

Bruxelas, 10.1.2017
COM(2017) 7 final

**COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO
CONSELHO**

Intercâmbio e proteção de dados pessoais num mundo globalizado

1. INTRODUÇÃO

A proteção de dados pessoais faz parte dos fundamentos constitucionais comuns da União Europeia e está consagrada no artigo 8.º do Carta dos Direitos Fundamentais da UE. Ocupa um lugar central na legislação da UE há mais de 20 anos, desde a Diretiva Proteção de Dados em 1995¹ («Diretiva de 1995»), até à adoção do Regulamento Geral sobre a Proteção de Dados (RGPD)² e da Diretiva Cooperação Policial³ em 2016.

Como salientou o Presidente Juncker no seu discurso sobre o estado da União, em 14 de setembro de 2016, *«[s]er europeu significa ter o direito a que os nossos dados pessoais sejam protegidos por legislação europeia eficaz. [...] Porque, na Europa, as questões da privacidade são importantes. Trata-se de uma questão de dignidade humana.»*

A exigência de proteção dos dados pessoais não se limita, porém, à Europa. Os consumidores de todo o mundo conferem uma importância cada vez maior ao respeito da sua privacidade. As empresas, por seu lado, reconhecem que uma sólida proteção da privacidade lhes confere vantagens competitivas à medida que a confiança nos seus serviços aumenta. São muitas as empresas, especialmente as de dimensão mundial, que estão a alinhar as suas políticas de privacidade com o Regulamento Geral sobre a Proteção de Dados, não só porque pretendem exercer as suas atividades na UE, mas também porque consideram o referido regulamento como um modelo a seguir.

No mesmo sentido, vários países e organizações regionais externos à UE, desde a nossa vizinhança mais próxima até à Ásia, América Latina e África, estão a adotar nova legislação ou a atualizar legislação existente em matéria de proteção de dados para aproveitar as oportunidades oferecidas pela economia digital global e responder à procura crescente de reforço da segurança dos dados e de proteção da privacidade. Embora existam diferenças entre os países no que toca à abordagem adotada e ao nível de desenvolvimento legislativo, existem sinais de uma maior convergência em relação a importantes princípios da proteção de dados, especialmente em determinadas regiões do mundo⁴. Uma compatibilidade acrescida entre os diferentes sistemas de proteção de dados poderia facilitar os fluxos internacionais de dados pessoais, seja para fins comerciais ou de cooperação entre entidades públicas (por exemplo, autoridades com funções coercivas). A UE deve aproveitar esta oportunidade para

¹ Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

² Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, pp. 1–88). Entrou em vigor em 24 de maio de 2016 e é aplicável a partir de 25 de maio de 2018.

³ Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, pp. 89-131). Entrou em vigor em 5 de maio de 2016. Os Estados-Membros da UE devem transpô-la para o direito nacional até 6 de maio de 2018.

⁴ Ver «Data protection regulations and international data flows: Implications for trade and development», CNUCED (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

promover os seus valores de proteção de dados e facilitar a circulação de dados, para tal incentivando a convergência dos sistemas jurídicos. Como foi anunciado no programa de trabalho da Comissão⁵, a presente comunicação define, portanto, o quadro estratégico da Comissão em termos de «decisões de adequação», bem como outras ferramentas aplicáveis às transferências de dados e instrumentos internacionais de proteção de dados.

2. O PACOTE LEGISLATIVO DE REFORMAS DA UE EM MATÉRIA DE PROTEÇÃO DE DADOS - UM QUADRO LEGISLATIVO MODERNO QUE CONFERE UM ELEVADO NÍVEL DE PROTEÇÃO AOS FLUXOS INTERNACIONAIS DE DADOS

A reforma da legislação da UE em matéria de proteção de dados, adotada em abril de 2016, estabelece um sistema que assegura um elevado nível de proteção e simultaneamente está aberto às oportunidades proporcionadas pela sociedade da informação mundial. Ao permitir aos indivíduos exercerem um maior controlo sobre os seus dados pessoais, a reforma reforça a confiança dos consumidores na economia digital. Ao harmonizar e simplificar o enquadramento jurídico, torna o exercício das atividades das empresas na UE, nacionais e estrangeiras, mais fácil e menos complexo, inclusive através de intercâmbios internacionais de dados. Atualmente, a UE combina a abertura à circulação internacional de dados com o mais elevado nível de proteção para os indivíduos, tendo potencial para se tornar numa plataforma de serviços de dados que exige livre circulação e confiança.

2.1 Um quadro abrangente, unificado e simplificado em matéria de proteção de dados na UE

A reforma da UE estabelece um quadro abrangente que regula o tratamento de dados pessoais, tanto nos setores privado e público, como nos setores comercial e de aplicação da lei (o Regulamento Geral sobre a Proteção de Dados e a Diretiva Cooperação Policial, respetivamente).

Por força do Regulamento Geral sobre a Proteção de Dados, a partir de maio de 2018 haverá um único conjunto pan-europeu de normas, ao contrário das atuais 28 legislações nacionais. O mecanismo de balcão único recentemente criado assegura que uma autoridade de proteção de dados (APD) será responsável pelo controlo das operações transnacionais de tratamento de dados realizadas por uma empresa na UE. A coerência na interpretação das novas normas será, portanto, garantida. Em especial, nos casos transnacionais em que estão envolvidas várias autoridades de proteção de dados nacionais, será adotada uma única decisão para assegurar que problemas comuns tenham soluções comuns. Além disso, o Regulamento Geral sobre a Proteção de Dados estabelece a igualdade de condições entre as empresas da UE e as empresas estrangeiras no sentido em que as empresas estabelecidas fora da UE terão de aplicar as mesmas normas das empresas europeias se oferecerem bens e serviços ou se monitorizarem o comportamento de pessoas na UE. Um nível de confiança dos consumidores mais elevado beneficiará tanto os operadores comerciais da UE como os operadores comerciais de países terceiros.

⁵ Programa de Trabalho da Comissão para 2017 - Realizar uma Europa que protege, capacita e defende, COM(2016) 710 final de 25.10.2016, p. 12 e anexo I.

A Diretiva Cooperação Policial prevê normas comuns para o tratamento de dados pessoais das pessoas envolvidas em ações penais, quer se trate de suspeitos, vítimas ou testemunhas, não deixando de ter em conta a natureza específica dos domínios policial e de justiça penal. A harmonização das normas de proteção de dados no domínio da aplicação coerciva da lei, incluindo normas sobre transferências internacionais, facilitará a cooperação transnacional entre as autoridades policiais e judiciais, tanto a nível da UE como com parceiros internacionais, criando desta forma condições para combater mais eficazmente a criminalidade. Trata-se de um importante contributo para a Agenda Europeia para a Segurança⁶.

