COMISSÃO
EUROPEIA

Bruxelas, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas)

(Texto relevante para efeitos do EEE)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

1.1. Justificação e objetivos da proposta

A Estratégia para o Mercado Único Digital («**Estratégia MUD**»)[1] tem como objetivo aumentar a confiança e a segurança nos serviços digitais. A reforma do quadro de proteção de dados e, nomeadamente, a adoção do Regulamento (UE) 2016/679, o Regulamento Geral sobre a Proteção de Dados («**RGPD**»)[2], foi uma ação fundamental para o efeito. A Estratégia MUD anunciou também a revisão da Diretiva 2002/58/CE («**Diretiva Privacidade e Comunicações Eletrónicas**»)[3], a fim de proporcionar um nível elevado de proteção da privacidade aos utilizadores de serviços de comunicações eletrónicas e condições de concorrência equitativas para todos os intervenientes no mercado. A presente proposta procede à revisão da Diretiva Privacidade e Comunicações Eletrónicas, antecipando os objetivos na Estratégia MUD e garantindo a coerência com o RGPD.

A Diretiva Privacidade e Comunicações Eletrónicas assegura a proteção dos direitos e liberdades fundamentais, nomeadamente o respeito pela vida privada, a confidencialidade das comunicações e a proteção dos dados pessoais no setor das comunicações eletrónicas. Assegura igualmente a livre circulação de dados, equipamentos e serviços de comunicações eletrónicas na União. Aplica, no direito secundário da União, o direito fundamental ao respeito pela vida privada, no que respeita às comunicações, como consagrado no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia («**Carta**»).

Em conformidade com os requisitos «Legislar Melhor», a Comissão procedeu a uma avaliação *ex post*, no âmbito do Programa para a adequação e a eficácia da regulamentação («**avaliação REFIT**») da Diretiva Privacidade e Comunicações Eletrónicas. Decorre da avaliação que os objetivos e princípios do quadro atual permanecem válidos. No entanto, desde a última revisão da Diretiva Privacidade e Comunicações Eletrónicas, em 2009, ocorreram no mercado desenvolvimentos tecnológicos e económicos importantes. Os consumidores e as empresas dependem cada vez mais de novos serviços baseados na Internet que permitem comunicações interpessoais, tais como a voz sobre IP, mensagens instantâneas e serviços de correio eletrónico com base na web, em detrimento dos serviços de comunicações tradicionais. Estes serviços de comunicações suplementares através da Internet («**OTT**») não são, de um modo geral, abrangidos pelo atual quadro para as comunicações eletrónicas da União, incluindo a Diretiva Privacidade e Comunicações Eletrónicas. Por conseguinte, a Diretiva não acompanhou a evolução tecnológica, daí resultando um vazio de proteção das comunicações transmitidas através de novos serviços.

---

1 Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, Estratégia para o Mercado Único Digital na Europa, COM(2015) 192 final.

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, p. 1-88).

3 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

1.2. Coerência com disposições vigentes no domínio de ação

Esta proposta constitui uma *lex specialis* no que respeita ao RGPD e pormenoriza-o e completa-o no que diz respeito aos dados de comunicações eletrónicas que sejam considerados dados pessoais. Todas as questões relativas ao tratamento de dados pessoais não abordadas especificamente pela proposta são abrangidas pelo RGPD. O alinhamento com o RGPD conduziu à revogação de algumas disposições, tais como as obrigações de segurança do artigo 4.º da Diretiva Privacidade e Comunicações Eletrónicas.

1.3. Coerência com outras políticas da União

A Diretiva Privacidade e Comunicações Eletrónicas faz parte do quadro regulamentar para as comunicações eletrónicas. Em 2016, a Comissão adotou uma proposta de diretiva que estabelece o Código Europeu das Comunicações Eletrónicas («**CECE**»)[4], que revê o quadro. Embora a presente proposta não faça parte integrante do CECE, baseia-se, em parte, nas definições nele previstas, incluindo a de «serviços de comunicações eletrónicas». Tal como o CECE, também a presente proposta inclui os fornecedores OTT no seu âmbito de aplicação, de modo a refletir a realidade do mercado. Além disso, o CECE complementa a presente proposta ao garantir a segurança dos serviços de comunicações eletrónicas.

A Diretiva Equipamentos de Rádio 2014/53/UE («**DER**»)[5] garante um mercado único dos equipamentos de rádio. Em especial, exige que, antes de serem colocados no mercado, os equipamentos de rádio incluam salvaguardas que assegurem a proteção dos dados pessoais e da privacidade do utilizador. Ao abrigo da DER e do Regulamento (UE) 1025/2012 relativo à normalização europeia[6], a Comissão fica habilitada a adotar medidas. Esta proposta não afeta a DER.

A proposta não inclui quaisquer disposições específicas no domínio da conservação dos dados. Mantém o essencial do artigo 15.º da Diretiva Privacidade e Comunicações Eletrónicas, alinhando-o com a redação específica do artigo 23.º do RGPD, que prevê motivos para os Estados-Membros restringirem o âmbito de aplicação dos direitos e obrigações previstos em artigos específicos da Diretiva Privacidade e Comunicações Eletrónicas. Por conseguinte, os Estados-Membros são livres de manter ou de criar quadros de conservação de dados nacionais que prevejam, nomeadamente, medidas de conservação específicas, na medida em que esses quadros respeitem o direito da União, tendo em conta a jurisprudência do Tribunal de Justiça sobre a interpretação da Diretiva Privacidade e Comunicações Eletrónicas e da Carta dos Direitos Fundamentais[7].

Por último, a proposta não é aplicável às atividades das instituições, organismos e agências da União. No entanto, os seus princípios e obrigações pertinentes, como o direito ao respeito pela vida privada e pelas comunicações no que respeita ao tratamento de dados de comunicações

---

4 Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece o Código Europeu das Comunicações Eletrónicas (Reformulação) [COM/2016/0590 final – 2016/0288 (COD)].

5 Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado e que revoga a Diretiva 1999/5/CE (JO L 153 de 22.5.2014, p. 62-106).

6 Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e que revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12-33).

7 Ver processos apensos C-293/12 e C-594/12 *Digital Rights Ireland e Seitlinger e Outros*, ECLI:EU:C:2014:238; Processos apensos C-203/15 e C-698/15 *Tele2 Sverige AB e Secretary of State for the Home Department*, ECLI: EU: C:2016:970.

eletrónicas, foram incluídos na Proposta de Regulamento que revoga o Regulamento (CE) n.º 45/2001[8].

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

2.1. Base jurídica

O artigo 16.º e o artigo 114.º do Tratado sobre o Funcionamento da União Europeia («**TFUE**») constituem as bases jurídica pertinentes da proposta.

O artigo 16.º do TFUE introduz uma base jurídica específica para a adoção de regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições da União, pelos Estados-Membros aquando da realização de atividades que recaiam no âmbito de aplicação da legislação da União, bem como de regras relativas à livre circulação desses dados. Uma vez que uma comunicação eletrónica que envolva uma pessoa singular é normalmente considerada como dados pessoais, a proteção das pessoas singulares no que respeita à privacidade das comunicações e ao tratamento desses dados deve basear-se no artigo 16.º.

