



PROTEÇÃO DOS DADOS PESSOAIS

A proteção dos dados pessoais e o respeito pela vida privada são direitos fundamentais europeus. O Parlamento Europeu sempre insistiu na necessidade de se alcançar um equilíbrio entre a melhoria da segurança e a preservação dos direitos humanos, incluindo a privacidade e a proteção de dados. Em maio de 2018 entraram em vigor novas regras da UE em matéria de proteção de dados que reforçam os direitos dos cidadãos e simplificam as regras para as empresas na era digital. De acordo com a investigação realizada para o Parlamento Europeu, a legislação da UE relacionada com a regulamentação do fluxo de dados contribui anualmente com 51,6 mil milhões de euros para o PIB da União Europeia. A investigação preparada para a Comissão de Inquérito do Parlamento Europeu para Investigar a Utilização do Software Espião de Vigilância Pegasus e Equivalentes (Comissão PEGA) confirma a importância da proteção de dados para a defesa da democracia e das liberdades individuais na UE.

BASE JURÍDICA

Artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE);
Artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia.

OBJETIVOS

A União deve garantir que o direito fundamental à proteção de dados, consagrado na Carta dos Direitos Fundamentais da União Europeia, é aplicado de uma forma coerente. Face ao crescimento exponencial do volume de transferências de dados – sendo as maiores quotas deste crescimento detidas pela UE, Estados Unidos e Canadá – é necessário reforçar a posição da UE em matéria de proteção dos dados pessoais no contexto de todas as políticas da UE.

REALIZAÇÕES

- A. Quadro institucional
- 1. Tratado de Lisboa

Antes da entrada em vigor do Tratado de Lisboa, a legislação relativa à proteção de dados no espaço de liberdade, segurança e justiça (ELSJ) estava dividida entre o primeiro pilar (proteção de dados para fins privados e comerciais, com a utilização do método comunitário) e o terceiro pilar (proteção de dados para efeitos de aplicação da lei, a nível intergovernamental). Consequentemente, os processos



de decisão nestes dois domínios seguiram normas diferentes. Esta estrutura com pilares desapareceu com o Tratado de Lisboa, pois este fornece uma base mais sólida para o desenvolvimento de um sistema de proteção de dados mais claro e eficaz, e simultaneamente prevê novos poderes para o Parlamento, que se tornou colegislador. O artigo 16.º do TFUE prevê que o Parlamento e o Conselho estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União.

2. Orientações estratégicas no espaço de liberdade, segurança e justiça

Na sequência dos programas de Tampere (outubro de 1999) e de Haia (novembro de 2004), o Conselho Europeu aprovou, em dezembro de 2009, o programa plurianual para o ELSJ durante o período 2010-2014, conhecido por Programa de Estocolmo. Nas suas conclusões de junho de 2014, o Conselho Europeu definiu as orientações estratégicas para a programação legislativa e operacional nos próximos anos no quadro do ELSJ, em conformidade com o artigo 68.º do TFUE. Um dos principais objetivos consiste em proteger melhor os dados pessoais na UE.

B. Principais instrumentos legislativos em matéria de proteção de dados

1. Carta dos Direitos Fundamentais da UE

Os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia reconhecem o respeito pela vida privada e a proteção dos dados pessoais como direitos fundamentais estreitamente relacionados, mas distintos.

2. Conselho da Europa

a. Convenção 108 de 1981

A Convenção 108 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, foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. Visa «garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal». O Protocolo que altera a Convenção visa alargar o seu âmbito de aplicação, aumentar o nível de proteção de dados e melhorar a sua eficácia.

b. Convenção Europeia dos Direitos Humanos (CEDH)

O artigo 8.º da Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, de 4 de novembro de 1950, consagra o direito de qualquer pessoa ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

3. Atuais instrumentos legislativos para proteção de dados na União Europeia

a. Regulamento Geral sobre a Proteção de Dados (RGPD)

O Regulamento (UE) n.º 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), entrou em vigor em maio de 2018. As suas regras destinam-se a proteger todos os cidadãos da UE contra



violações da privacidade e dos dados num mundo cada vez mais baseado em dados, criando simultaneamente um quadro mais claro e mais coerente para as empresas. Os direitos de que beneficiam os cidadãos incluem: o consentimento claro e positivo do tratamento dos seus dados e o direito de receber informações claras e compreensíveis sobre o mesmo; o direito a ser esquecido – um cidadão pode solicitar que os seus dados sejam suprimidos; o direito a transferir os dados para outro prestador de serviços (por exemplo, aquando da mudança de uma rede social para outra); e o direito de saber se os seus dados foram pirateados. As novas regras aplicam-se a todas as empresas que operam na UE, mesmo que tenham sede fora dela. Além disso, é possível impor medidas corretivas – tais como advertências e ordens – ou coimas às empresas que violem as regras. Em 24 de junho de 2020 a Comissão Europeia apresentou um [Relatório sobre a avaliação e revisão do regulamento](#)^[1].

