COMISSÃO
EUROPEIA

Bruxelas, 25.7.2024
COM(2024) 357 final

# COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

## Segundo relatório sobre a aplicação do Regulamento Geral sobre a Proteção de Dados

## 1 INTRODUÇÃO

O presente documento é o segundo relatório da Comissão sobre a aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD), adotado em conformidade com o artigo 97.º do mesmo regulamento. O primeiro relatório foi adotado em 24 de junho de 2020 («o relatório de 2020») [(1)].

O RGPD é uma das pedras angulares da abordagem da UE para a transformação digital. Os seus princípios básicos — tratamento leal, seguro e transparente dos dados pessoais, assegurando que as pessoas continuam a ter o controlo dos mesmos — estão subjacentes a todas as políticas da UE que envolvem o tratamento de dados pessoais.

Desde o relatório de 2020, a UE adotou uma série de iniciativas que visam colocar as pessoas no centro da transição digital. Cada iniciativa tem um objetivo específico, nomeadamente criar um ambiente em linha mais seguro, tornar a economia digital mais justa e mais competitiva, facilitar a investigação pioneira, assegurar o desenvolvimento de uma inteligência artificial (IA) segura e fiável e criar um verdadeiro mercado único dos dados. Sempre que estão em causa dados pessoais, estas iniciativas baseiam-se no RGPD, que proporciona igualmente uma base para iniciativas setoriais com impacto no tratamento de dados pessoais, por exemplo, nos domínios dos serviços financeiros, da saúde, do emprego, da mobilidade e da aplicação da lei.

Existe um amplo consenso entre as partes interessadas, as autoridades de proteção de dados e os Estados-Membros de que, apesar de algumas dificuldades, o RGPD proporcionou resultados significativos às pessoas e às empresas. A abordagem baseada no risco e tecnologicamente neutra confere uma forte proteção aos titulares dos dados e impõe obrigações proporcionadas aos responsáveis pelo tratamento e aos executantes do tratamento. Ao mesmo tempo, são necessários mais progressos em vários domínios. Em especial, nos próximos anos, há que colocar a tónica no apoio aos esforços de conformidade das partes interessadas, em especial as pequenas e médias empresas (PME), os pequenos operadores, bem como os investigadores e as organizações de investigação, assegurando orientações mais claras e mais úteis por parte das autoridades de proteção de dados e alcançando uma interpretação e aplicação mais coerentes do RGPD em toda a UE.

Nos termos do artigo 97.º do RGPD, a Comissão deve examinar, em especial, a aplicação e o funcionamento da transferência internacional de dados pessoais para países terceiros (ou seja, países fora da UE/EEE) (capítulo V do RGPD) e os procedimentos de cooperação e de controlo da coerência entre as autoridades nacionais de proteção de dados (capítulo VII do RGPD). No entanto, tal como no relatório de 2020, o presente relatório apresenta uma avaliação geral da aplicação do RGPD que vai além destes dois elementos. Identifica igualmente uma série de ações necessárias para apoiar a aplicação efetiva do RGPD em domínios prioritários fundamentais.

O presente relatório tem em conta as seguintes fontes: i) o documento sobre a posição e conclusões do Conselho, adotado em dezembro de 2023 ([2]); ii) contributos recolhidos junto das partes interessadas, em especial através do grupo multilateral sobre o RGPD ([3]) e de

---

([1]) A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital — dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados, 24.6.2020, COM(2020) 264 final.

([2]) https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/pt/pdf

([3]) Está disponível um resumo dos contributos do grupo de peritos multilateral sobre o RGPD em: Report from Multistakeholder Expert group on GDPR application - June 2024.pdf. Os contributos recebidos em

um convite público à apreciação ([4]); e iii) informações das autoridades de proteção de dados (através do contributo do Comité Europeu para a Proteção de Dados ([5]) («o Comité») e de um relatório elaborado pela Agência dos Direitos Fundamentais (FRA) com base em entrevistas realizadas com autoridades de proteção de dados individuais ([6]) («o relatório da FRA»). O presente relatório baseia-se igualmente no acompanhamento contínuo da aplicação do RGPD pela Comissão, incluindo diálogos bilaterais com os Estados-Membros sobre a conformidade da legislação nacional, um contributo ativo para os trabalhos do Comité e contactos estreitos com um vasto leque de partes interessadas sobre a aplicação prática do Regulamento.

## 2 APLICAÇÃO DO RGPD E FUNCIONAMENTO DOS PROCEDIMENTOS DE COOPERAÇÃO E DE CONTROLO DA COERÊNCIA

O sistema de balcão único para a aplicação do RGPD visa assegurar uma interpretação e aplicação harmonizadas pelas autoridades independentes de proteção de dados. Exige a cooperação entre as autoridades de proteção de dados nos casos de tratamento transfronteiriço, em que titulares dos dados de vários Estados-Membros são substancialmente afetados. Os litígios entre autoridades são resolvidos pelo Comité ao abrigo do procedimento de controlo da coerência do RGPD.

### 2.1 Aumentar a eficiência do tratamento dos casos transfronteiriços: a proposta relativa às normas processuais

O relatório de 2020 salientou a necessidade de um tratamento mais eficiente e harmonizado dos casos transfronteiriços em toda a UE, em especial tendo em conta as grandes diferenças nos procedimentos administrativos nacionais e nas interpretações de conceitos no mecanismo de cooperação do RGPD. Por conseguinte, em julho de 2023, a Comissão adotou uma proposta de regulamento relativo às normas processuais ([7]), com base também numa lista de questões apresentada pelo Comité à Comissão em outubro de 2022 ([8]), bem como nos contributos das partes interessadas ([9]) e dos Estados-Membros ([10]). A proposta completa o RGPD, estabelecendo regras pormenorizadas sobre as reclamações transfronteiriças, a participação do autor da reclamação, os direitos processuais das partes objeto de investigação (responsáveis pelo tratamento e executantes do tratamento) e a cooperação entre as autoridades de proteção de dados. A harmonização destes aspetos processuais favoreceria a conclusão atempada das investigações e a disponibilização de vias de recurso rápidas para os particulares. A proposta encontra-se atualmente em fase de negociação no Parlamento Europeu e no Conselho.

---

resposta ao convite público à apreciação e através de reuniões bilaterais com as partes interessadas refletem, em grande medida, os pontos de vista expressos pelos membros do grupo de peritos multilateral sobre o RGPD.

([4]) https://ec.europa.eu/info/law/better-regulation/have-your-say_pt

([5]) *Contribution of the EDPB to the evaluation of the GDPR under Article 97* | Comité Europeu para a Proteção de Dados (europa.eu) (não traduzido para português).

([6]) *GDPR in practice – Experiences of data protection authorities* | Agência dos Direitos Fundamentais da União Europeia (europa.eu) (não traduzido para português)

([7]) Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece normas processuais adicionais relativas à aplicação do Regulamento (UE) 2016/679 [COM(2023) 348 final].

([8]) https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_pt.

([9]) Através do grupo de peritos multilateral sobre o RGPD e de um convite à apreciação lançado em fevereiro de 2023.

([10]) Nomeadamente através do grupo de peritos dos Estados-Membros no âmbito do RGPD: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=pt&do=groupDetail.groupDetail&groupID=3461

### 2.2 Reforço da cooperação entre as autoridades de proteção de dados e utilização do procedimento de controlo da coerência

O número de processos transfronteiriços aumentou significativamente nos últimos anos. As autoridades de proteção de dados mostraram-se mais disponíveis para utilizar os instrumentos de cooperação previstos no RGPD. Todas as autoridades de proteção de

dados utilizaram o instrumento de assistência mútua ([11]), bem como pedidos «informais» de assistência mútua numa base voluntária. As autoridades de proteção de dados privilegiam os pedidos informais, que não impõem um prazo ou um dever estrito de resposta. Embora o Comité tenha adotado orientações sobre as operações conjuntas em

([11]) Artigo 61.º do RGPD.

2021 ([12]), as autoridades ainda não utilizaram significativamente este instrumento ([13]) e indicam as diferenças nos procedimentos nacionais e a falta de clareza sobre o procedimento como as principais razões para a sua utilização limitada.

O RGPD dá às autoridades de proteção de dados interessadas a possibilidade de suscitarem uma objeção pertinente e fundamentada caso discordem de um projeto de decisão da autoridade de proteção de dados principal num caso transfronteiriço. Se as autoridades de proteção de dados não conseguirem chegar a um consenso sobre uma objeção pertinente e fundamentada, o RGPD prevê que o litígio seja resolvido pelo Comité ([14]). Os temas mais frequentemente suscitados nas objeções pertinentes e fundamentadas foram os seguintes: i) o fundamento jurídico para o tratamento; ii) as obrigações de informação e transparência; iii) a notificação de violações de dados; iv) os direitos dos titulares dos dados; v) as derrogações relativas a transferências internacionais; vi) a utilização de medidas corretivas; e vii) o montante de uma coima.

O sistema de aplicação do RGPD baseia-se na premissa de uma cooperação leal e eficaz entre as autoridades de proteção de dados. Embora desempenhe um papel importante nesta arquitetura de aplicação, o procedimento de resolução de litígios deve ser utilizado de acordo com o espírito em que foi concebido, tendo em devida consideração, nomeadamente, a repartição de competências entre as autoridades de proteção de dados, a necessidade de respeitar os direitos processuais e o interesse dos titulares dos dados em obter uma resolução atempada do caso. Cada procedimento de resolução de litígios exige recursos significativos da autoridade principal, das autoridades interessadas e do secretariado do Comité e atrasa a apresentação de uma solução aos titulares dos dados.

*Maior utilização dos instrumentos de cooperação pelas autoridades de proteção de dados*

- Foram registadas quase 2 400 entradas de casos no sistema de intercâmbio de informações do Comité ([15]).
- As autoridades de proteção de dados principais emitiram cerca de 1 500 projetos de decisão ([16]), dos quais 990 resultaram em decisões finais que constataram uma violação do RGPD ([17]).
- As autoridades de proteção de dados desencadearam quase 1 000 pedidos de assistência mútua «formais» ([18]) e cerca de 12 300 pedidos «informais» ([19]).
- Foram iniciadas cinco operações conjuntas em que participaram autoridades de proteção de dados de sete Estados-Membros.
- Autoridades de proteção de dados de 18 Estados-Membros suscitaram objeções pertinentes e fundamentadas ([20]).

([12]) internal_edpb_document_1_2021_on_art_62_joint_operations_en.pdf (europa.eu).
([13]) Artigo 62.º do RGPD.
([14]) Artigo 65.º do RGPD.
([15]) Até 3 de novembro de 2023 (contributo do Comité).
([16]) Nos termos do artigo 60.º, n.º 3, do RGPD.
([17]) Até 3 de novembro de 2023.
([18]) A autoridade irlandesa apresentou o maior número de pedidos formais (246), enquanto as autoridades alemãs receberam o maior número de pedidos (516).
([19]) A autoridade irlandesa apresentou o maior número de pedidos informais (4 245), seguida das autoridades alemãs (2 036).
([20]) Das 289 objeções pertinentes e fundamentadas comunicadas pelas autoridades, 101 (35 %) foram suscitadas pelas autoridades alemãs. A taxa de êxito na obtenção de consenso sobre objeções pertinentes e fundamentadas varia entre 15 % (das objeções suscitadas pelas autoridades alemãs) e 100 % (das objeções suscitadas pela autoridade polaca).

O procedimento de controlo da coerência do RGPD é cada vez mais utilizado pelas autoridades de proteção de dados. Tem três componentes: i) pareceres do Comité; ii) resolução de litígios pelo Comité; e iii) procedimento de urgência ([21]).

O Comité aborda cada vez mais nos seus pareceres questões importantes de aplicação geral ([22]). Antes de adotar esses pareceres, o Comité deve assegurar uma consulta atempada e significativa. Os casos submetidos a resolução de litígios têm sido relativos a questões como a base jurídica subjacente ao tratamento de dados para publicidade comportamental nas redes sociais e o tratamento de dados das crianças em linha. A maior parte das decisões vinculativas subsequentes foram impugnadas no Tribunal Geral.

A transparência no processo de decisão do Comité é fundamental para garantir o respeito do direito a uma boa administração nos termos da Carta dos Direitos Fundamentais da UE. O procedimento de urgência do RGPD permite que as autoridades de proteção de dados derroguem o procedimento de cooperação e de controlo da coerência para tomar medidas urgentes, sempre que necessário, para proteger os direitos e liberdades dos titulares dos dados. Em derrogação do procedimento normal de cooperação ao abrigo do RGPD, instrumentos como o procedimento de urgência são concebidos para serem utilizados apenas em circunstâncias excecionais e quando o procedimento normal de cooperação não pode proteger os direitos e liberdades dos titulares dos dados.

*O procedimento de controlo da coerência*

- O Comité adotou 190 pareceres relativos à coerência.
- No âmbito da resolução de litígios, foram adotadas nove decisões vinculativas ([23]). Todas elas obrigaram a autoridade de proteção de dados principal a alterar o seu projeto de decisão, tendo várias delas resultado em coimas significativas.
- Cinco autoridades de proteção de dados adotaram medidas provisórias ao abrigo do procedimento de urgência (Alemanha, Finlândia, Itália, Noruega e Espanha).
- Duas autoridades de proteção de dados solicitaram uma decisão vinculativa urgente do Comité ([24]) , tendo este ordenado medidas definitivas urgentes num caso.

### 2.3 Reforço da aplicação

Nos últimos anos, registou-se um aumento significativo das medidas de aplicação tomadas pelas autoridades de proteção de dados, incluindo a aplicação de coimas substanciais em processos mediáticos contra «grandes empresas tecnológicas» multinacionais. Foram aplicadas coimas, por exemplo, por: i) violação da legalidade e da segurança do tratamento; ii) violação do tratamento de categorias especiais de dados pessoais; e iii) desrespeito dos direitos das pessoas ([25]). Estas medidas levaram as empresas privadas a ter seriamente em conta a proteção de dados ([26]) e ajudou a integrar uma cultura de conformidade nas organizações. As autoridades de proteção de dados adotam decisões que constatam violações do RGPD em casos baseados em reclamações ou abertos por sua própria iniciativa. Embora essa possibilidade não esteja disponível em todos os Estados-Membros,

([21]) Respetivamente, artigos 64.º, 65.º e 66.º do RGPD.
([22]) Pareceres nos termos do artigo 64.º, n.º 2, do RGPD.
([23]) Nos termos do artigo 65.º, n.º 1, alínea a), do RGPD.
([24]) Nos termos do artigo 66.º, n.º 2, do RGPD.
([25]) Ver secção 5.3.4 do contributo do Comité.
([26]) Relatório da FRA, página 36.

muitas autoridades de proteção de dados utilizaram eficazmente os procedimentos de «resolução amigável» para resolver rapidamente os processos baseados em reclamações, a contento do reclamante. A proposta relativa às normas processuais reconhece a possibilidade de as reclamações serem resolvidas de forma amigável ([27]).