Além disso, a proposta visa proteger as comunicações e os interesses legítimos conexos das pessoas coletivas. O significado e o âmbito de aplicação dos direitos ao abrigo do artigo 7.º da Carta devem, em conformidade com o artigo 52.º, n.º 3, da Carta, ser idênticos aos estabelecidos no artigo 8.º, n.º 1, da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais («**CEDH**»). No que respeita ao âmbito de aplicação do artigo 7.º da Carta, a jurisprudência do Tribunal de Justiça da União Europeia («**TJUE**»)[9] e do Tribunal Europeu dos Direitos do Homem[10] confirma que as atividades profissionais das pessoas coletivas não podem ser excluídas da proteção dos direitos garantidos pelo artigo 7.º da Carta e pelo artigo 8.º da CEDH.

Uma vez que a iniciativa persegue um duplo propósito e que a componente relativa à proteção das comunicações das pessoas coletivas e o objetivo de realização do mercado interno para essas comunicações eletrónicas e de garantir o seu funcionamento neste contexto não podem ser considerados meramente acessórios, a iniciativa deve, por conseguinte, basear-se também no artigo 114.º do TFUE.

2.2. Subsidiariedade

O respeito pelas comunicações é um direito fundamental reconhecido na Carta. O conteúdo das comunicações eletrónicas pode revelar informações altamente sensíveis sobre os utilizadores finais envolvidos na comunicação. De igual modo, os metadados derivados de comunicações eletrónicas podem também revelar informações muito sensíveis e pessoais, tal como expressamente reconhecido pelo TJUE[11]. A maioria dos Estados-Membros reconhece também a necessidade de proteger as comunicações como um direito constitucional distinto. Embora seja possível aos Estados-Membros adotar políticas que assegurem que este direito

---

8 Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1-22).

9 Ver processo C-450/06 *Varec SA*, ECLI:EU: C: 2008:91, ponto 48.

10 Ver, *inter alia*, CEDH, acórdãos *Niemietz/Alemanha*, acórdão de 16 de dezembro de 1992, série A, n.º 251-B, ponto 29; *Société Colas Est e outros/França*, n.º 37971/97, ponto 41; CEDH 2002-III; *Peck/Reino Unido* n.º 44647/98, ponto 57, CEDH 2003-I; e também *Vinci Construction e GTM Génie Civil et Services/França*, n.os 63629/10 e 60567/10, ponto 63, 2 de abril de 2015.

11 Ver nota de rodapé 7.

não é violado, tal não seria alcançado de maneira uniforme na ausência de regras da União e criaria restrições sobre os fluxos transfronteiriços de dados pessoais e não pessoais relacionados com a utilização de serviços de comunicações eletrónicas. Por último, a fim de manter a coerência com o RGPD, é necessário rever a Diretiva Privacidade e Comunicações Eletrónicas e adotar medidas para harmonizar os dois instrumentos.

A evolução tecnológica e as ambições da estratégia MUD reforçaram a necessidade de ação a nível da União. O êxito do MUD na UE depende da eficácia com que a UE elimina a compartimentação e as barreiras a nível nacional e aproveita as vantagens e economias de um mercado único digital europeu. Além disso, como a Internet e as tecnologias digitais não conhecem fronteiras, a dimensão do problema vai para além do território de um único Estado-Membro. Os Estados-Membros não conseguem resolver eficazmente os problemas no contexto da atual situação. Condições de concorrência equitativas para os operadores económicos que prestam serviços substituíveis e igual proteção dos utilizadores finais a nível da União são requisitos para que o MUD funcione adequadamente.

2.3. Proporcionalidade

A fim de assegurar a proteção jurídica efetiva do respeito pela privacidade e pelas comunicações, é necessário o alargamento do âmbito de aplicação para abranger os fornecedores OTT. Embora vários prestadores de serviços OTT populares já cumpram, total ou parcialmente, o princípio da confidencialidade das comunicações, a proteção dos direitos fundamentais não pode ser deixada ao critério da autorregulação por parte da indústria. Além disso, a importância da proteção efetiva da privacidade do equipamento terminal está a aumentar, uma vez que se tornou indispensável na vida pessoal e profissional para o armazenamento de informações sensíveis. A aplicação da Diretiva Privacidade e Comunicações Eletrónicas não tem sido eficaz para capacitar os utilizadores finais. Por conseguinte, para atingir o objetivo, é necessária a aplicação do princípio através da centralização do consentimento no *software* e facultando aos utilizadores informações sobre as suas preconfigurações de privacidade. Quanto à execução do presente regulamento, esta assenta nas autoridades de controlo e no procedimento de controlo da coerência do RGPD. Além disso, a proposta permite que os Estados-Membros tomem medidas derrogatórias nacionais para fins legítimos específicos. Assim, a proposta não vai além do necessário para alcançar os objetivos e respeita o princípio da proporcionalidade enunciado no artigo 5.º do Tratado da União Europeia. As obrigações impostas aos serviços afetados são mantidas ao nível mais baixo possível, sem prejuízo dos direitos fundamentais em causa.

2.4. Escolha do instrumento

A Comissão apresenta uma proposta de regulamento a fim de assegurar a coerência com o RGPD e a segurança jurídica tanto para utilizadores como para empresas, evitando divergências de interpretação nos Estados-Membros. Um regulamento pode assegurar um nível de proteção igual em toda a União para os utilizadores e custos de conformidade mais baixos para as empresas que operam além fronteiras.

3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

3.1. Avaliações *ex post*/balanços de qualidade da legislação existente

A avaliação REFIT analisou em que medida a Diretiva Privacidade e Comunicações Eletrónicas contribuiu para uma proteção adequada da vida privada e da confidencialidade das comunicações na UE. Procurou igualmente identificar possíveis redundâncias.

A avaliação REFIT concluiu que os objetivos da Diretiva acima referidos continuam a ser **pertinentes**. Enquanto o RGPD assegura a proteção dos dados pessoais, a Diretiva Privacidade e Comunicações Eletrónicas garante a confidencialidade das comunicações, que também podem conter dados não pessoais e dados relativos a uma pessoa coletiva. Por conseguinte, a proteção eficaz do artigo 7.º da Carta deve ser assegurada por um instrumento distinto. Outras disposições, tais como as regras relativas ao envio de comunicações promocionais não solicitadas, revelaram permanecer relevantes.

Em termos de **eficácia e eficiência**, a avaliação REFIT considerou que a diretiva não atingiu plenamente os seus objetivos. A redação pouco clara de certas disposições e a ambiguidade dos conceitos jurídicos prejudicaram a harmonização, criando problemas para as empresas desejosas de operar transfronteiras. A avaliação revelou ainda que algumas disposições criaram encargos desnecessários para as empresas e consumidores. Por exemplo, a regra do consentimento para proteger a confidencialidade dos equipamentos terminais não conseguiu atingir os seus objetivos, uma vez que os utilizadores finais se deparam com pedidos para aceitarem testemunhos persistentes sem compreenderem o seu significado e, em certos casos, estão ainda expostos à instalação de testemunhos de conexão sem o seu consentimento. A regra do consentimento é muito abrangente, uma vez que também engloba as práticas não intrusivas da vida privada, e pouco abrangente, visto não cobrir de forma clara algumas técnicas de rastreio (por exemplo, impressão digital do aparelho) que podem não implicar o acesso/armazenamento no aparelho. Por último, a sua aplicação pode ser onerosa para as empresas.