b. Diretiva Proteção de Dados na Aplicação da Lei

A 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 crimes ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, entrou em vigor em maio de 2018. A diretiva protege o direito fundamental dos cidadãos à proteção de dados quando os dados pessoais forem utilizados pelas autoridades responsáveis pela aplicação da lei. Ela garante que os dados pessoais de vítimas, testemunhas e suspeitos de crimes são devidamente protegidos e facilita a cooperação transfronteiriça na luta contra a criminalidade e o terrorismo. Em 25 de julho de 2022 a Comissão Europeia publicou com atraso o seu [Relatório sobre a aplicação e o funcionamento da Diretiva Proteção de Dados na Aplicação da Lei](#). Seguiu-se um [estudo de avaliação](#) encomendado pela Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (LIBE) com uma avaliação crítica da aplicação da Diretiva Proteção de Dados na Aplicação da Lei^[2].

c. Diretiva relativa à privacidade e às comunicações eletrónicas

A [Diretiva 2002/58/CE](#) do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), foi alterada pela [Diretiva 2009/136/CE](#) de 25 de novembro de 2009. Levanta a delicada questão da conservação de dados, que foi repetidamente submetida ao TJUE e conduziu a uma série de acórdãos – o mais recente em [2020](#) – que determinaram que o direito da UE obsta à conservação geral e indiscriminada dos dados de tráfego e de localização.

A [proposta de regulamento](#) do Parlamento Europeu e do Conselho de 2017 relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações

[1] Comunicação da Comissão, de 24 de junho de 2020, intitulada «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» (SWD(2020)0115).

[2] Vogiatzoglou, P. et al., [Assessment of the implementation of the Law Enforcement Directive](#) (Avaliação da aplicação da Diretiva Proteção de Dados na Aplicação da Lei), Parlamento Europeu, Direção-Geral das Políticas Internas da União, Departamento Temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais, 7 de dezembro de 2022.



eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas) tem estado a ser discutida nos últimos tempos. Os peritos do Parlamento Europeu indicaram que o Parlamento deveria resistir às tentativas do Conselho de excluir a aplicabilidade dos princípios europeus em matéria de proteção de dados^[3].

d. Regulamento relativo ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União

O [Regulamento \(UE\) n.º 2018/1725](#) do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE, entrou em vigor em 11 de dezembro de 2018.

e. Artigos sobre a proteção de dados em atos legislativos setoriais

Para além dos principais atos legislativos em matéria de proteção de dados acima referidos, também se encontram previstas disposições específicas em matéria de proteção de dados em atos legislativos setoriais como:

- O artigo 13.º (sobre a proteção dos dados pessoais) da Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave;
- O artigo 6.º (sobre o tratamento dos dados) da [Diretiva 2004/82/CE do Conselho](#), de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras (API);
- em 13 de dezembro de 2022, a Comissão adotou [duas propostas legislativas](#) sobre a recolha e transferência de dados API que substituirão a API^[4];
- O capítulo VI (sobre salvaguardas em matéria de proteção de dados) 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);
- O capítulo VIII (relativo à proteção de dados) do Regulamento (UE) 2017/1939 do Conselho, de 12 de outubro de 2017, que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia (EPPO).

[3]Sartor, G. et al., [The impact of Pegasus on fundamental rights and democratic processes](#), (Impacto do Software Espião de Vigilância Pegasus em matéria de direitos fundamentais e processos democráticos), Parlamento Europeu, Direção-Geral das Políticas Internas da União, Departamento Temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais, janeiro de 2023, pp. 56-57.

[4]Vavoula, N. et al., [Advance Passenger Information \(API\) – An analysis of the European Commission’s proposals to reform the API legal framework](#) [Informação Antecipada sobre Passageiros – Uma análise das propostas da Comissão Europeia para reformar o enquadramento jurídico da API], Parlamento Europeu, Direção-Geral das Políticas Internas da União, Departamento Temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais, 8 de junho de 2023.



4. Principais disposições internacionais da UE em matéria de transferência de dados

a. Transferências de dados comerciais: decisões de adequação

Nos termos do artigo 45.º do RGPD, a Comissão tem o poder de determinar se um país de fora da UE oferece um nível adequado de proteção de dados, seja com base na sua legislação interna ou nos compromissos internacionais que assumiu.