2.2 Um conjunto renovado e diversificado de instrumentos destinados às transferências internacionais

Desde a sua conceção que a legislação da UE em matéria de proteção de dados previu diversos mecanismos destinados a permitir as transferências internacionais de dados. O principal objetivo destas normas consiste em assegurar que, quando os dados pessoais de cidadãos europeus são transferidos para o estrangeiro, a proteção acompanha esses dados. Ao longo dos anos, estas normas serviram de referência à circulação internacional de dados em muitas jurisdições. Embora a arquitetura permaneça essencialmente a mesma que existia ao abrigo da Diretiva 1995, a reforma das normas relativas às transferências internacionais clarifica e simplifica a sua utilização e introduz novos instrumentos para as transferências.

Por força do direito da UE, um meio de transferir dados pessoais para o estrangeiro tem por base uma «decisão de adequação» da Comissão, na qual se estabelece que um país não pertencente à UE possui um nível de proteção de dados que é «substancialmente equivalente»⁷ ao garantido a nível da UE. O efeito de tal decisão consiste em permitir a livre circulação de dados pessoais para esse país terceiro sem haver necessidade de o exportador de dados apresentar outras garantias ou obter qualquer autorização. Os países ou as organizações internacionais interessados têm à disposição um catálogo rigoroso e pormenorizado de elementos que a Comissão deve ter em conta quando avalia a adequação da proteção de um sistema estrangeiro⁸. A Comissão também pode agora adotar decisões de adequação no

⁶ Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões intitulada «Agenda Europeia para a Segurança», COM(2015) 185 final de 28.4.2015.

⁷ Acórdão do Tribunal de Justiça da UE, de 6 de outubro de 2015, no processo C-362/14, *Maximillian Schrems/Data Protection Commissioner*, n.ºs 73, 74 e 96. Ver também o considerando 104 do Regulamento Geral sobre a Proteção de Dados e o considerando 67 da Diretiva Cooperação Policial que fazem referência à norma de equivalência essencial.

⁸ Ver artigo 45.º do Regulamento Geral sobre a Proteção de Dados. Como previsto no artigo 45.º, n.º 2, na sua avaliação, a Comissão deve ter em conta, entre outros, o primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, nomeadamente em matéria de proteção de dados, segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais. Estes devem estar sustentados por direitos efetivos e oponíveis, incluindo vias de recurso administrativo e judicial para pessoas singulares, e por uma autoridade de controlo independente com funcionamento efetivo para assegurar e impor o respeito das normas de proteção de dados. Também são tomadas em consideração a adesão a convenções juridicamente vinculativas, em particular a Convenção n.º 108 do Conselho da Europa, e a participação em sistemas multilaterais ou regionais relacionados com a proteção de dados.

domínio da aplicação coerciva da lei⁹. Além disso, a reforma, apoiando-se na experiência adquirida com a Diretiva de 1995, prevê explicitamente a avaliação da adequação da proteção num território específico de um país terceiro ou num setor ou indústria específicos de um país terceiro (a denominada adequação «parcial»)¹⁰.

Na falta de uma decisão de proteção adequada, as transferências internacionais podem efetuar-se com base em vários instrumentos de transferência alternativos que prevejam as garantias adequadas em matéria de proteção de dados¹¹. A reforma formaliza e alarga as possibilidades de utilização de instrumentos existentes, como as cláusulas contratuais-tipo¹² e as regras vinculativas aplicáveis às empresas¹³. Por exemplo, as cláusulas contratuais-tipo podem agora ser incluídas num contrato entre um subcontratante estabelecido na UE e subcontratantes estabelecidos num país terceiro (as denominadas cláusulas-tipo entre subcontratantes)¹⁴. No que diz respeito às regras vinculativas aplicáveis às empresas, que até à data se limitavam a acordos entre entidades do mesmo grupo empresarial, podem agora ser utilizadas por um grupo de empresas envolvidas numa atividade económica conjunta, mas que não façam necessariamente parte do mesmo grupo empresarial¹⁵. A reforma também reduz a burocracia, eliminando os requisitos gerais de notificação prévia e de autorização das autoridades de proteção de dados relativamente a transferências para um país terceiro com base em cláusulas contratuais-tipo ou regras vinculativas aplicáveis às empresas¹⁶. Trata-se de uma simplificação importante do sistema de transferências internacionais de dados da UE, uma vez que a existência desses requisitos, que atualmente variam de um Estado-Membro para outro, é frequentemente considerada um obstáculo significativo à circulação de dados, em especial para as pequenas empresas¹⁷.

Além disso, a reforma introduz novos instrumentos para as transferências internacionais¹⁸. Os responsáveis pelo tratamento e os subcontratantes poderão utilizar, em determinadas

⁹ Ver artigo 36.º, n.º 2, da Diretiva Cooperação Policial em relação aos elementos específicos de avaliação da adequação.

¹⁰ Ver artigo 45.º, n.º 1, do Regulamento Geral sobre a Proteção de Dados, e o artigo 36.º, n.º 1, da Diretiva Cooperação Policial.

¹¹ Ver, por exemplo, a Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (*Schrems*), COM(2015) 566 final de 6.11.2015.

¹² As cláusulas contratuais-tipo enunciam as obrigações de proteção de dados respetivas entre o exportador da UE e o importador do país terceiro.

¹³ As regras vinculativas aplicáveis às empresas são regras internas adotadas por um grupo multinacional de empresas que realiza transferências de dados dentro do mesmo grupo empresarial para entidades localizadas em países que não dispõem de um nível adequado de proteção. Embora as regras vinculativas aplicáveis às empresas já fossem utilizadas ao abrigo da Diretiva de 1995, o Regulamento Geral sobre a Proteção de Dados codifica e formaliza o seu papel enquanto ferramenta de transferência.

¹⁴ Ver artigo 46.º, n.º 2, alíneas c) e d), e considerando 168 do Regulamento Geral sobre a Proteção de Dados.

¹⁵ Ver artigo 46.º, n.º 2, alínea b), o artigo 47.º e considerando 110 do Regulamento Geral sobre a Proteção de Dados.

¹⁶ Ver artigo 46.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados.

¹⁷ O facto de as obrigações de registo constituírem uma barreira ao comércio para muitas empresas, em especial as PME, foi salientado, por exemplo, no relatório da CNUCED, p. 34.

¹⁸ Ver artigo 46.º, n.º 2, alíneas e) e f), do Regulamento Geral sobre a Proteção de Dados.

condições,¹⁹ códigos de conduta ou procedimentos de certificação aprovados (tais como selos ou marcas de proteção da privacidade) para estabelecer «garantias adequadas». Tal deve permitir o desenvolvimento de soluções mais adaptadas às transferências internacionais, refletindo, por exemplo, as características e as necessidades específicas de um dado setor ou indústria ou de circulação de dados particulares. A reforma também confere a possibilidade de prever garantias adequadas em relação às transferências de dados entre autoridades ou organismos públicos com base em acordos internacionais ou acordos administrativos²⁰. Por último, o Regulamento Geral sobre a Proteção de Dados clarifica a utilização das denominadas «derrogações»²¹ (por exemplo, o consentimento do interessado, o cumprimento de um contrato ou motivos importantes de interesse público) nas quais entidades, em situações específicas, possam basear as suas transferências de dados na falta de uma decisão de adequação e independentemente da utilização de um dos instrumentos referidos acima. Inclui especialmente uma derrogação nova, embora limitada, relativa às transferências que possam ocorrer em prol de interesses legítimos²² de uma empresa.