A avaliação concluiu que as regras em matéria de privacidade e comunicações eletrónicas ainda possuem **valor acrescentado a nível da UE** para melhor alcançar o objetivo de assegurar a privacidade em linha tendo em conta a dimensão cada vez mais transnacional do mercado de comunicações eletrónicas . Também demonstrou que, globalmente, as regras são **coerentes** com outra legislação pertinente, embora tenham sido identificadas algumas redundâncias em relação ao novo RGPD (ver secção 1.2).

3.2. Consulta das partes interessadas

A Comissão organizou uma consulta pública entre 12 de abril e 5 de julho de 2016, tendo recebido 421 respostas[12]. As principais conclusões são as seguintes[13]:

– **Necessidade de regras especiais para o setor das comunicações eletrónicas em matéria de confidencialidade das comunicações eletrónicas**: 83,4 % dos cidadãos, consumidores e organizações da sociedade civil e 88,9 % das autoridades públicas que responderam concordam, ao passo que 63,4 % dos inquiridos da indústria não concordam.

– **Alargamento do âmbito de aplicação aos novos serviços de comunicações (OTT)**: 76 % dos cidadãos e da sociedade civil e 93,1 % das autoridades públicas concordam, ao passo que apenas 36,2 % dos inquiridos da indústria estão a favor da referida extensão.

[12] 162 contribuições de cidadãos, 33 de organizações de sociedade civil e de consumidores; 186 da indústria e 40 das autoridades públicas, incluindo as autoridades responsáveis pela aplicação da Diretiva Privacidade e Comunicações Eletrónicas.

[13] O texto integral do relatório está disponível em: https://ec.europa.eu/digital-single-market/news-redirect/37204.

– **Alteração das derrogações ao consentimento para o tratamento de dados de tráfego e de localização**: 49,1 % dos cidadãos, consumidores e organizações da sociedade civil e 36 % das autoridades públicas preferem não alargar as derrogações, ao passo que 36 % da indústria é a favor do alargamento das derrogações e 2/3 da indústria defende a mera revogação das disposições.

– **Apoio às soluções propostas para a questão do consentimento dos testemunhos de conexão**: 81,2 % dos cidadãos e 63 % das autoridades públicas apoia a imposição de obrigações aos fabricantes de equipamentos terminais para a comercialização de produtos com predefinições de privacidade ativadas, embora 58,3 % da indústria seja a favor da opção de apoio à autorregulação ou à corregulação.

Além disso, a Comissão Europeia organizou dois seminários em abril de 2016, um aberto a todas as partes interessadas e um aberto às autoridades nacionais competentes, abordando as principais questões das consultas públicas. As opiniões expressas durante os seminários refletiram o resultado da consulta pública.

A fim de obter pareceres dos cidadãos, realizou-se um inquérito Eurobarómetro sobre privacidade e comunicações eletrónicas[14] em toda a UE. As principais conclusões são as seguintes[15]:

– 78 % das pessoas defendem que é muito importante que só se possa aceder às informações pessoais constantes do seu computador, telemóvel inteligente ou tablete com a sua autorização.

– 72 % declaram que é muito importante que seja garantida a confidencialidade das suas mensagens de correio eletrónico e mensagens instantâneas em linha.

– 89 % concordam com a opção sugerida de que as predefinições do seu programa de navegação devam parar a partilha das suas informações.

3.3. Obtenção e utilização de conhecimentos especializados

A Comissão baseou-se no seguinte aconselhamento especializado externo:

– consultas específicas a grupos de peritos da UE: parecer do Grupo de Trabalho do artigo 29.º; parecer da AEPD; parecer da Plataforma REFIT; pareceres do ORECE; pareceres da ENISA e dos membros da Rede de Cooperação no Domínio da Defesa do Consumidor.

– Conhecimentos especializados externos, nomeadamente os seguintes dois estudos:

  – Estudo «Diretiva Privacidade e Comunicações Eletrónicas: avaliação da transposição, da eficácia e da compatibilidade com a proposta de Regulamento sobre a Proteção de Dados» (SMART 2013/007116).

  – Estudo «Avaliação e revisão da Diretiva 2002/58 relativa à privacidade e ao setor das comunicações eletrónicas» (SMART 2016/0080).

[14] Inquérito Eurobarómetro 2016 (EB) 443 sobre privacidade e comunicações eletrónicas (SMART 2016/079).

[15] O texto integral do relatório está disponível em: https://ec.europa.eu/digital-single-market/news-redirect/37205.

3.4. Avaliação de impacto

A presente proposta foi objeto de uma avaliação de impacto sobre a qual, em 28 de setembro de 2016, o Comité de Controlo da Regulamentação emitiu um parecer positivo[16]. Para ter em conta as recomendações do Comité, a avaliação de impacto explica melhor o âmbito da iniciativa, a sua coerência com outros instrumentos jurídicos (RGPD, CECE, DER) e a necessidade de um instrumento separado. O cenário de base é mais desenvolvido e clarificado. A análise dos impactos é reforçada e equilibrada, clarificando e reforçando a descrição dos custos e benefícios esperados.

Foram examinadas as seguintes opções estratégicas em função dos critérios de eficácia, eficiência e coerência:

– **Opção 1:** Medidas não legislativas («instrumentos jurídicos não vinculativos»);

– **Opção 2:** Reforço limitado da privacidade/confidencialidade e simplificação;

– **Opção 3:** Reforço moderado da privacidade/confidencialidade e simplificação;

– **Opção 4:** Reforço considerável da privacidade/confidencialidade e simplificação;

– **Opção 5:** Revogação da Diretiva Privacidade e Comunicações Eletrónicas.

A **opção 3** foi, na maioria dos aspetos, identificada como a **opção preferida** para alcançar os objetivos, tendo em conta a sua eficiência e coerência. Os principais benefícios são:

– Reforçar a proteção da confidencialidade das comunicações eletrónicas mediante o alargamento do âmbito de aplicação do instrumento jurídico para a inclusão de novos serviços de comunicações eletrónicas funcionalmente equivalentes. Além disso, o Regulamento reforça o controlo por parte do utilizador final ao esclarecer que o consentimento pode ser expresso através de predefinições técnicas adequadas.

– Reforçar a proteção contra as comunicações não solicitadas, com a introdução de uma obrigação de identificação da linha chamadora ou de um prefixo obrigatório para as chamadas promocionais e possibilidades acrescidas de bloquear as chamadas de números indesejados.

– Simplificar e clarificar o quadro regulamentar, através da redução da margem de manobra deixada aos Estados-Membros, da revogação das disposições obsoletas e do alargamento das exceções às regras de consentimento.

O impacto económico da opção 3 deverá ser globalmente proporcional aos objetivos da proposta. Oferece aos serviços de comunicações eletrónicas tradicionais oportunidades comerciais relacionadas com o tratamento de dados de comunicações, ao passo que os prestadores de serviços OTT passam a estar sujeitos às mesmas regras, o que implica alguns custos de conformidade adicionais para estes operadores. No entanto, esta alteração não irá afetar substancialmente os OTT que já operam com base no consentimento. Por último, o impacto da opção não seria sentido nos Estados-Membros que já alargaram essas regras aos OTT.

