 7.º e 8.º da Carta não são prerrogativas absolutas, mas devem ser tomados em consideração de acordo com a sua função na

[10] Ver, por exemplo, Declaração do CEPD relativa à revisão do Regulamento Privacidade Eletrónica e ao seu impacto sobre a proteção das pessoas singulares no que diz respeito à privacidade e à confidencialidade das suas comunicações (25 de maio de 2018).

[11] Quase todas as constituições europeias incluem um direito que protege a confidencialidade das comunicações. Ver, por exemplo, o artigo 15.º da Constituição da República Italiana, o artigo 10.º da Lei Fundamental da República Federal da Alemanha, o artigo 22.º da Constituição belga e o artigo 13.º da Constituição do Reino dos Países Baixos.

sociedade[12]. O abuso sexual de crianças é um crime particularmente grave e hediondo e o objetivo de permitir uma ação eficaz para o combater constitui um objetivo de interesse geral reconhecido pela União, com vista a proteger os direitos e as liberdades das vítimas. No que diz respeito à luta efetiva contra as infrações penais de que são vítimas menores e outras pessoas vulneráveis, o Tribunal de Justiça da União Europeia (TJUE) sublinhou que podem resultar do artigo 7.º da Carta obrigações positivas, exigindo que os poderes públicos adotem medidas jurídicas destinadas a proteger a vida privada e familiar, o domicílio e as comunicações. Tais obrigações são igualmente suscetíveis de decorrer dos artigos 3.º e 4.º da Carta no que diz respeito à proteção da integridade física e psíquica das pessoas e à proibição da tortura e dos tratos desumanos e degradantes[13].

11. Simultaneamente, quaisquer limitações dos direitos garantidos pela Carta, como as previstas na proposta[14], têm de cumprir os requisitos estabelecidos no artigo 52.º, n.º 1, da Carta. Qualquer medida que interfira com o direito à confidencialidade das comunicações e com o direito à vida privada e familiar deve, antes de mais, respeitar o conteúdo essencial dos direitos em causa[15]. O conteúdo essencial de um direito é afetado se o direito for esvaziado do seu conteúdo básico e a pessoa singular não o puder exercer[16]. A ingerência não pode constituir, relativamente à finalidade prosseguida, uma intervenção excessiva e intolerável que atente contra a própria substância do direito assim garantido[17]. Por conseguinte, mesmo um direito fundamental que não tem caráter absoluto, como o direito à confidencialidade das comunicações e o direito à proteção dos dados pessoais, tem alguns componentes fundamentais que podem não ser limitados.

12. O TJUE aplicou, em várias ocasiões, o teste do «conteúdo essencial de um direito» no domínio da privacidade das comunicações eletrónicas. No Acórdão Tele2 Sverige e Watson, o Tribunal estabeleceu que a regulamentação que não autoriza a conservação do conteúdo de uma comunicação não é suscetível de violar o conteúdo essencial dos direitos à vida privada e à proteção dos dados pessoais[18]. No Acórdão Schrems, o Tribunal declarou que uma regulamentação que permita às autoridades públicas aceder de modo generalizado ao conteúdo das comunicações eletrónicas deve ser considerada lesiva do conteúdo essencial do direito fundamental ao respeito da vida privada, tal como é garantido pelo artigo 7.º da Carta[19]. No Acórdão Digital Rights Ireland e Seitlinger e outros, o Tribunal declarou que, embora a conservação dos dados imposta pela Diretiva 2006/24/CE constitua uma ingerência particularmente grave no direito fundamental à privacidade e nos outros direitos consagrados no artigo 7.º da Carta, não era suscetível de afetar o respetivo conteúdo essencial, tendo em conta que a referida diretiva não permitia tomar conhecimento do conteúdo das comunicações

---

[12] Ver, nomeadamente, o acórdão do TJUE no processo C-311/18, Facebook Ireland e Schrems, n.º 172, e jurisprudência aí referida. Ver também o considerando 4 do RGPD.

[13] TJUE, processos apensos C-511/18, C-512/18 e C-520/18, La Quadrature du Net e outros, n.ºs 126 a 128. Ver também o Parecer 7/2020 da AEPD sobre a proposta de derrogações temporárias à Diretiva 2002/58/CE para efeitos de luta contra o abuso sexual de crianças em linha (10 de novembro de 2020), ponto 12.

[14] Ver COM(2022) 209 final, p. 14.

[15] Artigo 52.º, n.º 1, da Carta.

[16] Ver «EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data» [Orientações da AEPD sobre a avaliação da proporcionalidade de medidas que limitem os direitos fundamentais à privacidade e à proteção dos dados pessoais], 19 de dezembro de 2019, p. 8, disponíveis em https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf..

[17] TJUE, processo C-393/19, OM, n.º 53.

[18] TJUE, processos apensos C-203/15 e C-698/15, Tele2 Sverige e Watson, n.º 101.

[19] TJUE, processo C-362/14, Schrems, n.º 94.

eletrónicas, enquanto tal[20]. É possível deduzir desta jurisprudência que as medidas que permitem às autoridades públicas ter acesso generalizado ao conteúdo de uma comunicação são mais suscetíveis de afetar o conteúdo essencial dos direitos garantidos pelos artigos 7.º e 8.º da Carta. Estas considerações são igualmente relevantes no que diz respeito às medidas para a deteção de material referente a abusos sexuais de crianças e do aliciamento de crianças, como as previstas na proposta.

13. Além disso, o TJUE declarou que as medidas de segurança dos dados são essenciais para impedir que o conteúdo essencial do direito fundamental à proteção dos dados pessoais, consagrado no artigo 8.º da Carta, seja afetado[21]. Na era digital, as soluções técnicas para garantir e proteger a confidencialidade das comunicações eletrónicas, incluindo medidas de cifragem, são fundamentais para garantir o exercício de todos os direitos fundamentais[22]. Este aspeto deve ser devidamente tido em conta aquando da avaliação das medidas para a deteção obrigatória de material referente a abusos sexuais de crianças ou do aliciamento de crianças, em especial se resultarem no enfraquecimento ou deterioração da cifragem[23].

14. O artigo 52.º, n.º 1, da Carta estabelece igualmente que qualquer restrição ao exercício de um direito fundamental garantido pela Carta deve ser prevista por lei. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros[24]. Para cumprir a exigência de proporcionalidade, uma regulamentação deve prever normas claras e precisas que regulem o âmbito e a aplicação das medidas em causa e impor requisitos mínimos, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso[25]. Essa regulamentação deve indicar em que circunstâncias e em que condições uma medida que prevê o tratamento de tais dados pode ser adotada, garantindo assim que a ingerência seja limitada ao estritamente necessário[26]. Tal como clarificado pelo TJUE, a necessidade de dispor de tais garantias é ainda maior quando os dados pessoais são sujeitos a um tratamento automatizado e quando está em jogo a proteção desta categoria específica de dados pessoais, que são os dados sensíveis[27].

15. A proposta limitaria o exercício dos direitos e obrigações previstos no artigo 5.º, n.os 1 e 3, e no artigo 6.º, n.º 1, da Diretiva 2002/58/CE («Diretiva Privacidade Eletrónica»)[28], na medida em que tal seja necessário para a execução das ordens de deteção emitidas em conformidade com o capítulo 1,

---

[20] TJUE, processos apensos C-293/12 e C-594/12, Digital Rights Ireland e Seitlinger e outros, n.º 39.
[21] *Ibid*., n.º 40.
[22] Ver Conselho dos Direitos Humanos, Resolução 47/16 intitulada «The promotion, protection and enjoyment of human rights on the Internet» [A promoção, proteção e gozo dos direitos humanos na Internet], UN Doc. A/HRC/RES/47/16 (26 de julho de 2021).
[23] Ver também o considerando 25 do regulamento provisório.
[24] Ver «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit» [Guia para a avaliação da necessidade de medidas que limitem o direito fundamental à proteção de dados pessoais], 11 de abril de 2019, disponível em https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[25] TJUE, processos apensos C-511/18, C-512/18 e C-520/18, La Quadrature du Net e outros, n.º 132.
[26] *Ibid*.
[27] *Ibid*.
[28] 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), com a redação que lhe foi dada pela Diretiva 2006/24/CE e a Diretiva 2009/136/CE.

secção 2, da proposta. Por conseguinte, o CEPD e a AEPD consideram que é necessário avaliar a proposta não só à luz da Carta e do RGPD, mas também à luz do artigo 5.º, do artigo 6.º e do artigo 15.º, n.º 1, da Diretiva Privacidade Eletrónica.

4. OBSERVAÇÕES ESPECÍFICAS

4.1 Relação com a legislação em vigor

4.1.1 Relação com o RGPD e a Diretiva Privacidade Eletrónica

16. A proposta refere que não prejudica as regras decorrentes de outros atos da União, em especial o RGPD[29] e a Diretiva Privacidade Eletrónica. Contrariamente ao regulamento provisório, a proposta não prevê uma derrogação temporária explícita, mas uma limitação do exercício dos direitos e obrigações estabelecidos no artigo 5.º, n.ºs 1 e 3, e no artigo 6.º, n.º 1, da Diretiva Privacidade Eletrónica. Além disso, importa salientar que o regulamento provisório prevê uma derrogação exclusiva ao disposto no artigo 5.º, n.º 1, e no artigo 6.º, n.º 1, e não ao disposto no artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica.

17. A proposta remete ainda para o artigo 15.º, n.º 1, da Diretiva Privacidade Eletrónica, que permite aos Estados-Membros adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º dessa diretiva, sempre que tais restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática, nomeadamente para prevenir, investigar, detetar e reprimir infrações penais. Nos termos da proposta, o artigo 15.º, n.º 1, da Diretiva Privacidade Eletrónica é aplicado por analogia quando a proposta limita o exercício dos direitos e obrigações previstos no artigo 5.º, n.ºs 1 e 3, e no artigo 6.º, n.º 1, da Diretiva Privacidade Eletrónica.

18. O CEPD e a AEPD recordam que o TJUE deixou claro que o artigo 15.º, n.º 1, da Diretiva Privacidade Eletrónica deve ser interpretado em sentido estrito, o que significa que a exceção ao princípio da confidencialidade das comunicações permitida pelo artigo 15.º, n.º 1, deve continuar a ser uma exceção e não se pode converter na regra[30]. Tal como explicado mais adiante no presente parecer conjunto, o CEPD e a AEPD consideram que a proposta não preenche os requisitos de (estrita) necessidade, eficácia e proporcionalidade. Além disso, o CEPD e a AEPD concluem que, nos termos da proposta, a ingerência na confidencialidade das comunicações poderia, de facto, converter-se na regra e deixar de ser a exceção.

4.1.2 Relação com o Regulamento (UE) 2021/1232 e impacto na deteção voluntária de abusos sexuais de crianças em linha

19. Nos termos do artigo 88.º da proposta, esta revogaria o regulamento provisório, que prevê uma derrogação temporária a determinadas disposições da Diretiva Privacidade Eletrónica, a fim de permitir a utilização voluntária de tecnologias para a deteção de material referente a abusos sexuais de crianças e do aliciamento de crianças por prestadores de serviços de comunicações interpessoais independentes do número. Por conseguinte, a partir da data de aplicação do regulamento proposto, não existiria qualquer derrogação à Diretiva Privacidade Eletrónica que permitisse a deteção voluntária de abusos sexuais de crianças em linha por esses prestadores de serviços.

---

[29] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE) (JO L 119 de 4.5.2016, p. 1).
[30] Acórdão de 21 de dezembro de 2016 nos processos apensos C-203/15 e C-698/15, Tele2 Sverige AB e Watson, n.º 89.

20. Uma vez que as obrigações de deteção introduzidas pela proposta se aplicariam apenas aos destinatários das ordens de deteção, seria importante clarificar no texto do regulamento proposto que a utilização voluntária de tecnologias para a deteção de material referente a abusos sexuais de crianças e do aliciamento de crianças continua a ser permitida apenas na medida em que seja permitida ao abrigo da Diretiva Privacidade Eletrónica e do RGPD. Tal implicaria, por exemplo, que os prestadores de serviços de comunicações interpessoais independentes do número fossem impedidos de utilizar essas tecnologias voluntariamente, a menos que tal fosse permitido pela legislação nacional que transpõe a Diretiva Privacidade Eletrónica, em conformidade com o artigo 15.º, n.º 1, da Diretiva Privacidade Eletrónica e com a Carta.

21. De um modo mais geral, o regulamento proposto beneficiaria de mais clareza quanto ao estatuto da deteção voluntária de abusos sexuais de crianças em linha após a sua data de aplicação e quanto à transição do regime de deteção voluntária estabelecido no regulamento provisório para as obrigações de deteção estabelecidas no regulamento proposto. Por exemplo, o CEPD e a AEPD recomendam que fique claro que o regulamento proposto não prevê uma base lícita para o tratamento de dados pessoais com o único objetivo de detetar abusos sexuais de crianças em linha a título voluntário.