Por último, a reforma confere à Comissão os poderes para elaborar mecanismos internacionais de cooperação destinados a facilitar a aplicação da legislação em matéria de proteção de dados pessoais, inclusive através de acordos de assistência mútua²³. Trata-se, portanto, de um reconhecimento do contributo que formas de cooperação mais estreitas entre as autoridades de controlo a nível internacional podem dar para assegurar simultaneamente uma proteção mais eficaz dos direitos individuais e uma maior segurança jurídica para as empresas.

3. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS NO SETOR COMERCIAL: FACILITAR O COMÉRCIO PROTEGENDO A VIDA PRIVADA

O respeito da vida privada constitui uma condição prévia de fluxos comerciais mundiais estáveis, seguros e competitivos. A vida privada não é um produto negociável²⁴. A Internet e a digitalização de bens e serviços transformaram a economia mundial e a transferência de dados transfronteiras, incluindo os dados pessoais, enquanto parte das operações diárias das empresas europeias de todas as dimensões e de todos os setores de atividade. Atendendo a que as trocas comerciais dependem cada vez mais da circulação de dados pessoais, a confidencialidade e a segurança desses dados tornaram-se essenciais à confiança dos consumidores. Por exemplo, dois terços dos europeus dizem estar preocupados com o facto de não terem qualquer tipo de controlo em relação às informações que facultam em linha, ao

¹⁹ Os responsáveis pela proteção de dados não pertencentes à UE poderão aderir a um código de conduta ou a um procedimento de certificação da UE, assumindo compromissos vinculativos e com força executória, através de acordos contratuais ou outros tipos de compromissos juridicamente vinculativos, no sentido de aplicarem as garantias de proteção de dados incluídas nesses instrumentos. Ver artigo 42.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados.

²⁰ Ver artigo 46.º, n.º 2, alínea a), e artigo 46.º, n.º 3, alínea b), do Regulamento Geral sobre a Proteção de Dados.

²¹ Ver artigo 49.º do Regulamento Geral sobre a Proteção de Dados.

²² Ver artigo 49.º, n.º 1, segundo parágrafo, do Regulamento Geral sobre a Proteção de Dados.

²³ Ver artigo 50.º do Regulamento Geral sobre a Proteção de Dados.

²⁴ Ver, por exemplo, a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões intitulada «Comércio para Todos - Rumo a uma política mais responsável em matéria de comércio e de investimento», COM(2015) 497 final de 14.10.2015, p. 7.

passo que metade dos inquiridos receiam vir a ser vítimas de fraude²⁵. Paralelamente, as empresas europeias que operam em alguns países terceiros são cada vez mais confrontadas com restrições protecionistas que não se podem justificar por considerações legítimas de proteção da vida privada.

Na era digital, a promoção de níveis elevados de proteção de dados deve necessariamente acompanhar a facilitação do comércio internacional. Tendo em conta que a proteção de dados pessoais não é negociável²⁶ nos acordos comerciais, o regime da UE aplicável às transferências internacionais de dados, tal como acima descrito, prevê um amplo e variado conjunto de instrumentos que assegura os fluxos de dados em várias situações, garantindo simultaneamente um elevado nível de proteção.

3.1 Decisões de adequação

Uma decisão de adequação permite a livre circulação de dados pessoais a partir da UE, sem que o exportador de dados da UE tenha de aplicar garantias adicionais ou estar sujeito a outras condições. Ao concluir que a ordem jurídica do país em causa dispõe de um nível adequado de proteção, tal decisão reconhece que o sistema desse país se aproxima do sistema dos Estados-Membros da UE. Daí resulta que as transferências para o país em causa serão equiparadas a transmissões de dados no interior da UE, o que permitirá conceder um acesso privilegiado ao mercado único da UE ao abrir simultaneamente os canais comerciais para os operadores da UE. Como explicado acima, tal reconhecimento requer necessariamente um nível de proteção comparável (ou «essencialmente equivalente»)²⁷ àquele garantido na União. Implica uma avaliação exaustiva do sistema do país terceiro, incluindo as suas normas de acesso aos dados pessoais por parte das autoridades públicas para efeitos de aplicação coerciva da lei, de segurança nacional e outros fins de interesse público.

Simultaneamente, como foi confirmado em 2015 pelo Tribunal de Justiça no acórdão *Schrems*, para que se verifique a adequação não é necessário que as normas da UE sejam reproduzidas ponto por ponto²⁸. Em vez disso, é necessário aferir sobretudo se, através da substância dos direitos de privacidade e da sua aplicação efetiva, execução e controlo, o sistema estrangeiro em causa consegue, no seu conjunto, garantir o nível elevado de proteção exigido. Como demonstram até à data as decisões de adequação, a Comissão está em condições de reconhecer o carácter adequado de um conjunto variado de sistemas de proteção da privacidade que representam diferentes tradições jurídicas. Estas decisões dizem respeito a países que estão estreitamente integrados na União Europeia e seus Estados-Membros (Suíça, Andorra, Ilhas Faroé, Guernsey, Jersey, Ilha de Man), bem como a parceiros comerciais importantes (Argentina, Canadá, Israel, Estados Unidos) e a países que assumem um papel pioneiro na elaboração de legislação em matéria de proteção de dados nas suas regiões respetivas (Nova Zelândia, Uruguai).

²⁵ Eurobarómetro Especial 431 — Proteção dos Dados, junho de 2015.

²⁶ Orientações políticas do Presidente Juncker: «Um novo começo para a Europa: o meu programa para o emprego, o crescimento, a equidade e a mudança democrática».

²⁷ Ver nota de rodapé 7.

²⁸ Cf. n.º 74 do acórdão *Schrems*.

As decisões relativas ao Canadá e aos Estados Unidos são decisões de adequação «parciais». A decisão respeitante ao Canadá aplica-se apenas a entidades privadas abrangidas pela lei canadiana relativa à proteção de informações pessoais e documentos eletrónicos (*Canadian Personal Information Protection and Electronic Documents Act*). A decisão recentemente adotada sobre o nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA²⁹ é um caso particular, na medida em que, na falta de legislação geral em matéria de proteção de dados nos EUA,³⁰ baseia-se em compromissos assumidos pelas empresas participantes tendo em vista aplicar normas estritas de proteção de dados enunciadas nesse acordo, as quais, por sua vez, são executórias por força da legislação americana. Além disso, o Escudo de Proteção da Privacidade assenta nas declarações e garantias específicas dadas pelo governo dos EUA relativamente ao acesso para fins de segurança nacional³¹ que estão na base da decisão de adequação. O respeito desses compromissos será acompanhado de perto pela Comissão e será integrado no reexame anual do funcionamento do quadro.