O facto de centralizar o consentimento em *software* como os programas de navegação Internet, de incentivar os utilizadores a escolherem as suas predefinições de privacidade e de alargar as exceções à regra do consentimento de testemunhos de conexão, permitiria a uma parte significativa das empresas eliminar as mensagens e avisos de testemunhos de conexão, conduzindo a poupanças de custos potencialmente significativas e à simplificação. No

[16] http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

entanto, pode tornar-se mais difícil para anunciantes com publicidade orientada em linha obter o consentimento se uma grande parte dos utilizadores optar por «rejeitar testemunhos de conexão de terceiros» nas suas definições. Ao mesmo tempo, centralizar o consentimento não priva os operadores de sítios web da possibilidade de obterem o consentimento por meio de pedidos individuais aos utilizadores finais, mantendo assim o seu modelo de negócios. Tal traduzir-se-ia em custos adicionais para alguns fornecedores de programas de navegação ou de *software* similar, uma vez que estes teriam de garantir predefinições que respeitem a privacidade.

O estudo externo identificou três cenários de aplicação da opção 3 distintos, de acordo com a entidade que estabelecerá a caixa de diálogo entre o utilizador que escolheu «rejeitar testemunhos de conexão de terceiros» e «não rastrear» nas suas predefinições e os sítios Web visitados que pretendam que o utilizador da Internet reconsidere a sua escolha. As entidades que poderiam ser encarregadas desta tarefa técnica são as seguintes: 1) *software*, como programas de navegação Internet; 2) o rastreador terceiro; 3) os sítios Web individuais (ou seja, o serviço da sociedade da informação solicitado pelo utilizador). Em relação ao cenário de referência, a opção 3 conduziria a poupanças globais em termos de custos de conformidade de 70 % (poupanças de 948,8 milhões de euros) no caso do primeiro cenário (solução do programa de navegação), executado na presente proposta. As poupanças de custos seriam inferiores nos outros cenários. Uma vez que as poupanças globais resultam, em grande medida, de uma redução muito significativa do número de empresas afetadas, o montante individual dos custos de conformidade que uma empresa incorreria – em média – seria mais elevado do que atualmente.

3.5. Adequação e simplificação da legislação

As medidas propostas no âmbito da opção preferida visam o objetivo da simplificação e da redução dos encargos administrativos, em conformidade com as conclusões da avaliação REFIT e o parecer da Plataforma REFIT[17].

A Plataforma REFIT emitiu três conjuntos de recomendações à Comissão:

– A proteção da vida privada dos cidadãos deverá ser reforçada através de um alinhamento da Diretiva Privacidade e Comunicações Eletrónicas com o Regulamento Geral sobre a Proteção de Dados;

– A eficácia da proteção dos cidadãos contra marketing não solicitado deverá ser reforçada mediante exceções à regra do «consentimento» de testemunhos de conexão;

– A Comissão deve tratar os problemas de aplicação nacionais e facilitar o intercâmbio de boas práticas entre Estados-Membros.

A proposta inclui especificamente:

– Utilização de definições tecnologicamente neutras para englobar novos serviços e tecnologias, a fim de assegurar que o presente regulamento é orientado para o futuro;

– Revogação das regras de segurança a fim de eliminar a duplicação de regulamentação;

– Clarificação do âmbito de aplicação a fim de contribuir para a eliminação/redução do risco de divergências na aplicação pelos Estados-Membros (ponto 3 do Parecer);

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

– Clarificação e simplificação da regra de consentimento para a utilização de testemunhos de conexão e outros identificadores, tal como explicado nas secções 3.1 e 3.4 (ponto 2 do Parecer);

– Alinhamento das autoridades de controlo com as autoridades competentes para executar o RGPD e recurso ao procedimento de controlo da coerência do RGPD.

3.6. Impacto sobre os direitos fundamentais

A proposta visa aumentar a eficácia da proteção da privacidade e dos dados pessoais tratados no contexto das comunicações eletrónicas, em conformidade com os artigos 7.º e 8.º da Carta e assegurar uma maior segurança jurídica. A proposta completa e pormenoriza o RGPD. A proteção eficaz da confidencialidade das comunicações é essencial para o exercício da liberdade de expressão e de informação e de outros direitos conexos, tais como o direito à proteção dos dados pessoais ou a liberdade de pensamento, de consciência e de religião.

4. INCIDÊNCIA ORÇAMENTAL

A presente proposta não tem incidência no orçamento da União.

5. OUTROS ELEMENTOS

5.1. Planos de execução e mecanismos de acompanhamento, avaliação e informação

A Comissão acompanhará a aplicação do regulamento e apresentará um relatório sobre a sua avaliação ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu, de três em três anos. Estes relatórios serão públicos e descreverão pormenorizadamente a aplicação efetiva e a execução do presente regulamento.

5.2. Explicação pormenorizada das disposições específicas da proposta

O capítulo I contém as disposições gerais: o objeto (artigo 1.º), o âmbito de aplicação (artigos 2.º e 3.º) e as suas definições, incluindo referências a definições pertinentes de outros instrumentos da UE, como o RGPD.

O capítulo II contém as principais disposições que garantem a confidencialidade das comunicações eletrónicas (artigo 5.º) e precisa para que fins e em que condições limitadas é permitido o tratamento desses dados de comunicações (artigos 6.º e 7.º). Aborda igualmente a proteção dos equipamentos terminais, através da i) garantia da integridade da informação armazenada nos mesmos e da ii) proteção da informação proveniente do equipamento terminal, uma vez que pode permitir a identificação do respetivo utilizador final (artigo 8.º). Por último, o artigo 9.º especifica o consentimento dos utilizadores finais, um fundamento legal central do presente regulamento, referindo-se expressamente à sua definição e às condições previstas no RGPD, ao passo que o artigo 10.º impõe aos fornecedores de *software* que permite comunicações eletrónicas a obrigação de ajudar os utilizadores finais a fazerem escolhas eficazes quanto às predefinições de privacidade. O artigo 11.º especifica os objetivos e condições para os Estados-Membros restringirem as disposições acima referidas.

O capítulo III diz respeito aos direitos de os utilizadores finais controlarem o envio e a receção de comunicações eletrónicas, a fim de protegerem a sua privacidade: i) o direito de os utilizadores finais impedirem a apresentação da identificação da linha chamadora, a fim de garantirem o anonimato (artigo 12.º), com as suas limitações (artigo 13.º); e ii) a obrigação de os fornecedores de comunicações interpessoais associadas a um número e acessíveis ao público preverem a possibilidade de limitar a receção de chamadas indesejadas (artigo 14.º). Este capítulo regula ainda as condições em que os utilizadores finais podem ser incluídos em

listas acessíveis ao público (artigo 15.º) e as condições em que as comunicações comerciais diretas não solicitadas podem ser efetuadas (artigo 17.º). Também se refere a riscos de segurança e prevê a obrigação, por parte dos prestadores de serviços de comunicações eletrónicas, de alertarem os utilizadores finais caso um determinado risco possa comprometer a segurança das redes e serviços. As obrigações de segurança que constam no RGPD e no CECE aplicam-se aos prestadores de serviços de comunicações eletrónicas.

O capítulo IV prevê a supervisão e o controlo da execução do presente regulamento e confia estas tarefas às autoridades de controlo encarregadas do RGPD, tendo em conta as fortes sinergias entre as questões gerais de proteção de dados e a confidencialidade das comunicações (artigo 18.º). Os poderes do Comité Europeu para a Proteção de Dados são alargados (artigo 19.º) e o procedimento de controlo da coerência e da cooperação previsto no âmbito do RGPD será aplicável às questões transfronteiras relacionadas com o presente regulamento (artigo 20.º).