As autoridades de proteção de dados utilizaram amplamente os seus poderes de correção, embora o número de medidas corretivas impostas varie consideravelmente entre autoridades. Para além das coimas, as medidas corretivas mais frequentemente utilizadas foram advertências, repreensões e ordens de cumprimento do RGPD. Os responsáveis pelo tratamento e os executantes do tratamento contestam frequentemente nos tribunais nacionais decisões que constatam violações do RGPD, geralmente por motivos processuais ([28]).

*Reforço da aplicação*

- As autoridades de proteção de dados lançaram mais de 20 000 investigações por iniciativa própria ([29]).
- Em conjunto, recebem mais de 100 000 reclamações por ano ([30]).
- O tempo médio para as autoridades de proteção de dados tratarem as reclamações (desde a receção até ao encerramento do processo) varia entre 1 e 12 meses, sendo igual ou inferior a 3 meses em cinco Estados-Membros [Dinamarca (1 mês), Espanha (1,5 meses), Estónia (3 meses), Grécia (3 meses) e Irlanda (3 meses)].
- Mais de 20 000 reclamações foram resolvidas de forma amigável. A resolução amigável é mais frequentemente utilizada na Áustria, na Hungria, no Luxemburgo e na Irlanda.
- Em 2022, as autoridades de proteção de dados da Alemanha adotaram o maior número de decisões que impõem uma medida corretiva (3 261), seguindo-se a Espanha (774), a Lituânia (308) e a Estónia (332). Os números mais baixos de medidas corretivas registaram-se no Listenstaine (8), na Chéquia (8), na Islândia (10), nos Países Baixos (17) e no Luxemburgo (22).
- As autoridades de proteção de dados aplicaram mais de 6 680 coimas no valor de cerca de 4 200 milhões de EUR ([31]). A autoridade irlandesa impôs o montante total mais elevado de coimas (2 800 milhões de EUR), seguindo-se o Luxemburgo (746 milhões de EUR), Itália (197 milhões de EUR) e França (131 milhões de EUR). O Listenstaine (9 600 EUR), a Estónia (201 000 EUR) e a Lituânia (435 000 EUR) aplicaram os montantes mais baixos de coimas.

([27]) Proposta relativa às normas processuais, artigo 5.º.

([28]) Na Roménia, as 26 decisões que constataram uma violação foram impugnadas em tribunal, enquanto nos Países Baixos a taxa de impugnação foi de 23 %. A taxa de êxito mais elevada em matéria de impugnações foi registada na Bélgica (39 %).

([29]) As autoridades de proteção de dados lançaram o maior número de investigações por iniciativa própria na Alemanha (7 647), seguindo-se a Hungria (3 332), a Áustria (1 681) e a França (1 571).

([30]) Em 2022, nove autoridades de proteção de dados receberam mais de 2 000 reclamações. Os números mais elevados de reclamações foram registados pela Alemanha (32 300), Itália (30 880), Espanha (15 128), Países Baixos (13 133) e França (12 193), enquanto os números mais baixos foram registados pelo Listenstaine (40), pela Islândia (140) e pela Croácia (271).

([31]) Todas as autoridades aplicaram coimas, com exceção da Dinamarca, onde as mesmas não estão previstas. Os números mais elevados de coimas registaram-se na Alemanha (2 106) e em Espanha (1 596). Os números mais baixos de coimas registaram-se no Listenstaine (3), na Islândia (15) e na Finlândia (20).

Embora a maioria das autoridades de proteção de dados considerem que os instrumentos de investigação de que dispõem são adequados, algumas necessitam de instrumentos adicionais a nível nacional, tais como sanções adequadas, nos casos em que os responsáveis pelo tratamento não cooperam ou não fornecem as informações necessárias ([32]). As autoridades de proteção de dados consideram que a insuficiência de recursos e as lacunas nos conhecimentos técnicos e jurídicos constituem o principal obstáculo à sua capacidade de aplicação ([33]).

### 2.4 O Comité

O Comité é composto pelo diretor de uma autoridade de proteção de dados de cada Estado-Membro e pela Autoridade Europeia para a Proteção de Dados, com a participação da Comissão sem direito de voto. Cabe ao Comité, apoiado no seu trabalho pelo respetivo secretariado, assegurar a aplicação coerente do RGPD ([34]). A maioria das autoridades de proteção de dados considera que o Comité desempenhou um papel positivo no reforço da cooperação entre as mesmas ([35]). Muitas autoridades de proteção de dados dedicam recursos significativos às atividades do Comité, embora as autoridades de menor dimensão refiram que a sua dimensão as impede de participar de forma plena ([36]). Algumas autoridades consideram importante melhorar a eficiência dos processos do Comité, nomeadamente reduzindo o número de reuniões e dedicando menos atenção a questões de menor importância ([37]). Em função do resultado das negociações sobre a proposta relativa às normas processuais do RGPD, que visa reduzir o número de casos apresentados ao Comité para resolução de litígios, poderá ser necessário analisar se o Comité necessita de recursos adicionais.

Até novembro de 2023, o Comité tinha adotado 35 orientações. As partes interessadas e as autoridades de proteção de dados reconhecem a utilidade dessas orientações, mas consideram que elas devem ser fornecidas mais rapidamente e que é necessário melhorar a respetiva qualidade ([38]). As partes interessadas observam que, muitas vezes, as orientações são excessivamente teóricas, demasiado longas e não refletem a abordagem baseado no risco do RGPD ([39]). As autoridades de proteção de dados e o Comité devem disponibilizar orientações concisas e práticas que deem resposta a problemas concretos e reflitam um equilíbrio entre a proteção de dados e outros direitos fundamentais. As orientações devem também ser facilmente compreensíveis para as pessoas sem formação jurídica, por exemplo nas PME e nas organizações de voluntariado ([40]). Uma forma de o conseguir é tornar a elaboração das orientações mais transparente e proceder a consultas numa fase precoce, a fim de permitir uma melhor compreensão da dinâmica do mercado, das práticas comerciais e da forma de aplicar as orientações na prática ([41]). É de saudar o facto de, na sua estratégia para 2024-2027, o Comité ter salientado o seu objetivo de disponibilizar orientações práticas acessíveis ao público pertinente ([42]).

---

([32]) Relatório da FRA, página 38.
([33]) Relatório da FRA, páginas 20 e 23. Ver também o documento sobre a posição e conclusões do Conselho, n.º 17.
([34]) Artigo 70.º, n.º 1, do RGPD.
([35]) Relatório da FRA, página 64.
([36]) Relatório da FRA, página 67. Em 2023, as autoridades alemãs de proteção de dados dedicaram o maior número de recursos às atividades do Comité [26 equivalentes a tempo completo (ETC)], seguindo-se a Irlanda (16) e França (12) (contributo do Comité).
([37]) Relatório da FRA, página 67.
([38]) Relatório da FRA, p. 67; resumo das reações do grupo de peritos multilateral sobre o RGPD.
([39]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([40]) Ver também o documento sobre a posição e conclusões do Conselho, n.º 45.
([41]) Ver também o documento sobre a posição e conclusões do Conselho, n.º 34.
([42]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf

As partes interessadas sublinham a necessidade de orientações adicionais, em especial sobre a anonimização e a pseudonimização ([43]), o interesse legítimo e a investigação científica ([44]). No relatório de 2020, a Comissão instou o Comité a adotar orientações em matéria de investigação científica, mas tal ainda não aconteceu. Tendo em conta a importância da investigação científica na sociedade, em especial para monitorizar doenças e desenvolver tratamentos, bem como para promover a inovação, é essencial que as autoridades de proteção de dados tomem medidas para esclarecer estas questões sem mais demora ([45]). As autoridades públicas também beneficiariam de orientações que abordassem os desafios específicos que enfrentam ([46]).

## 2.5 Autoridades de proteção de dados

### *2.5.1 Independência e recursos*

A independência das autoridades de proteção de dados está consagrada na Carta dos Direitos Fundamentais da UE e no Tratado sobre o Funcionamento da União Europeia. O RGPD estabelece requisitos para assegurar a «total independência» das autoridades de proteção de dados ([47]). Segundo o relatório da FRA, a maioria das autoridades de proteção de dados opera de forma independente do governo, do Parlamento ou de quaisquer outros organismos públicos ([48]).

As autoridades de proteção de dados necessitam de recursos humanos, técnicos e financeiros adequados para poderem desempenhar de forma eficaz e independente as suas funções ao abrigo do RGPD. No relatório de 2020, a Comissão observou que os recursos das autoridades de proteção de dados continuavam a não ser satisfatórios e que a Comissão tinha suscitado sistematicamente esta questão junto dos Estados-Membros. Desde então, a situação melhorou.

*Aumento dos recursos para as autoridades de proteção de dados ([49])*

- Entre 2020 e 2024, todas as autoridades de proteção de dados, com exceção de duas, beneficiaram de um aumento do pessoal, que foi superior a 25 % em 14 Estados-Membros.
- A autoridade de proteção de dados da Irlanda registou o maior aumento de pessoal (79 %), seguindo-se a Estónia, a Suécia (ambas com 57 %) e a Bulgária (56 %).
- Registou-se uma ligeira diminuição do pessoal da autoridade na Chéquia (-1 %), enquanto no Listenstaine não se registou qualquer aumento e em Chipre (4 %) e na Hungria (8 %) se registaram aumentos pouco significativos.
- Entre 2020 e 2024, todas as autoridades de proteção de dados, exceto uma, beneficiaram de um aumento do orçamento, que foi superior a 50 % em 13 Estados-Membros.

([43]) Ver também o documento sobre a posição e conclusões do Conselho, n.º 31, alínea d).
([44]) Exigem clareza, em especial, sobre o significado do termo «investigação científica», o papel do consentimento no tratamento de dados pessoais para fins de investigação, a base jurídica pertinente e as funções e responsabilidades dos intervenientes envolvidos.
([45]) Ver também o documento sobre a posição e conclusões do Conselho, n.º 31, alínea b).
([46]) Documento sobre a posição e conclusões do Conselho, n.os 27 e 28.
([47]) Artigo 52.º do RGPD.
([48]) Relatório da FRA, página 31.
([49]) Ver secção 4.4.1 do contributo do Comité, que inclui também os valores absolutos.

- A autoridade de proteção de dados de Chipre registou o maior aumento do orçamento (130 %), seguindo-se a Áustria (107 %), a Bulgária (100 %) e a Estónia (97 %).
- O orçamento da autoridade grega de proteção de dados diminuiu 15 %, tendo ocorrido pequenos aumentos orçamentais para as autoridades do Listenstaine (1 %), da Eslováquia (6 %) e da Chéquia (8 %).

Embora estas estatísticas revelem uma tendência geral de aumento dos recursos das autoridades de proteção de dados, as próprias autoridades consideram que ainda não dispõem de recursos humanos suficientes ([50]). Sublinham a necessidade de conhecimentos técnicos muito especializados, em especial sobre tecnologias novas e emergentes ([51]), cuja ausência afeta a quantidade e a qualidade do seu trabalho, e realçam as dificuldades em competir com o setor privado pelos recursos humanos. As autoridades de proteção de dados mencionam os conhecimentos jurídicos insuficientes e a falta de competências linguísticas como fatores que afetam o seu desempenho. A baixa remuneração, a incapacidade de selecionar autonomamente o pessoal e o elevado volume de trabalho são apontados como os principais fatores que afetam a capacidade das autoridades para recrutar e reter pessoal ([52]). As autoridades de proteção de dados salientam igualmente que necessitam de recursos financeiros para modernizar e digitalizar os seus processos e adquirir equipamento técnico ([53]). Todas as autoridades de proteção de dados desempenham funções para além das que lhes são confiadas pelo RGPD ([54]), por exemplo, enquanto autoridades de controlo no âmbito da Diretiva Proteção de Dados na Aplicação da Lei e da Diretiva Privacidade Eletrónica, mas muitas delas manifestam preocupações quanto à possibilidade de assumir responsabilidades adicionais ao abrigo da nova legislação digital ([55]).

### *2.5.2 Dificuldades no tratamento de um elevado número de reclamações*

Várias autoridades de proteção de dados referem que dedicam demasiados recursos ao tratamento de um elevado número de reclamações, a maioria das quais consideram ser triviais e sem fundamento, uma vez que o RGPD lhes impõe a obrigação, sujeita a controlo jurisdicional, de tratar todas as reclamações ([56]). Ou seja, as autoridades de proteção de dados não podem afetar recursos suficientes a outras atividades, tais como investigações por iniciativa própria, campanhas de sensibilização do público e colaboração com os responsáveis pelo tratamento ([57]). Enquanto autoridades públicas, as autoridades de proteção de dados têm o poder discricionário de afetar os seus recursos da forma que considerem adequada para prosseguirem cada uma das suas atribuições de interesse público (enumeradas no artigo 57.º, n.º 1, do RGPD). Muitas autoridades de proteção de dados adotaram estratégias para aumentar a eficiência do tratamento de reclamações, como

([50]) Apenas cinco autoridades de proteção de dados consideram que dispõem de recursos humanos adequados (contributo do Comité, página 33).
([51]) Relatório da FRA, página 20. Algumas autoridades de proteção de dados subcontratam determinadas tarefas a contratantes externos, como o tratamento de reclamações, a análise jurídica e a análise forense.
([52]) Relatório da FRA, página 24.
([53]) Relatório da FRA, página 22.
([54]) Ver secção 4.4.5 do contributo do Comité.
([55]) Contributo do Comité, página 32.
([56]) Relatório da FRA, página 48.
([57]) Relatório da FRA, página 45. As autoridades de proteção de dados consideram as investigações *ex officio* particularmente importantes, uma vez que os reclamantes podem não estar cientes de muitas violações do RGPD.

a automatização ([58]), a utilização de procedimentos de resolução amigável ([59]) e o «agrupamento» de reclamações relacionadas com questões semelhantes ([60]).