Nos últimos anos, cada vez mais países em todo o mundo adotaram, ou estão em vias de o fazer, legislação nova em matéria de proteção de dados e privacidade. Em 2015, o número de países que já adotara legislação neste domínio ascendia a 109, um aumento significativo em comparação com os 76 países identificados em meados de 2011³². Além disso, cerca de 35 países estão atualmente a elaborar leis em matéria de proteção de dados³³. Estas leis novas ou revistas tendem a basear-se num conjunto estrutural de princípios comuns, nomeadamente o reconhecimento da proteção de dados como um direito fundamental, a adoção de legislação abrangente neste domínio, a existência de direitos oponíveis de privacidade individual e a criação de uma autoridade de controlo independente. Tal evolução proporciona novas oportunidades de continuar a facilitar a circulação de dados, não deixando de garantir um nível elevado de proteção de dados pessoais constante, nomeadamente através das decisões de adequação.

Por força do direito da UE, uma decisão de adequação requer a vigência de normas de proteção de dados comparáveis às que existem na UE³⁴. Tal diz respeito tanto às proteções de fundo aplicáveis aos dados pessoais como aos mecanismos conexos de controlo e de recurso disponíveis no país terceiro.

²⁹ Decisão de Execução UE (2016) 1250 de 12 de julho de 2016.

³⁰ A Comissão incentiva os EUA a prosseguirem os seus esforços para criar um sistema global de proteção da privacidade e dos dados, permitindo assim a convergência entre os dois sistemas a longo prazo. Ver a Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Transferência transatlântica de dados: restaurar a confiança através de garantias sólidas», COM(2016) 117 final de 29.2.2016.

³¹ Tal inclui, em especial, a aplicação da *Presidential Policy Directive 28* (PPD-28), que impõe várias limitações e garantias para as atividades de «informação de origem eletromagnética» e a nomeação de um provedor específico para tratar as queixas apresentadas por cidadãos da UE nesta matéria.

³² G. Greenleaf, «Global data privacy laws 2015: 109 countries, with European laws now in a minority», (2015) relatório incluído na publicação *Privacy Laws & Business International*, n.º 133, pp. 14-17.

³³ Estudo da CNUCED, pp. 8 e 42 (nota de rodapé 4 supra).

³⁴ A este respeito, a Comissão também toma em consideração as obrigações do país terceiro decorrentes de convenções juridicamente vinculativas, em especial da sua adesão à Convenção n.º 108 e aos respetivos protocolos adicionais, quando efetua uma avaliação de adequação. Ver artigo 45.º, n.º 2, alínea c), e considerando 105 do Regulamento Geral sobre a Proteção de Dados.

Ao abrigo do quadro relativo às decisões de adequação, a Comissão considera que os critérios seguintes devem ser tidos em conta ao avaliar com que países terceiros se deve estabelecer um diálogo em matéria de adequação³⁵:

- i) A importância das relações comerciais (reais ou potenciais) da UE com determinado país terceiro, incluindo a existência de um acordo de comércio livre ou de negociações em curso;
- ii) A importância da circulação de dados pessoais a partir da UE, refletindo os laços geográficos e/ou culturais;
- iii) O papel precursor do país terceiro no domínio da proteção da privacidade e dos dados, que pode servir de modelo a outros países na sua região³⁶; e
- iv) A relação política global com o país terceiro em causa, em especial no contexto da promoção de valores comuns e de objetivos partilhados a nível internacional.

Com base nestas considerações, a Comissão colaborará ativamente com os principais parceiros comerciais do Leste e Sudeste Asiático, começando com o Japão e a Coreia em 2017³⁷, e também com a Índia, em função dos progressos na modernização da sua legislação em matéria de proteção de dados, bem como com os países da América Latina, nomeadamente do Mercosul, e países abrangidos pela Política Europeia de Vizinhança que manifestaram interesse em obter uma «decisão de adequação». Além disso, a Comissão acolhe favoravelmente manifestações de interesse de outros países terceiros que estejam dispostos a colaborar e dialogar sobre estas questões. As discussões respeitantes a uma possível decisão de adequação são um diálogo em dois sentidos que passa por prestar os esclarecimentos necessários sobre as normas de proteção de dados da UE e explorar formas de melhorar a convergência com as leis e práticas dos países terceiros.

Em determinadas situações, em vez de se optar por uma abordagem que englobe todo o país, pode ser mais adequado recorrer a outras opções, tais como uma adequação parcial ou específica para um setor (por exemplo, para os serviços financeiros ou o setor das tecnologias da informação), que podem abranger áreas geográficas ou indústrias que constituem uma parte importante da economia de determinado país terceiro. Tais opções devem ser consideradas à luz de certos elementos, por exemplo, a natureza e o estado de desenvolvimento do regime de proteção da privacidade (legislação única, leis múltiplas ou setoriais, etc.), bem como a estrutura constitucional do país terceiro ou a possibilidade de saber se determinados setores da economia estão particularmente expostos à circulação de dados provenientes da UE.

³⁵ No caso dos países em relação aos quais existem interesses relevantes de cooperação no domínio da segurança interna e da aplicação coerciva da lei, a Comissão explora a possibilidade de emitir decisões de adequação específicas ao abrigo da Diretiva Cooperação Policial (ver secção 4).

³⁶ Este critério pode ser particularmente importante para os países em desenvolvimento e em transição, uma vez que a proteção de dados pessoais é simultaneamente um elemento crucial do Estado de direito e um fator importante da competitividade económica.

³⁷ O Japão e a Coreia adotaram ou modernizaram recentemente a sua legislação visando instituir regimes abrangentes em matéria de proteção dos dados.

A adoção de uma decisão de adequação envolve a abertura de um diálogo específico e formas de cooperação estreita com o país terceiro em causa. As decisões de adequação são documentos evolutivos que devem ser objeto de um acompanhamento atento por parte da Comissão e adaptadas em caso de um acontecimento que afete o nível de proteção assegurado pelo país terceiro em causa³⁸. Para esse efeito, serão realizados reexames periodicamente (pelo menos de quatro em quatro anos), a fim de responder a questões emergentes e proceder ao intercâmbio das melhores práticas entre parceiros próximos³⁹. Esta abordagem dinâmica aplica-se também às decisões de adequação já emitidas que foram adotadas ao abrigo da Diretiva de 1995, e que deverão ser revistas se deixarem de satisfazer as normas aplicáveis⁴⁰. Por conseguinte, os países terceiros em causa são convidados a informar a Comissão acerca de qualquer alteração pertinente da legislação ou prática introduzida desde a adoção da decisão de adequação que lhes diga respeito. Tal é essencial para garantir a continuidade destas decisões segundo os termos das novas normas da reforma⁴¹.