4.2 Base lícita ao abrigo do RGPD

22. A proposta visa estabelecer uma base lícita, na aceção do RGPD, para o tratamento de dados pessoais para efeitos de deteção de material referente a abusos sexuais de crianças e do aliciamento de crianças. Por conseguinte, a exposição de motivos assinala o seguinte: «No que diz respeito às atividades de deteção obrigatória que envolvem o tratamento de dados pessoais, a proposta, em especial as ordens de deteção emitidas com base na mesma, estabelece assim o motivo para tratamento referido no artigo 6.º, n.º 1, alínea c), do RGPD, que prevê o tratamento de dados pessoais necessário para o cumprimento de uma obrigação jurídica ao abrigo do direito da União ou dos Estados-Membros a que o responsável pelo tratamento esteja sujeito»[31].

23. O CEPD e a AEPD congratulam-se com a decisão da Comissão de eliminar a incerteza jurídica quanto à base jurídica do tratamento de dados pessoais que resultou do regulamento provisório. O CEPD e a AEPD também concordam com a conclusão da Comissão segundo a qual as consequências da implantação de medidas de deteção são demasiado abrangentes e graves para deixar a decisão de aplicar ou não essas medidas ao critério dos prestadores de serviços[32]. Ao mesmo tempo, o CEPD e a AEPD observam que qualquer base jurídica que obrigue os prestadores de serviços a interferir com os direitos fundamentais à proteção de dados e à privacidade só será válida na medida em que respeite as condições estabelecidas no artigo 52.º, n.º 1, da Carta, tal como analisado nas secções seguintes.

4.3 Obrigações de avaliação e atenuação dos riscos

24. Nos termos do capítulo II, secção 1, da proposta, os prestadores de serviços de armazenagem em servidor e os prestadores de serviços de comunicações interpessoais são obrigados a identificar, analisar e avaliar, para cada um dos serviços que oferecem, o risco de utilização desse serviço para efeitos de abuso sexual de crianças em linha e, posteriormente, procurar minimizar o risco identificado aplicando «medidas de atenuação razoáveis, adaptadas ao risco identificado».

25. O CEPD e a AEPD observam que, ao realizar uma avaliação dos riscos, o prestador de serviços deve ter em conta, em especial, os elementos enumerados no artigo 3.º, n.º 2, alíneas a) a e), da proposta,

[31] *Ibid*, p. 4.
[32] Ver proposta, COM(2022) 209 final, pp. 15-16.

incluindo: proibições e restrições estabelecidas nos termos e condições do prestador de serviços; a forma como os utilizadores utilizam o serviço e o seu impacto nesse risco; a forma como o prestador de serviços concebeu e gere o serviço, incluindo o modelo de negócio, o sistema e processos de governação e outros sistemas e processos relevantes, bem como o seu impacto nesse risco. No que diz respeito ao risco de aliciamento de crianças, os elementos propostos a considerar são os seguintes: a medida em que o serviço é utilizado ou é suscetível de ser utilizado por crianças; os grupos etários e o risco de aliciamento de crianças por grupo etário; a disponibilidade de funcionalidades que permitam a procura de utilizadores, funcionalidades que permitam aos utilizadores estabelecer diretamente contacto com outros utilizadores, especialmente através de comunicações privadas, e funcionalidades que permitam aos utilizadores partilhar imagens ou vídeos com outros utilizadores.

26. Embora reconheçam que esses critérios se afiguram relevantes, o CEPD e a AEPD manifestam preocupação com o facto de os mesmos permitirem uma ampla margem de interpretação e apreciação. Vários critérios são descritos em termos muito genéricos (por exemplo, a «forma como os utilizadores utilizam o serviço e o seu impacto nesse risco») ou estão relacionados com funcionalidades básicas comuns a muitos serviços em linha (por exemplo, «permitir que os utilizadores partilhem imagens ou vídeos com outros utilizadores»). Por conseguinte, esse critérios afiguram-se propensos a uma avaliação subjetiva (e não objetiva).

27. O CEPD e a AEPD consideram que o mesmo se aplica às medidas de atenuação dos riscos a tomar nos termos do artigo 4.º da proposta. Medidas como a adaptação, através de medidas técnicas e operacionais adequadas e do pessoal necessário, os sistemas de moderação de conteúdos ou de recomendação do prestador de serviços afiguram-se adequadas para reduzir o risco identificado. No entanto, se forem aplicados no âmbito de um processo complexo de avaliação dos riscos e combinados com termos abstratos e vagos para descrever o nível aceitável de risco (por exemplo, «de forma significativa»), esses critérios não cumprem os requisitos de segurança jurídica e previsibilidade necessários para justificar uma ingerência na confidencialidade das comunicações entre particulares, o que constitui uma clara ingerência nos direitos fundamentais à privacidade e à liberdade de expressão.

28. Embora os prestadores de serviços não sejam autorizados a interferir com a confidencialidade das comunicações no âmbito das suas estratégias de avaliação e atenuação dos riscos, antes de receberem uma ordem de deteção, existe uma ligação direta entre as obrigações de avaliação e atenuação dos riscos e as obrigações de deteção daí decorrentes. O artigo 7.º, n.º 4, da proposta faz depender a emissão de uma ordem de deteção da existência de provas de um risco significativo de o serviço em causa ser utilizado para efeitos de abuso sexual de crianças em linha. Antes da emissão de uma ordem de deteção, deve cumprir-se um processo complexo que envolva os prestadores de serviços, a autoridade de coordenação e a autoridade judicial ou outra autoridade administrativa independente responsável pela emissão da ordem. Em primeiro lugar, os prestadores de serviços devem avaliar o risco de utilização dos seus serviços para efeitos de abuso sexual de crianças em linha (artigo 3.º da proposta) e avaliar eventuais medidas de atenuação dos riscos (artigo 4.º da proposta) para reduzir esse risco. Em seguida, cumpre comunicar os resultados deste exercício à autoridade de coordenação competente (artigo 5.º da proposta). Se a avaliação dos riscos revelar que subsiste um risco significativo apesar dos esforços para o atenuar, a autoridade de coordenação deve ouvir o prestador de serviços sobre um projeto de pedido de emissão de uma ordem de deteção e dar-lhe a possibilidade de apresentar observações. O prestador de serviços é ainda obrigado a apresentar um plano de execução, incluindo um parecer da autoridade de proteção de dados competente no caso da deteção de aliciamento de crianças. Se a autoridade de coordenação der seguimento ao processo, é solicitada uma ordem de deteção, eventualmente emitida por um tribunal ou por outra autoridade

administrativa independente. Por conseguinte, a avaliação inicial dos riscos e as medidas escolhidas para reduzir o risco identificado constituem uma base decisiva para a avaliação, pela autoridade de coordenação, bem como pela autoridade judicial ou administrativa competente, da necessidade de uma ordem de deteção.

29. O CEPD e a AEPD registam as medidas complexas conducentes à emissão de uma ordem de deteção, que incluem uma avaliação inicial dos riscos pelo prestador de serviços e a sua proposta relativa a medidas de atenuação dos riscos, bem como a interação posterior do prestador de serviços com a autoridade de coordenação competente. O CEPD e a AEPD consideram que existe uma possibilidade substancial de o prestador de serviços influenciar o resultado do processo. A este respeito, o CEPD e a AEPD observam que o considerando 17 da proposta estipula que os prestadores de serviços devem poder indicar, como parte da comunicação dos riscos, «a sua recetividade e preparação» para a eventual emissão de uma ordem de deteção. Por conseguinte, não se pode presumir que cada prestador de serviços procurará evitar a emissão de uma ordem de deteção, a fim de preservar a confidencialidade das comunicações dos seus utilizadores, aplicando as medidas de atenuação mais eficazes, mas menos intrusivas, especialmente quando essas medidas de atenuação interferem com a liberdade de empresa do prestador de serviços, nos termos do artigo 16.º da Carta.

30. A AEPD e o CEPD gostariam de salientar que as garantias processuais nunca podem substituir totalmente as garantias substantivas. Por conseguinte, o processo complexo, acima descrito, que conduz à eventual emissão de uma ordem de deteção deve ser acompanhado por obrigações substantivas claras. O CEPD e a AEPD consideram que a proposta carece de clareza em vários elementos essenciais (por exemplo, os conceitos de «risco significativo», «de forma significativa», etc.) e que os vários níveis de garantias processuais não permitem corrigir esse problema. Tal é especialmente importante devido ao facto de as entidades responsáveis pela aplicação dessas garantias (por exemplo, prestadores de serviços, autoridades judiciais, etc.) gozarem de uma ampla margem de apreciação quanto à forma de equilibrar os direitos em causa em cada caso. Tendo em conta as ingerências significativas nos direitos fundamentais que resultariam da adoção da proposta, o legislador deve assegurar que a proposta proporciona maior clareza sobre quando e onde tais ingerências são permitidas. Embora reconheçam que as medidas legislativas não podem ser demasiado prescritivas e devem permitir alguma flexibilidade na sua aplicação prática, o CEPD e a AEPD consideram que o texto atual da proposta deixa demasiada margem para possíveis abusos devido à ausência de normas substantivas claras.

31. Tendo em conta o potencial impacto significativo num número muito elevado de titulares de dados (ou seja, potencialmente todos os utilizadores de serviços de comunicações interpessoais), o CEPD e a AEPD salientam a necessidade de um elevado nível de segurança jurídica, clareza e previsibilidade da legislação, a fim de assegurar que as medidas propostas são verdadeiramente eficazes na consecução do objetivo que prosseguem e, ao mesmo tempo, menos lesivas dos direitos fundamentais em causa.

4.4 Condições para a emissão de ordens de deteção

32. O artigo 7.º da proposta prevê que a autoridade de coordenação do local de estabelecimento tenha poderes para solicitar à autoridade judicial ou outra autoridade administrativa independente competente do Estado-Membro em causa que emita uma ordem de deteção que obrigue um prestador de serviços de armazenagem em servidor ou um prestador de serviços de comunicações interpessoais a tomar as medidas especificadas no artigo 10.º para detetar abusos sexuais de crianças em linha num serviço específico.

33. O CEPD e a AEPD registam os seguintes elementos a cumprir antes da emissão de uma ordem de deteção:

    a. Existem provas de um risco significativo de o serviço ser utilizado para efeitos de abuso sexual de crianças em linha, na aceção do artigo 7.º, n.os 5, 6 e 7, consoante os casos;

    b. Os motivos para a emissão da ordem de deteção superam as consequências negativas para os direitos e interesses legítimos de todas as partes afetadas, tendo especialmente em conta a necessidade de assegurar um equilíbrio justo entre os direitos fundamentais dessas partes.

34. O significado de «risco significativo» é especificado no artigo 7.º, n.º 5 e seguintes, em função do tipo de ordem de deteção em causa. Presume-se que existe um risco significativo no caso de ordens de deteção relativas à deteção de material referente a abusos sexuais de crianças conhecido se:

    a. Não obstante as medidas de atenuação que o prestador de serviços possa ter tomado ou venha a tomar, for provável que o serviço seja utilizado, de forma significativa, para a difusão de material referente a abusos sexuais de crianças conhecido; e

    b. Existirem provas de que o serviço ou, caso este ainda não fosse oferecido na União à data do pedido de emissão da ordem de deteção, um serviço comparável foi utilizado nos últimos 12 meses e de forma significativa para a difusão de material referente a abusos sexuais de crianças conhecido.

35. Para emitir uma ordem de deteção de material referente a abusos sexuais de crianças desconhecido, é necessário que a probabilidade e as provas factuais se refiram a material desconhecido e que tenha sido emitida uma ordem de deteção prévia de material conhecido conducente a um número significativo de denúncias de material referente a abusos sexuais de crianças pelo prestador de serviços (artigo 7.º, n.º 6, da proposta). No caso de uma ordem de deteção de aliciamento de crianças, considera-se que existe um risco significativo quando o prestador de serviços é considerado um prestador de serviços de comunicações interpessoais, é provável que o serviço seja utilizado, de forma significativa, para o aliciamento de crianças e existem provas de que o serviço foi utilizado de forma significativa para o aliciamento de crianças (artigo 7.º, n.º 7, da proposta).

36. O CEPD e a AEPD observam que, mesmo com as especificações do artigo 7.º, n.os 5 a 7, da proposta, as condições para a emissão de uma ordem de deteção caracterizam-se por termos jurídicos vagos, tais como «de forma significativa» ou «número significativo», e são em parte repetitivas, uma vez que as provas de abuso anterior contribuirão frequentemente para determinar a probabilidade de abuso futuro.