### *2.5.3 Interpretação do RGPD pelas autoridades nacionais de proteção de dados*

Um objetivo central do RGPD era eliminar a abordagem fragmentada da proteção de dados que decorria da anterior Diretiva Proteção de Dados (Diretiva 95/46/CE) ([61]). No entanto, as autoridades de proteção de dados continuam a adotar interpretações divergentes sobre conceitos fundamentais da proteção de dados ([62]). As partes interessadas identificam este aspeto como o principal obstáculo à aplicação coerente do RGPD na UE. A persistência de interpretações divergentes cria insegurança jurídica e aumenta os custos para as empresas (por exemplo, ao exigir documentação diferente para vários Estados-Membros), perturbando a livre circulação de dados pessoais na UE, dificultando os negócios transfronteiras e criando obstáculos à investigação e à inovação sobre problemas societais urgentes.

As questões específicas suscitadas pelas partes interessadas incluem as seguintes: i) as autoridades de proteção de dados de três Estados-Membros têm opiniões diferentes quanto à base jurídica adequada para o tratamento de dados pessoais aquando da realização de um ensaio clínico; ii) existem frequentemente opiniões divergentes sobre se uma entidade é responsável pelo tratamento ou executante do tratamento; e iii) em alguns casos, as autoridades de proteção de dados não seguem as orientações do Comité ou publicam orientações a nível nacional que colidem com as do Comité ([63]). Estas questões agravam-se quando várias autoridades de proteção de dados num único Estado-Membro adotam interpretações contraditórias.

Algumas partes interessadas consideram igualmente que determinadas autoridades de proteção de dados e o Comité adotam interpretações que se desviam da abordagem baseada no risco do RGPD, o que constitui um desafio para o desenvolvimento da economia digital ([64]) e para a liberdade e pluralidade dos meios de comunicação social. Mencionam os seguintes domínios que suscitam preocupação: i) a interpretação da anonimização; ii) a base jurídica do interesse legítimo e do consentimento ([65]); e iii) as exceções à proibição de decisões individuais automatizadas ([66]). Importa recordar que as autoridades de proteção de dados e o Comité estão incumbidos de assegurar tanto a proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais como a livre circulação de dados pessoais na UE. Conforme reconhecido no RGPD ([67]), o direito à proteção de dados pessoais deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

### *2.5.4 Colaboração com os responsáveis pelo tratamento e os executantes do tratamento*

As partes interessadas sublinham as vantagens da oportunidade de encetar um diálogo construtivo com as autoridades de proteção de dados, a fim de assegurar que estas cumprem o RGPD desde o início, em especial no que diz respeito às tecnologias

([58]) Relatório da FRA, página 8.
([59]) Relatório da FRA, página 39.
([60]) Relatório da FRA, página 41.
([61]) Considerando 9 do RGPD.
([62]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([63]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([64]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([65]) Artigo 6.º, n.º 1, alíneas f) e a), respetivamente, do RGPD.
([66]) Artigo 22.º, n.º 2, do RGPD.
([67]) Considerando 4.

emergentes. As partes interessadas observam que algumas autoridades de proteção de dados colaboram ativamente com os responsáveis pelo tratamento, enquanto outras demoram a responder, dão respostas vagas ou simplesmente não respondem ([68]).

# 3 APLICAÇÃO DO RGPD PELOS ESTADOS-MEMBROS

## 3.1 Fragmentação na aplicação nacional

Embora o RGPD, por ser um regulamento, seja diretamente aplicável, exige que os Estados-Membros legislem em determinados domínios e permite-lhes especificar melhor a sua aplicação num número limitado de domínios ([69]). Ao legislar a nível nacional, os Estados-Membros devem respeitar as condições e os limites estabelecidos pelo RGPD. Como em 2020, as partes interessadas referem que enfrentam dificuldades decorrentes da fragmentação das regras nacionais em que os Estados-Membros têm a possibilidade de especificar o RGPD, em especial no que diz respeito:

- à idade mínima para o consentimento de uma criança em relação aos serviços da sociedade da informação que lhe são oferecidos ([70]),
- à imposição pelos Estados-Membros de novas condições relativas ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde ([71]),
- ao tratamento de dados pessoais relacionados com condenações penais e infrações ([72]), que cria dificuldades em determinados setores regulamentados.

Ao mesmo tempo, é importante salientar que, de acordo com muitas partes interessadas, as questões de fragmentação decorrem principalmente de interpretações divergentes do RGPD pelas autoridades de proteção de dados, e não da utilização de cláusulas de especificação facultativas pelos Estados-Membros.

Os Estados-Membros consideram que um grau limitado de fragmentação pode ser aceitável e que as cláusulas de especificação previstas no RGPD continuam a ser benéficas, em especial para o tratamento pelas autoridades públicas ([73]). O RGPD exige que os Estados-Membros consultem a sua autoridade nacional de proteção de dados aquando da elaboração de legislação relacionada com o tratamento de dados pessoais ([74]). O relatório da FRA concluiu que alguns governos impõem prazos muito curtos a essas autoridades e, em alguns casos, simplesmente não as consultam ([75]).

## 3.2 Acompanhamento pela Comissão

A Comissão acompanha continuamente a aplicação do RGPD. Deu início a procedimentos de infração contra Estados-Membros sobre questões como a independência das autoridades de proteção de dados (incluindo a não sujeição a influências externas e a possibilidade de recurso judicial em caso de recusa) ([76]) e o direito à ação judicial para os titulares dos dados nos casos em que a autoridade de proteção de dados não trata uma reclamação ([77]). No âmbito do seu acompanhamento, a Comissão solicita igualmente que as autoridades de

([68]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([69]) Por exemplo, a idade mínima para o consentimento de crianças em relação aos serviços da sociedade da informação (artigo 8.º, n.º 1, do RGPD).
([70]) Artigo 8.º, n.º 1, do RGPD.
([71]) Uma possibilidade prevista no artigo 9.º, n.º 4, do RGPD.
([72]) Artigo 10.º do RGPD.
([73]) Documento sobre a posição e conclusões do Conselho, n.º 30.
([74]) Artigo 36.º do RGPD.
([75]) Relatório da FRA, página 11.
([76]) Bélgica (2021/4045) e Bélgica (2022/2160).
([77]) Finlândia (2022/4010) e Suécia (2022/2022).

proteção de dados forneçam, numa base estritamente confidencial, informações regulares ([78]) sobre casos transfronteiriços de larga escala em curso, nomeadamente os que dizem respeito a grandes empresas tecnológicas multinacionais.

A Comissão mantém uma comunicação regular com os Estados-Membros sobre a aplicação do RGPD. Como se definiu no relatório de 2020, a Comissão continuou a utilizar o grupo de peritos dos Estados-Membros no âmbito do RGPD ([79]) para facilitar os debates e a partilha de experiências sobre a aplicação efetiva do mesmo. O grupo de peritos realizou debates específicos sobre: i) o controlo dos tribunais que atuem no exercício da sua função jurisdicional (artigo 55.º do RGPD; artigo 8.º da Carta); ii) a conciliação do direito à proteção de dados com o direito à liberdade de expressão (artigo 85.º do RGPD); e iii) o direito à ação judicial contra uma autoridade de controlo (artigo 78.º do RGPD). Na sequência destes debates, a Comissão elaborou sínteses das abordagens adotadas para aplicar essas disposições nos Estados-Membros ([80]). A Comissão utilizou igualmente o referido grupo para trocar pontos de vista com os Estados-Membros aquando da elaboração da proposta relativa às normas processuais.

As avaliações de Schengen, realizadas conjuntamente pelos Estados-Membros e pela Comissão, também analisam a conformidade da legislação e das práticas nacionais com as regras de proteção de dados estabelecidas no acervo legislativo da UE relativo ao espaço Schengen. São realizadas anualmente pelo menos cinco avaliações da proteção de dados no local, que incidem atualmente nos sistemas informáticos de grande escala e no Sistema de informação Schengen, no Sistema de Informação sobre Vistos, bem como no papel de supervisão desses sistemas confiado às autoridades nacionais de proteção de dados.

A Comissão está a contribuir ativamente para o elevado número de processos no Tribunal de Justiça (com cerca de 30 decisões prejudiciais por ano nos últimos anos), que desempenham um papel central na interpretação coerente dos conceitos fundamentais do RGPD. A jurisprudência cada vez mais vasta do Tribunal forneceu vários esclarecimentos, nomeadamente sobre a definição de dados pessoais ([81]), categorias especiais de dados pessoais ([82]), responsável pelo tratamento ([83]), consentimento ([84]), interesse legítimo ([85]), direito de acesso ([86]), direito ao apagamento dos dados ([87]), direito de indemnização ([88]), decisões individuais automatizadas ([89]), coimas ([90]), encarregados da proteção de

([78]) Incluindo informações sobre a referência do processo, o tipo de investigação (por iniciativa própria ou baseada numa reclamação), um resumo do âmbito da investigação, as autoridades de proteção de dados em causa, as principais diligências processuais realizadas e respetivas datas, bem como as medidas de investigação ou quaisquer outras medidas tomadas e respetivas datas.

([79]) https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=pt&do=groupDetail.groupDetail&groupID=3461

([80]) https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=pt&meetingId=31754&fromExpertGroups=3461

([81]) Processo C-319/22, ECLI:EU:C:2023:837.

([82]) Processos C-184/20, ECLI:EU:C:2022:601; C-252/21, ECLI:EU:C:2023:537.

([83]) Processos C-683/21, ECLI:EU:C:2023:949; C-604/22, ECLI:EU:C:2024:214; C-231/22, ECLI:EU:C:2024:7.

([84]) Processo C-61/19, ECLI:EU:C:2020:901.

([85]) Processos C-597/19, ECLI:EU:C:2021:492; C-252/21, ECLI:EU:C:2023:537.

([86]) Processos C-307/22, ECLI:EU:C:2023:811; C-154/21, ECLI:EU:C:2023:3.

([87]) Processo C-460/20, ECLI:EU:C:2022:962.

([88]) Processo C-300/21, ECLI:EU:C:2023:370; Processo C-687/21, ECLI:EU:C:2024:72; Processo C-667/21, ECLI:EU:C:2023:1022.

([89]) Processos apensos C-26/22 e C-64/22, ECLI:EU:C:2023:958.

([90]) Processos C-807/21, ECLI:EU:C:2023:950; Processo C-683/21, ECLI:EU:C:2023:949.

dados ([91]), publicação de dados pessoais em registos ([92]) e aplicação do RGPD às atividades dos parlamentos ([93]).

## 4 DIREITOS DOS TITULARES DOS DADOS

*Sensibilização das pessoas para o RGPD e as autoridades de proteção de dados (Eurobarómetro 549 sobre justiça, direitos e valores, de 2024)*

- Entre os inquiridos em toda a UE, 72 % afirmam ter ouvido falar do RGPD, incluindo 40 % que sabem o que é.
- Em 19 Estados-Membros, mais de 70 % dos inquiridos indicam ter conhecimento do RGPD, sendo os inquiridos na Suécia (92 %) os mais sensibilizados, acima dos Países Baixos (88 %), Malta e Dinamarca (84 %), enquanto os inquiridos na Bulgária (59 %) são os menos sensibilizados, seguindo-se a Lituânia (63 %) e França (64 %).
- Entre os inquiridos em toda a UE, 68 % afirmam ter ouvido falar de uma autoridade nacional responsável pela proteção dos seus direitos em matéria de proteção de dados e 24 % de todos os inquiridos afirmam também que sabem qual é a autoridade pública responsável.
- Em todos os Estados-Membros, pelo menos metade dos inquiridos ouviu falar dessa autoridade nacional, registando-se os níveis mais elevados nos Países Baixos (82 %), na Chéquia, Eslovénia e Polónia (todos com 75 %) e em Portugal (74 %). Os inquiridos na Áustria (56 %) e em Espanha (58 %) são os que menos conhecem a autoridade em causa.

Cada vez mais, as pessoas conhecem e exercem ativamente os seus direitos ao abrigo do RGPD ([94]). As autoridades de proteção de dados afetam recursos substanciais à promoção da sensibilização do público em geral para os direitos e obrigações em matéria de proteção de dados, nomeadamente através das redes sociais e campanhas televisivas, de linhas telefónicas de apoio, de boletins informativos e de apresentações em instituições de ensino ([95]). Muitas destas iniciativas beneficiaram de financiamento da UE ([96]). A Agência dos Direitos Fundamentais observa que, embora a sensibilização do público em geral para a proteção de dados tenha aumentado, a compreensão da proteção de dados continua a ser insuficiente, como demonstra o elevado número de reclamações triviais ou infundadas ([97]). Foram desenvolvidas várias ferramentas digitais conviviais para facilitar o exercício dos direitos dos titulares dos dados ([98]). Certos atos legislativos, nomeadamente o Regulamento Governação de Dados ([99]), deverão conduzir à criação de formas adicionais de exercício desses direitos no futuro. As empresas observam que o direito ao apagamento dos dados é cada vez mais utilizado, embora o mesmo raramente aconteça com o direito de retificação e o direito de oposição.

([91]) Processo C-453/21, ECLI:EU:C:2023:79.
([92]) Processos C-439/19, ECLI:EU:C:2021:504; C-184/20, ECLI:EU:C:2022:601.
([93]) Processos C-33/22, ECLI:EU:C:2024:46; C-272/19, ECLI:EU:C:2020:535.
([94]) Documento sobre a posição e conclusões do Conselho, n.º 13.
([95]) Contributo do Comité, secção 6.
([96]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=pt
([97]) Relatório da FRA, páginas 9 e 48.
([98]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([99]) Artigo 10.º do Regulamento (UE) 2022/868 (Regulamento Governação de Dados) (JO L 152 de 3.6.2022, p. 1).

### 4.1 O direito de acesso

Os responsáveis pelo tratamento referem que o direito de acesso (artigo 15.º do RGPD) é o direito mais frequentemente invocado pelos titulares dos dados. Embora o Comité tenha adotado orientações sobre este direito em 2022, os responsáveis pelo tratamento continuam a comunicar dificuldades, por exemplo, na interpretação do conceito de pedidos infundados ou excessivos ([100]), na resposta a um elevado número de pedidos e no tratamento de pedidos apresentados para fins não relacionados com a proteção de dados, por exemplo, a recolha de elementos de prova para processos judiciais ([101]). As organizações da sociedade civil observam que as respostas aos pedidos de acesso são frequentemente tardias ou incompletas, ao passo que os dados recebidos nem sempre se encontram num formato legível ([102]). As autoridades públicas mencionam dificuldades na interação entre o direito de acesso e as regras relativas ao acesso do público aos documentos ([103]). Por conseguinte, é de saudar o facto de o Comité ter lançado, em fevereiro de 2024, uma ação conjunta do Quadro de Supervisão Coordenada relativa ao direito de acesso ([104]).