As normas de proteção de dados da UE não podem ser objeto de negociações no quadro de um acordo de comércio livre⁴². Embora os diálogos sobre proteção de dados devam seguir uma via distinta das negociações comerciais com países terceiros, uma decisão de adequação, mesmo parcial ou setorial, é a melhor forma de instaurar a confiança mútua, o que garante a circulação de dados pessoais sem restrições e facilita, portanto, as trocas comerciais que envolvem transferências de dados pessoais para o país terceiro em causa. Por conseguinte, tais decisões podem facilitar as negociações comerciais ou completar os acordos comerciais existentes, permitindo multiplicar os seus benefícios. Ao mesmo tempo, ao fomentar a convergência dos níveis de proteção garantidos na UE e no país terceiro, uma decisão de adequação reduz o risco de esse país invocar motivos de proteção de dados pessoais para impor exigências injustificadas em matéria de localização ou de conservação dos dados. Além disso, tal como indicado na sua Comunicação intitulada «Comércio para Todos», a Comissão procurará utilizar os acordos comerciais da UE a fim de estabelecer regras para o comércio

³⁸ O artigo 45.º, n.ºs 4 e 5, do Regulamento Geral sobre a Proteção de Dados prevê que a Comissão deve controlar, de forma continuada, os desenvolvimentos nos países terceiros e atribui-lhe poderes para revogar, alterar ou suspender uma decisão de adequação caso considere que o país em causa deixou de assegurar um nível de proteção adequado.

³⁹ Artigo 45.º, n.º 3, do Regulamento Geral sobre a Proteção de Dados.

⁴⁰ O artigo 97.º, n.º 2, alínea a), do Regulamento Geral sobre a Proteção de Dados também exige que a Comissão apresente um relatório de avaliação, até 2020, ao Parlamento Europeu e ao Conselho.

⁴¹ No sentido de retirar as consequências do acórdão *Schrems*, que considerou que a Comissão ultrapassou a competência que lhe foi conferida ao restringir os poderes das autoridades de proteção de dados de suspender ou proibir a circulação de dados na decisão relativa ao «porto seguro», a Comissão, em 16 de dezembro de 2016, adotou uma decisão de alteração abrangente («omnibus») que suprime disposições idênticas nas decisões de adequação existentes e substitui-as por disposições que apenas preveem obrigações de informação entre os Estados-Membros e a Comissão no caso de uma autoridade de proteção de dados suspender ou proibir transferências para um país terceiro. A referida decisão abrangente introduz igualmente a obrigação de a Comissão acompanhar os desenvolvimentos pertinentes no país terceiro. Ver JO L 344 de 17.12.2016, p. 83.

⁴² Em particular, uma decisão de adequação é uma decisão de execução unilateral da Comissão que é adotada em conformidade com a legislação da UE em matéria de proteção de dados, com base nos critérios nela definidos.

eletrónico e os fluxos de dados transfronteiras e combater as novas formas de protecionismo digital, no pleno respeito e sem prejuízo das normas de proteção de dados da UE⁴³.

A Comissão:

- Dará prioridade aos debates sobre eventuais decisões de adequação com os principais parceiros comerciais do Leste e do Sudeste Asiático, começando com o Japão e a Coreia em 2017, mas tendo também em conta outros parceiros estratégicos como a Índia, e com os países da América Latina, nomeadamente do Mercosul, e países da Vizinhança Europeia.
- Acompanhará de perto o funcionamento das decisões de adequação existentes. Mais concretamente, tal inclui a aplicação do quadro do Escudo de Proteção da Privacidade UE-EUA, nomeadamente no âmbito do reexame anual conjunto.
- Colaborará com os países interessados em adotar uma legislação mais estrita em matéria de proteção de dados e apoiá-los-á no processo de convergência com os princípios de proteção de dados da UE.

3.2 Mecanismos alternativos de transferência de dados

As normas de proteção de dados da UE sempre reconheceram que não existe uma abordagem única às transferências internacionais de dados. Este princípio ainda se revela mais verdadeiro para as normas resultantes da reforma. Embora as decisões de adequação estejam apenas disponíveis para os países terceiros que cumprem os critérios pertinentes, o Regulamento Geral sobre a Proteção de Dados prevê um conjunto diversificado de mecanismos que são suficientemente flexíveis para se adaptarem a uma variedade de situações de transferência diferentes. Podem ser desenvolvidos instrumentos que tomem em consideração as necessidades ou condições particulares de certos setores, modelos de negócio e/ou operadores. Pode tratar-se, por exemplo, de cláusulas contratuais-tipo elaboradas especificamente para dar respostas às exigências de um setor particular, como as garantias específicas para o tratamento de dados sensíveis no setor da saúde, ou de um tipo específico de atividades de tratamento predominantes em determinados países terceiros, como os serviços de externalização prestados para empresas europeias. Tal poderá ser alcançado através da adoção de novos conjuntos de cláusulas-tipo ou completando as existentes, através de garantias adicionais, que podem ir desde soluções técnicas até soluções de organização, passando por soluções ligadas ao modelo de negócio⁴⁴. Algumas necessidades setoriais específicas também podem ser satisfeitas através de regras vinculativas aplicáveis a grupos de empresas envolvidas numa atividade económica conjunta, por exemplo, no setor das viagens. As transferências internacionais entre subcontratantes pode beneficiar do desenvolvimento de cláusulas contratuais-tipo entre subcontratantes e/ou de regras vinculativas aplicáveis às empresas para os subcontratantes. Por último, os novos mecanismos de transferência, tais como os códigos

⁴³ Ver Comunicação intitulada «Comércio para Todos», p. 12 (nota de rodapé 24).

⁴⁴ Ver artigo 46.º, n.º 2, alíneas c) e d), e considerando 109 do Regulamento Geral sobre a Proteção de Dados, que clarificam que são possíveis adaptações a cláusulas-tipo aprovadas desde que tais adaptações não sejam contrárias, direta ou indiretamente, a essas cláusulas-tipo nem prejudiquem os direitos ou liberdades fundamentais de pessoas singulares.

de conduta aprovados e as certificações de terceiros acreditados, dão às empresas a possibilidade de introduzirem soluções personalizadas para as transferências internacionais, não deixando de beneficiar das vantagens competitivas associadas, por exemplo, a um selo ou a uma marca de proteção da privacidade. Alguns destes instrumentos podem ser desenvolvidos enquanto mecanismos de transferência específicos ou como parte de instrumentos mais gerais para demonstrar a conformidade com todas as disposições do Regulamento Geral sobre a Proteção de Dados, como acontece no caso de um código de conduta aprovado.