37. A proposta prevê um sistema através do qual, ao decidir se uma ordem de deteção é necessária, tem de ser tomada uma decisão sobre a utilização futura de um serviço para efeitos de abuso sexual de crianças em linha. Por conseguinte, é compreensível que os elementos estabelecidos no artigo 7.º tenham um caráter prognóstico. No entanto, o recurso a conceitos vagos na proposta torna difícil para os prestadores de serviços, bem como para a autoridade judicial ou outra autoridade administrativa independente competente, aplicar os requisitos legais introduzidos pela proposta de forma previsível e não arbitrária. O CEPD e a AEPD receiam que estes conceitos amplos e vagos resultem em falta de segurança jurídica e conduzam também a divergências consideráveis na aplicação concreta da proposta em toda a União, consoante as interpretações que serão dadas a conceitos como «probabilidade» e «de forma significativa» pelas autoridades judiciais ou outras autoridades administrativas independentes nos Estados-Membros. Tal resultado não seria aceitável, tendo em conta que as disposições relativas às ordens de deteção para os prestadores de serviços de

comunicações interpessoais constituirão «restrições» ao princípio da confidencialidade das comunicações estabelecido no artigo 5.º da Diretiva Privacidade Eletrónica, sendo a sua clareza e previsibilidade muito importantes para assegurar que essas restrições são uniformemente aplicadas em toda a União.

4.5 Análise da necessidade e da proporcionalidade das medidas previstas[33]

38. Conforme indicado acima, podem ser emitidos três tipos de ordens de deteção: ordens de deteção relativas à difusão de material referente a abusos sexuais de crianças conhecido (artigo 7.º, n.º 5, da proposta), ordens de deteção relativas à difusão de material referente a abusos sexuais de crianças novo (artigo 7.º, n.º 6, da proposta) e ordens de deteção relativas ao aliciamento de crianças (artigo 7.º, n.º 7, da proposta). Cada ordem de deteção exigiria normalmente uma tecnologia diferente para a sua aplicação prática. Como tal, implicam níveis de intrusão diferentes e, por conseguinte, impactos diferentes nos direitos à privacidade e à proteção dos dados pessoais.

39. As tecnologias de deteção de material referente a abusos sexuais de crianças conhecido são normalmente tecnologias de correspondência, uma vez que recorrem a uma base de dados existente de material desse tipo com a qual podem comparar imagens (incluindo imagens fixas de vídeos). A correspondência só é possível se as imagens que o prestador de serviços está a processar e as imagens na base de dados tiverem sido digitalizadas, geralmente convertendo-as em valores de dispersão. Este tipo de tecnologia de dispersão tem uma taxa estimada de falsos positivos não superior a 1 em 50 mil milhões (ou seja, uma taxa de falsos positivos de 0,000000002 %). [34]

40. Para detetar material referente a abusos sexuais de crianças novo, é normalmente utilizado um tipo diferente de tecnologia, que inclui classificadores e inteligência artificial (IA)[35]. No entanto, as suas taxas de erro são, em geral, significativamente mais elevadas. Por exemplo, o relatório de avaliação de impacto indica que existem tecnologias para a deteção de material referente a abusos sexuais de crianças novo cuja taxa de precisão pode ser fixada em 99,9 % (ou seja, uma taxa de falsos positivos de 0,1 %), mas, com essa taxa de precisão, só conseguem identificar 80 % do material referente a abusos sexuais de crianças total no conjunto de dados pertinente[36].

41. No que diz respeito à deteção do aliciamento de crianças em comunicações por mensagens de texto, o relatório de avaliação de impacto explica que ela se baseia normalmente na deteção de padrões. O relatório de avaliação de impacto observa que algumas das tecnologias existentes para a deteção do aliciamento de crianças apresentam uma «taxa de exatidão» de 88 %[37]. Segundo a Comissão, tal significa que em 100 conversas assinaladas como possível aliciamento criminoso de crianças, 12 podem ser excluídas após revisão (pelo Centro da UE, nos termos da proposta) e não serão

---

[33] Ver também «The EDPS quick guide to necessity and proportionality» [Guia rápido da AEPD sobre a necessidade e a proporcionalidade], disponível em: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

[34] Ver Comissão Europeia, «Commission Staff Working Document – Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse» [Documento de trabalho dos serviços da Comissão – Relatório de avaliação de impacto que acompanha a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual de crianças], SWD(2022) 209 final («relatório de avaliação de impacto» ou «SWD(2022) 209 final»), p. 281, nota de rodapé n.º 511.

[35] Relatório de avaliação de impacto, p. 281.

[36] *Ibid.*, p. 282.

[37] *Ibid.*, p. 283.

comunicadas às autoridades policiais[38]. No entanto, apesar de – contrariamente ao disposto no regulamento provisório – a proposta ser aplicável também às comunicações áudio, o relatório de avaliação de impacto não especifica as soluções tecnológicas que poderiam ser utilizadas para detetar o aliciamento de crianças nesse contexto.

4.5.1 Eficácia da deteção

42. O respeito pelo princípio da necessidade exige uma avaliação factual da eficácia das medidas previstas para alcançar o objetivo prosseguido e implica avaliar se as mesmas são menos intrusivas do que outras opções para alcançar o mesmo objetivo[39]. Outro fator a ter em conta na avaliação da proporcionalidade de uma medida proposta é a maior eficácia das medidas existentes em relação à medida proposta[40]. Se já existirem medidas para uma finalidade idêntica ou semelhante, é necessário avaliar a sua eficácia no âmbito da avaliação da proporcionalidade. Sem essa avaliação da eficácia das medidas existentes com uma finalidade idêntica ou semelhante, não se pode considerar que o teste de proporcionalidade de uma nova medida tenha sido devidamente realizado.

43. A deteção de material referente a abusos sexuais de crianças ou do aliciamento de crianças por prestadores de serviços de armazenagem em servidor e prestadores de serviços de comunicações interpessoais pode contribuir para o objetivo global de prevenção e luta contra o abuso sexual de crianças e a difusão de material referente a abusos sexuais de crianças em linha. Simultaneamente, a necessidade de avaliar a eficácia das medidas previstas na proposta suscita três questões fundamentais:

- É possível contornar facilmente as medidas de deteção de abusos sexuais de crianças em linha?
- Que efeitos terão as atividades de deteção na ação das autoridades policiais[41]?
- De que forma a proposta reduziria a incerteza jurídica?

44. Não compete ao CEPD e à AEPD responder em pormenor a estas perguntas. No entanto, o CEPD e a AEPD observam que nem o relatório de avaliação de impacto nem a proposta abordam plenamente estas questões.

45. No que diz respeito à possibilidade de contornar a deteção de material referente a abusos sexuais de crianças, importa salientar que, atualmente, não parece existir para o efeito uma solução tecnológica que seja partilhada de forma cifrada. Por conseguinte, qualquer atividade de deteção – mesmo a

---

[38] Proposta, COM(2022)209 final, p. 14, nota de rodapé n.º 32.
[39] AEPD, «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit» [Guia para a avaliação da necessidade de medidas que limitem o direito fundamental à proteção de dados pessoais], 11 de abril de 2017, p. 5; AEPD, «EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data» [Orientações da AEPD sobre a avaliação da proporcionalidade de medidas que limitem os direitos fundamentais à privacidade e à proteção de dados pessoais] (19 de dezembro de 2019), p. 8.
[40] AEPD, «EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data» [Orientações da AEPD sobre a avaliação da proporcionalidade de medidas que limitem os direitos fundamentais à privacidade e à proteção de dados pessoais] (19 de dezembro de 2019), p. 11.
[41] De acordo com o relatório de avaliação de impacto (anexo II, p. 132), 85,71 % dos participantes no inquérito às autoridades policiais manifestaram preocupação com o aumento da quantidade de material referente a abusos sexuais de crianças na última década e com a falta de recursos (nomeadamente humanos e técnicos).

análise do lado do cliente destinada a contornar a cifragem de ponta a ponta oferecida pelo prestador de serviços[42] – pode ser facilmente contornada através da cifragem do conteúdo com a ajuda de uma aplicação separada antes do seu envio ou carregamento. Assim, as medidas de deteção previstas na proposta poderão ter menos impacto do que o esperado na difusão de material referente a abusos sexuais de crianças na Internet.

46. Além disso, a Comissão espera que a adoção das obrigações de deteção introduzidas pela proposta aumente o número de denúncias de abusos sexuais de crianças às autoridades policiais[43]. No entanto, nem a proposta nem o relatório de avaliação de impacto explicam de que forma tal permitirá colmatar as lacunas da situação atual. Tendo em conta os recursos limitados das autoridades policiais, afigura-se necessário compreender melhor se o aumento do número de denúncias teria um impacto significativo nas atividades das autoridades policiais contra o abuso sexual de crianças. Em todo o caso, o CEPD e a AEPD gostariam de salientar que essas denúncias devem ser avaliadas em tempo útil, a fim de assegurar que é tomada o mais cedo possível uma decisão sobre a relevância penal do material denunciado e de limitar, tanto quanto possível, a conservação de dados irrelevantes.

4.5.2 Inexistência de uma medida menos intrusiva

47. Mesmo que seja possível concretizar os efeitos positivos da deteção de material referente a abusos sexuais de crianças e do aliciamento de crianças previstos pela Comissão, a deteção tem de ser a medida menos intrusiva entre medidas igualmente eficazes. O artigo 4.º da proposta prevê que, numa primeira fase, os prestadores de serviços devem ponderar a adoção de medidas de atenuação para reduzir o risco de utilização do seu serviço para efeitos de abuso sexual de crianças em linha abaixo do limiar que justifica a emissão de uma ordem de deteção. Se existirem medidas de atenuação que possam conduzir a uma redução substancial da quantidade de situações de aliciamento de crianças ou material referente a abusos sexuais de crianças trocado no serviço em causa, essas medidas constituiriam frequentemente medidas menos intrusivas do que uma ordem de deteção[44]. Por conseguinte, caso o prestador de serviços em causa não adote tais medidas voluntariamente, a autoridade judicial ou autoridade administrativa independente competente deverá ter a possibilidade de tornar obrigatória e executória a aplicação de medidas de atenuação em vez de emitir uma ordem de deteção. Na opinião do CEPD e da AEPD, o facto de o artigo 5.º, n.º 4, da proposta permitir que a autoridade de coordenação «exija» ao prestador de serviços que introduza, reveja, suspenda ou alargue as medidas de atenuação não é suficiente, uma vez que tal requisito não seria executório de forma independente; o incumprimento apenas seria «sancionado» através da emissão de uma ordem de deteção.

48. Por conseguinte, o CEPD e a AEPD consideram que a autoridade de coordenação ou a autoridade judicial ou autoridade administrativa independente competente deve ser explicitamente habilitada a impor medidas de atenuação menos intrusivas antes ou em vez de emitir uma ordem de deteção.

---

[42] Ver também a secção 4.10 *infra*.

[43] Ver, nomeadamente, o relatório de avaliação de impacto, anexo 3, SWD(2022) 209 final, p. 176.

[44] Por exemplo, poderiam ser ponderadas medidas como o bloqueio, do lado do cliente, da transmissão de material referente a abusos sexuais de crianças, impedindo o carregamento e o envio de conteúdos das comunicações eletrónicas, uma vez que poderiam ajudar, em determinados contextos, a impedir a circulação de material referente a abusos sexuais de crianças conhecido.

4.5.3 Proporcionalidade em sentido estrito

49. Para que uma medida respeite o princípio da proporcionalidade consagrado no artigo 52.º, n.º 1, da Carta, as vantagens resultantes dessa medida não devem ser superadas pelas desvantagens que a medida acarreta no que respeita ao exercício dos direitos fundamentais. Por conseguinte, o princípio da proporcionalidade limita as autoridades no exercício dos seus poderes exigindo que se alcance um equilíbrio entre os meios utilizados e o objetivo prosseguido (ou o resultado alcançado)[45].

50. A fim de poder avaliar o impacto de uma medida nos direitos fundamentais à privacidade e à proteção dos dados pessoais, é particularmente importante identificar com precisão: [46]

- o **âmbito da medida**, incluindo o número de pessoas afetadas e se a mesma suscita «intrusões colaterais» (ou seja, ingerência na privacidade de pessoas que não as visadas pela medida);
- a **extensão da medida**, incluindo a quantidade de informações recolhidas; se a medida em apreço exige a recolha e o tratamento de categorias especiais de dados;
- o **nível de intrusão**, tendo em conta: a natureza da atividade sujeita à medida (se afeta ou não atividades abrangidas pelo dever de confidencialidade, relações entre advogados e clientes ou atividade médica); o contexto; se representa ou não uma definição de perfis das pessoas singulares em causa; se o tratamento implica a utilização de um sistema (parcial ou totalmente) automatizado de tomada de decisões com uma «margem de erro»;
- se diz ou não respeito a **pessoas vulneráveis**;
- se afeta também **outros direitos fundamentais** (por exemplo, o direito à liberdade de expressão, como nos processos Digital Rights Ireland e Seitlinger e outros e Tele2 Sverige e Watson)[47].

51. Neste contexto, é igualmente importante salientar que o impacto pode ser reduzido no que diz respeito à pessoa em causa, mas, ainda assim, ser significativo ou altamente significativo coletivamente/para a sociedade no seu conjunto[48].