### 4.2 O direito à portabilidade

No relatório de 2020, a Comissão comprometeu-se a explorar meios práticos para facilitar uma maior utilização do direito à portabilidade dos dados pelas pessoas (artigo 20.º do RGPD), em consonância com a estratégia para os dados. Desde então, a Comissão adotou uma série de iniciativas que complementam este direito. Estas iniciativas facilitam a mudança de serviço e, dessa forma, aumentam as possibilidades de escolha das pessoas, apoiam a concorrência e a inovação e permitem que as pessoas colham os benefícios da utilização dos seus dados. O Regulamento dos Dados confere aos utilizadores de dispositivos inteligentes um direito reforçado à portabilidade dos dados gerados através desses dispositivos e exige que a conceção do produto ou um servidor de retaguarda do fabricante ou do detentor dos dados torne essa portabilidade tecnicamente possível. O Regulamento dos Mercados Digitais exige que os prestadores de serviços essenciais de plataforma identificados como «controladores de acesso» ofereçam uma portabilidade efetiva dos dados dos utilizadores, incluindo o acesso contínuo e em tempo real a esses dados. Várias outras iniciativas da Comissão atualmente em negociação ou que já foram objeto de acordo político preveem o reforço dos direitos de portabilidade em domínios específicos, como a diretiva relativa ao trabalho nas plataformas digitais ([105]), o Espaço Europeu de Dados de Saúde ([106]) e o quadro de acesso aos dados financeiros ([107]).

### 4.3 O direito de apresentar reclamação

O elevado número de reclamações demonstra um amplo conhecimento do direito de apresentar reclamação a uma autoridade de proteção de dados. As organizações da

([100]) Artigo 12.º, n.º 5, do RGPD.
([101]) No entanto, o Tribunal de Justiça esclareceu que o titular dos dados não é obrigado a indicar os motivos do pedido de acesso aos dados pessoais: processo C-307/22, ECLI:EU:C:2023:811, n.º 38.
([102]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([103]) Documento sobre a posição e conclusões do Conselho, n.os 27 e 28.
([104]) https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_pt.
([105]) Trabalhadores das plataformas: Conselho confirma acordo sobre novas regras para melhorar as suas condições de trabalho — Consilium (europa.eu).
([106]) Proposta de regulamento relativo ao relativo ao Espaço Europeu de Dados de Saúde [COM(2022) 197 final].
([107]) Proposta de regulamento relativo a um quadro de acesso aos dados financeiros e que altera os Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010, (UE) n.º 1095/2010 e (UE) 2022/2554 [COM(2023) 360 final].

sociedade civil destacam diferenças injustificadas nas práticas nacionais de tratamento de reclamações, sendo esta questão abordada na proposta da Comissão relativa às normas processuais. Poucos Estados-Membros exerceram a opção prevista no RGPD de conceder a um organismo sem fins lucrativos o direito de tomar medidas independentemente de um mandato conferido pelo titular dos dados (artigo 80.º, n.º 2). No entanto, a Diretiva Ações Coletivas ([108]), adotada em 2020, conduzirá a uma maior harmonização a este respeito, ao facilitar ações coletivas de pessoas singulares por violação do RGPD. As medidas nacionais de transposição da diretiva entraram em vigor em junho de 2023.

### 4.4 Proteção dos dados pessoais das crianças

As crianças necessitam de proteção específica quando os seus dados pessoais são objeto de tratamento ([109]). O RGPD faz parte de um quadro jurídico abrangente que garante a proteção das crianças tanto em linha como fora de linha ([110]). Tendo em conta a presença crescente de crianças em linha, foram empreendidas nos últimos anos várias ações a nível nacional e da UE para apoiar a proteção das crianças em linha. As autoridades de proteção de dados aplicaram coimas significativas às empresas de redes sociais por violação do RGPD no âmbito do tratamento de dados de crianças. Cooperam igualmente com outras autoridades para apelar a uma maior proteção das crianças no domínio da publicidade. No relatório de 2020, a Comissão convidou o Comité a adotar orientações sobre o tratamento de dados das crianças, estando este trabalho em curso ([111]). O Regulamento dos Serviços Digitais inclui disposições específicas para assegurar um elevado nível de privacidade, segurança e proteção das crianças que utilizam plataformas em linha.

Algumas partes interessadas comunicam dificuldades no exercício dos direitos dos titulares dos dados quando estes são crianças. Em especial, referem que as crianças não compreendem plenamente os seus direitos, carecem de competências de literacia digital e podem estar sujeitas a influências indevidas ([112]). A Comissão financiou várias iniciativas a nível nacional relativas à proteção dos dados das crianças e à promoção da sensibilização das crianças para a proteção de dados ([113]). No âmbito da Estratégia para uma Internet Melhor para as Crianças, a Comissão disponibiliza recursos de sensibilização e ações de formação para as crianças sobre os seus direitos digitais, incluindo a proteção de dados (por exemplo, consentimento digital) ([114]). É dada cada vez mais atenção à necessidade de ferramentas de verificação da idade eficazes e respeitadoras da privacidade. No início de 2024, a Comissão criou um grupo de trabalho para a verificação da idade com os Estados-Membros, o Comité e o Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual, com o objetivo de debater e apoiar o desenvolvimento de uma abordagem europeia à verificação da idade. Este trabalho continuará agora no âmbito do comité do Regulamento dos Serviços Digitais, no grupo de trabalho de proteção de menores. No contexto do Regulamento Identidade Digital da UE ([115]), que entrou em vigor

([108]) Diretiva (UE) 2020/1828, de 25 de novembro de 2020, relativa a ações coletivas para proteção dos interesses coletivos dos consumidores e que revoga a Diretiva 2009/22/CE (JO L 409 de 4.12.2020, p. 1).
([109]) Considerando 38 do RGPD.
([110]) Recomendação sobre o desenvolvimento e o reforço de sistemas integrados de proteção das crianças no interesse superior da criança: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection_pt.
([111]) Ver também o documento sobre a posição e conclusões do Conselho, n.º 31, alínea a).
([112]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([113]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=pt
([114]) https://digital-strategy.ec.europa.eu/pt/policies/strategy-better-internet-kids
([115]) Regulamento (UE) 2024/1183 que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação do Regime Europeu para a Identidade Digital (JO L, 2024/1183, 30.4.2024).

em maio de 2024, a Comissão está a trabalhar no sentido de garantir que a carteira europeia de identidade digital é disponibilizada a todos os cidadãos e residentes da UE em 2026, incluindo para fins de verificação da idade. Entretanto, até que o ecossistema da carteira esteja plenamente operacional, será desenvolvida e disponibilizada em toda a UE uma solução de curto prazo para a verificação da idade.

# 5 OPORTUNIDADES E DESAFIOS PARA AS ORGANIZAÇÕES, EM ESPECIAL AS PME

O RGPD criou condições de concorrência equitativas para as empresas que operam no mercado interno e a sua abordagem tecnologicamente neutra e favorável à inovação permite às empresas reduzir a burocracia e beneficiar de uma maior confiança dos consumidores ([116]). Muitas empresas desenvolveram uma cultura interna de proteção de dados e encaram a privacidade e a proteção de dados como parâmetros fundamentais da concorrência. As empresas valorizam a abordagem baseada no risco do RGPD como um princípio orientador que permite flexibilizar e ajustar as suas obrigações ([117]).

## 5.1 Conjunto de instrumentos para empresas

O RGPD prevê um conjunto de instrumentos que permitem às organizações gerir de forma flexível e demonstrar a sua conformidade, incluindo códigos de conduta, mecanismos de certificação e cláusulas contratuais-tipo. Tal como anunciado no relatório de 2020, a Comissão adotou em 2021 cláusulas contratuais-tipo para o relacionamento entre o responsável pelo tratamento e o respetivo executante do tratamento ([118]). Estas cláusulas contratuais-tipo proporcionam um instrumento voluntário de conformidade pronto a utilizar e fácil de aplicar, o que é particularmente útil para as PME ou as organizações que possam não dispor de recursos para negociar contratos individuais com os seus parceiros comerciais. As empresas têm opiniões díspares sobre a utilização das cláusulas contratuais-tipo, na medida em que algumas empresas (principalmente PME) as utilizam total ou parcialmente, enquanto outras (sobretudo as empresas de maior dimensão) tendem a não o fazer porque preferem utilizar cláusulas próprias.

As empresas sublinham que os códigos de conduta têm um grande potencial enquanto instrumento de conformidade setorial e eficaz em termos de custos ([119]). No entanto, a elaboração de códigos de conduta tem sido limitada ([120]). De acordo com as informações disponíveis até à data, apenas foram aprovados dois códigos a nível da UE (ambos no setor da computação em nuvem) e seis a nível nacional ([121]). As partes interessadas referem os requisitos onerosos (incluindo a necessidade de criar um organismo de supervisão acreditado), a falta de empenho das autoridades de proteção de dados e o processo de

([116]) Como é reconhecido no relatório da Plataforma Prontos para o Futuro, um grupo de peritos de alto nível criado para ajudar a Comissão a simplificar a legislação da UE e a reduzir os custos desnecessários que lhe estão associados: https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f_pt. Ver também o resumo das reações do grupo de peritos multilateral sobre o RGPD e o documento sobre a posição e conclusões do Conselho, n.º 12.

([117]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.

([118]) Decisão de Execução (UE) 2021/915 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo entre os responsáveis pelo tratamento de dados pessoais e os subcontratantes nos termos do artigo 28.º, n.º 7, do RGPD e do artigo 29.º, n.º 7, do RGPD (C/2021/3701) (JO L 199 de 7.6.2021, p. 18).

([119]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.

([120]) Documento sobre a posição e conclusões do Conselho, n.º 25.

([121]) https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_pt?f%5B0%5D=coc_scope%3Anational

aprovação moroso como principais fatores que limitam a adoção de códigos de conduta ([122]).

É necessário aumentar a transparência do processo e definir prazos de aprovação claros. As autoridades de proteção de dados e, no caso dos códigos a nível da UE, o Comité devem incentivar mais ativamente a elaboração de códigos de conduta, colaborando com as associações que os desenvolvem, o que ajudará a resolver as divergências de interpretação e a acelerar o processo de aprovação. As partes interessadas lamentam os longos atrasos na adoção de códigos de conduta, causados pelo facto de, no âmbito dos trabalhos sobre as orientações, estarem a ser debatidas paralelamente outras questões. Do mesmo modo, as empresas referem que a certificação não é amplamente utilizada, uma vez que o processo de desenvolvimento é lento e complexo. Como no caso dos códigos de conduta, as autoridades de proteção de dados devem prever prazos mais claros para a revisão e aprovação das certificações.

Na sua estratégia para 2024-2027, o Comité comprometeu-se a continuar a apoiar medidas de conformidade, como a certificação e os códigos de conduta, nomeadamente colaborando com os principais grupos de partes interessadas para explicar as possibilidades de utilização dos instrumentos ([123]).

### 5.2 Problemas específicos das PME e dos pequenos operadores

No relatório de 2020, a Comissão apelou à intensificação dos esforços para apoiar a conformidade das PME com o RGPD. Nos últimos anos, as autoridades de proteção de dados e o Comité continuaram a desenvolver instrumentos de conformidade para as PME, apoiados, em parte, por financiamento da Comissão ([124]). Em abril de 2023, o Comité lançou um guia sobre a proteção de dados para as pequenas empresas ([125]), que fornece informações práticas às PME num formato acessível e facilmente compreensível.

As PME de muitos Estados-Membros sublinham os benefícios de um apoio personalizado por parte das autoridades locais de proteção de dados. No entanto, devido às diferentes abordagens das autoridades de proteção de dados em matéria de sensibilização e orientação, as PME de alguns Estados-Membros encaram a conformidade como uma questão complexa e receiam ser objeto de medidas de execução ([126]). As autoridades de proteção de dados devem redobrar os seus esforços para fazer face a estes problemas, nomeadamente colaborando proativamente com as PME para dissipar quaisquer preocupações infundadas relativas à conformidade. As autoridades de proteção de dados devem concentrar-se na disponibilização de apoio personalizado e ferramentas práticas, tais como modelos (por exemplo, para a realização de avaliações de impacto sobre a proteção de dados), linhas telefónicas de apoio, exemplos ilustrativos, listas de verificação e orientações sobre operações de tratamento específicas (por exemplo, faturação ou boletins informativos) e medidas técnicas e organizativas. Uma vez que a maioria das PME não dispõe de conhecimentos especializados internos em matéria de proteção de dados, quaisquer orientações dirigidas a essas empresas devem ser fáceis de compreender por quem não tem formação jurídica ([127]).

([122]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([123]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf
([124]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=pt
([125]) https://edpb.europa.eu/sme-data-protection-guide/home_en
([126]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([127]) Ver o documento sobre a posição e conclusões do Conselho, n.º 24; resumo das reações do grupo de peritos multilateral sobre o RGPD.

Em conformidade com a abordagem baseada no risco do RGPD, as PME que realizam atividades de tratamento de baixo risco não estão sujeitas a encargos de conformidade substanciais. Embora a derrogação relativa à conservação de registos das atividades de tratamento ([128]) se aplique em circunstâncias limitadas ([129]), as PME que efetuam um tratamento de baixo risco podem cumprir essa obrigação mantendo registos simplificados baseados em modelos fornecidos pelas autoridades de proteção de dados. Além disso, há que encarar esses registos como um instrumento útil para as PME fazerem um balanço das suas atividades de tratamento.

### 5.3 Encarregados da proteção de dados

Os encarregados da proteção de dados desempenham um papel importante na garantia do cumprimento do RGPD nas organizações em que trabalham. Em geral, os encarregados da proteção de dados que operam na UE têm os conhecimentos e as competências necessários para desempenhar as suas funções ao abrigo do RGPD e a sua independência é respeitada ([130]). No entanto, subsistem vários problemas, nomeadamente: i) dificuldades em designar encarregados da proteção de dados com os conhecimentos especializados necessários; ii) falta de normas a nível da UE em matéria de educação e formação; iii) ausência de uma integração adequada dos encarregados da proteção de dados nos processos organizacionais; iv) falta de recursos; v) funções adicionais não relacionadas com a proteção de dados; e vi) antiguidade insuficiente ([131]). O Comité observou que é necessário que as autoridades de proteção de dados intensifiquem as atividades de sensibilização, bem como as suas ações de informação e execução, a fim de assegurar que os encarregados da proteção de dados possam desempenhar as suas funções ao abrigo do RGPD ([132]).

## 6 O RGPD COMO PEDRA ANGULAR DA POLÍTICA DA UE NA ESFERA DIGITAL

### 6.1 Uma política digital baseada no RGPD

No relatório de 2020, a Comissão comprometeu-se a apoiar uma aplicação coerente do quadro de proteção de dados no que se refere às novas tecnologias para incentivar a inovação e o desenvolvimento tecnológico. Desde então, a UE adotou uma série de iniciativas, algumas das quais completam o RGPD ou especificam a forma como este deve ser aplicado em domínios específicos, a fim de prosseguir objetivos específicos, como a seguir se apresenta.