A Comissão colaborará com as empresas, a sociedade civil e as autoridades de proteção de dados, a fim de aproveitar ao máximo todo o potencial do conjunto de instrumentos previstos pelo Regulamento Geral sobre a Proteção de Dados no que toca a transferências internacionais. O diálogo contínuo com as partes interessadas no contexto da aplicação da reforma ajudará a identificar os domínios de ação prioritários a este respeito. Pode tratar-se, nomeadamente, da conclusão de trabalhos já iniciados, como o da elaboração, em cooperação com o Grupo de Trabalho do artigo 29.º (que será substituído, em 2018, pelo Comité Europeu para a Proteção de Dados), de cláusulas contratuais-tipo entre subcontratantes⁴⁵. Pode igualmente tratar-se da elaboração de novos componentes da infraestrutura da UE de conformidade com os princípios, graças, por exemplo, à definição pela Comissão de requisitos e normas técnicas para a criação e o funcionamento de mecanismos de certificação, incluindo os aspetos relacionados com as transferências internacionais⁴⁶. Algumas destas medidas podem ser completadas por trabalhos a nível internacional, mais concretamente com organizações que desenvolveram procedimentos de transferência idênticos. Por exemplo, seria conveniente explorar formas de promover a convergência entre as regras vinculativas aplicáveis às empresas por força do direito da UE e as normas transfronteiras de proteção da privacidade desenvolvidas pela Cooperação Económica Ásia-Pacífico (APEC)⁴⁷, no que respeita tanto às normas aplicáveis como ao processo de aplicação no âmbito de cada sistema. Tal deveria contribuir para promover normas estritas de proteção de dados a nível mundial, reduzindo simultaneamente as diferenças de abordagens sobre a proteção da privacidade e dos dados, bem como para ajudar os operadores comerciais a abrirem caminho entre os diferentes sistemas e para elaborar políticas consequentes.

A Comissão:

- Colaborará com as partes interessadas na elaboração de mecanismos alternativos de transferências de dados pessoais adaptados às necessidades ou condições particulares de determinados setores, modelos de negócio e/ou operadores.

⁴⁵ Atualmente, não existem cláusulas contratuais-tipo de subcontratante da UE para subcontratante de países terceiros.

⁴⁶ Artigo 43.º, n.ºs 8 e 9, do Regulamento Geral sobre a Proteção de Dados.

⁴⁷ Ver o documento comum APEC/UE de 2014 que serve de referencial para a estrutura das regras vinculativas aplicáveis às empresas da UE e o sistema de normas transnacionais de proteção da privacidade da APEC, que compara os requisitos de conformidade e de certificação dos dois sistemas: http://www.apec.org/~media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

3.3 Cooperação internacional no domínio da proteção de dados pessoais

3.3.1. Promover normas de proteção de dados através de instrumentos e instâncias multilaterais

O quadro jurídico da UE em matéria de proteção de dados serve frequentemente de referência a países terceiros que pretendem desenvolver legislação neste domínio. A UE continuará a dialogar ativamente com os seus parceiros internacionais, tanto a nível bilateral como multilateral, para fomentar a convergência através da elaboração, a nível mundial, de normas estritas e interoperáveis no domínio da proteção de dados pessoais. Tal contribui para uma proteção mais eficaz dos direitos das pessoas singulares e, ao mesmo tempo, reduz os obstáculos à circulação transnacional de dados enquanto elemento importante do comércio livre.

Em particular, a Comissão incentiva a adesão de países terceiros à Convenção n.º 108 do Conselho da Europa e ao seu protocolo adicional⁴⁸. A Convenção, que está aberta a Estados não membros do Conselho da Europa e já foi ratificada por 50 países, incluindo países de África e da América do Sul⁴⁹, é o único instrumento multilateral juridicamente vinculativo no domínio da proteção de dados. Encontra-se atualmente em processo de revisão e a Comissão promoverá ativamente a rápida adoção do texto modernizado para que a UE se torne parte nessa convenção. Esta última refletirá os mesmos princípios que estão consagrados nas novas normas da UE de proteção de dados, contribuindo assim para a convergência rumo a um conjunto de normas estritas em matéria de proteção de dados.

A reunião do G20 que se realizará em 2017, constituirá uma nova oportunidade para a UE trabalhar no sentido da convergência em torno do princípio segundo o qual normas estritas de proteção de dados são um elemento essencial do desenvolvimento de uma sociedade da informação mundial capaz de promover a inovação, o crescimento e a prosperidade social⁵⁰.

A Comissão também aguarda com interesse o início do diálogo com novos intervenientes importantes, tais como o Relator Especial da ONU sobre o direito à privacidade⁵¹, e o aprofundamento das suas relações de trabalho com organizações regionais, como a APEC, a fim de promover, à escala mundial, uma cultura de respeito dos direitos à vida privada e à proteção dos dados pessoais.

No âmbito dos seus esforços mais vastos visando reforçar a sensibilização para a proteção da privacidade e aumentar as garantias de proteção de dados a nível internacional, a Comissão Europeia aprovou, em 15 de novembro de 2016, um projeto a título do Instrumento de

⁴⁸ Convenção do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981 (STE n.º 108) e Protocolo Adicional à Convenção para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 2001, relativo às autoridades de controlo e à circulação transfronteiriça de dados (STE n.º 181).

⁴⁹ A Maurícia, o Senegal e o Uruguai ratificaram a Convenção. Além disso, Cabo Verde, Marrocos e a Tunísia foram convidados a aderir.

⁵⁰ Ver também a Declaração Ministerial da OCDE sobre a Economia Digital: Inovação, Crescimento e Prosperidade Social («Declaração de Cancun»), 23 de junho de 2016.

⁵¹ Ver: <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

Parceria para reforçar a cooperação com os países parceiros neste domínio⁵². Este projeto incluirá o financiamento de atividades como a formação e a sensibilização. Por sua vez, no contexto da aplicação da reforma, a UE pode beneficiar do intercâmbio de boas práticas e da experiência de outros sistemas com novos desafios no domínio da proteção da privacidade e soluções jurídicas e técnicas emergentes, inclusive em termos de instrumentos de execução e cumprimento (por exemplo, procedimentos de certificação, avaliações de impacto sobre a privacidade) ou proteções de determinados conjuntos específicos de dados (por exemplo, dados relativos a crianças).

3.3.2. Cooperação no domínio da aplicação da legislação

O reforço da cooperação com as autoridades de países terceiros responsáveis pela aplicação e controlo do respeito da privacidade é cada vez mais necessária, tendo em conta a dimensão global das empresas multinacionais que tratam grandes quantidades de dados pessoais num grande número de países. Muitas vezes, os problemas de não conformidade com as normas de proteção de dados ou de violações de dados afetam pessoas em várias jurisdições simultaneamente. Nestes casos, a proteção dos indivíduos pode tornar-se mais eficaz através de uma ação comum. Ao mesmo tempo, os operadores económicos beneficiariam de um ambiente jurídico mais claro se fossem elaborados instrumentos comuns de interpretação e práticas comuns de aplicação a nível mundial.