52. Nos três tipos de ordens de deteção (deteção de material referente a abusos sexuais de crianças conhecido, material referente a abusos sexuais de crianças novo e aliciamento de crianças), as

---

[45] Ver processo C-343/09, Afton Chemical, n.º 45; processos apensos C-92/09 e C-93/09, Volker und Markus Schecke e Hartmut Eifert, n.º 74; processos C-581/10 e C-629/10, Nelson e outros, n.º 71; processo C-283/11, Sky Österreich, n.º 50; e processo C-101/12, Schaible, n.º 29. Ver também AEPD, «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit» [Guia para a avaliação da necessidade de medidas que limitem o direito fundamental à proteção de dados pessoais] (11 de abril de 2017).

[46] «EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data» [Orientações da AEPD sobre a avaliação da proporcionalidade de medidas que limitem os direitos fundamentais à privacidade e à proteção de dados pessoais] (19 de dezembro de 2019), p. 23.

[47] Ver também o Parecer 7/2020 da AEPD sobre a proposta de derrogações temporárias à Diretiva 2002/58/CE para efeitos de luta contra o abuso sexual de crianças em linha (10 de novembro de 2020), p. 9 e seguintes.

[48] «EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data» [Orientações da AEPD sobre a avaliação da proporcionalidade de medidas que limitem os direitos fundamentais à privacidade e à proteção de dados pessoais] (19 de dezembro de 2019), p. 20.

tecnologias atualmente disponíveis baseiam-se no tratamento automatizado de dados de conteúdo de todos os utilizadores afetados. As tecnologias utilizadas para analisar os conteúdos são frequentemente complexas, envolvendo normalmente a utilização de IA. Consequentemente, o comportamento desta tecnologia pode não ser totalmente compreensível para o utilizador do serviço. Além disso, sabe-se que as tecnologias atualmente disponíveis, em especial as que se destinam a detetar material referente a abusos sexuais de crianças novo ou aliciamento de crianças, apresentam taxas de erro relativamente elevadas[49]. Além disso, existe o risco de denúncia ao Centro da UE em conformidade com o artigo 12.º, n.º 1, e o artigo 48.º, n.º 1, da proposta, com base na deteção de «potencial» material referente a abusos sexuais de crianças.

53. Além disso, as condições gerais para a emissão de uma ordem de deteção ao abrigo da proposta, ou seja, aplicadas a um serviço completo e não apenas a comunicações selecionadas[50], a duração até 24 meses para material referente a abusos sexuais de crianças conhecido ou novo e até 12 meses para o aliciamento[51], etc., podem conduzir, na prática, a ordens com um âmbito de aplicação muito alargado. Consequentemente, na prática, a monitorização seria efetivamente de natureza geral e indiscriminada e não específica.

54. À luz do que precede, o CEPD e a AEPD estão também preocupados com os possíveis efeitos dissuasores do exercício da liberdade de expressão. O CEPD e a AEPD recordam que esse efeito dissuasor é considerado mais provável quanto menor for a clareza da legislação.

55. Na ausência da especificidade, da precisão e da clareza necessárias para que seja satisfeita a exigência da segurança jurídica[52], e tendo em conta o seu vasto âmbito de aplicação, ou seja, todos os prestadores de serviços da sociedade da informação relevantes que oferecem esses serviços na União[53], a proposta não garante que apenas existirá uma abordagem orientada para a deteção de material referente a abusos sexuais de crianças e do aliciamento de crianças. Por conseguinte, o CEPD e a AEPD consideram que, na prática, a proposta poderia tornar-se a base para uma análise generalizada e indiscriminada *de facto* do conteúdo de praticamente todos os tipos de comunicações eletrónicas de todos os utilizadores na UE/EEE. Consequentemente, a legislação pode levar as pessoas a absterem-se de partilhar conteúdos legais por receio de poderem ser visadas com base na sua ação.

56. Não obstante, o CEPD e a AEPD reconhecem que as diferentes medidas de combate ao abuso sexual de crianças em linha podem envolver diferentes níveis de intrusão. A título preliminar, o CEPD e a AEPD observam que a análise automatizada da voz ou do texto com vista a identificar potenciais casos de aliciamento de crianças é suscetível de constituir uma interferência mais significativa do que a correspondência de imagens ou vídeos com base em casos de material referente a abusos sexuais de crianças anteriormente confirmados, com vista a detetar a sua difusão. Além disso, deve ser feita uma distinção entre a deteção de «material referente a abusos sexuais de crianças conhecido» e de «material referente a abusos sexuais de crianças novo». É também importante diferenciar melhor o impacto das medidas destinadas aos prestadores de serviços de armazenagem em servidor e das medidas impostas aos prestadores de serviços de comunicações interpessoais.

[49] Ver mais pormenores *supra*, na secção 4.5, e *infra*, na subsecção 4.8.2.
[50] Ver artigo 7.º, n.º 1, da proposta.
[51] Ver artigo 7.º, n.º 9, terceiro parágrafo, da proposta.
[52] Ver TJUE, processo C-197/96, Comissão das Comunidades Europeias/República Francesa, n.º 15.
[53] Ver artigo 1.º, n.º 2, da proposta.

4.5.4 Deteção de material referente a abusos sexuais de crianças conhecido

57. Embora, de acordo com o considerando 4, a proposta deva ser «tecnologicamente neutra», tanto a eficácia das medidas de deteção propostas como o seu impacto nas pessoas singulares dependerão muito da escolha da tecnologia aplicada e dos indicadores selecionados. Este facto é reconhecido pela Comissão no relatório de avaliação de impacto (anexo 8)[54] e confirmado por outros estudos, como a avaliação de impacto substituta específica do Serviços de Estudos do Parlamento Europeu sobre a proposta relativa a uma derrogação temporária da Diretiva Privacidade Eletrónica para efeitos de luta contra o abuso sexual de crianças em linha, de fevereiro de 2021[55].

58. O artigo 10.º da proposta estabelece uma série de requisitos para as tecnologias a utilizar para efeitos de deteção, em especial no que diz respeito à sua eficácia, à sua fiabilidade e ao seu menor caráter intrusivo em termos de impacto nos direitos dos utilizadores à vida privada e familiar, incluindo a confidencialidade das comunicações, e à proteção dos dados pessoais.

59. Neste contexto, o CEPD e a AEPD observam que, atualmente, as únicas tecnologias que parecem ser capazes de cumprir, de um modo geral, estas normas são as utilizadas para detetar material referente a abusos sexuais de crianças conhecido, ou seja, as tecnologias de correspondência que utilizam uma base de dados de valores de dispersão como referência.

4.5.5 Deteção de material referente a abusos sexuais de crianças anteriormente desconhecido

60. A avaliação das medidas destinadas a detetar material referente a abusos sexuais de crianças (novo) anteriormente desconhecido conduz a conclusões diferentes quanto à sua eficácia, à sua fiabilidade e à limitação do impacto nos direitos fundamentais à privacidade e à proteção de dados.

61. Em primeiro lugar, tal como explicado no relatório de avaliação de impacto da proposta, as tecnologias atualmente utilizadas para a deteção de material referente a abusos sexuais de crianças anteriormente desconhecido incluem classificadores e IA. Um classificador é qualquer algoritmo que separa os dados em classes rotuladas, ou categorias de informação, mediante o reconhecimento de padrões[56]. Por conseguinte, estas tecnologias têm resultados e impactos diferentes em termos de exatidão, eficácia e nível de intrusão. Ao mesmo tempo, são também mais propensas a erros.

62. As técnicas utilizadas para detetar material referente a abusos sexuais de crianças anteriormente desconhecido são semelhantes às utilizadas para detetar o aliciamento de crianças, uma vez que ambas se baseiam não em tecnologias de correspondência simples, mas em modelos preditivos, que utilizam tecnologias de IA. O CEPD e a AEPD consideram que deve aplicar-se um elevado nível de prudência aquando da deteção de material referente a abusos sexuais de crianças anteriormente desconhecido, uma vez que um erro do sistema teria consequências graves para os titulares dos dados, que seriam automaticamente assinalados como possíveis autores de um crime muito grave, sendo os seus dados pessoais e os pormenores das suas comunicações objeto de denúncia.

---

[54] Ver informações sobre as taxas de falsos positivos no relatório de avaliação de impacto, anexo 8, p. 279 e seguintes.
[55] Ver a avaliação de impacto substituta específica sobre a proposta da Comissão relativa a uma derrogação temporária da Diretiva Privacidade Eletrónica para efeitos de luta contra o abuso sexual de crianças em linha (Serviço de Estudos do Parlamento Europeu, fevereiro de 2021), p. 14 e seguintes.
[56] Relatório de avaliação de impacto, anexo 8, p. 281.

63. Em segundo lugar, os indicadores de desempenho encontrados na literatura, alguns dos quais destacados no relatório de avaliação de impacto que acompanhou a proposta [57], fornecem muito poucas informações sobre as condições utilizadas para o seu cálculo e a sua adequação às condições reais, o que significa que o seu desempenho real pode ser significativamente inferior ao esperado, conduzindo a uma menor exatidão e a uma percentagem mais elevada de «falsos positivos».

64. Em terceiro lugar, os indicadores de desempenho devem ser considerados no contexto específico da utilização dos instrumentos de deteção pertinentes e proporcionar uma visão exaustiva do comportamento dos instrumentos de deteção. É um facto bem documentado que, ao utilizar algoritmos de inteligência artificial em imagens ou texto, podem ocorrer enviesamentos e discriminação devido à falta de representatividade de determinados grupos da população nos dados utilizados para treinar o algoritmo. Estes enviesamentos devem ser identificados, medidos e reduzidos a um nível aceitável, a fim de assegurar que os sistemas de deteção são verdadeiramente benéficos para a sociedade no seu conjunto.

65. Embora tenha sido realizado um estudo das tecnologias utilizadas para a deteção [58], o CEPD e a AEPD consideram que é necessária uma análise mais aprofundada para avaliar a fiabilidade dos instrumentos existentes. Esta análise deve basear-se em indicadores de desempenho exaustivos e avaliar o impacto de potenciais erros em condições reais para todos os titulares de dados abrangidos pela proposta.

66. Tal como acima referido, o CEPD e a AEPD têm sérias dúvidas quanto à medida em que as garantias processuais previstas no artigo 7.º, n.º 6, da proposta são suficientes para compensar estes riscos. Além disso, tal como indicado anteriormente, a proposta utiliza termos bastante abstratos e vagos para descrever a quantidade aceitável de risco (por exemplo, «de forma significativa»).

67. O CEPD e a AEPD receiam que estes conceitos amplos e vagos resultem em falta de segurança jurídica e originem também fortes divergências na aplicação concreta da proposta em toda a União, consoante as interpretações que serão dadas a conceitos como «probabilidade» e «de forma significativa» pelas autoridades judiciais ou outras autoridades administrativas independentes nos Estados-Membros. Esta situação é preocupante também à luz do facto de as disposições relativas às ordens de deteção constituírem «restrições» ao princípio da confidencialidade estabelecido no artigo 5.º da Diretiva Privacidade Eletrónica. Por conseguinte, é necessário melhorar a sua clareza e previsibilidade no regulamento proposto.

4.5.6 Deteção do aliciamento de crianças

68. O CEPD e a AEPD observam que as medidas propostas relativas à deteção do aliciamento de crianças, que implicam a análise automatizada de voz ou texto, são suscetíveis de constituir a ingerência mais significativa nos direitos dos utilizadores à vida privada e familiar, incluindo a confidencialidade das comunicações, e à proteção dos dados pessoais.

69. Embora o âmbito da deteção de material referente a abusos sexuais de crianças conhecido, ou mesmo novo, possa ser limitado à análise de imagens e vídeos, a deteção do aliciamento de crianças alargar-se-ia, por definição, a todas as comunicações por mensagens de texto (e possivelmente comunicações

[57] Relatório de avaliação de impacto, anexo 8, pp. 281-283.
[58] Relatório de avaliação de impacto, pp. 279 e seguintes.

áudio) abrangidas por uma ordem de deteção. Consequentemente, a intensidade da ingerência na confidencialidade das comunicações em causa é muito maior.

70. O CEPD e a AEPD consideram que uma análise automatizada geral e indiscriminada *de facto* das comunicações por mensagens de texto transmitidas através de serviços de comunicações interpessoais, com vista a identificar o potencial aliciamento de crianças, não respeita os requisitos de necessidade e proporcionalidade. Mesmo que a tecnologia utilizada se limite à utilização de indicadores, o CEPD e a AEPD consideram que a implantação dessa análise geral e indiscriminada é excessiva e pode mesmo afetar o conteúdo essencial do direito fundamental à privacidade consagrado no artigo 7.º da Carta.

71. Como já foi referido, a falta de garantias substantivas no contexto das medidas de deteção do aliciamento de crianças não pode ser compensada apenas por garantias processuais. Além disso, o problema da falta de clareza e segurança jurídicas suficientes (por exemplo, a utilização de linguagem jurídica vaga como «de forma significativa») é ainda mais grave no caso da análise automatizada de comunicações pessoais por mensagens de texto do que na comparação de fotografias baseada na tecnologia de dispersão.