- O Regulamento dos Serviços Digitais ([133]), que visa proporcionar um ambiente em linha seguro para as pessoas e as empresas, proíbe as plataformas em linha de exibirem anúncios publicitários com base na definição de perfis utilizando «categorias especiais de dados pessoais», tal como definidas no RGPD.

([128]) Artigo 30.º, n.º 5, do RGPD.
([129]) Se a organização empregar menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.º, n.º 1, do RGPD ou dados pessoais relativos a condenações penais e infrações referido no artigo 10.º do mesmo regulamento.
([130]) Documento sobre a posição e conclusões do Conselho, n.º 26; CEPD, *2023 Coordinated Enforcement Action: Designation and Position of Data Protection Officers* (não traduzido para português): https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf
([131]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.
([132]) Ver recomendações no âmbito da Ação de Supervisão Coordenada do CEPD.
([133]) Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) (JO L 277 de 27.10.2022, p. 1).

- Para tornar os mercados digitais mais equitativos e mais disputáveis, o Regulamento dos Mercados Digitais ([134]) proíbe os operadores designados como «controladores de acesso» de «combinar» e «utilizar de forma cruzada» dados pessoais entre os seus serviços essenciais de plataforma e outros serviços, a menos que o utilizador tenha dado o seu «consentimento», tal como definido no RGPD.
- O Regulamento Inteligência Artificial ([135]) especifica as regras da UE em matéria de proteção de dados para domínios específicos em que se utiliza a IA, por exemplo, os sistemas de identificação biométrica à distância, o tratamento de categorias especiais de dados para detetar enviesamentos e o tratamento adicional de dados pessoais em ambientes de testagem da regulamentação.
- A diretiva relativa ao trabalho nas plataformas digitais ([136]) completa o RGPD no domínio do emprego, estabelecendo regras sobre os sistemas automatizados de monitorização e tomada de decisões utilizados pelas plataformas de trabalho digitais e, em especial, limitações ao tratamento de dados pessoais, e prevendo obrigações em matéria de transparência, supervisão e revisão humanas e portabilidade.
- O Regulamento Propaganda Política ([137]) proíbe a utilização de categorias especiais de dados pessoais na propaganda política e exige uma maior transparência nas técnicas de direcionamento e de amplificação utilizadas.
- O Regulamento Identidade Digital Europeia possibilita a criação de uma carteira europeia de identidade digital universal, fiável e segura, que permitirá às pessoas apresentar provas de atributos pessoais como cartas de condução, diplomas e contas bancárias, com pleno controlo sobre os seus dados pessoais e sem partilha desnecessária de dados.

A proposta de Regulamento Privacidade Eletrónica ([138]), que visa substituir a atual Diretiva Privacidade Eletrónica ([139]) e completar o quadro legislativo em matéria de privacidade e proteção de dados, está a ser negociada há vários anos. É necessária uma reflexão sobre as próximas etapas desta iniciativa, incluindo a sua relação com o RGPD.

O Regulamento Europa Interoperável ([140]) visa tornar os serviços públicos digitais interoperáveis em toda a UE. Apoia a cooperação entre as autoridades de proteção de dados, em especial através de ambientes de testagem da regulamentação da interoperabilidade.

Várias iniciativas da UE proporcionam uma base jurídica para o tratamento de dados pessoais por entidades privadas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais. Qualquer legislação deste tipo deve ser cuidadosamente especificada para minimizar a interferência com o direito à proteção dos dados pessoais e deve ser proporcional ao objetivo prosseguido ([141]). A Carta, o RGPD e a jurisprudência do Tribunal de Justiça proporcionam um quadro que deve servir de base para a avaliação destas iniciativas. O pacote proposto em matéria de luta contra o branqueamento de capitais

([134]) Regulamento (UE) 2022/1925 (Regulamento dos Mercados Digitais) (JO L 265 de 12.10.2022, p. 1).
([135]) Regulamento (UE) 2024/1689 (Regulamento da Inteligência Artificial), JO L, 2024/1689, de 12.7.2024.
([136]) Trabalhadores das plataformas: Conselho confirma acordo sobre novas regras para melhorar as suas condições de trabalho — Consilium (europa.eu).
([137]) Regulamento (UE) 2024/900 sobre a transparência e o direcionamento da propaganda política (JO L, 2024/900, 20.3.2024).
([138]) Proposta de regulamento relativo à privacidade e às comunicações eletrónicas, COM(2017) 10 final.
([139]) Diretiva 2002/58/CE (Diretiva Privacidade Eletrónica) (JO L 201 de 31.7.2002, p. 37).
([140]) Regulamento (UE) 2024/903 (Regulamento Europa Interoperável) (JO L, 2024/903, 22.3.2024).
([141]) Ver o documento sobre a posição e conclusões do Conselho, n.º 31, alínea f).

([142]) contém garantias substanciais para a proteção dos dados pessoais, sem comprometer os objetivos de atenuar os riscos de branqueamento de capitais e de financiamento do terrorismo e detetar eficazmente as tentativas criminosas de utilização abusiva do sistema financeiro da UE.

Neste contexto, o Conselho salientou que qualquer nova legislação da UE que contenha disposições relativas ao tratamento de dados pessoais deverá ser coerente com o RGPD e a jurisprudência do Tribunal de Justiça.

### 6.2 Um quadro jurídico para reforçar a partilha de dados

A estratégia para os dados visa criar um mercado único de dados, que permita a livre circulação de dados na UE e entre setores, em prol das empresas, dos investigadores e das administrações públicas. Um dos principais objetivos da estratégia para os dados é a criação de espaços comuns europeus de dados que facilitem o agrupamento, o acesso e a partilha de dados. Quanto aos dados pessoais, o RGPD estabelece o quadro para todas as iniciativas que visam reforçar a livre circulação de dados na UE (um objetivo estabelecido no próprio RGPD). No que diz respeito aos dados pessoais, as proteções do RGPD não são alteradas.

O Regulamento Governação de Dados ([143]) e o Regulamento dos Dados ([144]) são pilares da estratégia para os dados. O Regulamento Governação de Dados estabelece regras concretas no contexto da reutilização de dados do setor público que incluam dados pessoais e estabelece um quadro legislativo para os serviços de intermediação de dados, incluindo os serviços de gestão de informações pessoais (SGIP) ou os serviços de computação em nuvem para dados pessoais oferecidos, a fim de capacitar os titulares dos dados no exercício dos seus direitos ao abrigo do RGPD. Define igualmente as condições de utilização dos dados para fins altruístas. O Regulamento dos Dados reforça o controlo dos titulares dos dados sobre os dados que geram através da utilização de objetos inteligentes de que são proprietários ou locatários, impondo requisitos técnicos em matéria de acesso e portabilidade dos dados.

O Espaço Europeu de Dados de Saúde (EEDS) ([145]) reflete as necessidades específicas identificadas no setor dos dados de saúde, baseando-se também no RGPD. Permite às pessoas aceder facilmente aos seus dados de saúde em formato eletrónico e partilhá-los com os profissionais de saúde, nomeadamente noutros Estados-Membros, melhorando a prestação de cuidados de saúde e aumentando o controlo dos doentes sobre os seus dados. Estabelece igualmente um quadro jurídico comum para a reutilização de dados de saúde para fins como a investigação, a inovação e a saúde pública, com base numa autorização emitida por um organismo responsável pelo acesso aos dados de saúde. A fim de assegurar a proteção dos dados pessoais, o EEDS proporcionará um enquadramento fiável para o acesso seguro aos dados de saúde e para o tratamento desses dados. A Comissão continua a apoiar os esforços para desenvolver espaços comuns europeus de dados em 14 setores, através da aplicação do novo quadro legislativo e do financiamento de iniciativas setoriais específicas.

([142]) https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en?prefLang=pt.
([143]) Regulamento (UE) 2022/868 (Regulamento Governação de Dados) (JO L 152 de 3.6.2022, p. 1).
([144]) Regulamento (UE) 2023/2854 (Regulamento dos Dados) (JO L, 2023/2854, 22.12.2023).
([145]) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_PT.html.

### 6.3 Governação das novas regras digitais

O desenvolvimento da regulamentação digital torna necessária uma cooperação estreita em todos os domínios regulamentares ([146]). Esta cooperação é tanto mais necessária quanto as questões relativas à proteção de dados estão cada vez mais interligadas com questões como, por exemplo, o direito da concorrência, a legislação de proteção dos consumidores, as regras dos mercados digitais, a regulação das comunicações eletrónicas e a cibersegurança. É o caso, por exemplo, da apreciação da compatibilidade dos modelos de «consentimento ou pagamento» com o direito da União.

Em alguns casos, as autoridades de proteção de dados são responsáveis pela aplicação de disposições específicas da nova legislação digital da UE ([147]). A nova regulamentação digital também cria estruturas específicas que reúnem os reguladores competentes para assegurar uma aplicação coerente, como o grupo de alto nível para o Regulamento dos Mercados Digitais, o Comité Europeu da Inovação de Dados (criado ao abrigo do Regulamento Governação de Dados) e o Comité Europeu dos Serviços Digitais (criado ao abrigo do Regulamento dos Serviços Digitais). A Diretiva SRI 2 ([148]) estabelece regras mais pormenorizadas sobre a cooperação entre as autoridades reguladoras e as autoridades de proteção de dados no tratamento de incidentes de segurança que constituem violações de dados pessoais.

Fora destas estruturas formais, as autoridades de proteção de dados estão a tomar medidas para assegurar que as suas ações são complementares e coerentes com outros domínios regulamentares. Em julho de 2020, as autoridades de defesa dos consumidores e de proteção de dados criaram um «grupo de voluntários» para determinar boas práticas e partilhar experiências em matéria de aplicação. As autoridades de proteção de dados continuam a participar em seminários conjuntos com a rede de cooperação de defesa do consumidor. Em 2023, o Comité criou um grupo de trabalho sobre a interação entre a proteção de dados, a concorrência e a proteção dos consumidores.

Embora esta evolução seja positiva, são necessários meios de cooperação mais estruturados e eficientes, em especial para fazer face a situações que afetam um grande número de pessoas na UE e envolvem vários reguladores ([149]). Essas estruturas devem assegurar que as autoridades continuam sempre a ser responsáveis por todas as questões relativas ao cumprimento das regras nos seus domínios de competência. Os Estados-Membros devem também procurar garantir uma cooperação adequada a nível nacional ([150]).

## 7 TRANSFERÊNCIAS INTERNACIONAIS E COOPERAÇÃO A NÍVEL MUNDIAL

### 7.1 Conjunto de instrumentos de transferência previsto no RGPD

Os fluxos de dados tornaram-se parte integrante da transformação digital da sociedade e da globalização da economia. Mais do que nunca, o respeito da privacidade constitui uma condição prévia de fluxos comerciais estáveis, seguros e competitivos, bem como um elemento facilitador de muitas formas de cooperação internacional. O conjunto de

([146]) Ver o documento sobre a posição e conclusões do Conselho, n.º 40 e 41; resumo das reações do grupo de peritos multilateral sobre o RGPD.
([147]) Ver, por exemplo, o artigo 37.º, n.º 3, do Regulamento dos Dados.
([148]) Diretiva (UE) 2022/2555 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80).
([149]) Ver o documento sobre a posição e conclusões do Conselho, pontos 18, 40 e 41, e o resumo das reações do grupo de peritos multilateral sobre o RGPD.
([150]) A Alemanha criou um «agregado digital», que inclui reguladores de vários domínios, com vista a alargar a sua cooperação em todos os aspetos da digitalização e partilhar conhecimentos e boas práticas: https://www.dataguidance.com/news/germany-bsi-announces-formation-digital-cluster-bonn

instrumentos de transferência previsto no capítulo V do RGPD oferece uma variedade de instrumentos para enfrentar diferentes cenários de transferência, assegurando simultaneamente que os dados continuam a beneficiar de um elevado nível de proteção quando saem da UE.

Desde o relatório de 2020, os requisitos para as transferências de dados estabelecidos na legislação da UE em matéria de proteção de dados foram esclarecidos e o conjunto de instrumentos de transferência continuou a evoluir. Há um esclarecimento importante relativamente ao conceito de «transferência internacional», que foi definido pelo Comité ([151]) como abrangendo qualquer divulgação de dados pessoais por um responsável pelo tratamento ou executante do tratamento cujo tratamento esteja sujeito ao RGPD a outro responsável pelo tratamento ou executante do tratamento num país terceiro, independentemente de o tratamento por este último estar ou não sujeito ao RGPD ([152]). Estas orientações do Comité foram particularmente importantes para proporcionar segurança jurídica aos responsáveis pelo tratamento e executantes do tratamento europeus quanto aos cenários em que é necessário um instrumento de transferência ao abrigo do capítulo V do RGPD.

O Tribunal de Justiça também forneceu esclarecimentos adicionais, no seu acórdão Schrems II ([153]), sobre a proteção que diferentes instrumentos de transferência têm de proporcionar para assegurar que não é comprometido o nível de proteção garantido pelo RGPD ([154]). Em especial, estes instrumentos têm de assegurar que as pessoas cujos dados pessoais são transferidos para fora da UE beneficiam de um nível de proteção substancialmente equivalente ao garantido na União ([155]). Cabe ao exportador de dados da UE avaliar se é esse o caso, tendo em conta as circunstâncias específicas das suas transferências ([156]).

Para avaliar o nível de proteção, os exportadores de dados devem ter em consideração as garantias em matéria de proteção de dados estabelecidas no instrumento de transferência celebrado com um importador de dados de um país terceiro (por exemplo, um contrato), bem como elementos pertinentes do sistema jurídico do país em que o importador de dados está localizado, em especial no que diz respeito ao eventual acesso aos dados pelas autoridades públicas desse país ([157]). Esses elementos devem ser apreciados à luz dos critérios de avaliação da adequação previstos no artigo 45.º do RGPD. O Tribunal de Justiça também aprofundou estes critérios, em especial no que se refere às regras relativas ao acesso aos dados pessoais pelas autoridades públicas para efeitos de aplicação da lei e de segurança nacional.

Esta interpretação também se refletiu nas orientações do Comité, que atualizou o seu «referencial de adequação» ([158]) (o qual forneceu orientações sobre os elementos que a Comissão deve ter em conta ao realizar uma avaliação da adequação). O Comité adotou igualmente novas orientações que fornecem esclarecimentos adicionais sobre: i) os elementos a ter em conta pelos exportadores de dados individuais ao avaliar o nível de proteção; ii) uma visão geral das possíveis fontes que podem ser utilizadas; e iii) exemplos de possíveis medidas complementares (por exemplo, garantias contratuais e técnicas) ([159]).