Num mundo interligado e sem fronteiras na circulação dos fluxos de dados, chegou o momento, portanto, de intensificar a cooperação entre as autoridades responsáveis pela aplicação da legislação⁵³. A UE está pronta a assumir as suas responsabilidades. Como foi relembrado acima, o Regulamento Geral sobre a Proteção de Dados habilita a Comissão a elaborar mecanismos de cooperação internacional para facilitar a aplicação efetiva da legislação em matéria de proteção de dados, incluindo através de acordos de assistência mútua. Neste contexto, deve ser explorada a possibilidade de desenvolver um acordo-quadro de cooperação entre as autoridades responsáveis pela proteção de dados na UE e as autoridades responsáveis pela aplicação da legislação em determinados países terceiros, tirando também partido da experiência adquirida pela Comissão noutros domínios, como a concorrência e a defesa dos consumidores.

⁵² Decisão de Execução da Comissão C(2016)7198, que aprova a segunda fase do Programa de Ação Anual 2016 (PAA 2016) no âmbito do Instrumento de Parceria.

⁵³ As redes existentes incluem a «Global Privacy Enforcement Network» (GPEN) lançada em 2010 sob a égide da OCDE. Trata-se de uma rede de autoridades responsáveis pela aplicação da legislação em matéria de privacidade, na qual estão envolvidas as autoridades de proteção de dados, encarregadas, designadamente, da cooperação no domínio da aplicação da lei, da partilha de boas práticas em matéria de luta contra os desafios transnacionais e do apoio a iniciativas conjuntas de aplicação da legislação e campanhas de sensibilização. Esta rede não cria novas obrigações juridicamente vinculativas entre os participantes e centra-se sobretudo em facilitar a cooperação na aplicação das leis que regulam a proteção da privacidade no setor privado. Ver <https://privacyenforcement.net/>.

A Comissão:

- Promoverá a rápida adoção do texto modernizado da Convenção n.º 108 do Conselho da Europa para que a UE se torne parte na convenção e encorajar a adesão de países terceiros.
- Utilizará as instâncias multilaterais, como as Nações Unidas, o G20 e a APEC, para fomentar uma cultura mundial de respeito pelos direitos no domínio da proteção de dados.
- Elaborará mecanismos de cooperação internacional com os parceiros internacionais importantes para facilitar a aplicação efetiva desses direitos.

4. UMA COOPERAÇÃO MAIS EFICAZ NA APLICAÇÃO DA LEI ACOMPANHADA DE GARANTIAS SÓLIDAS DE PROTEÇÃO DE DADOS

O intercâmbio de dados pessoais é parte integrante da prevenção, investigação e repressão de infrações penais. Num mundo interconectado em que a criminalidade raramente pára nas fronteiras nacionais, o rápido intercâmbio de dados pessoais é essencial para assegurar o êxito da cooperação dos serviços com funções coercivas e a eficácia da resposta à criminalidade. Estes intercâmbios devem ter por base garantias sólidas em matéria de proteção de dados. Esta abordagem também contribui para criar confiança entre as autoridades competentes e reforçar a segurança jurídica quando as informações são recolhidas e/ou trocadas.

As normas sobre transferências internacionais constantes da Diretiva Cooperação Policial regem os intercâmbios de dados entre autoridades com funções coercivas da UE e de países terceiros, bem como, em situações específicas, as transferências dessas autoridades para outras entidades. A referida diretiva introduz a possibilidade de emitir decisões de adequação no contexto da ação penal. A Comissão promoverá a possibilidade de emissão dessas decisões de adequação com países terceiros, em particular aqueles com os quais é necessária uma cooperação estreita e rápida na luta contra a criminalidade e o terrorismo, e quando importantes intercâmbios de dados pessoais já são realizados. Assim sendo, a Comissão dará prioridade aos debates sobre decisões de adequação com os países terceiros que são parceiros essenciais neste esforço.

Em alternativa, o acordo-quadro sobre a proteção de dados entre a UE e os EUA⁵⁴, celebrado em dezembro de 2016, é um bom exemplo da forma como a cooperação em matéria de aplicação coerciva da lei com um importante parceiro internacional pode ser reforçada através da negociação de um conjunto sólido de garantias em matéria de proteção de dados. Ao completar automaticamente os instrumentos jurídicos existentes nos quais se baseiam os

⁵⁴ Acordo entre a UE e os Estados Unidos sobre a proteção de dados pessoais quando transferidos e tratados para efeitos de prevenção, investigação, deteção e repressão de infrações penais, incluindo atos terroristas, no contexto da cooperação policial e judiciária em matéria penal: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf («Acordo-Quadro»)

intercâmbios de dados (em especial os acordos bilaterais a nível quer da UE quer dos Estados-Membros), esse acordo-quadro proporciona benefícios imediatos e diretos para as pessoas singulares e reforça a cooperação entre os serviços com funções coercivas ao facilitar o intercâmbio de informações. Além disso, ao estabelecer uma base de referência para futuros acordos de transferência de dados com os Estados Unidos, esse acordo-quadro suprime a necessidade de renegociar repetidamente as mesmas garantias. O referido acordo-quadro constitui o primeiro acordo internacional bilateral que é acompanhado de um conjunto completo de direitos e obrigações em matéria de proteção de dados conforme com o acervo da UE. Pode, portanto, servir de base para negociar acordos semelhantes com países terceiros, não apenas no domínio da cooperação judiciária e policial, mas também noutros domínios da esfera pública (por exemplo, a política da concorrência ou a proteção dos consumidores). Tal abrangeria tanto os intercâmbios entre governos como as transferências de dados entre empresas privadas e autoridades responsáveis pela aplicação da lei. Poderia também facilitar a celebração, pela União, de acordos relativos ao intercâmbio de dados entre as agências da UE pertinentes (nomeadamente a Europol e a Eurojust) e países terceiros⁵⁵. A Comissão examinará, portanto, a possibilidade de celebrar acordos-quadro com os seus parceiros mais importantes no domínio da aplicação coerciva da lei.

Além disso, a Diretiva Cooperação Policial prevê a possibilidade, sob garantias estritas e em determinadas circunstâncias, de as autoridades com funções coercivas da UE solicitarem diretamente informações a uma empresa privada num país terceiro e transmitirem dados pessoais (normalmente um nome ou um endereço IP) nesse pedido⁵⁶. Em contrapartida, o Regulamento Geral sobre a Proteção de Dados aborda especificamente os casos em que entidades privadas estabelecidas na UE transmitem dados pessoais a autoridades com funções coercivas de um país terceiro na sequência de um pedido: tais transferências para o exterior da UE apenas são autorizadas sob determinadas condições, por exemplo com base num acordo internacional ou quando a divulgação for necessária por um motivo importante de interesse público reconhecido pelo direito da União ou dos Estados-Membros⁵⁷.