72. Além disso, o CEPD e a AEPD consideram que o «efeito dissuasor» da liberdade de expressão é particularmente significativo quando as comunicações de texto (ou áudio) das pessoas singulares são escrutinadas e analisadas em grande escala. O CEPD e a AEPD recordam que esse efeito dissuasor é mais acentuado quanto menor for a clareza da legislação.

73. Além disso, tal como indicado no relatório de avaliação de impacto[59] e no estudo do Serviço de Estudos do Parlamento Europeu[60], a taxa de exatidão das tecnologias de deteção do aliciamento de crianças por mensagens de texto é muito inferior à taxa de exatidão das tecnologias de deteção de material referente a abusos sexuais de crianças conhecido[61]. As técnicas de deteção do aliciamento de crianças são concebidas para analisar e atribuir avaliações de probabilidade a cada aspeto da conversa, pelo que o CEPD e a AEPD também as consideram propensas a erros e vulneráveis a abusos.

4.5.7 Conclusão sobre a necessidade e a proporcionalidade das medidas previstas

74. No que diz respeito à necessidade e à proporcionalidade das medidas de deteção previstas, o CEPD e a AEPD estão particularmente preocupados com as medidas previstas para a deteção de material referente a abusos sexuais de crianças desconhecido e do aliciamento de crianças, devido ao seu nível de intrusão, decorrente da potencial concessão de acesso generalizado ao conteúdo das comunicações, à sua natureza probabilística e às taxas de erro associadas a essas tecnologias.

75. Além disso, é possível deduzir da jurisprudência do TJUE que as medidas que permitem às autoridades públicas ter acesso generalizado ao conteúdo de uma comunicação são mais suscetíveis de afetar o conteúdo essencial dos direitos garantidos pelos artigos 7.º e 8.º da Carta. Estas considerações são especificamente relevantes no que diz respeito às medidas para a deteção do aliciamento de crianças previstas na proposta.

[59] Relatório de avaliação de impacto, anexo 8, pp. 281-283.
[60] Páginas 15-18.
[61] Ver n.º 40 *supra*.

76. Em todo o caso, o CEPD e a AEPD consideram que a ingerência criada, em especial, pelas medidas de deteção do aliciamento de crianças vai além do estritamente necessário e proporcionado. Por conseguinte, estas medidas devem ser suprimidas da proposta.

4.6 Obrigações de denúncia

77. O CEPD e a AEPD recomendam que se complemente a lista de requisitos específicos em matéria de denúncias constante do artigo 13.º da proposta com a obrigação de incluir nas denúncias informações sobre a tecnologia específica que permitiu ao prestador de serviços tomar conhecimento dos conteúdos abusivos pertinentes, caso esse prestador de serviços tenha tido conhecimento do potencial abuso sexual de crianças na sequência de medidas tomadas para executar uma ordem de deteção emitida em conformidade com o artigo 7.º da proposta.

4.7 Obrigações de supressão e bloqueio

78. Uma das medidas previstas na proposta para atenuar os riscos de difusão de material referente a abusos sexuais de crianças é a emissão de ordens de supressão e bloqueio, que obrigariam os prestadores de serviços a suprimir ou desativar o acesso a material referente a abusos sexuais de crianças em linha ou a bloquear esse material[62].

79. Embora o impacto das ordens de supressão na proteção de dados e na privacidade das comunicações seja relativamente limitado, o CEPD e a AEPD recordam, a título geral, o princípio global a respeitar, segundo o qual qualquer medida deste tipo deve ser tão direcionada quanto possível.

80. Simultaneamente, o CEPD e a AEPD chamam a atenção para o facto de os prestadores de serviços de acesso à Internet só terem acesso ao URL exato do conteúdo se este for disponibilizado em texto simples. Sempre que os conteúdos são disponibilizados através de HTTPS, o prestador do serviço de acesso à Internet não tem acesso ao URL exato, a menos que decifre a cifragem da comunicação. Por conseguinte, o CEPD e a AEPD também têm dúvidas quanto à eficiência das medidas de bloqueio e consideram que seria desproporcionado exigir aos prestadores de serviços de acesso à Internet que decifrassem comunicações em linha para bloquear as que contêm material referente a abusos sexuais de crianças.

81. Além disso, e de um modo mais geral, importa salientar que o bloqueio (ou a desativação) do acesso a um elemento digital é uma operação que tem lugar a nível da rede e que a sua aplicação pode revelar-se ineficaz caso existam várias cópias (possivelmente semelhantes e não idênticas) do mesmo elemento. Ademais, essa operação pode revelar-se desproporcionada se o bloqueio afetar outros elementos digitais, não ilegais, quando conservados no mesmo servidor e tornados inacessíveis através de comandos de rede (por exemplo, endereço IP ou listas negras baseadas em DNS). Acresce que nem todas as abordagens de bloqueio a nível da rede são igualmente eficazes, podendo algumas ser facilmente contornadas com competências técnicas bastante rudimentares.

82. Por último, os poderes das autoridades de coordenação no que diz respeito à emissão de ordens de bloqueio devem ser clarificados no regulamento proposto. Por exemplo, a atual redação do

[62] Proposta, artigos 14.º e 16.º.

artigo 16.º, n.º 1, e do artigo 17.º, n.º 1, não esclarece se as autoridades de coordenação ficam habilitadas a emitir ordens de bloqueio ou apenas a solicitar a sua emissão[63].

4.8 Tecnologias e salvaguardas relevantes

4.8.1 Proteção de dados desde a conceção e por defeito

83. Os requisitos da proposta aplicáveis às tecnologias a utilizar para a deteção de material referente a abusos sexuais de crianças e do aliciamento de crianças não se afiguram suficientemente rigorosos. Em especial, o CEPD e a AEPD constataram que – contrariamente às disposições análogas do regulamento provisório[64] – a proposta não faz qualquer referência expressa ao princípio da proteção de dados desde a conceção e por defeito, nem estabelece que as tecnologias utilizadas para analisar o texto das comunicações não devem ser capazes de deduzir a substância do conteúdo das comunicações. A proposta prevê apenas, no artigo 10.º, n.º 3, alínea b), que as tecnologias devem permitir unicamente que sejam «extraídas» das comunicações pertinentes as informações estritamente necessárias para detetar. No entanto, esta norma não se afigura suficientemente rigorosa, uma vez que seria possível *deduzir* outras informações da substância do conteúdo de uma comunicação sem dela *extrair* informações enquanto tal.

84. Por conseguinte, a AEPD e o CEPD recomendam a introdução na proposta de um considerando que estipule que o princípio da proteção de dados desde a conceção e por defeito, estabelecido no artigo 25.º do Regulamento (UE) 2016/679, se aplica às tecnologias reguladas pelo artigo 10.º da proposta por força do direito, sem que, por conseguinte, seja necessário repeti-lo no texto jurídico. Além disso, cumpre alterar o artigo 10.º, n.º 3, alínea b), para garantir que não só não sejam extraídas, mas também não sejam deduzidas, outras informações, como atualmente previsto no artigo 3.º, n.º 1, alínea b), do regulamento provisório.

4.8.2 Fiabilidade das tecnologias

85. A proposta pressupõe que os prestadores de serviços podem utilizar vários tipos de soluções tecnológicas para executar ordens de deteção. Em especial, a proposta parte do princípio de que estão disponíveis sistemas de inteligência artificial que contribuem para a deteção de material referente a abusos sexuais de crianças desconhecido e para a deteção do aliciamento de crianças[65] e que podem ser considerados como os mais avançados por algumas autoridades de coordenação. Embora a eficácia da proposta dependa da fiabilidade destas soluções tecnológicas, há muito pouca informação disponível sobre a utilização generalizada e sistemática destas técnicas, o que justifica uma análise cuidadosa.

86. Além disso, embora o CEPD e a AEPD tenham sido obrigados a utilizá-los na sua avaliação da proporcionalidade, devido à falta de alternativas, importa salientar que os indicadores de desempenho das tecnologias de deteção mencionados no relatório de avaliação de impacto que

---

[63] O artigo 16.º, n.º 1, da proposta estabelece que «[a] autoridade de coordenação do local de estabelecimento tem poderes para solicitar à autoridade judicial competente do Estado-Membro que a designou, ou a uma autoridade administrativa independente desse Estado-Membro, que emita uma ordem de bloqueio […]», enquanto o artigo 17.º, n.º 1, estipula que «[a] autoridade de coordenação do local de estabelecimento deve […] emitir as ordens de bloqueio referidas no artigo 16.º […]» (sublinhado nosso).

[64] Regulamento provisório, artigo 3.º, n.º 1, alínea b).

[65] Ver o relatório de avaliação de impacto, pp. 281-282.

acompanhou a proposta fornecem muito poucas informações sobre a forma como foram avaliados e sobre se refletem o desempenho real das tecnologias pertinentes. Não existem informações sobre os testes ou os parâmetros de referência utilizados pelos fornecedores de tecnologias para medir esses desempenhos. Sem essas informações, não é possível replicar os testes ou avaliar a validade das declarações de desempenho. A este respeito, importa salientar que, embora os indicadores de desempenho possam ser interpretados como sugerindo que alguns instrumentos de deteção têm um elevado nível de exatidão (por exemplo, a exatidão de determinados instrumentos de deteção do aliciamento de crianças é de 88 %)[66], estes indicadores devem ser considerados à luz da utilização prática prevista dos instrumentos de deteção e da gravidade dos riscos que uma avaliação incorreta de um determinado material implicaria para os titulares de dados em causa. Além disso, o CEPD e a AEPD consideram que, com um tratamento de risco tão elevado, uma taxa de insucesso de 12 % representa um risco elevado para os titulares de dados que tenham sido objeto de falsos positivos, mesmo quando existem garantias para evitar denúncias falsas às autoridades policiais. É altamente improvável que os prestadores de serviços possam afetar recursos suficientes para rever essa percentagem de falsos positivos.

87. Tal como referido anteriormente[67], os indicadores de desempenho devem proporcionar uma visão exaustiva do comportamento dos instrumentos de deteção. É um facto bem documentado que, ao utilizar algoritmos de inteligência artificial em imagens ou texto, podem ocorrer enviesamentos e discriminação devido à falta de representatividade de determinados grupos da população nos dados utilizados para treinar o algoritmo. Estes enviesamentos devem ser identificados, medidos e reduzidos a um nível aceitável, a fim de assegurar que os sistemas de deteção são verdadeiramente proveitosos para a sociedade no seu conjunto.

88. Embora tenha sido realizado um estudo das tecnologias utilizadas para a deteção[68], o CEPD e a AEPD consideram que é necessária uma análise mais aprofundada para avaliar de forma independente a fiabilidade dos instrumentos existentes em casos de utilização real. Esta análise deve basear-se em indicadores de desempenho exaustivos e avaliar o impacto de potenciais erros em condições reais para todos os titulares de dados abrangidos pela proposta. Uma vez que estas tecnologias constituem a base em que assenta a proposta, o CEPD e a AEPD consideram que esta análise é da maior importância para avaliar a adequação da proposta.

89. O CEPD e a AEPD observam igualmente que a proposta não define requisitos tecnológicos específicos, seja no que diz respeito às taxas de erro, à utilização de classificadores e à sua validação, ou a outras restrições. Por conseguinte, tais critérios serão desenvolvidos na prática, ao avaliar a proporcionalidade da utilização de uma tecnologia específica, o que agrava ainda mais a falta de precisão e clareza.

90. Dada a importância das consequências para os titulares de dados em caso de falsos positivos, o CEPD e a AEPD consideram que as taxas de falsos positivos devem ser reduzidas ao mínimo e que esses sistemas devem ser concebidos tendo em conta que a grande maioria das comunicações eletrónicas não inclui qualquer material referente a abusos sexuais de crianças ou aliciamento de crianças, e também que mesmo uma taxa muito baixa de falsos positivos implicará um número muito elevado de falsos positivos, dado o volume de dados que serão objeto de deteção. De um modo mais geral, o CEPD e a AEPD também estão preocupados com o facto de o desempenho dos instrumentos

[66] *Ibid.*, p. 283.
[67] Ver pontos 63-64 *supra*.
[68] Ver o relatório de avaliação de impacto, pp. 279 e seguintes.

disponíveis indicado no relatório de avaliação de impacto não refletir indicadores precisos e comparáveis relativos a taxas de falsos positivos e falsos negativos e consideram que devem ser emitidos indicadores de desempenho comparáveis e significativos para essas tecnologias antes de os considerar disponíveis e eficientes.

4.8.3 Análise de comunicações áudio

91. Contrariamente ao regulamento provisório[69], a proposta não exclui do seu âmbito de aplicação a análise de comunicações áudio no contexto da deteção de aliciamento de crianças[70]. O CEPD e a AEPD consideram que a análise de comunicações áudio é particularmente intrusiva, uma vez que exigiria normalmente uma interceção ativa, contínua e «em direto». Além disso, em alguns Estados-Membros, a privacidade da palavra falada beneficia de uma proteção especial[71]. Ademais, uma vez que, em princípio, seria necessário analisar todo o conteúdo da comunicação áudio, esta medida é suscetível de afetar o conteúdo essencial dos direitos garantidos pelos artigos 7.º e 8.º da Carta. Por conseguinte, este método de deteção deve permanecer fora do âmbito das obrigações de deteção estabelecidas no regulamento proposto, tanto no que diz respeito às mensagens de voz como às comunicações em direto, tanto mais que o relatório de avaliação de impacto que acompanhou a proposta não identificou quaisquer riscos específicos ou alterações no cenário de ameaças que justificassem a sua utilização[72].