Embora as transferências de dados entre a UE e a América do Norte tenham aumentado exponencialmente, com os Estados Unidos a dominar a publicidade e a vigilância privadas em linha^[5], o Parlamento adotou numerosas resoluções que suscitam preocupações sobre os fluxos transatlânticos de dados. Em especial, considerou que a Decisão relativa ao Escudo de Proteção da Privacidade UE-EUA não proporciona o nível adequado de proteção exigido pelo direito da UE, ao passo que o TJUE tem repetidamente invalidado as decisões de adequação da Comissão Europeia relativas aos Estados Unidos (ver o seu acórdão de 2015 sobre o regime de «Porto Seguro» no processo [Schrems](#) e o seu acórdão de 2020 sobre o Escudo de Proteção da Privacidade UE-EUA no processo [Schrems II](#)).

Apesar da falta de reforma do regime de proteção de dados nos Estados Unidos, a Comissão Europeia chegou a outro acordo com os Estados Unidos e apresentou uma [proposta](#) relativa a um novo Quadro de Privacidade de Dados UE-EUA. Na sequência da apresentação de uma proposta da Comissão LIBE, em 11 de maio de 2023, o Parlamento adotou uma [resolução](#) sobre a adequação da proteção conferida pelo Quadro de Privacidade de Dados UE-EUA, concluindo que este quadro não institui uma equivalência essencial no nível de proteção e exortando a Comissão a prosseguir as negociações com os seus homólogos dos Estados Unidos, mas a abster-se de adotar a decisão de adequação até que todas as recomendações formuladas na resolução do Parlamento e no parecer do Comité Europeu para a Proteção de Dados (CEPD) sejam plenamente aplicadas.

A Comissão adotou o seu terceiro [Quadro de Privacidade de Dados UE-EUA](#) em 10 de julho de 2023. .

b. Acordo Global UE-EUA

Ao abrigo do processo de aprovação, o Parlamento participou na aprovação do acordo entre os Estados Unidos e a UE sobre a proteção de dados pessoais relacionados com a prevenção, investigação, deteção e repressão de infrações penais, também conhecido como «Acordo-Quadro». Este acordo tem como objetivo assegurar um elevado nível de proteção das informações pessoais transferidas no quadro da cooperação transatlântica para efeitos de aplicação da lei, nomeadamente para o combate ao terrorismo e à criminalidade organizada.

[5]Maciejewski, M., [Metaverse](#), Parlamento Europeu, Direção-Geral das Políticas Internas da União, Departamento Temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais, 26 de junho de 2023.



c. Acordos UE-EUA, UE-Austrália e UE-Canadá relativos aos registos de identificação dos passageiros (PNR)

A UE assinou acordos bilaterais relativos aos registos de identificação dos passageiros (PNR) com os EUA, a Austrália e o Canadá. Os dados PNR incluem as informações fornecidas pelos passageiros no momento da reserva ou do registo de embarque nos voos e os dados recolhidos pelas transportadoras aéreas para os seus próprios fins comerciais. Os dados PNR podem ser utilizados pelas autoridades responsáveis pela aplicação da lei para combater a criminalidade grave e o terrorismo.

d. Programa UE-EUA de Detecção do Financiamento do Terrorismo (TFTP)

A UE assinou um acordo bilateral com os Estados Unidos sobre o tratamento e a transferência de dados relativos a mensagens de pagamentos da UE para os EUA, para efeitos do Programa de Detecção do Financiamento do Terrorismo.

5. Abordar os aspetos da proteção de dados nas resoluções setoriais

Várias resoluções do Parlamento sobre diferentes domínios de intervenção abordam também a proteção de dados pessoais, a fim de assegurar a coerência com a legislação geral da UE em matéria de proteção de dados e a proteção da privacidade nesses setores específicos.

6. Autoridades de supervisão da proteção de dados da UE

[A Autoridade Europeia para a Proteção de Dados \(AEPD\)](#) é uma entidade supervisora independente que assegura que as instituições e órgãos da União Europeia cumprem as suas obrigações no que respeita à proteção de dados. Os deveres principais da AEPD são a supervisão, a consulta e a cooperação.

O [Comité Europeu para a Proteção de Dados \(CEPD\)](#) – anteriormente designado Grupo de Trabalho do Artigo 29.º – tem o estatuto de um organismo da UE dotado de personalidade jurídica e possui um secretariado independente. O CEPD reúne as autoridades de supervisão nacionais da UE, a AEPD e a Comissão. O CEPD dispõe de vastos poderes para decidir os litígios entre as autoridades de supervisão nacionais e prestar aconselhamento e orientação sobre os principais conceitos do RGPD e a Diretiva Proteção de Dados na Aplicação da Lei.