Esta cooperação, que se tornou central para o êxito das investigações e repressão da criminalidade e do terrorismo, é realçada nas conclusões do Conselho sobre a melhoria da justiça penal no ciberespaço. O Conselho convidou a Comissão a adotar medidas concretas baseadas numa abordagem comum da UE, a fim de melhorar a cooperação com os prestadores de serviços, tornar o auxílio judiciário mútuo mais eficaz e propor soluções para os problemas de determinação e de aplicação da competência jurisdicional no ciberespaço⁵⁸. Tais medidas abrangem tanto os intercâmbios entre autoridades com funções coercivas e os prestadores de serviços estabelecidos na UE, como o intercâmbio com as autoridades e as empresas de países

⁵⁵ A celebração de acordos operacionais com a Europol e a Eurojust também tem constituído um parâmetro de referência nos diálogos sobre a liberalização do regime de vistos com determinados países terceiros, por exemplo no contexto do diálogo em curso com a Turquia.

⁵⁶ Ver artigo 39.º e considerando 73 da Diretiva Cooperação Policial.

⁵⁷ Ver artigo 48.º e considerando 115 do Regulamento Geral sobre a Proteção de Dados.

⁵⁸ Conclusões do Conselho da União Europeia sobre a melhoria da justiça penal no ciberespaço, 9 de junho de 2016: www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. A Comissão foi incumbida de apresentar resultados nesta matéria ao Conselho, até junho de 2017, no seguimento do seu relatório de avaliação dos progressos realizados apresentado ao Conselho em dezembro de 2016.

terceiros. A Comissão apresentará opções para o acesso a provas eletrónicas, em junho de 2017, tendo em conta a necessidade de uma cooperação rápida e fiável, assente em normas sólidas em matéria de proteção de dados previstas na Diretiva Cooperação Policial e no Regulamento Geral sobre a Proteção de Dados, tanto em situações internas da UE como para as transferências internacionais.

Por último, em conformidade com a nova base jurídica aplicável à Europol, a Comissão avaliará as disposições dos acordos de cooperação operacional entre a Europol e terceiros, celebrados ao abrigo da Decisão 2009/371/JAI do Conselho, incluindo as suas disposições relativas à proteção de dados⁵⁹. Além disso, como indicado na Agenda Europeia para a Segurança de 2015, a futura abordagem da União sobre o intercâmbio de dados PNR com países terceiros terá em conta a necessidade de aplicar normas coerentes e garantias específicas aos direitos fundamentais. A Comissão procurará obter soluções juridicamente sólidas e sustentáveis para o intercâmbio dos registos de identificação dos passageiros (PNR) com países terceiros, nomeadamente a possibilidade de elaborar um modelo de acordo sobre os PNR que defina os requisitos que os países terceiros têm de respeitar para receber dados PNR da União. Todavia, qualquer política futura neste domínio dependerá, em especial, do parecer do Tribunal de Justiça da União Europeia sobre o Acordo PNR previsto entre a UE e o Canadá⁶⁰.

UMA COOPERAÇÃO MAIS EFICAZ NA APLICAÇÃO DA LEI ACOMPANHADA DE GARANTIAS SÓLIDAS DE PROTEÇÃO DE DADOS

A Comissão:

- Promoverá a possibilidade de adotar decisões de adequação ao abrigo da Diretiva Cooperação Policial com os países terceiros que reúnam os requisitos pertinentes.
- Promoverá a negociação de acordos no domínio da aplicação coerciva da lei com importantes parceiros internacionais, de acordo com o modelo fornecido pelo acordo-quadro com os Estados Unidos.
- Dará seguimento às conclusões do Conselho sobre a melhoria da justiça penal no ciberespaço para facilitar o intercâmbio transnacional de provas eletrónicas em conformidade com as normas de proteção de dados.

⁵⁹ Ver artigo 25.º, n.º 4, do Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, pp. 53-114). A Comissão é solicitada a apresentar um relatório de avaliação até 14 de junho de 2021 sobre os acordos de cooperação da Europol celebrados antes de 1 de maio de 2017.

⁶⁰ Parecer do Tribunal de Justiça sobre o projeto de acordo PNR entre a UE e o Canadá de 2014, apresentado ao Tribunal pelo Parlamento Europeu (Parecer 1/15). Foi solicitado ao Tribunal que apreciasse a compatibilidade do projeto de acordo com a Carta dos Direitos Fundamentais da UE.

5. CONCLUSÃO

A proteção e o intercâmbio de dados pessoais não são incompatíveis. Um sistema de proteção de dados sólido facilita a sua circulação, aumentando a confiança dos consumidores nas empresas que se preocupam com a forma como tratam os dados pessoais dos seus clientes. Desta forma, a existência de normas estritas de proteção de dados torna-se uma vantagem na economia digital mundial. O mesmo se aplica à cooperação no domínio da aplicação coerciva da lei: as garantias em matéria de privacidade são parte integrante de um intercâmbio de dados eficaz e rápido no quadro da luta contra a criminalidade, com base na confiança mútua e na segurança jurídica.

Após concluir a reforma das suas normas sobre a proteção de dados, a UE deve colaborar de forma pró-ativa com países terceiros neste domínio. Deve esforçar-se por procurar uma maior convergência dos princípios em matéria de proteção de dados à escala internacional, quer a nível bilateral quer multilateral, o que traz vantagens e benefícios tanto aos cidadãos como às empresas. O novo quadro legislativo de proteção de dados proporciona à UE os instrumentos necessários e adequados para alcançar tais objetivos. Com base na abordagem estratégica apresentada na presente comunicação, a Comissão cooperará ativamente com os principais países terceiros, a fim de examinar a possibilidade de adotar declarações de adequação, começando com o Japão e a Coreia em 2017, visando promover a convergência regulamentar com as normas da UE e facilitar as relações comerciais. Simultaneamente, a UE deverá utilizar plenamente a diversidade de instrumentos alternativos de transferência de dados para proteger os direitos em matéria de proteção de dados e apoiar os operadores económicos aquando da transferência de dados para países cujo direito interno não assegura um nível adequado de proteção neste domínio. Esses instrumentos devem igualmente ser utilizados para continuar a facilitar a cooperação entre, por um lado, as autoridades de controlo e de aplicação coerciva da lei da UE e, por outro, os seus parceiros internacionais. A Comissão assegurará a coerência da dimensão interna e externa da política de proteção de dados da UE e promoverá uma sólida proteção de dados a nível internacional com vista a reforçar a cooperação em matéria de aplicação da lei, contribuir para o comércio livre e elaborar normas estritas de proteção de dados pessoais à escala mundial.