4.8.4 Verificação da idade

92. A proposta incentiva os prestadores de serviços a utilizarem medidas de verificação da idade e de avaliação da idade para identificar crianças utilizadoras nos seus serviços[73]. A este respeito, o CEPD e a AEPD observam que não existe atualmente uma solução tecnológica capaz de avaliar de forma inequívoca a idade de um utilizador num contexto em linha sem recorrer a uma identidade digital oficial, a qual, nesta fase, não está disponível para todos os cidadãos europeus[74]. Por conseguinte, a utilização prevista na proposta de medidas de verificação da idade poderia eventualmente conduzir à exclusão, por exemplo, de adultos com um aspeto jovem do acesso a serviços em linha, ou à utilização de ferramentas muito intrusivas de verificação da idade, o que poderia inibir ou desencorajar a utilização legítima dos serviços em causa.

93. A este respeito, e embora o considerando 16 da proposta se refira a ferramentas de controlo parental como possíveis medidas de atenuação, o CEPD e a AEPD recomendam que o regulamento proposto seja alterado de modo a permitir expressamente que os prestadores de serviços recorram a mecanismos de controlo parental adicional ou alternativamente à verificação da idade.

4.9 Conservação das informações

94. O artigo 22.º da proposta limita as finalidades para as quais os prestadores de serviços sujeitos à proposta podem conservar os dados de conteúdo e outros dados tratados no âmbito das medidas tomadas para cumprir as obrigações estabelecidas na proposta. No entanto, a proposta indica que os

[69] Ver o regulamento provisório, artigo 1.º, n.º 2.
[70] Ver proposta, artigo 1.º.
[71] Ver, por exemplo, o Código Penal alemão, secção 201.
[72] Ver o relatório de avaliação de impacto.
[73] Ver proposta, artigo 4.º, n.º 3, artigo 6.º, n.º 1, alínea c), e considerando 16.
[74] Ver, por exemplo, a recomendação n.º 7 da CNIL: verificar a idade da criança e o consentimento parental, respeitando simultaneamente a privacidade da criança (9 de agosto de 2021).

prestadores de serviços podem também conservar estas informações com o objetivo de melhorar a eficácia e a exatidão das tecnologias de deteção de abusos sexuais de crianças em linha com vista à execução de uma ordem de deteção, mas não podem conservar dados pessoais para esse efeito[75].

95. O CEPD e a AEPD consideram que apenas os prestadores de serviços que utilizam as suas próprias tecnologias de deteção devem ser autorizados a conservar dados para melhorar a eficácia e a exatidão das tecnologias, ao passo que os prestadores de serviços que utilizam tecnologias fornecidas pelo Centro da UE não devem beneficiar desta possibilidade. Além disso, o CEPD e a AEPD observam que, na prática, poderá ser difícil assegurar que não sejam armazenados dados pessoais para esse efeito, uma vez que a maioria dos dados de conteúdo e outros dados tratados para efeitos de deteção são suscetíveis de serem considerados dados pessoais.

4.10 Impacto na cifragem

96. As autoridades europeias de proteção de dados têm defendido sistematicamente a disponibilidade generalizada de ferramentas de cifragem robustas e medidas contra qualquer tipo de funções-alçapão[76], uma vez que a cifragem é importante para assegurar o exercício de todos os direitos humanos em linha e fora de linha[77]. Além disso, as tecnologias de cifragem contribuem de modo fundamental para o respeito pela vida privada e pela confidencialidade das comunicações, bem como para a inovação e o crescimento da economia digital, que depende do elevado nível de confiança e segurança proporcionado por essas tecnologias.

97. No contexto das comunicações interpessoais, a cifragem de ponta a ponta é um instrumento fundamental para garantir a confidencialidade das comunicações eletrónicas, uma vez que proporciona fortes salvaguardas técnicas contra o acesso ao conteúdo das comunicações por qualquer outra pessoa que não o remetente e o(s) destinatário(s), incluindo o prestador de serviços. Impedir ou desencorajar de qualquer forma a utilização da cifragem de ponta a ponta, impor aos prestadores de serviços a obrigação de tratar dados de comunicações eletrónicas para fins diferentes da prestação dos seus serviços, ou impor-lhes uma obrigação de transmitir proativamente comunicações eletrónicas a terceiros implicaria o risco de os prestadores de serviços oferecerem serviços menos cifrados, a fim de melhor cumprirem as suas obrigações, o que enfraqueceria o papel da cifragem em geral e comprometeria o respeito pelos direitos fundamentais dos cidadãos europeus. Note-se que, embora a cifragem de ponta a ponta seja uma das medidas de segurança mais frequentemente utilizadas no contexto das comunicações eletrónicas, outras soluções técnicas (por exemplo, a utilização de outros sistemas criptográficos) podem ser ou tornar-se igualmente importantes para garantir e proteger a confidencialidade das comunicações digitais. Por conseguinte, a sua utilização também não deve ser impedida ou desencorajada.

---

[75] Proposta, artigo 22.º, n.º 1.

[76] Ver, por exemplo, Grupo do Artigo 29.º para a Proteção de Dados, «Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU» [Declaração do Grupo do Artigo 29.º sobre a cifragem e o seu impacto na proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais] (11 de abril de 2018).

[77] Ver Conselho dos Direitos Humanos, Resolução 47/16 intitulada «The promotion, protection and enjoyment of human rights on the Internet» [A promoção, proteção e gozo dos direitos humanos na Internet], UN Doc. A/HRC/RES/47/16 (26 de julho de 2021).

98. A implantação de ferramentas para a interceção e análise de comunicações eletrónicas interpessoais é fundamentalmente contrária à cifragem de ponta a ponta, uma vez que esta última visa, do ponto de vista técnico, garantir que uma comunicação permanece confidencial entre o emissor e o recetor.

99. Por conseguinte, embora a proposta não estabeleça uma obrigação de interceção sistemática para os prestadores de serviços, é provável que a mera possibilidade de emissão de uma ordem de deteção afete fortemente as escolhas técnicas dos prestadores de serviços, especialmente tendo em conta o prazo limitado que terão para cumprir essa ordem e as pesadas sanções que lhes seriam aplicadas se não o fizessem[78]. Na prática, tal poderia conduzir determinados prestadores de serviços a deixar de utilizar a cifragem de ponta a ponta.

100. É necessário avaliar de forma adequada o impacto da desvalorização ou do desincentivo da utilização da encriptação de ponta a ponta que podem resultar da proposta. Cada uma das técnicas destinadas a contornar a função de preservação da privacidade da cifragem de ponta a ponta apresentadas no relatório de avaliação de impacto que acompanhou a proposta introduziria lacunas de segurança[79]. Por exemplo, a análise do lado do cliente[80] conduziria provavelmente a um acesso e tratamento substanciais e não direcionados de conteúdos não cifrados nos dispositivos dos utilizadores finais. Uma tal deterioração substancial da confidencialidade afetaria especialmente as crianças, uma vez que os serviços que utilizam são mais suscetíveis de serem visados por ordens de deteção, tornando-os vulneráveis à monitorização ou à escuta clandestina. Ao mesmo tempo, a análise *do lado do servidor* é também fundamentalmente incompatível com o paradigma da cifragem de ponta a ponta, uma vez que o canal de comunicação, cifrado posto-a-posto, teria de ser decifrado, conduzindo assim ao tratamento em larga escala de dados pessoais nos servidores dos prestadores de serviços.

101. Embora a proposta afirme que «deixa ao critério do prestador de serviços em causa a escolha das tecnologias a utilizar para cumprir eficazmente as ordens de deteção e [que o regulamento] não deve ser entendido como um incentivo ou desincentivo à utilização de uma determinada tecnologia»[81], a incompatibilidade estrutural de algumas ordens de deteção com a cifragem de ponta a ponta torna-se, com efeito, um forte desincentivo à utilização dessa tecnologia. A impossibilidade de aceder e utilizar serviços que utilizam a cifragem de ponta a ponta (que constituem as formas atualmente mais avançadas de garantia técnica de confidencialidade) pode ter um efeito dissuasor da liberdade de expressão e da utilização privada lícita dos serviços de comunicações eletrónicas. A relação antagónica entre a deteção de material referente a abusos sexuais de crianças ou do aliciamento de crianças e a cifragem de ponta a ponta é igualmente reconhecida pela Comissão quando assinala, no relatório de avaliação de impacto[82], que é provável que a aplicação da cifragem de ponta a ponta pelo Facebook em 2023 ponha termo ao seu escrutínio voluntário.

---

[78] Ver proposta, artigo 35.º.

[79] Ver secção 4.2 em Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague e Carmela Troncoso, «Bugs in our Pockets: The Risks of Client-Side Scanning» [Escutas nos nossos bolsos: os riscos da análise do lado do cliente], ArXiv abs/2110.07450 (2021).

[80] A análise do lado do cliente refere-se, em termos gerais, a sistemas que analisam o conteúdo das mensagens para obter correspondências com uma base de dados de conteúdos censuráveis antes de a mensagem ser enviada ao destinatário previsto.

[81] Proposta, considerando 26.

[82] Relatório de avaliação de impacto, p. 27.

102. A fim de assegurar que o regulamento proposto não compromete a segurança ou a confidencialidade das comunicações eletrónicas dos cidadãos europeus, o CEPD e a AEPD consideram que o dispositivo da proposta deve indicar claramente que nada no regulamento proposto deverá ser interpretado como uma proibição ou enfraquecimento da cifragem, em conformidade com o disposto no considerando 25 do regulamento provisório.

4.11 Supervisão, execução coerciva e cooperação

4.11.1 Papel das autoridades nacionais de controlo ao abrigo do RGPD

103. A proposta prevê a criação de uma rede de autoridades de coordenação nacionais, que serão responsáveis pela aplicação e execução coerciva do regulamento proposto[83]. Embora o considerando 54 da proposta afirme que «[a]s regras do [...] 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», o CEPD e a AEPD consideram que é importante enquadrar melhor a relação entre as atribuições das autoridades de coordenação e as atribuições das autoridades de proteção de dados e conferir a estas últimas um papel mais proeminente no regulamento proposto.

104. Em especial, os prestadores de serviços devem ser obrigados a consultar as autoridades de proteção de dados através de um procedimento de consulta prévia, tal como referido no artigo 36.º do RGPD, antes da aplicação de quaisquer medidas de deteção de material referente a abusos sexuais de crianças ou do aliciamento de crianças, e não exclusivamente no âmbito da utilização de medidas para detetar o aliciamento de crianças, conforme atualmente previsto na proposta[84] . Todas as medidas de deteção devem ser consideradas como conducentes a «risco elevado» por defeito, devendo, por conseguinte, ser submetidas a um procedimento de consulta prévia independentemente de dizerem respeito ao aliciamento de crianças ou a material referente a abusos sexuais de crianças, como já acontece ao abrigo do regulamento provisório[85]. Além disso, as autoridades de proteção de dados competentes, designadas ao abrigo do RGPD, devem ficar sempre habilitadas a apresentar os seus pontos de vista sobre as medidas de deteção previstas em qualquer situação e não apenas em circunstâncias específicas[86].

105. Além disso, o regulamento proposto deve criar um sistema para abordar e resolver os diferendos entre as autoridades competentes e as autoridades de proteção de dados em matéria de ordens de deteção. Em especial, as autoridades de proteção de dados devem ter o direito de contestar uma ordem de deteção junto dos tribunais do Estado-Membro da autoridade judicial ou autoridade administrativa independente competente que emitiu a ordem de deteção. A este respeito, o CEPD e a AEPD observam que, na versão atual da proposta, o parecer das autoridades de proteção de dados competentes pode ser rejeitado pela autoridade competente aquando da emissão de uma ordem de deteção. Tal poderá conduzir a decisões contraditórias, uma vez que as autoridades de proteção de dados, tal como confirmado pelo artigo 36.º, n.º 2, do RGPD, conservam todos os seus poderes de correção nos termos do artigo 58.º do RGPD, incluindo o poder de ordenar uma proibição do tratamento.

---

[83] Proposta, artigo 25.º.
[84] Proposta, artigo 7.º, n.º 3, segundo parágrafo, alínea b).
[85] Regulamento provisório, artigo 3.º, n.º 1, alínea c).
[86] Ver proposta, artigo 7.º, n.º 3, segundo parágrafo, alínea c).