O capítulo V descreve as diferentes vias de recurso disponíveis para os utilizadores finais (artigos 21.º e 22.º) e as sanções que podem ser impostas (artigo 24.º), incluindo as condições gerais para a aplicação de coimas (artigo 23.º).

O capítulo VI diz respeito à adoção de atos delegados e de atos de execução nos termos dos artigos 290.º e 291.º do Tratado.

Por último, o capítulo VII contém as disposições finais do presente regulamento: a revogação da Diretiva Privacidade e Comunicações Eletrónicas, o acompanhamento e a revisão, a entrada em vigor e a aplicação. No que respeita à revisão, a Comissão tenciona avaliar, nomeadamente, se continua a ser necessário um ato jurídico distinto à luz da evolução jurídica, técnica ou económica e tendo em conta a primeira avaliação do Regulamento (UE) 2016/679 prevista para 25 de maio de 2020.

2017/0003 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas)

(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente os artigos 16.º e 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu[1],

Tendo em conta o parecer do Comité das Regiões[2],

Tendo em conta o parecer da Autoridade Europeia para a Proteção de Dados[3],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) O artigo 7.º da Carta dos Direitos Fundamentais da União Europeia («a Carta») protege o direito fundamental de todas as pessoas ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. O respeito pela privacidade das comunicações constitui uma dimensão essencial deste direito. A confidencialidade das comunicações eletrónicas garante que a informação trocada entre partes e os elementos externos dessa comunicação, nomeadamente, quando a informação foi enviada, a partir de onde e a quem, não sejam revelados a uma pessoa distinta das partes envolvidas na comunicação. O princípio da confidencialidade deve ser aplicável às formas de comunicação atuais e futuras, incluindo chamadas, acesso à Internet, mensagens instantâneas, correio eletrónico, chamadas telefónicas pela Internet e mensagens pessoais nas redes sociais.

(2) O conteúdo das comunicações eletrónicas pode revelar informações altamente sensíveis acerca das pessoas singulares envolvidas na comunicação, desde experiências e emoções pessoais a condições de saúde, preferências sexuais e opiniões políticas, cuja divulgação poderia resultar em danos pessoais e sociais, prejuízos económicos ou constrangimento. De igual modo, os metadados derivados de comunicações eletrónicas podem também revelar informações muito sensíveis e

[1] JO C , , p. .
[2] JO C , , p. .
[3] JO C , , p. .

pessoais. Estes metadados incluem os números ligados, os sítios web visitados, a localização geográfica, a hora, a data e duração da chamada, etc., permitindo tirar conclusões precisas relativas à vida privada das pessoas envolvidas na comunicação eletrónica, tais como as suas relações sociais, os seus hábitos e atividades da vida quotidiana, os seus interesses, gostos, etc.

(3) Os dados das comunicações eletrónicas podem também revelar informações sobre pessoas coletivas, tais como os seus segredos comerciais ou outras informações sensíveis com valor económico. Por conseguinte, as disposições do presente regulamento devem aplicar-se tanto a pessoas singulares como coletivas. Além disso, o presente regulamento deve assegurar que as disposições do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[4] são igualmente aplicáveis a utilizadores finais que sejam pessoas coletivas. Tal inclui a definição de consentimento que consta do Regulamento (UE) 2016/679. Quando é feita referência ao consentimento por parte de um utilizador final, incluindo pessoas coletivas, aplica-se esta definição. Além disso, as pessoas coletivas devem ter os mesmos direitos que os utilizadores finais que são pessoas singulares no que respeita às autoridades de controlo; ademais, as autoridades de controlo ao abrigo do presente regulamento devem ser responsáveis pelo acompanhamento da aplicação do mesmo às pessoas coletivas.

(4) Nos termos do artigo 8.º, n.º 1, da Carta e do artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia, todas as pessoas têm o direito à proteção dos dados pessoais que lhes digam respeito. O Regulamento (UE) 2016/679 estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Os dados de comunicações eletrónicas podem incluir dados pessoais, na aceção Regulamento (UE) 2016/679.

(5) As disposições do presente regulamento precisam e completam as regras gerais relativas à proteção dos dados pessoais estabelecidas no Regulamento (UE) n.º 2016/679 no que respeita aos dados de comunicações eletrónicas que possam ser considerados dados pessoais. O presente regulamento, por conseguinte, não baixa o nível de proteção de que beneficiam as pessoas singulares ao abrigo do Regulamento (UE) 2016/679. O tratamento de dados das comunicações eletrónicas pelos prestadores de serviços de comunicações eletrónicas deve apenas ser permitido em conformidade com o presente regulamento.

(6) Embora os princípios e as principais disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho[5] permaneçam, de um modo geral, adequados, esta diretiva não acompanhou plenamente a evolução da realidade tecnológica e do mercado, o que resultou numa proteção efetiva insuficiente ou incoerente da privacidade e da confidencialidade relativamente às comunicações eletrónicas. Esses desenvolvimentos incluem a entrada no mercado de serviços de comunicações eletrónicas que, na perspetiva de um consumidor, são alternativas aos serviços tradicionais, mas que não têm de cumprir o mesmo conjunto de regras. Outro

[4] 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, p. 1-88).

[5] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

desenvolvimento diz respeito a novas técnicas que permitem o rastreio do comportamento em linha dos utilizadores finais que não são abrangidas pela Diretiva 2002/58/CE. A Diretiva 2002/58/CE deve, por conseguinte, ser revogada e substituída pelo presente regulamento.

(7) Os Estados-Membros devem ser autorizados, dentro dos limites do presente regulamento, a manter ou a introduzir disposições nacionais para especificar e clarificar a aplicação das regras do presente regulamento, a fim de assegurar uma aplicação e interpretação eficazes das referidas regras. Por conseguinte, a margem de apreciação de que os Estados-Membros dispõem a este respeito deve permitir manter um equilíbrio entre a proteção da vida privada e dos dados pessoais e a livre circulação de dados de comunicações eletrónicas.

(8) O presente regulamento deve aplicar-se aos prestadores de serviços de comunicações eletrónicas, aos fornecedores de listas acessíveis ao público e aos fornecedores de *software* que permita comunicações eletrónicas, incluindo a recuperação e a apresentação de informações na Internet. Deve aplicar-se igualmente às pessoas singulares e coletivas que utilizam serviços de comunicações eletrónicas para enviar comunicações comerciais diretas ou recolher informações relacionadas com equipamentos terminais dos utilizadores finais ou neles armazenadas.

(9) O presente regulamento deve aplicar-se aos dados das comunicações eletrónicas tratados no contexto da prestação e utilização de serviços de comunicações eletrónicas na União, independentemente de serem ou não tratados na União. Além disso, a fim de não privar os utilizadores finais na União de uma proteção eficaz, o presente regulamento deve aplicar-se igualmente aos dados das comunicações eletrónicas tratados no contexto da prestação de serviços de comunicações eletrónicas de fora da União a utilizadores finais na União.

(10) O equipamento de rádio e respetivo *software* que seja colocado no mercado interno na União deve ser estar em conformidade com a Diretiva 2014/53/UE do Parlamento Europeu e do Conselho[6]. O presente regulamento não deve afetar a aplicabilidade de quaisquer requisitos da Diretiva 2014/53/UE, nem a competência conferida à Comissão para adotar atos delegados nos termos da Diretiva 2014/53/UE que exijam que determinadas categorias ou classes de equipamentos de rádio incluam salvaguardas que assegurem a proteção dos dados pessoais e da privacidade dos utilizadores finais.