O PAPEL DO PARLAMENTO EUROPEU

O Parlamento desempenhou um papel fundamental na elaboração da legislação da UE no domínio da proteção de dados pessoais, ao fazer da proteção da privacidade uma prioridade política. Além disso, ao abrigo do processo legislativo ordinário, tem vindo a trabalhar na reforma da proteção de dados em pé de igualdade com o Conselho. Em 2017 concluiu os seus trabalhos sobre a última peça significativa do puzzle – o novo regulamento relativo à privacidade e às comunicações eletrónicas – e aguarda com expectativa que o Conselho conclua finalmente o seu trabalho para dar início às negociações interinstitucionais.

O Parlamento manifestou dúvidas em numerosas resoluções sobre a adequação da proteção concedida aos cidadãos da UE ao abrigo do Quadro Porto Seguro UE-EUA, e subsequentemente do Escudo de Proteção da Privacidade UE-EUA. Após o processo



Schrems II ter conduzido à anulação da [Decisão de Execução \(UE\) 2016/1250](#) da Comissão Europeia relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com base na preocupação de que os poderes de supervisão do Governo dos Estados Unidos não fossem limitados, tal como exigido pelo direito da UE, e de os cidadãos da UE não disporem de vias de recurso eficazes, o Parlamento Europeu adotou uma resolução na qual lamentava o facto de a Comissão ter colocado as relações com os Estados Unidos à frente dos interesses dos cidadãos da UE^[6].

Na sequência da apresentação da [proposta](#) da Comissão LIBE, em 11 de maio de 2023, o Parlamento [adotou](#) uma resolução sobre a adequação da proteção assegurada pelo Quadro de Privacidade de Dados UE-EUA, concluindo que este quadro não institui uma equivalência essencial no nível de proteção e instando a Comissão a prosseguir as negociações com os seus homólogos dos Estados Unidos, embora abstendo-se de adotar a decisão sobre a verificação da adequação até que todas as recomendações formuladas na resolução e no parecer do CEPD sejam plenamente aplicadas. A Comissão adotou a sua decisão sobre o [Quadro de Privacidade de Dados UE-EUA](#) em 10 de julho de 2023.

O Parlamento criou uma [Comissão de Inquérito para Investigar a Utilização do Software Espião de Vigilância Pegasus e Equivalentes](#) nos Estados-Membros da UE (PEGA). Presidida pelo [Deputado ao Parlamento Europeu Jeroen Lenaers](#), a Comissão PEGA investigou exaustivamente as práticas de utilização de software espião para investigar membros da oposição, jornalistas, advogados e ativistas da sociedade civil, bem como a forma como essas práticas afetam os processos democráticos e os direitos individuais na UE. Durante o seu inquérito, a Comissão PEGA consultou [académicos](#), profissionais e autoridades de renome na UE e em todo o mundo. O Departamento Temático do Parlamento preparou relatórios para as missões PEGA à [Polónia](#), [Grécia](#) e Chipre. Em 8 de maio de 2023, a Comissão PEGA votou a aprovação do seu [relatório final](#), extremamente crítico e com recomendações sobre a investigação de alegadas infrações e má administração na aplicação do direito da UE relacionadas com a utilização de software espião de vigilância Pegasus e equivalentes, e incluindo, entre muitos outros pontos, uma recomendação para a criação de um laboratório tecnológico da UE para a investigação e o controlo da utilização de software espião contra os cidadãos da UE. A recomendação do Parlamento ao Conselho e à Comissão na sequência do relatório PEGA foi adotada na sessão plenária de 15 de junho de 2023. No entanto, a Comissão não deu uma resposta atempada à recomendação e bloqueou o projeto-piloto de um laboratório tecnológico da UE proposto pelos deputados ao Parlamento Europeu.

O Parlamento encomendou vários estudos de investigação a fim de dispor de uma base científica para as suas atividades legislativas dedicadas à vanguarda da evolução tecnológica e da proteção de dados, incluindo um estudo sobre [o impacto do Regulamento Geral Proteção de Dados \(RGPD\) na inteligência artificial](#), um estudo sobre [biometria e deteção de comportamentos](#) e um estudo sobre o [Metaverso](#).

[6] [Resolução do Parlamento Europeu, de 20 de maio de 2021, sobre o acórdão do TJUE de 16 de julho de 2020 – Data Protection Commissioner/Facebook Ireland Limited, Maximilian Schrems \(«Schrems II»\) – Processo C-311/18](#), n.º 28.



A presente ficha temática foi elaborada pelo Departamento Temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais do Parlamento Europeu.

Mariusz Maciejewski
11/2023