([151]) Diretrizes 05/2021 do CEPD.
([152]) Secção 2 das Diretrizes 05/2021 do CEPD.
([153]) Processo C-311/18, ECLI:EU:C:2020:559 (Schrems II).
([154]) Acórdão Schrems II, n.º 93.
([155]) Acórdão Schrems II, n.os 96 e 105.
([156]) Acórdão Schrems II, n.º 131.
([157]) Acórdão Schrems II, n.º 105.
([158]) Recomendações 02/2020 do CEPD e referencial de adequação, WP 254 rev. 01.
([159]) Recomendações 01/2020 do CEPD, completadas pelas Recomendações 02/2020.

As orientações salientam especificamente que cada avaliação efetuada pelos exportadores de dados é única e que estes, por conseguinte, devem ter em conta as características específicas de cada transferência, que podem diferir em função da finalidade da transferência de dados, dos tipos de entidades envolvidas, do setor em que a transferência ocorre, das categorias de dados pessoais transferidos, etc. ([160]).

Tendo em conta estes diferentes esclarecimentos sobre os requisitos aplicáveis às transferências internacionais de dados, foram tomadas medidas significativas nos últimos anos para continuar a desenvolver e operacionalizar o conjunto de instrumentos de transferência previsto no RGPD.

#### *7.1.1 Decisões de adequação*

As reações recebidas das partes interessadas refletiram também que as decisões de adequação continuam a desempenhar um papel fundamental no conjunto de instrumentos de transferência previsto no RGPD ([161]), proporcionando uma solução simples e abrangente para as transferências de dados, sem necessidade de o exportador de dados fornecer garantias adicionais ou obter qualquer autorização. Ao permitirem a livre circulação de dados pessoais, estas decisões abriram canais comerciais aos operadores da UE, nomeadamente ao complementar e ampliar os benefícios dos acordos comerciais, e facilitaram a colaboração com parceiros estrangeiros num vasto leque de domínios, desde a cooperação regulamentar à investigação.

Desde o relatório de 2020, continuou a aumentar o número de países que adotaram legislação moderna em matéria de proteção de dados, que prevê, nomeadamente, princípios fundamentais de proteção de dados, direitos individuais e aplicação efetiva por parte de reguladores independentes. Esta tendência ([162]) permitiu igualmente à Comissão intensificar o seu trabalho de adequação, incluindo a adoção de uma decisão de adequação relativa ao Reino Unido ([163]), que é fundamental para assegurar o bom funcionamento dos vários acordos celebrados com o Reino Unido na sequência do Brexit. A fim de assegurar que continua preparada para o futuro, a decisão de adequação inclui uma «cláusula de caducidade» que expira em 2025, mas pode ser renovada se o nível de proteção se mantiver adequado. A Comissão adotou igualmente uma decisão de adequação relativa à República da Coreia ([164]), que completa o Acordo de Comércio Livre UE-Coreia no que diz respeito aos fluxos de dados pessoais e facilita a cooperação regulamentar. Está prevista para o final de 2024 uma primeira avaliação da decisão de adequação.

Além disso, na sequência da invalidação da decisão de adequação relativa ao Escudo de Proteção da Privacidade UE-EUA, a Comissão encetou conversações com o Governo dos Estados Unidos tendo em vista um novo acordo em conformidade com os requisitos clarificados pelo Tribunal de Justiça ([165]). O presidente dos EUA adotou um novo decreto presidencial sobre o reforço das garantias para as atividades de recolha de informações de origem eletromagnética dos Estados Unidos, que introduziu novas garantias vinculativas e executórias para assegurar que o acesso aos dados para fins de segurança nacional só seja possível na medida do necessário e proporcionado e que os europeus disponham de vias de recurso eficazes. Nessa base, a Comissão adotou a sua decisão de adequação relativa ao

([160]) Ver, por exemplo, n.ºs 8 a 13, 32 e 33 das Recomendações 01/2020 do CEPD.
([161]) Ver, por exemplo, o contributo do Comité, páginas 7 e 8; documento sobre a posição e conclusões do Conselho, n.º 36; resumo das reações do grupo de peritos multilateral sobre o RGPD.
([162]) Comunicação da Comissão intitulada «Intercâmbio e proteção de dados pessoais num mundo globalizado», 10.1.2017 [COM(2017) 7 final].
([163]) Decisão de Execução (UE) 2021/1772 da Comissão (JO L 360 de 11.10.2021, p. 1).
([164]) Decisão de Execução (UE) 2022/254 da Comissão (JO L 44 de 24.2.2022, p. 1).
([165]) https://commission.europa.eu/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-2020-08-10_en?prefLang=pt

Quadro de Privacidade de Dados UE-EUA (QPD) ([166]), que permite que os dados pessoais circulem livremente da UE para as empresas norte-americanas que aderem ao QPD. Uma vez que as garantias instituídas pelo Governo dos EUA no domínio da segurança nacional se aplicam a todas as transferências de dados para empresas nos EUA, independentemente do mecanismo de transferência do RGPD que seja utilizado, o recurso a outros instrumentos, como cláusulas contratuais-tipo e regras vinculativas aplicáveis às empresas, foi significativamente facilitado. No verão de 2024, terá lugar uma primeira avaliação do funcionamento do QPD, a fim de verificar se todos os elementos pertinentes foram integralmente aplicados no quadro jurídico dos EUA e se estão a funcionar eficazmente na prática.

Estão atualmente em curso negociações sobre a adequação com o Brasil e o Quénia, bem como, pela primeira vez, com várias organizações internacionais (por exemplo, as conversações sobre a adequação com a Organização Europeia de Patentes encontram-se em fase avançada) ([167]). Em consonância também com os apelos de várias partes interessadas ([168]), a Comissão empenhou-se ativamente em conversações exploratórias com países de diferentes regiões do mundo.

A Comissão também acompanha continuamente a evolução nos países que já beneficiam das conclusões de adequação e revê periodicamente as decisões existentes, em conformidade com as obrigações correspondentes ao abrigo do RGPD ([169]). Em abril de 2023, a Comissão adotou o seu relatório sobre a primeira avaliação periódica da decisão de adequação relativa ao Japão ([170]), que concluiu que o Japão continua a assegurar um nível de proteção adequado ([171]). A avaliação demonstrou que os quadros de proteção de dados da UE e do Japão continuaram a convergir desde a adoção das decisões de adequação mútua.

Além disso, em conformidade com o artigo 97.º do RGPD, teve início, no âmbito da avaliação de 2020 da aplicação e do funcionamento do RGPD, a primeira avaliação das 11 decisões de adequação ([172]) adotadas ao abrigo do antigo quadro de proteção de dados da UE (Diretiva Proteção de Dados). A conclusão deste aspeto da avaliação foi adiada, nomeadamente para ter em conta o acórdão do Tribunal de Justiça no processo Schrems II e a subsequente interpretação pelo Comité. Os esclarecimentos acima referidos do Tribunal sobre os principais elementos do padrão de adequação conduziram a intercâmbios pormenorizados com os países e territórios em causa sobre aspetos pertinentes do seu quadro jurídico, bem como sobre os mecanismos de supervisão e execução.

Em 15 de janeiro de 2024, a Comissão publicou o seu relatório sobre estas 11 decisões, juntamente com relatórios pormenorizados por país que descrevem a evolução em cada um dos países e territórios desde a adoção das decisões de adequação, bem como as regras que regem o acesso aos dados pessoais pelas autoridades públicas, em especial para efeitos de

([166]) Decisão de Execução (UE) 2023/1795 da Comissão (JO L 231 de 20.9.2023, p. 118).

([167]) A Organização Europeia de Patentes é uma organização intergovernamental instituída com base na Convenção sobre a Patente Europeia e que tem como principal função conceder as patentes europeias. Neste contexto, coopera estreitamente com as empresas e as autoridades públicas dos Estados-Membros da UE, bem como com diferentes instituições e organismos da UE.

([168]) Contributo do Comité, páginas 7 e 8.

([169]) Artigo 45.º, n.ºs 4 e 5, do RGPD. Ver também acórdão Schrems I, n.º 76.

([170]) Decisão de Execução (UE) 2019/419 da Comissão (JO L 76 de 19.3.2019, p. 1). Ver também https://ec.europa.eu/commission/presscorner/detail/pt/IP_19_421. Esta decisão constituiu a primeira decisão de adequação adotada ao abrigo do RGPD e o primeiro acordo de adequação recíproca.

([171]) Relatório da Comissão sobre a primeira avaliação da aplicação da decisão de adequação relativa ao Japão, 3.4.2023, COM(2023) 275 final [e SWD(2023) 75 final].

([172]) Andorra, Argentina, Canadá (para os operadores comerciais), Ilhas Faroé, Guernesey, Ilha de Man, Israel, Jersey, Nova Zelândia, Suíça e Uruguai.

aplicação da lei e de segurança nacional ([173]). O relatório conclui que os 11 países e territórios continuam a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE e que todos os países e territórios em causa modernizaram e reforçaram de diferentes formas o seu quadro jurídico em matéria de privacidade. Além disso, a fim de colmatar as diferenças pertinentes no que se refere ao nível de proteção, foram negociadas e acordadas garantias adicionais para os dados pessoais transferidos da Europa, sempre que necessário para assegurar a continuidade da decisão de adequação, com alguns desses países e territórios.

Estas avaliações mostram igualmente que as decisões de adequação, em vez de serem um «ponto final», lançaram as bases para uma cooperação mais estreita e uma maior convergência regulamentar entre a UE e estes parceiros que partilham a mesma visão. Por exemplo, o relatório sobre a primeira avaliação da decisão de adequação relativa ao Japão reconhece que o reforço do quadro japonês em matéria de proteção de dados pode abrir caminho para um alargamento da decisão de adequação para além das trocas comerciais, a fim de abranger as transferências atualmente excluídas do seu âmbito de aplicação, como acontece no domínio da investigação e da cooperação regulamentar. Estão em curso conversações para estudar esse eventual alargamento. Em geral, as decisões de adequação tornaram-se uma componente estratégica da relação global da UE com estes parceiros estrangeiros e são reconhecidas como um importante elemento facilitador do aprofundamento da cooperação numa vasta gama de domínios.

Além de proporcionar uma base sólida para uma maior cooperação bilateral, a rede crescente de países e territórios relativamente aos quais a UE adotou uma decisão de adequação oferece novas oportunidades para maximizar os benefícios de fluxos de dados seguros e livres e para estreitar a cooperação entre parceiros que partilham a mesma visão na aplicação das regras de proteção de dados. Por conseguinte, em março de 2024, a Comissão organizou a primeira reunião de alto nível sobre fluxos de dados seguros, que reuniu os ministros responsáveis e os diretores das autoridades de proteção de dados de 15 países e territórios relativamente aos quais a UE adotou uma decisão de adequação, bem como o presidente do Comité Europeu para a Proteção de Dados ([174]). Na reunião, foram identificados vários pontos de ação concretos que estão a ser acompanhados no âmbito deste grupo.

Em termos mais gerais, graças ao seu «efeito de rede», as decisões de adequação adotadas pela Comissão Europeia são cada vez mais pertinentes também fora da UE, uma vez que permitem não só a livre circulação de dados com as 30 economias do EEE, mas também com muitas mais jurisdições em todo o mundo que reconhecem os países para os quais existe uma decisão de adequação da UE como «destinos seguros» ao abrigo das suas próprias regras de proteção de dados ([175]).

#### *7.1.2 Instrumentos que proporcionam garantias adequadas*

Desde o relatório de 2020, foram desenvolvidos instrumentos adicionais que proporcionam garantias adequadas e foram emitidas orientações práticas para facilitar a sua utilização.

Seguindo o que fora anunciado no relatório de 2020, a Comissão adotou cláusulas contratuais-tipo (CCT) ([176]) modernizadas desenvolvidas, em grande medida, com base

([173]) Relatório da Comissão sobre a primeira revisão do funcionamento das decisões de adequação adotadas nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE, 15.1.2024, COM(2024) 7 final [e SWD(2024) 3 final].

([174]) https://ec.europa.eu/commission/presscorner/detail/pt/mex_24_1307#11

([175]) Por exemplo, Argentina, Colômbia, Israel, Marrocos, Suíça e Uruguai.

([176]) Decisão de Execução (UE) 2021/914 da Comissão (JO L 199 de 7.6.2021, p. 31).

nas reações de várias partes interessadas ([177]). As novas CCT substituíram os três conjuntos de CCT que foram adotados ao abrigo da Diretiva Proteção de Dados. As principais inovações incluem: i) garantias atualizadas em conformidade com o RGPD; ii) uma abordagem modular com um ponto de entrada único que abrange um vasto leque de cenários de transferência; iii) maior flexibilidade para a utilização de CCT por múltiplas partes; e iv) um conjunto de instrumentos práticos para executar o acórdão Schrems II.

As CCT modernizadas foram bem acolhidas pelas partes interessadas e as reações recebidas confirmam que as CCT continuam a ser, de longe, o instrumento mais utilizado para as transferências pelos exportadores de dados da UE ([178]). Para ajudar os exportadores de dados nos seus esforços de conformidade, a Comissão elaborou um conjunto de perguntas e respostas com orientações adicionais sobre a utilização das cláusulas ([179]), que serão atualizadas caso surjam novas questões, nomeadamente à luz de novas reações recebidas no âmbito desta avaliação.

Muitos exportadores de dados indicam que têm dificuldades em realizar as «avaliações de impacto das transferências» exigidas pelo acórdão Schrems II, referindo, em especial, a sua complexidade, bem como os custos e o tempo necessários para as realizar ([180]). Embora se congratulem com as orientações do Comité e com as CCT, solicitam orientações adicionais (por exemplo, sobre as responsabilidades das partes envolvidas e o nível de pormenor exigido nas avaliações de impacto das transferências) e instrumentos suplementares para apoiar a realização dessas avaliações (por exemplo, modelos, avaliações gerais por país, catálogos de riscos). Apesar de as partes interessadas se terem referido principalmente às CCT, as mesmas avaliações são igualmente necessárias para outros instrumentos de transferência (como as regras vinculativas aplicáveis às empresas). Por conseguinte, é importante que o Comité — com base na experiência adquirida com a aplicação dos requisitos do acórdão Schrems II nos últimos anos, nomeadamente no âmbito das atividades de execução das autoridades nacionais de proteção de dados — pondere estudar formas/instrumentos para continuar a ajudar os exportadores de dados nos seus esforços de conformidade neste contexto.