(11) Os serviços utilizados para fins de comunicações e os meios técnicos para a sua prestação evoluíram consideravelmente. Os utilizadores finais substituem cada vez mais os serviços tradicionais de telefonia vocal, de mensagens de texto (SMS) e de envio de correio eletrónico, por serviços em linha funcionalmente equivalentes, como a voz sobre IP, os serviços de mensagens e de correio eletrónico com base na web. A fim de assegurar uma proteção eficaz e equitativa dos utilizadores finais aquando da utilização de serviços funcionalmente equivalentes, o presente regulamento utiliza a definição de serviços de comunicações eletrónicas estabelecida na [Diretiva do Parlamento Europeu e do Conselho que estabelece o Código Europeu das

[6] Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado e que revoga a Diretiva 1999/5/CE (JO L 153 de 22.5.2014, p. 62).

Comunicações Eletrónicas[7]]. Esta definição abrange não só os serviços de acesso à Internet e os serviços que consistem total ou parcialmente no envio de sinais, mas também os serviços de comunicações interpessoais, que podem ou não estar associados a um número, como por exemplo, voz sobre IP, serviços de mensagens e de correio eletrónico com base na web. A proteção da confidencialidade das comunicações é igualmente crucial no que respeita aos serviços de comunicações interpessoais que são acessórios de outro serviço; por conseguinte, este tipo de serviços que também possuem uma funcionalidade de comunicação devem ser abrangidos pelo presente regulamento.

(12) As máquinas e dispositivos conectados comunicam cada vez mais entre si mediante a utilização de redes de comunicações eletrónicas (Internet das Coisas). A transmissão de comunicações máquina-máquina implica o envio de sinais através de uma rede e, por conseguinte, constitui normalmente um serviço de comunicações eletrónicas. A fim de assegurar a plena proteção dos direitos à privacidade e à confidencialidade das comunicações, e para promover uma Internet das Coisas segura e de confiança no mercado único digital, é necessário esclarecer que o presente regulamento deve aplicar-se à transmissão de comunicações máquina-máquina. Por conseguinte, o princípio da confidencialidade consagrado no presente regulamento deve aplicar-se igualmente à transmissão de comunicações deste tipo. Podem também ser adotadas salvaguardas específicas ao abrigo da legislação setorial, como por exemplo a Diretiva 2014/53/UE.

(13) O desenvolvimento de tecnologias sem fios rápidas e eficientes permitiu que o público dispusesse de um acesso crescente à Internet através de redes sem fios abertas a todos em espaços públicos e semiprivados, como zonas de Internet sem fios situadas em locais diferentes de uma cidade, grandes armazéns, centros comerciais e hospitais. Uma vez que essas redes de comunicações são disponibilizadas a um grupo indefinido de utilizadores finais, a confidencialidade das comunicações transmitidas através dessas redes deve ser protegida. O facto de os serviços de comunicações eletrónicas sem fios poderem ser acessórios de outros serviços não deve impedir a proteção da confidencialidade dos dados das comunicações e a aplicação do presente regulamento. Por conseguinte, o presente regulamento deve aplicar-se aos dados de comunicações eletrónicas que utilizam serviços de comunicações eletrónicas e redes de comunicações públicas. Em contrapartida, não deve ser aplicável a grupos fechados de utilizadores finais, tais como redes de empresas, cujo acesso é limitado aos membros da sociedade.

(14) Os dados de comunicações eletrónicas devem ser definidos de uma forma suficientemente abrangente e tecnologicamente neutra de modo a incluírem todas as informações relativas ao conteúdo transmitido ou trocado (conteúdo das comunicações eletrónicas) e as informações relativas a um utilizador final de serviços de comunicações eletrónicas tratadas para efeitos de transmissão, distribuição ou intercâmbio desse conteúdo, incluindo dados que permitam encontrar e identificar a fonte e o destino de uma comunicação, a localização geográfica e a data, hora, duração e o tipo de comunicação. Se esses sinais e os respetivos dados forem enviados por cabo, rádio, meios óticos ou eletromagnéticos, incluindo redes de satélite, redes de cabo, redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, sistemas de eletricidade por cabo, os dados relativos a esses sinais

[7] Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece o Código Europeu das Comunicações Eletrónicas (Reformulação) [COM/2016/0590 final – 2016/0288 (COD)].

devem ser considerados metadados de comunicações eletrónicas e, por conseguinte, ser sujeitos às disposições do presente regulamento. Os metadados de comunicações eletrónicas podem incluir informações que façam parte da subscrição do serviço se essas informações forem tratadas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas.

(15) Os dados das comunicações eletrónicas devem ser tratados como dados confidenciais. Isto significa que qualquer interferência com a transmissão de dados de comunicações eletrónicas, seja diretamente por intervenção humana ou através de tratamento automatizado por máquinas, sem o consentimento de todas as partes comunicantes deve ser proibida. A proibição da interceção de dados de comunicações deve ser aplicável durante o seu envio, ou seja, até à receção do conteúdo da comunicação eletrónica pelo destinatário desejado. A interceção de dados de comunicações eletrónicas pode ocorrer, por exemplo, quando alguém, que não as partes comunicantes, ouve as chamadas, lê, digitaliza ou armazena o conteúdo das comunicações eletrónicas, ou os metadados associados, para fins que não a troca de comunicações. A interceção ocorre também quando terceiros controlam os sítios web visitados, o calendário das visitas, a interação com outros, etc., sem o consentimento do utilizador final em causa. À medida que a tecnologia evoluiu, os meios técnicos para proceder à interceção também multiplicaram. Esses meios podem incluir desde a instalação de equipamento que reúne dados provenientes de equipamentos terminais em zonas específicas, tais como os chamados intercetores de IMSI (Identidade Internacional de Assinante Móvel), aos programas e técnicas que, por exemplo, monitorizam sub-repticiamente os hábitos de navegação na Internet para criar perfis de utilizador final. Outros exemplos de interceção incluem a captação de dados sobre a carga útil ou o conteúdo provenientes de redes sem fios não encriptadas e roteadores, incluindo os hábitos de navegação na Internet, sem o consentimento dos utilizadores finais.

(16) A proibição de armazenamento das comunicações não tem por objetivo proibir qualquer armazenamento automático, intermédio e transitório das informações, na medida em que este sirva exclusivamente para a execução da transmissão na rede de comunicações eletrónicas. Não deve proibir o tratamento de dados de comunicações eletrónicas para garantir a segurança e a continuidade dos serviços de comunicações eletrónicas, incluindo a verificação das ameaças à segurança, tais como a presença de programas maliciosos, nem o tratamento dos metadados para assegurar a necessária qualidade dos serviços, em termos de controlo de latência, instabilidade, etc.