4.11.2 Papel do CEPD

106. O CEPD e a AEPD observam que a proposta estabelece, no artigo 50.º, n.º 1, terceiro período, que «o Centro da UE deve solicitar o parecer do seu Comité da Tecnologia e do Comité Europeu para a Proteção de Dados» antes de acrescentar uma tecnologia específica às listas de tecnologias que os prestadores de serviços de armazenagem em servidor e os prestadores de serviços de comunicações interpessoais podem ponderar utilizar para executar ordens de deteção. A proposta prevê igualmente que o CEPD deve emitir os seus pareceres num prazo de oito semanas, que pode ser prorrogado por mais seis semanas, se necessário, em virtude da complexidade do assunto em apreço. A proposta estabelece ainda que o CEPD deve informar o Centro da UE de tal prorrogação no prazo de um mês a contar da data de receção do pedido de consulta, indicando os motivos do atraso.

107. As atuais atribuições do CEPD estão estabelecidas no artigo 70.º do RGPD e no artigo 51.º da Diretiva (UE) 2016/680 (Diretiva Proteção de Dados na Aplicação da Lei)[87]. Nestas atribuições, estabelece-se que o CEPD presta aconselhamento à Comissão e emite pareceres a pedido da Comissão, de uma autoridade nacional de controlo ou do seu próprio presidente. Embora o artigo 1.º, n.º 3, alínea d), da proposta afirme que esta não prejudica as regras estabelecidas no RGPD e na Diretiva Proteção de Dados na Aplicação da Lei, habilitar o Centro da UE a solicitar pareceres ao CEPD vai além das atribuições conferidas a este último ao abrigo desses atos legislativos. Por conseguinte, deve ficar claro no regulamento proposto – pelo menos num considerando – que a proposta alarga as atribuições do CEPD. A este respeito, o CEPD e a AEPD valorizam o importante papel que a proposta atribui ao CEPD, exigindo a sua participação na aplicação prática do regulamento proposto. Na prática, o Secretariado do CEPD desempenha um papel essencial na prestação do apoio analítico, administrativo e logístico necessário para a adoção dos pareceres do CEPD. Por conseguinte, a fim de assegurar que o CEPD e os seus membros conseguem exercer as suas atribuições, é essencial afetar um orçamento e pessoal suficientes ao Comité. Infelizmente, a ficha financeira legislativa da proposta não indica que serão disponibilizados recursos suplementares para o exercício das atribuições adicionais que a proposta confere ao CEPD[88].

108. Além disso, o CEPD e a AEPD observam que o artigo 50.º da proposta não indica de que forma procederá o Centro da UE após a receção de um parecer do CEPD[89]. O considerando 27 da proposta limita-se a afirmar que o aconselhamento prestado pelo CEPD deve ser tido em conta pelo Centro da UE e pela Comissão Europeia. Por conseguinte, importa clarificar qual será a finalidade do parecer solicitado no processo previsto no artigo 50.º da proposta e de que forma atuará o Centro da UE após a receção de um parecer do CEPD.

109. Além disso, o CEPD e a AEPD consideram que, embora quaisquer orientações ou eventuais pareceres do CEPD sobre a utilização de tecnologias de deteção avaliem a utilização dessas tecnologias a nível geral, uma consulta prévia nos termos do artigo 36.º do RGPD exigirá que a autoridade nacional de controlo tenha em conta as circunstâncias específicas e realize uma avaliação caso a caso do tratamento previsto pelo responsável pelo tratamento em causa. O CEPD e a AEPD observam que as

---

[87] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

[88] Ver proposta, pp. 105 e seguintes.

[89] Ver, em contraste, o artigo 51.º, n.º 4, da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

autoridades de controlo podem e devem aplicar os critérios estabelecidos no artigo 36.º do RGPD para decidir se é necessário prorrogar o prazo estabelecido no RGPD para emitir os seus pareceres em resposta a uma consulta prévia, não sendo necessário aplicar normas diferentes quando uma consulta prévia diga respeito à utilização de uma tecnologia de deteção[90].

110. Por último, na aplicação do artigo 11.º («Orientações relativas às obrigações de deteção»), a proposta estipula que a Comissão pode emitir orientações sobre a aplicação dos respetivos artigos 7.º a 10.º. O artigo 11.º da proposta deve ser alterado para deixar claro que, para além das autoridades de coordenação e do Centro da UE, a Comissão deve consultar o CEPD a respeito do projeto de orientações, fora do processo de consulta pública previsto, antes da emissão de orientações relativas às obrigações de deteção.

111. Por conseguinte, esta atribuição do CEPD, bem como o seu papel no quadro jurídico que seria introduzido pela proposta, justifica uma avaliação mais aprofundada por parte do legislador.

4.11.3 Papel do Centro da UE sobre o Abuso Sexual de Crianças

112. O capítulo IV da proposta criaria o Centro da UE, enquanto nova agência descentralizada para facilitar a aplicação da proposta. Entre outras tarefas, o Centro da UE deverá facilitar o acesso dos prestadores de serviços a tecnologias de deteção fiáveis; disponibilizar indicadores criados com base em abusos sexuais de crianças em linha confirmados por tribunais ou por autoridades administrativas independentes dos Estados-Membros para efeitos de deteção; prestar assistência, mediante pedido, no contexto da realização de avaliações de riscos; e prestar apoio na comunicação com as autoridades nacionais competentes[91].

113. A este respeito, o CEPD e a AEPD congratulam-se com o artigo 77.º, n.º 1, da proposta, que confirma que o tratamento de dados pessoais pelo Centro da UE está sujeito ao RPDUE, e com a especificação de que as medidas de aplicação do referido regulamento por parte do Centro da UE, incluindo as que dizem respeito à nomeação de um encarregado da proteção de dados do Centro da UE, são estabelecidas após consulta da AEPD. No entanto, o CEPD e a AEPD consideram que várias disposições do capítulo em causa merecem uma análise mais aprofundada.

114. Em primeiro lugar, o CEPD e a AEPD observam que o artigo 48.º da proposta prevê o reencaminhamento de todas as denúncias que não sejam manifestamente infundadas[92] para as autoridades policiais nacionais e para a Agência da União Europeia para a Cooperação Policial («Europol»). Este limiar a partir do qual o Centro da UE reencaminha denúncias para as autoridades policiais nacionais e para a Europol (denúncias que não sejam manifestamente infundadas) afigura-se demasiado baixo, especialmente tendo em conta que o objetivo da criação do Centro da UE, tal como estabelecido no relatório de avaliação de impacto da Comissão[93], é aliviar a pressão sobre as autoridades policiais e a Europol decorrente da filtragem de conteúdos incorretamente assinalados como material referente a abusos sexuais de crianças. A este respeito, não é claro por que razão o Centro da UE, enquanto plataforma de conhecimentos especializados, não poderia realizar uma

[90] Ver proposta, considerando 24.
[91] Ver COM(2022) 209 final, p. 8.
[92] O termo «manifestamente infundadas» é descrito no considerando 65 da proposta como aplicável aos «casos em que é imediatamente evidente, sem qualquer análise material de direito ou de facto, que as atividades denunciadas não constituem abuso sexual de crianças na Internet».
[93] Ver, por exemplo, a página 349 do relatório de avaliação de impacto.

avaliação jurídica e factual mais aprofundada para limitar os riscos de transmissão de dados de pessoas inocentes às autoridades policiais.

115. Em segundo lugar, a disposição relativa à duração da conservação de dados pessoais pelo Centro da UE afigura-se relativamente aberta, dada a sensibilidade dos dados em causa. Mesmo que não seja possível fixar um período máximo para a conservação desses dados, o CEPD e a AEPD recomendam que a proposta estabeleça, pelo menos, um prazo máximo para reavaliar a necessidade de continuar a conservá-los, exigindo uma justificação para prolongar a conservação após esse período.

116. Além disso, tendo em conta a enorme sensibilidade dos dados pessoais a tratar pelo Centro da UE, o CEPD e a AEPD consideram que o tratamento deve estar sujeito a garantias adicionais, em especial para assegurar uma supervisão eficaz. Tal poderá incluir a obrigação de o Centro da UE conservar registos cronológicos das operações de tratamento em sistemas automatizados de tratamento de dados (ou seja, refletindo o requisito relativo aos dados pessoais operacionais previsto no capítulo IX do RPDUE), incluindo o registo cronológico da introdução, alteração, acesso, consulta, divulgação, combinação e apagamento de dados pessoais. Os registos cronológicos das operações de consulta e divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identidade da pessoa que consultou ou divulgou os dados pessoais operacionais e, na medida do possível, a identidade dos destinatários. Tais registos cronológicos seriam utilizados para efeitos de verificação da licitude do tratamento, de autocontrolo e de garantia da integridade e segurança dos dados pessoais operacionais, sendo disponibilizados, a pedido, ao encarregado da proteção de dados do Centro da UE e à AEPD.

117. Além disso, a proposta faz referência à obrigação de os prestadores de serviços informarem os utilizadores sobre a deteção de material referente a abusos sexuais de crianças através de ordens de deteção, bem como ao direito de apresentar uma queixa a uma autoridade de coordenação[94]. No entanto, a proposta não estabelece procedimentos para o exercício dos direitos dos titulares dos dados, tendo igualmente em conta os múltiplos locais onde os dados pessoais podem ser transmitidos e conservados ao abrigo da proposta (Centro da UE, Europol, serviços nacionais responsáveis pela aplicação da lei). A obrigação de informar os utilizadores deve incluir a obrigação de informar as pessoas singulares que os seus dados foram reencaminhados e estão a ser tratados por diferentes entidades, se for caso disso (por exemplo, pelos serviços nacionais responsáveis pela aplicação da lei e pela Europol). Além disso, deverá existir um procedimento centralizado para a receção e coordenação dos pedidos de direito de acesso, retificação e apagamento ou, em alternativa, a obrigação de a entidade que recebe um pedido de um titular dos dados se coordenar com as outras entidades em causa.

118. O CEPD e a AEPD observam que, nos termos do artigo 50.º da proposta, cabe ao Centro da UE especificar a lista das tecnologias que podem ser utilizadas para executar ordens de deteção. No entanto, nos termos do artigo 12.º, n.º 1, da proposta, os prestadores de serviços são obrigados a comunicar todas as informações que indiquem um potencial abuso sexual de crianças nos serviços que presta na Internet e não apenas as que resultam da execução de uma ordem de deteção. É altamente provável que uma quantidade significativa dessas informações resulte da gestão das medidas de atenuação dos prestadores de serviços, em conformidade com o artigo 4.º da proposta. Por conseguinte, afigura-se fundamental determinar que medidas poderão estar em causa, a sua eficácia, a sua taxa de erro na denúncia de potenciais abusos sexuais de crianças e o seu impacto nos

[94] Ver artigo 10.º, n.º 6, e, após a apresentação de uma denúncia ao Centro da UE, o artigo 12.º, n.º 2, da proposta.

direitos e liberdades das pessoas singulares. Embora o artigo 4.º, n.º 5, da proposta estabeleça que a Comissão, em cooperação com as autoridades de coordenação e o Centro da UE e após consulta pública, pode emitir orientações pertinentes, o CEPD e a AEPD consideram importante que, no artigo 50.º, o legislador encarregue o Centro da UE de fornecer também uma lista das medidas de atenuação recomendadas e das melhores práticas pertinentes que são eficazes, em especial, na identificação de potenciais abusos sexuais de crianças em linha. Uma vez que tais medidas podem interferir com os direitos fundamentais à proteção de dados e à privacidade, recomenda-se igualmente que o Centro da UE solicite o parecer do CEPD antes de emitir essa lista.

119. Por último, os requisitos de segurança estabelecidos no artigo 51.º, n.º 4, da proposta devem ser mais específicos. A este respeito, é possível obter inspiração nos requisitos de segurança estabelecidos noutros regulamentos relativos a sistemas de grande escala que implicam tratamento de elevado risco, como o Regulamento (CE) n.º 767/2008[95] (ver artigo 32.º), o Regulamento (CE) n.º 1987/2006[96] (ver artigo 16.º), o Regulamento (UE) 2018/1862 [97] (ver artigo 16.º) e o Regulamento (UE) n.º 603/2013[98] (ver artigo 34.º).

4.11.4 Papel da Europol

120. A proposta prevê uma estreita cooperação entre o Centro da UE e a Europol. Nos termos do capítulo IV da proposta, após receber denúncias de prestadores de serviços sobre presumível material referente a abusos sexuais de crianças, o Centro da UE deve verificá-las para avaliar quais as denúncias que podem ser objeto de ação (não manifestamente infundadas) e reencaminhá-las para a Europol, bem como para as autoridades policiais nacionais[99]. O Centro da UE deve conceder à Europol acesso às suas bases de dados de indicadores e bases de dados de denúncias para apoiar os inquéritos da Europol sobre presumíveis crimes de abuso sexual de crianças[100]. Além disso, o Centro da UE teria o

[95] Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração (Regulamento VIS) (JO L 218 de 13.8.2008, p. 60).

[96] Regulamento (CE) n.º 1987/2006 do Parlamento Europeu e do Conselho, de 20 de dezembro de 2006, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SIS II) (JO L 381 de 28.12.2006, p. 4).