A fim de complementar as CCT existentes, a Comissão está a desenvolver conjuntos adicionais de cláusulas para proporcionar um pacote abrangente e coerente aos exportadores de dados da UE. Esse pacote incluirá CCT, ao abrigo do Regulamento (UE) 2018/1725, relativas a transferências de dados pelas instituições e organismos da UE para operadores comerciais em países terceiros ([181]) e CCT relativas a transferências de dados para importadores de dados de países terceiros cujas operações de tratamento estejam diretamente sujeitas ao RGPD. Estas últimas dão resposta ao apelo das partes interessadas no sentido de abordar especificamente cenários em que o importador de dados é abrangido pelo âmbito de aplicação territorial do RGPD (por exemplo, porque o tratamento em causa visa o mercado da UE, em conformidade com o artigo 3.º, n.º 2, do RGPD) ([182]). O Comité esclareceu que também neste caso é necessário um instrumento de transferência ao abrigo do capítulo V do RGPD, tendo em conta os riscos acrescidos para os dados pessoais tratados fora da UE, por exemplo devido a legislações nacionais eventualmente

([177]) Incluindo, por exemplo, o Parecer conjunto 2/2021 do CEPD e da AEPD no âmbito do procedimento de adoção das CCT.

([178]) Documento sobre a posição e conclusões do Conselho, n.º 37, contributo do Comité, página 9, resumo das reações do grupo de peritos multilateral sobre o RGPD.

([179]) https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_pt.

([180]) Ver, por exemplo, o resumo das reações do grupo de peritos multilateral sobre o RGPD.

([181]) Em conformidade com o artigo 48.º, n.º 2, alínea b), do Regulamento (UE) 2018/1725.

([182]) Documento sobre a posição e conclusões do Conselho, n.º 37, contributo do Comité, página 9, resumo das reações do grupo de peritos multilateral sobre o RGPD.

contraditórias ou a um acesso governamental desproporcionado no país terceiro ([183]). As novas CCT que a Comissão está a elaborar abordarão especificamente este cenário e terão plenamente em conta os requisitos que já se aplicam diretamente a esses responsáveis pelo tratamento e executantes do tratamento ao abrigo do RGPD ([184]).

Como também foi reconhecido por diferentes tipos de partes interessadas ([185]), as cláusulas-modelo desempenham um papel cada vez mais central na facilitação dos fluxos de dados em todo o mundo. Várias jurisdições aprovaram as CCT da UE como um mecanismo de transferência ao abrigo da sua própria legislação em matéria de proteção de dados, com um número limitado de adaptações formais à sua ordem jurídica interna ([186]). Vários outros países adotaram cláusulas-modelo próprias que partilham características comuns importantes com as CCT da UE ([187]). Um exemplo particularmente pertinente é a criação de cláusulas-modelo por outras organizações ou redes internacionais/regionais, como o Comité Consultivo da Convenção 108 do Conselho da Europa, a Rede Ibero-Americana de Proteção de Dados e a Associação das Nações do Sudeste Asiático (ASEAN) ([188]), da qual resultam novas oportunidades para facilitar os fluxos de dados entre as diferentes regiões do mundo com base em cláusulas-modelo. Um exemplo concreto é o Guia UE-ASEAN sobre as CCT da UE e as cláusulas-modelo da ASEAN, baseado nos contributos das empresas, que apoia estas últimas nos seus esforços de conformidade ao abrigo de ambos os conjuntos de cláusulas ([189]).

Para além das CCT, as regras vinculativas aplicáveis às empresas (RVE) continuam a ser amplamente utilizadas para os fluxos de dados entre membros de grupos empresariais ou entre empresas envolvidas numa atividade económica conjunta. Desde a aplicação do RGPD, o Comité adotou 80 pareceres favoráveis sobre decisões nacionais que aprovaram RVE ([190]). O Comité emitiu igualmente orientações sobre os elementos a incluir nas RVE para os responsáveis pelo tratamento (e as informações a disponibilizar no âmbito de um pedido de RVE), que foram atualizadas para refletir os requisitos do RGPD e o acórdão Schrems II ([191]). Estão também a ser elaboradas orientações atualizadas sobre as RVE para os executantes do tratamento ([192]). Uma vez que as RVE visam pôr em prática políticas/programas vinculativos de proteção de dados nas empresas, muitas partes interessadas consideram-nas um instrumento de conformidade particularmente útil e um instrumento de transferência fiável ([193]). Ao mesmo tempo, as partes interessadas continuam a indicar que a duração e a complexidade do processo de aprovação pelas autoridades nacionais de proteção de dados estão a impedir uma adoção mais ampla das

([183]) Diretrizes 05/2021 do CEPD, p. 3.
([184]) Conforme estabelecido também nas Diretrizes 05/2021 do CEPD, secção 4.
([185]) Contributo do Comité, página 9, resumo das reações do grupo de peritos multilateral sobre o RGPD.
([186]) Por exemplo, o Reino Unido (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) e a Suíça (https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html).
([187]) Por exemplo, a Nova Zelândia (https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/) e a Argentina (https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm).
([188]) Ver https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4; https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-pt.pdf e https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
([189]) https://commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062_en?filename=%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf.
([190]) Contributo do Comité, página 9.
([191]) Recomendações 1/2022 do CEPD.
([192]) Contributo do Comité, página 9.
([193]) Resumo das reações do grupo de peritos multilateral sobre o RGPD.

RVE. Por conseguinte, é importante que as autoridades continuem a trabalhar no sentido de racionalizar e encurtar o processo de aprovação.

Desde o relatório de 2020, foram igualmente tomadas medidas para facilitar a utilização da certificação e dos códigos de conduta como instrumentos para as transferências, por exemplo, através da adoção de orientações específicas do Comité sobre ambos os instrumentos ([194]). Ao mesmo tempo, as partes interessadas reiteram as questões supramencionadas relativas ao calendário e à complexidade do processo de aprovação no que diz respeito à certificação e aos códigos de conduta enquanto instrumentos de responsabilização.

Por último, o RGPD prevê igualmente instrumentos específicos — acordos internacionais e acordos administrativos aprovados pelas autoridades de proteção de dados — a utilizar pelas autoridades públicas para transferir dados pessoais para as suas homólogas em países terceiros ou para organizações internacionais. O Comité adotou orientações sobre as garantias a incluir nesses instrumentos ([195]), que podem apoiar a negociação desses dois tipos de acordos.

#### *7.1.3 Assegurar a complementaridade com outras políticas*

Uma vez que os fluxos de dados se tornaram essenciais para tantas atividades, é fundamental assegurar a complementaridade entre as políticas de proteção de dados e outras políticas. A inclusão de garantias em matéria de proteção de dados nos instrumentos internacionais é, muitas vezes, não apenas uma condição prévia para os fluxos de dados, mas também um importante elemento facilitador de uma cooperação estável e fiável.

Por exemplo, os acordos internacionais que preveem as garantias necessárias em matéria de proteção de dados, nomeadamente assegurando a continuidade da proteção por parte da autoridade requerente, são essenciais para garantir a cortesia e facilitar o acesso transfronteiras das autoridades de aplicação da lei às provas eletrónicas na posse das empresas e, desta forma, uma luta mais eficaz contra a criminalidade. Esta abordagem reflete-se no Segundo Protocolo Adicional à Convenção sobre o Cibercrime ([196]), que reforça as regras em vigor para a obtenção de acesso transfronteiras a provas eletrónicas em investigações criminais, assegurando simultaneamente garantias adequadas em matéria de proteção de dados. O Protocolo foi entretanto assinado por vários Estados-Membros da UE. Do mesmo modo, estão a avançar as negociações bilaterais entre a UE e os EUA relativas a um acordo sobre o acesso transfronteiras a provas eletrónicas para efeitos de cooperação em matéria penal ([197]).

O intercâmbio de dados dos registos de identificação dos passageiros (PNR) é outro domínio da política de segurança da UE que beneficiou do desenvolvimento de garantias sólidas em matéria de proteção de dados. Em 2023, a UE e o Canadá concluíram as negociações sobre um novo acordo PNR, em conformidade com os requisitos estabelecidos pelo Tribunal de Justiça no seu Parecer 1/15 ([198]). Foram introduzidas garantias semelhantes no capítulo PNR do Acordo de Comércio e Cooperação UE-Reino Unido. A inclusão de proteções reforçadas da privacidade nestes acordos, que pode servir de modelo para futuros acordos com outros parceiros, proporciona segurança jurídica às

([194]) Diretrizes 07/2022 e 04/2021 do CEPD.
([195]) Diretrizes 2/2020 do CEPD.
([196]) Segundo Protocolo Adicional à Convenção sobre o Cibercrime, relativo ao reforço da cooperação e da divulgação de provas eletrónicas (STCE n.º 224).
([197]) https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en?prefLang=pt.
([198]) Proposta da Comissão de decisão do Conselho relativa à assinatura, em nome da União Europeia, de um acordo entre o Canadá e a União Europeia sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros (PNR), COM(2024) 94 final.

transportadoras aéreas, assegurando simultaneamente a estabilidade de importantes intercâmbios de informações para combater o terrorismo e outros crimes transnacionais graves.

A Comissão defende também, no âmbito das negociações em curso na Organização Mundial do Comércio relativas à iniciativa de declaração conjunta sobre o comércio eletrónico, disposições sólidas para proteger a privacidade e impulsionar o comércio digital. Foram sistematicamente incluídas disposições semelhantes sobre a luta contra os obstáculos injustificados ao comércio digital, protegendo simultaneamente o espaço político necessário das partes no domínio da proteção de dados, nos acordos de comércio livre celebrados pela UE após a entrada em vigor do RGPD, nomeadamente no Acordo de Comércio e Cooperação UE-Reino Unido e nos acordos com o Chile, o Japão e a Nova Zelândia. Estão também a ser debatidas disposições relativas à privacidade e aos fluxos de dados nas negociações em curso com Singapura e a Coreia do Sul sobre o comércio digital.

## 7.2 Cooperação internacional em matéria de proteção de dados

### *7.2.1 A dimensão bilateral*

A Comissão continuou a dialogar com países e organizações internacionais sobre a elaboração, a reforma e a aplicação das regras em matéria de privacidade, nomeadamente apresentando observações em relação a consultas públicas sobre projetos de legislação ou medidas regulamentares no domínio da privacidade ([199]), testemunhando perante as instâncias parlamentares competentes ([200]) e participando em reuniões específicas com representantes governamentais, delegações parlamentares e reguladores de muitas regiões do mundo ([201]). Algumas destas atividades foram realizadas através do projeto «Reforço da proteção e do fluxo de dados», financiado pela UE, que apoia os países que pretendem desenvolver quadros modernos de proteção de dados ou reforçar a capacidade das suas autoridades reguladoras, através da formação, da partilha de conhecimentos, do reforço das capacidades e do intercâmbio de boas práticas. A Comissão também contribuiu para outras iniciativas, como a Aliança Digital UE-CELAC.

A proteção de dados continuará também a desempenhar um papel fundamental nos trabalhos da Comissão relacionados com o alargamento. A legislação da UE em matéria de proteção de dados é uma componente importante do esforço global dos países do alargamento para alinhar os seus quadros jurídicos com os da UE (especialmente porque o tratamento e o intercâmbio de dados pessoais estão no cerne de muitas políticas). Além disso, a independência e o bom funcionamento de uma autoridade de proteção de dados constituem um elemento fundamental do equilíbrio de poderes e do Estado de direito em geral e tornar-se-ão cada vez mais importantes à medida que a UE integra gradualmente os países do alargamento no mercado único (tal como previsto em iniciativas como o plano de crescimento para os Balcãs Ocidentais).

Um aspeto cada vez mais importante do diálogo da UE com países terceiros é o dos intercâmbios entre reguladores. Tal como anunciado no relatório de 2020, a Comissão criou um «Instituto de Proteção de Dados» para promover intercâmbios entre as autoridades de proteção de dados da UE e de países terceiros e, desta forma, contribuir para o reforço das capacidades e melhorar a cooperação «no terreno». O Instituto disponibiliza ações de formação personalizadas a pedido das autoridades de países terceiros e reúne os conhecimentos especializados de representantes da comunidade de

([199]) Organizadas, por exemplo, pela Austrália, China, Ruanda, Argentina, Brasil, Etiópia, Indonésia, Peru, Malásia e Tailândia.

([200]) Por exemplo, perante as instâncias parlamentares do Chile, do Equador e do Paraguai.

([201]) Incluindo também a organização de seminários e visitas de estudo, por exemplo com o Quénia, a Indonésia e Singapura.

autoridades de aplicação da lei, do meio académico, do setor privado e das instituições europeias. O valor acrescentado das ações de formação reside na adaptação das diferentes componentes aos interesses e necessidades da autoridade que as solicita. Além disso, estas ações de formação permitem às autoridades de proteção de dados da UE e de países terceiros estabelecer contactos, partilhar conhecimentos, trocar experiências e boas práticas e identificar potenciais domínios de cooperação. Até à data, o Instituto prestou formação às autoridades de proteção de dados da Indonésia, do Brasil, do Quénia, da Nigéria e do Ruanda e está atualmente a preparar ações de formação para vários outros países.

Além de ser importante manter um diálogo entre os reguladores, é cada vez mais necessário, tal como reconhecido nas reações recebidas do Conselho e do Comité ([202]), desenvolver instrumentos jurídicos adequados para formas mais estreitas de cooperação e assistência mútua, nomeadamente permitindo o necessário intercâmbio de informações no contexto das investigações. Com efeito, uma vez que as violações da privacidade produzem cada vez mais efeitos além-fronteiras, muitas vezes só a cooperação entre os reguladores da UE e de países terceiros permite investigá-las e abordá-las de forma eficaz. Por conseguinte, a Comissão procurará obter autorização para encetar negociações com vista à celebração de acordos de cooperação em matéria de aplicação da lei com países terceiros pertinentes (tal como previsto no artigo 50.º do RGPD). A este respeito, a Comissão regista o apelo do Comité para que se considerem especificamente os países com mais operadores diretamente sujeitos ao RGPD como potenciais homólogos, em especial os países do G7 e/ou os países que beneficiam de decisões de adequação ([203]).