(17) O tratamento dos dados de comunicações eletrónicas pode ser útil para as empresas, consumidores e sociedade em geral. Em relação à Diretiva 2002/58/CE, o presente regulamento alarga as possibilidades de tratamento de metadados das comunicações eletrónicas pelos prestadores de serviços de comunicações eletrónicas, com base no consentimento do utilizador final. No entanto, os utilizadores finais conferem grande importância à confidencialidade das suas comunicações, incluindo as suas atividades em linha, e desejam controlar a utilização dos dados das comunicações eletrónicas para fins diferentes do envio de comunicação. Por conseguinte, o presente regulamento deve exigir que os prestadores de serviços de comunicações eletrónicas obtenham o consentimento dos utilizadores finais para procederem ao tratamento dos metadados de comunicações eletrónicas. Os dados de localização que são gerados fora do contexto de uma comunicação não devem ser considerados metadados. Os exemplos de utilizações comerciais dos metadados das comunicações eletrónicas por prestadores de serviços de comunicações eletrónicas podem incluir o fornecimento de mapas

térmicos (*heatmaps*); uma representação gráfica dos dados utilizando cores para indicar a presença de pessoas. Para apresentar os movimentos de tráfego em certas direções durante um determinado período de tempo é necessário um identificador para estabelecer a ligação entre as posições das pessoas em certos intervalos de tempo. Este identificador seria omisso se fossem utilizados dados anónimos e esse movimento não poderia ser visto. Essa utilização de metadados de comunicações eletrónicas pode, por exemplo, ajudar as autoridades públicas e os operadores de transporte coletivo a definirem onde desenvolver novas infraestruturas, com base na utilização e na pressão sobre a estrutura existente. Sempre que um tipo de tratamento de metadados de comunicações eletrónicas, nomeadamente que utilize novas tecnologias, e tendo em conta a natureza, o âmbito de aplicação, o contexto e as finalidades do tratamento, seja suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares, deve realizar-se uma avaliação de impacto sobre a proteção dos dados e, se for caso disso, uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) 2016/679.

(18) Os utilizadores finais podem consentir o tratamento dos seus metadados a fim de receberem serviços específicos, tais como serviços de proteção contra atividades fraudulentas (através da análise dos dados de utilização, da localização e da conta de cliente em tempo real). Na economia digital, os serviços são frequentemente prestados em troca de uma contrapartida que não dinheiro, por exemplo, mediante a exposição dos utilizadores finais a anúncios. Para efeitos do presente regulamento, o consentimento de um utilizador final, independentemente de este ser uma pessoa singular ou coletiva, deve ter o mesmo significado e estar subordinado às mesmas condições que o consentimento do titular de dados ao abrigo do Regulamento (UE) 2016/679. Os serviços de acesso à Internet de banda larga básica e de comunicações de voz devem ser considerados serviços essenciais para que as pessoas sejam capazes de comunicar e participar nos benefícios da economia digital. O consentimento para o tratamento de dados provenientes da Internet ou da utilização de comunicações de voz não será válido se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.

(19) O conteúdo das comunicações eletrónicas inscreve-se na essência do direito fundamental ao respeito pela vida privada e familiar, pelo domicílio e pelas comunicações protegido pelo artigo 7.º da Carta. Qualquer interferência no conteúdo das comunicações eletrónicas deve ser permitida apenas sob condições muito claramente definidas, para fins específicos e mediante garantias adequadas contra abusos. O presente regulamento prevê a possibilidade de os prestadores de serviços de comunicações eletrónicas tratarem os dados de comunicações eletrónicas em trânsito, com o consentimento informado de todos os utilizadores finais em causa. Por exemplo, os prestadores podem oferecer serviços que impliquem a digitalização das mensagens de correio eletrónico para a eliminação de certos materiais pré-definidos. Dado o caráter sensível do conteúdo das comunicações, o presente regulamento estabelece uma presunção de que o tratamento desses dados de conteúdo terá como resultado um elevado risco para os direitos e liberdades das pessoas singulares. Aquando do tratamento deste tipo de dados, o prestador do serviço de comunicações eletrónicas deve consultar sempre a autoridade de controlo antes do tratamento. Tal consulta deve estar em conformidade com o artigo 36.º, n.^{os} 2 e 3, do Regulamento (UE) 2016/679. A presunção não abrange o tratamento de dados de conteúdo para a prestação de um serviço solicitado pelo utilizador final quando este consentiu tal tratamento e o tratamento for efetuado para os fins e duração estritamente necessários e proporcionados para esse serviço. Após o conteúdo das comunicações eletrónicas ter

sido enviado pelo utilizador final e recebido pelo ou pelos utilizadores finais destinatários, pode ser registado ou armazenado pelo utilizador final, utilizadores finais ou por um terceiro por eles mandatado para registar ou armazenar esses dados. Qualquer tratamento desses dados deve ser conforme com o Regulamento (UE) 2016/679.

(20) Os equipamentos terminais dos utilizadores finais de redes de comunicações eletrónicas e quaisquer informações relativas à utilização de tais equipamentos terminais, em especial as armazenadas ou emitidas por tais equipamentos, solicitadas ou tratadas para permitir a sua ligação a outro dispositivo e/ou equipamento de rede, fazem parte da esfera privada dos utilizadores finais, que deve ser protegida por força da Carta dos Direitos Fundamentais da União Europeia e da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Tendo em conta que esses equipamentos contêm ou tratam informações suscetíveis de revelar pormenores sobre as complexidades emocionais, políticas e sociais de uma pessoa singular, incluindo o conteúdo das comunicações, imagens, a localização das pessoas através do acesso às capacidades de GPS do dispositivo, listas de contactos, bem como outras informações já armazenadas no dispositivo, as informações relacionadas com o referido equipamento exigem uma proteção da privacidade reforçada. Além disso, os denominados programas espiões, os pixels espiões, os identificadores ocultos, os testemunhos persistentes e outros dispositivos de rastreio indesejado análogos podem introduzir-se nos equipamentos terminais dos utilizadores finais, sem o seu conhecimento, a fim de aceder a informações, armazenar informações ocultas ou rastrear atividades. As informações relacionadas com o dispositivo do utilizador final podem igualmente ser recolhidas à distância para efeitos de identificação e rastreio, recorrendo a técnicas como a recolha da «impressão digital do aparelho», muitas vezes sem o conhecimento do utilizador final, e podem constituir uma grave intrusão na privacidade desses utilizadores finais. As técnicas que controlam sub-repticiamente as ações dos utilizadores finais, mediante o rastreio das suas atividades em linha ou a localização do seu equipamento terminal, por exemplo, ou que alteram o funcionamento do equipamento terminal dos utilizadores finais, representam uma séria ameaça à privacidade destes utilizadores. Por conseguinte, as interferências com o equipamento terminal do utilizador final só devem ser permitidas com o consentimento deste último e para fins específicos e transparentes.

(21) As exceções à obrigação de obter o consentimento para utilizar as capacidades de tratamento e de armazenamento do equipamento terminal ou para aceder à informação armazenada no equipamento terminal devem ser limitadas a situações que envolvam nenhuma, ou apenas uma muito limitada, intrusão na privacidade. Por exemplo, o consentimento não deve ser solicitado para autorizar o armazenamento técnico o ou acesso que sejam estritamente necessários e proporcionados para o objetivo legítimo de permitir a utilização de um serviço específico explicitamente solicitado pelo utilizador final. Tal pode incluir o armazenamento de testemunhos de conexão enquanto durar uma sessão única determinada num sítio web, a fim de conservar os dados do utilizador final aquando do preenchimento de formulários em linha de várias páginas. Os testemunhos de conexão também podem ser um instrumento legítimo e útil, nomeadamente para medir o tráfego de um sítio web. O facto de o prestador de serviços da sociedade da informação verificar a configuração para prestar o serviço em conformidade com as predefinições do utilizador final e o mero registo do facto de o dispositivo do utilizador final não permitir receber o conteúdo solicitado pelo utilizador final não devem ser considerados um acesso ao referido dispositivo nem uma utilização das capacidades de tratamento do dispositivo.