[97] Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

[98] Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva do Regulamento (UE) n.º 604/2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera o Regulamento (UE) n.º 1077/2011 que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça (JO L 180 de 29.6.2013, p. 1).

[99] Ver artigo 48.º da proposta.

[100] Ver artigo 46.º, n.os 4 e 5, da proposta.

«mais amplo acesso possível» aos sistemas de informação da Europol[101]. As duas agências partilharão igualmente instalações e determinadas infraestruturas (não operacionais)[102].

121. O CEPD e a AEPD observam que vários aspetos relacionados com a cooperação entre o Centro da UE proposto e a Europol suscitam preocupações ou devem ser mais especificados.

Sobre o reencaminhamento de denúncias do Centro da UE para a Europol (artigo 48.º)

122. O artigo 48.º do regulamento proposto exige que o Centro da UE reencaminhe as denúncias que não sejam consideradas manifestamente infundadas, juntamente com quaisquer informações adicionais pertinentes, para a Europol e para a autoridade ou autoridades policiais competentes dos Estados-Membros suscetíveis de serem competentes para investigar ou instaurar ações penais relativas ao potencial abuso sexual de crianças. Embora o referido artigo encarregue a Europol de identificar a autoridade policial competente quando não é claro qual é o Estado-Membro em causa, a disposição prevê, de facto, que todas as denúncias sejam transmitidas à Europol, independentemente de a autoridade nacional ter sido identificada e já ter recebido a denúncia transmitida pelo Centro da UE.

123. No entanto, a proposta não esclarece qual seria o valor acrescentado da participação da Europol ou como deveria esta proceder após a receção das denúncias, em especial nos casos em que a autoridade policial nacional tenha sido identificada e notificada paralelamente[103].

124. O CEPD e a AEPD recordam que o mandato da Europol consiste apenas em apoiar a ação das autoridades competentes dos Estados-Membros e a sua cooperação mútua em matéria de prevenção e luta contra a criminalidade grave que afete dois ou mais Estados-Membros[104]. O artigo 19.º do Regulamento (UE) 2016/794[105], com a redação que lhe foi dada pelo Regulamento (UE) 2022/991[106] («Regulamento Europol alterado»), estabelece que um organismo da União que forneça informações à Europol é obrigado a determinar a finalidade, ou as finalidades, para que a Europol trata essas informações, bem como as condições para esse tratamento. É igualmente responsável por assegurar a exatidão dos dados pessoais transferidos[107].

125. Por conseguinte, um reencaminhamento geral de denúncias para a Europol violaria o Regulamento Europol alterado e acarretaria uma série de riscos em matéria de proteção de dados. A duplicação do tratamento de dados pessoais poderia levar a que fossem conservadas paralelamente várias cópias dos mesmos dados pessoais altamente sensíveis (por exemplo, no Centro da UE, na Europol, na

[101] Ver artigo 53.º, n.º 2, da proposta.
[102] Nomeadamente as relacionadas com a gestão dos recursos humanos, tecnologias da informação (TI), incluindo cibersegurança, edifício e comunicações.
[103] O considerando 71 da proposta faz apenas uma referência geral à experiência da Europol na identificação das autoridades nacionais competentes em situações pouco claras e à sua base de dados de informações criminais, que pode contribuir para identificar ligações a inquéritos noutros Estados-Membros.
[104] Ver artigo 3.º do Regulamento Europol alterado.
[105] Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, p. 53).
[106] Regulamento (UE) 2022/991 do Parlamento Europeu e do Conselho, de 8 de junho de 2022, que altera o Regulamento (UE) 2016/794 no que diz respeito à cooperação da Europol com os organismos privados, ao tratamento de dados pessoais pela Europol para apoiar investigações criminais, e ao papel da Europol na investigação e inovação (JO L 169 de 27.6.2022, p. 1).
[107] Artigo 38.º, n.º 2, alínea a), do Regulamento Europol alterado.

autoridade policial nacional), o que comportaria riscos para a exatidão dos dados em resultado da potencial dessincronização das bases de dados, bem como para o exercício dos direitos dos titulares dos dados. Além disso, devido ao limiar baixo estabelecido na proposta para a partilha de denúncias com as autoridades policiais (denúncias não manifestamente infundadas), existe uma elevada probabilidade de os falsos positivos (ou seja, conteúdos incorretamente assinalados como relacionados com o abuso sexual de crianças) serem conservados nos sistemas de informação da Europol, potencialmente durante períodos prolongados[108].

126. Por conseguinte, o CEPD e a AEPD recomendam que a proposta especifique e limite as circunstâncias e as finalidades que justificam o reencaminhamento de denúncias do Centro da UE para a Europol, em conformidade com o Regulamento Europol alterado. Tal deverá excluir explicitamente as circunstâncias em que as denúncias foram transmitidas à autoridade policial do Estado-Membro em causa, o que não implica qualquer dimensão transfronteiriça. Além disso, a proposta deve exigir que o Centro da UE apenas transfira para a Europol dados pessoais adequados, pertinentes e limitados ao que é estritamente necessário. Devem também ser previstas garantias específicas para assegurar a qualidade e a fiabilidade dos dados.

[108] De acordo com o relatório de avaliação de impacto da Comissão, a Europol apenas pôde examinar 20 % dos 50 milhões de imagens e vídeos únicos de material referente a abusos sexuais de crianças na sua base de dados, o que sugere que faltam recursos para fazer face aos materiais referentes a abusos sexuais de crianças que recebe atualmente. Ver o relatório de avaliação de impacto que acompanha a proposta de regulamento que estabelece regras para prevenir e combater o abuso sexual de crianças, SWD(2022) 209, pp. 47-48.

Artigo 53.º, n.º 2, relativo à cooperação entre o Centro da UE e a Europol

127. O artigo 53.º, n.º 2, da proposta exige que a Europol e o Centro da UE facultem um ao outro «o mais amplo acesso possível às informações e aos sistemas de informação pertinentes, sempre que necessário para o desempenho das respetivas atribuições e em conformidade com os atos legislativos da União que regem esse acesso».

128. O artigo 46.º, n.os 4 e 5, da proposta especificam que a Europol deve ter acesso à base de dados de indicadores e à base de dados de denúncias do Centro da UE, e o artigo 46.º, n.º 6, estabelece o procedimento para a concessão desse acesso: a Europol apresenta um pedido, especificando a finalidade do pedido e o grau de acesso necessário para alcançar essa finalidade, que deve ser devidamente avaliado pelo Centro da UE.

129. A proposta não especifica os critérios e as garantias que condicionam o acesso da Europol e a subsequente utilização dos dados obtidos a partir dos sistemas de informação do Centro da UE. Além disso, não explica por que motivo é necessário conceder à Europol acesso direto aos sistemas de informação de um serviço não policial, que contêm dados pessoais altamente sensíveis, eventualmente sem ter comprovado a sua ligação à atividade criminosa e à prevenção da criminalidade. A fim de assegurar um elevado nível de proteção de dados e o cumprimento do princípio da limitação da finalidade, o CEPD e a AEPD recomendam que a transmissão de dados pessoais do Centro da UE para a Europol só se possa realizar caso a caso, na sequência de um pedido devidamente avaliado e através de uma ferramenta de intercâmbio seguro de comunicações, como a rede SIENA[109].

130. O artigo 53.º, n.º 2, constitui a única referência na proposta ao acesso do Centro da UE aos sistemas de informação da Europol. Por conseguinte, não é claro para que finalidades, e com que garantias específicas, esse acesso teria lugar.

131. O CEPD e a AEPD recordam que a Europol é um serviço responsável pela aplicação da lei, criado ao abrigo dos Tratados da UE, que tem como mandato principal a prevenção e luta contra a criminalidade grave. Consequentemente, os dados pessoais operacionais tratados pela Europol estão sujeitos a regras e garantias rigorosas em matéria de tratamento de dados. O Centro da UE proposto não é um organismo responsável pela aplicação da lei e não deve, em caso algum, ter acesso direto aos sistemas de informação da Europol.

132. O CEPD e a AEPD observam ainda que grande parte das informações de interesse comum para o Centro da UE e a Europol dirão respeito a dados pessoais relativos a vítimas de alegados crimes, dados pessoais de menores e dados pessoais relativos à vida sexual, que representam categorias especiais de dados pessoais ao abrigo do Regulamento Europol alterado. O Regulamento Europol alterado impõe condições rigorosas no que diz respeito ao acesso a categorias especiais de dados pessoais. O artigo 30.º, n.º 3, do Regulamento Europol alterado estabelece que apenas a Europol tem acesso direto a esses dados pessoais, mais concretamente um número limitado de funcionários da Europol devidamente autorizados pelo diretor executivo[110].

133. Por conseguinte, o CEPD e a AEPD recomendam que se clarifique a redação do artigo 53.º, n.º 2, da proposta, a fim de refletir adequadamente as restrições em vigor ao abrigo do Regulamento Europol

[109] Aplicação de Intercâmbio Seguro de Informações.

[110] O Regulamento Europol alterado prevê exceções a esta proibição para as agências da União criadas ao abrigo do título V do TFUE. No entanto, dada a base jurídica da proposta (artigo 114.º do TFUE, relativo à harmonização do mercado interno), esta exceção não incluiria o Centro da UE proposto.

alterado e especificar as modalidades de acesso do Centro da UE. Em especial, qualquer acesso aos dados pessoais tratados nos sistemas de informação da Europol, sempre que tal seja considerado estritamente necessário para o exercício das atribuições do Centro da UE, só deverá ser concedido caso a caso, mediante a apresentação de um pedido explícito, que documente a sua finalidade específica e a sua justificação. A Europol deverá ser obrigada a apreciar diligentemente esses pedidos e apenas transmitir dados pessoais ao Centro da UE se tal for estritamente necessário e proporcional à finalidade pretendida.

Artigo 10.º, n.º 6, relativo ao papel da Europol na informação dos utilizadores na sequência da execução de uma ordem de deteção

134. O CEPD e a AEPD congratulam-se com a obrigação, estabelecida no artigo 10.º, n.º 6, da proposta, de os prestadores de serviços informarem os utilizadores cujos dados pessoais possam ser afetados pela execução de uma ordem de deteção. Estas informações só devem ser fornecidas aos utilizadores depois de a Europol ou a autoridade policial nacional de um Estado-Membro que recebeu a denúncia nos termos do artigo 48.º ter confirmado que o fornecimento de informações aos utilizadores não interfere em atividades de prevenção, deteção, investigação e ação penal respeitantes a crimes de abuso sexual de crianças.

135. No entanto, falta especificidade quanto à aplicação prática desta disposição. Nos casos em que as denúncias são reencaminhadas tanto para a Europol como para uma autoridade policial de um Estado-Membro, a proposta não estipula se é necessária uma confirmação de um ou de ambos os destinatários, nem os procedimentos/modalidades de obtenção dessa confirmação são especificados na proposta (por exemplo, se as confirmações devem ser enviadas através do Centro da UE). Tendo em conta o elevado volume de material referente a abusos sexuais de crianças que a Europol e as autoridades policiais nacionais poderão ter de tratar, bem como a ausência de um prazo preciso para a apresentação da confirmação («sem demora injustificada»), o CEPD e a AEPD recomendam que se clarifiquem os procedimentos aplicáveis, a fim de assegurar a concretização prática desta garantia. Além disso, a obrigação de informar os utilizadores deve também incluir informações sobre os destinatários dos dados pessoais em causa.

Sobre a recolha de dados e a apresentação de relatórios de transparência (artigo 83.º)

136. O artigo 83.º, n.º 3, da proposta prevê que o Centro da UE recolha dados e elabore estatísticas relativas a algumas das suas atribuições ao abrigo do regulamento proposto. Para efeitos de acompanhamento, o CEPD e a AEPD recomendam que esta lista inclua também estatísticas sobre o número de denúncias reencaminhadas para a Europol em conformidade com o artigo 48.º, bem como sobre o número de pedidos de acesso recebidos pela Europol nos termos do artigo 46.º, n.ºs 4 e 5, incluindo o número de pedidos deferidos e indeferidos pelo Centro da UE.

5. CONCLUSÃO

137. Embora se congratulem com os esforços da Comissão para assegurar uma ação eficaz contra o abuso sexual de crianças em linha, o CEPD e a AEPD consideram que a proposta suscita graves preocupações em matéria de proteção de dados e privacidade. Por conseguinte, o CEPD e a AEPD convidam os colegisladores a alterarem o regulamento proposto, em especial para assegurar que as obrigações de deteção previstas cumprem as normas aplicáveis em matéria de necessidade e proporcionalidade e não resultam no enfraquecimento ou deterioração da cifragem a nível geral. O CEPD e a AEPD

permanecem disponíveis para prestar apoio durante o processo legislativo, caso o seu contributo seja considerado necessário para dar resposta às preocupações salientadas no presente parecer conjunto.

Pela Autoridade Europeia para a Proteção de Dados	Pelo Comité Europeu para a Proteção de Dados
A Autoridade Europeia para a Proteção de Dados	A Presidente
(Wojciech Wiewiorowski)	(Andrea Jelinek)