O estabelecimento de tais acordos de cooperação em matéria de aplicação da lei e de assistência mútua contribuiria igualmente para assegurar a conformidade dos operadores estrangeiros que estão sujeitos ao RGPD porque, por exemplo, visam especificamente o mercado da UE através da oferta de bens ou serviços, e garantir uma aplicação eficaz face a esses operadores. O Conselho regista a importância de assegurar o cumprimento do RGPD nesses casos e manifesta preocupação quanto à igualdade de condições de concorrência com as entidades na UE, bem como à proteção efetiva dos direitos das pessoas singulares ([204]). A Comissão concorda com o apelo do Conselho no sentido de explorar diferentes formas de facilitar a aplicação neste cenário. Embora as modalidades mais formais de cooperação com os reguladores de países terceiros possam certamente desempenhar um papel importante, há que prosseguir também com maior determinação a utilização de outras vias já existentes, nomeadamente tirando pleno partido do conjunto de instrumentos de aplicação do artigo 58.º do RGPD e envolvendo os representantes de empresas estrangeiras na UE (designados em conformidade com o artigo 27.º do RGPD).

### *7.2.2 A dimensão multilateral*

A Comissão continua também a participar ativamente numa série de fóruns internacionais para promover valores partilhados e a convergência a nível regional e mundial.

Aí se inclui, por exemplo, um contributo ativo para os trabalhos do Comité Consultivo sobre a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108), o único instrumento multilateral juridicamente vinculativo no domínio da proteção dos dados pessoais. Até à data, 31 Estados ratificaram o protocolo de alteração para modernizar a Convenção 108

([202]) Contributo do Comité, p. 8; documento sobre a posição e conclusões do Conselho, n.º 38.
([203]) Contributo do Comité, página 8.
([204]) Documento sobre a posição e conclusões do Conselho, n.º 39.

([205]), incluindo muitos Estados-Membros da UE, bem como alguns Estados não membros do Conselho da Europa (Argentina, Maurícia e Uruguai). Entre os Estados-Membros da UE, apenas um ([206]) ainda não assinou a Convenção modernizada, enquanto oito ([207]) a assinaram, mas não a ratificaram. A Comissão insta o Estado-Membro restante a assinar a Convenção modernizada e os outros a procederem rapidamente à sua ratificação, a fim de permitir a sua entrada em vigor num futuro próximo. Além disso, a Comissão continua a incentivar proativamente a adesão de países terceiros.

A nível do G20 e do G7, os debates sobre a privacidade e os fluxos de dados centraram-se na operacionalização do conceito de «livre circulação de dados com confiança», inicialmente proposto pelo Japão, que reconhece que a proteção e a segurança dos dados podem contribuir para a confiança na economia digital e facilitar os fluxos de dados ([208]). A OCDE desempenha um papel particularmente importante neste contexto, ao proporcionar um fórum para uma comunidade de peritos em livre circulação de dados com confiança, que reúne um vasto leque de partes interessadas (governos, reguladores, indústria, sociedade civil, meio académico), a fim de contribuir para projetos e questões específicos relacionados com este tema. Além disso, um resultado significativo da iniciativa de livre circulação de dados com confiança, para o qual a Comissão contribuiu significativamente, é a adoção pela OCDE de uma declaração sobre o acesso governamental aos dados pessoais detidos por entidades do setor privado, o primeiro instrumento internacional neste domínio, que contém uma série de requisitos partilhados para salvaguardar a privacidade no acesso a dados pessoais para efeitos de segurança nacional e de aplicação da lei. No contexto do reconhecimento crescente a nível mundial de que um acesso desproporcionado dos governos afeta negativamente a confiança nas transferências de dados, a referida declaração constitui um contributo importante para facilitar os fluxos de dados fiáveis. A Comissão continuará a incentivar os países a aderirem à declaração, que também está aberta a países que não são membros da OCDE.

A Comissão está também a colaborar com diferentes organizações e redes regionais que definem garantias comuns em matéria de proteção de dados. É o caso, por exemplo, da ASEAN, da União Africana, do Fórum das Autoridades de Privacidade da Ásia-Pacífico, da Rede Ibero-Americana de Proteção de Dados e da Rede de Autoridades Africanas de Proteção de Dados (NADPA — RADPD). A elaboração do suprarreferido guia da UE-ASEAN sobre cláusulas-modelo constitui um exemplo concreto dessa cooperação frutuosa.

Por último, a Comissão mantém um diálogo com diferentes organizações internacionais, nomeadamente para explorar formas de facilitar ainda mais os fluxos de dados entre a UE e essas organizações. Uma vez que muitas organizações modernizaram os seus quadros de proteção de dados nos últimos anos, ou estão em vias de o fazer, estão também a surgir novas oportunidades de intercâmbio de experiências e de boas práticas. A este respeito, a Autoridade Europeia para a Proteção de Dados organizou seminários anuais com organizações internacionais e constituiu um grupo de trabalho dedicado às transferências internacionais de dados, que se revelaram fóruns particularmente úteis para o intercâmbio

([205]) Protocolo que altera a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (STCE n.º 223).
([206]) Dinamarca.
([207]) Bélgica, Chéquia, Grécia, Irlanda, Letónia, Luxemburgo, Países Baixos e Suécia.
([208]) Ver, por exemplo, https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communique-data.pdf?download=1.

e a exploração de instrumentos concretos de cooperação, incluindo o intercâmbio de dados pessoais ([209]).

## 8 CONCLUSÃO

Nos seis anos desde que passou a ser aplicável, o RGPD tem capacitado as pessoas ao permitir-lhes ter controlo sobre os seus dados. Contribuiu igualmente para criar condições de concorrência equitativas para as empresas e proporcionou uma pedra angular para as múltiplas iniciativas que estão a impulsionar a transição digital na UE.

De modo a conseguir a plena consecução do duplo objetivo do RGPD, nomeadamente uma forte proteção para as pessoas singulares e ao mesmo tempo a garantia da livre circulação de dados pessoais na UE e a segurança dos fluxos de dados fora da UE, é necessário dar prioridade ao seguinte:

- uma aplicação sólida do RGPD, começando pela rápida adoção da proposta da Comissão relativa a normas processuais para proporcionar vias de recurso céleres e segurança jurídica nos casos que afetam pessoas singulares em toda a UE,
- apoio proativo das autoridades de proteção de dados às partes interessadas nos seus esforços de conformidade, em especial as PME e os pequenos operadores,
- uma interpretação e aplicação coerentes do RGPD em toda a UE,
- cooperação eficaz entre os reguladores, tanto a nível nacional como da UE, a fim de garantir a aplicação uniforme e coerente do conjunto crescente de regras digitais da UE,
- aprofundamento da estratégia internacional da Comissão em matéria de proteção de dados.

De modo a apoiar a aplicação do RGPD e fundamentar reflexões posteriores sobre a proteção de dados, algumas das ações aqui enumeradas foram identificadas como necessárias. A Comissão apoiará e acompanhará a sua aplicação, tendo igualmente em vista o próximo relatório, em 2028.

*Desenvolver estruturas de cooperação eficazes*

O Parlamento Europeu e o Conselho são convidados a adotar rapidamente a proposta relativa às normas processuais do RGPD.

O Comité e as autoridades de proteção de dados são convidados a:

- estabelecer uma cooperação regular com outros reguladores setoriais sobre questões com impacto na proteção de dados, em especial os instituídos ao abrigo da nova legislação digital da UE, e participar ativamente em estruturas a nível da UE concebidas para facilitar a cooperação entre reguladores,
- utilizar os instrumentos previstos no RGPD num espírito de cooperação leal e eficaz, para que a resolução de litígios seja utilizada apenas em último recurso,
- aplicar modalidades de trabalho mais eficientes e específicas em matéria de orientações, pareceres e decisões e dar prioridade a questões fundamentais, a fim de reduzir os encargos para as autoridades de proteção de dados e responder mais rapidamente à evolução do mercado.

Os Estados-Membros têm de:

([209]) https://www.edps.europa.eu/data-protection/our-work/edps-worldwide/data-protection-and-international-organisations_en

- assegurar a independência absoluta e efetiva das autoridades nacionais de proteção de dados,
- afetar recursos suficientes às autoridades de proteção de dados para que possam desempenhar as suas funções, nomeadamente dotando-as dos recursos técnicos e dos conhecimentos especializados necessários para fazer face às tecnologias emergentes e cumprir novas responsabilidades ao abrigo da legislação digital,
- dotar as autoridades de proteção de dados dos instrumentos de investigação necessários para que possam utilizar eficazmente os poderes de execução previstos no RGPD,
- apoiar o diálogo entre as autoridades de proteção de dados e outros reguladores nacionais, em especial os instituídos ao abrigo da nova legislação digital.

A Comissão irá:

- apoiar ativamente a rápida adoção da proposta relativa às normas processuais do RGPD pelos colegisladores,
- continuar a acompanhar de perto a independência absoluta e efetiva das autoridades nacionais de proteção de dados,
- estabelecer sinergias e coerência entre o RGPD e toda a legislação relativa ao tratamento de dados pessoais com base na experiência adquirida e, se necessário, tomar as medidas adequadas para proporcionar segurança jurídica,
- refletir sobre a melhor forma de confrontar a necessidade de uma cooperação estruturada e eficiente entre reguladores para garantir a aplicação eficaz, uniforme e coerente das regras digitais da UE, respeitando simultaneamente a competência das autoridades de proteção de dados em relação a todas as questões relativas ao tratamento de dados pessoais.

*Aplicar e completar o quadro jurídico*

Os Estados-Membros têm de:

- assegurar que as autoridades de proteção de dados são consultadas em tempo útil, antes da adoção de legislação sobre o tratamento de dados pessoais.

A Comissão irá:

- continuar a utilizar todos os instrumentos à sua disposição, incluindo procedimentos de infração, para assegurar o cumprimento do RGPD pelos Estados-Membros,
- continuar a apoiar as trocas de pontos de vista e práticas nacionais entre os Estados-Membros, nomeadamente através do grupo de peritos dos Estados-Membros no âmbito do RGPD,
- tomar medidas para garantir que as crianças sejam protegidas, capacitadas e respeitadas em linha,
- refletir sobre as possíveis próximas etapas no âmbito da proposta de Regulamento Privacidade Eletrónica, incluindo a sua relação com o RGPD.

*Apoiar as partes interessadas*

O Comité e as autoridades de proteção de dados são convidados a:

- encetar um diálogo construtivo com os responsáveis pelo tratamento e os executantes do tratamento sobre a conformidade com o RGPD,
- intensificar os esforços para apoiar a conformidade das PME, fornecendo orientações e instrumentos adaptados, eliminando quaisquer preocupações infundadas das PME

relativamente à conformidade quando não têm o tratamento de dados pessoais como atividade principal e acompanhando-as nos seus esforços de conformidade;

- apoiar a aplicação de medidas de conformidade eficazes pelas empresas, como a certificação e os códigos de conduta (nomeadamente como instrumentos de transferência), colaborando com as partes interessadas durante o processo de aprovação, estabelecendo prazos claros para as aprovações e, tal como prometido na estratégia do Comité para 2024-2027, explicando aos principais grupos de partes interessadas as possibilidades de utilização destes instrumentos,
- assegurar que as orientações nacionais e a aplicação do RGPD a nível nacional são coerentes com as orientações do Comité e com a jurisprudência do Tribunal de Justiça,
- resolver interpretações divergentes do RGPD entre as autoridades de proteção de dados, incluindo autoridades do mesmo Estado-Membro,
- disponibilizar orientações concisas, práticas e acessíveis ao público pertinente, como prometido na estratégia do Comité para 2024-2027,
- assegurar uma consulta mais precoce e mais substancial sobre orientações e pareceres, a fim de compreender melhor a dinâmica do mercado e as práticas comerciais, ter devidamente em conta as reações recebidas e ter em consideração a aplicação concreta das interpretações adotadas,
- concluir, com caráter prioritário, os trabalhos em curso relativos às orientações sobre os dados das crianças, a investigação científica, a anonimização, a pseudonimização e o interesse legítimo,
- intensificar as atividades de sensibilização, a informação e as medidas de execução, a fim de assegurar que os encarregados da proteção de dados possam desempenhar as suas funções ao abrigo do RGPD.

A Comissão irá:

- continuar a prestar apoio financeiro às atividades das autoridades de proteção de dados que facilitem o cumprimento das obrigações decorrentes do RGPD por parte das PME,
- utilizar todos os meios disponíveis para prestar esclarecimentos expeditos sobre questões importantes para as partes interessadas, incluindo as PME, em especial solicitando pareceres ao Comité.

*Continuar a desenvolver o conjunto de instrumentos para as transferências de dados e a cooperação internacional*

O Comité e as autoridades de proteção de dados são convidados a:

- concluir os trabalhos sobre a racionalização e o encurtamento do processo de aprovação de regras vinculativas para as empresas, bem como sobre a atualização das orientações relativas aos elementos a incluir nas regras vinculativas aplicáveis às empresas para os executantes do tratamento,
- explorar formas/instrumentos para continuar a ajudar os exportadores de dados nos seus esforços de conformidade com os requisitos do acórdão Schrems II,
- estudar outras formas de assegurar uma aplicação eficaz face a operadores estabelecidos em países terceiros abrangidos pelo âmbito de aplicação territorial do RGPD.

Os Estados-Membros têm de:

- assegurar a assinatura e as ratificações ainda pendentes da Convenção 108+ modernizada do Conselho da Europa o mais rapidamente possível, a fim de permitir a sua entrada em vigor.

A Comissão irá:

- continuar a realizar progressos nas conversações em curso sobre a adequação, explorar o aprofundamento das conclusões de adequação existentes e encetar novos diálogos sobre a adequação com os parceiros interessados,
- apoiar uma maior cooperação entre a rede de países que beneficiam de decisões de adequação,
- concluir os trabalhos sobre cláusulas contratuais-tipo adicionais, em especial no que diz respeito às transferências de dados para importadores de dados cujo tratamento esteja diretamente sujeito ao RGPD e às transferências de dados pelas instituições e organismos da UE ao abrigo do Regulamento (UE) 2018/1725,
- cooperar com parceiros internacionais para facilitar os fluxos de dados com base em cláusulas contratuais-modelo,
- apoiar os processos de reformas em curso em países terceiros sobre regras novas ou regras atualizadas em matéria de proteção de dados, através da partilha de experiências e de boas práticas,
- colaborar com organizações internacionais e regionais, como a OCDE e o G7, para promover fluxos de dados fiáveis com base em normas elevadas de proteção de dados, nomeadamente no âmbito da iniciativa de circulação de dados com confiança,
- facilitar e apoiar os intercâmbios entre os reguladores europeus e internacionais, nomeadamente através do seu Instituto de Proteção de Dados,
- contribuir para facilitar a cooperação internacional em matéria de aplicação da lei entre as autoridades de supervisão, nomeadamente através da negociação de acordos de cooperação e de assistência mútua.