(22) Os métodos utilizados para a prestação de informações e a obtenção do consentimento do utilizador final deverão ser tão conviviais quanto possível. Atendendo à utilização omnipresente de testemunhos persistentes e outras técnicas de rastreio, os utilizadores finais são cada vez mais convidados a dar o seu consentimento para o armazenamento de tais testemunhos persistentes no seu equipamento terminal. Em consequência, os utilizadores finais são sobrecarregados com pedidos de consentimento. A utilização de meios técnicos para expressar o consentimento, nomeadamente, através de predefinições transparentes e de fácil utilização, pode resolver este problema. O presente regulamento deverá, pois, prever a possibilidade de expressar o consentimento utilizando as predefinições adequadas do programa de navegação ou outra aplicação. As escolhas efetuadas pelos utilizadores finais quando estabelecem as suas predefinições gerais de privacidade de um programa de navegação ou de outra aplicação devem ser vinculativas e aplicáveis a quaisquer terceiros. Os navegadores web são um tipo de aplicação de *software* que permite a recuperação e a apresentação de informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente, os programas de navegação podem ser utilizados como filtro, ajudando assim os utilizadores finais a impedir o acesso a informações provenientes do seu equipamento terminal (por exemplo, telemóvel inteligente, tablete ou computador) ou o armazenamento dessas informações.

(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) 2016/679. Atualmente, a maioria dos programas de navegação estão configurados, por defeito, para «aceitarem todos os testemunhos de conexão». Por conseguinte, os fornecedores de *software* que permitam a recuperação e a apresentação de informações da Internet devem ser obrigados a configurar o *software* de modo a que ofereça a possibilidade de impedir que terceiros armazenem informações nos equipamentos terminais; este procedimento é frequentemente apresentado como «rejeitar testemunhos de conexão de terceiros». Os utilizadores finais devem dispor da configuração que lhes permita escolher entre diferentes níveis um conjunto de opções de privacidade, desde o nível mais elevado (por exemplo, «nunca aceitar testemunhos de conexão») ao nível mais baixo (por exemplo, «aceitar sempre testemunhos de conexão»), passando pelo nível intermédio (por exemplo, «rejeitar testemunhos de conexão de terceiros» ou «aceitar apenas testemunhos do sítio visitado»). Essas predefinições de privacidade devem ser apresentadas de uma forma compreensível e facilmente visível.

(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) 2016/679, por exemplo, para o armazenamento de testemunhos persistentes de terceiros, os programas de navegação devem, nomeadamente, solicitar ao utilizador final dos equipamentos terminais um ato positivo inequívoco a manifestar o seu acordo livre, específico, informado e explícito em relação ao armazenamento e ao acesso desses testemunhos de conexão no e a partir do equipamento terminal. Tal ato pode ser considerado positivo, por exemplo, se os utilizadores finais forem obrigados a selecionar de forma ativa «aceitar testemunhos de conexão de terceiros» a fim de confirmar o seu acordo e lhes forem facultadas as informações necessárias para efetuar a escolha. Para o efeito, é necessário exigir aos fornecedores de *software* que permite o acesso à Internet que, no momento da instalação, os utilizadores finais sejam

informados da possibilidade de escolher as predefinições de privacidade de entre as diferentes opções e que lhes seja solicitada uma escolha. As informações prestadas não devem dissuadir os utilizadores finais de selecionar as predefinições de privacidade mais elevadas e devem incluir informações sobre os riscos associados à permissão do armazenamento de testemunhos de conexão de terceiros no computador, incluindo a compilação a longo prazo de registos do histórico de navegação das pessoas singulares e a utilização desses registos para enviar publicidade orientada. Os programas de navegação da web são incentivados a proporcionar aos utilizadores finais meios para alterar facilmente as predefinições de privacidade em qualquer momento durante a utilização e a permitir que o utilizador faça exceções ou dê permissão a certos sítios web ou que especifique para que sítios web são sempre ou nunca consentidos testemunhos de conexão (de terceiros).

(25) O acesso às redes de comunicações eletrónicas exige o envio regular de determinados pacotes de dados por forma a descobrir ou a manter uma ligação à rede ou a outros dispositivos na rede. Além disso, deve ser atribuído um endereço único a cada aparelho para que este possa ser identificável nessa rede. Do mesmo modo, as normas em matéria de telefones celulares e sem fios preveem a emissão de sinais ativos que contêm identificadores únicos, como o endereço MAC, a IMEI (Identidade Internacional de Equipamento Móvel), a IMSI, etc. Uma única estação de base sem fios (ou seja, um transmissor e recetor), como um ponto de acesso sem fios, tem um alcance específico dentro do qual essas informações podem ser capturadas. Surgiram prestadores de serviços que oferecem serviços de rastreio com base em informações relativas a equipamentos com funcionalidades diversas, incluindo a contagem de pessoas, o fornecimento de dados sobre o número de pessoas em fila de espera, a determinação do número de pessoas numa determinada zona, etc. Esta informação pode ser utilizada para fins mais invasivos, como para enviar mensagens comerciais aos utilizadores finais, por exemplo quando estes entram em lojas, com ofertas personalizadas. Embora algumas destas funcionalidades não acarretem riscos de privacidade elevados, outras sim, como por exemplo as que envolvem o rastreio das pessoas ao longo do tempo, incluindo visitas repetidas a locais específicos. Os fornecedores envolvidos em tais práticas devem afixar avisos visíveis, localizados na extremidade da zona de cobertura, que informem os utilizadores finais, antes da entrada na zona definida, de que a tecnologia está em funcionamento num determinado perímetro, do objetivo do rastreio, da pessoa responsável e da existência de qualquer medida que o utilizador final dos equipamentos terminais possa tomar para reduzir ou fazer cessar a recolha de dados. Devem ser fornecidas informações adicionais sempre que sejam recolhidos os dados pessoais em conformidade com o artigo 13.º do Regulamento (UE) 2016/679.

(26) Nos casos em que o tratamento de dados de comunicações eletrónicas pelos prestadores de serviços de comunicações eletrónicas estiver abrangido pelo seu âmbito de aplicação, o presente regulamento deverá prever a possibilidade de a União ou os Estados-Membros restringirem legalmente, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar interesses públicos específicos, como a segurança nacional, a defesa e a segurança pública e a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública e outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, em especial um interesse económico ou financeiro importante da União ou de um Estado-Membro, ou uma missão de controlo, de inspeção ou de regulamentação

associada ao exercício da autoridade pública relativamente a tais interesses. Por conseguinte, o presente regulamento não deve afetar a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário e proporcionado para salvaguardar os interesses públicos acima referidos, em conformidade com a Carta dos Direitos Fundamentais da União Europeia e a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, segundo a interpretação do Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos do Homem. Os prestadores de serviços de comunicações eletrónicas devem estabelecer procedimentos adequados para facilitar pedidos legítimos das autoridades competentes, tendo igualmente em conta, sempre que relevante, o papel do representante designado nos termos do artigo 3.º, n.º 3.

(27) No que respeita à identificação da linha chamadora, é necessário proteger o direito da parte que efetua a chamada de suprimir a apresentação da identificação da linha da qual a chamada é feita e o direito da parte destinatária de rejeitar chamadas de linhas não identificadas. Certos utilizadores finais, em especial as linhas de apoio, e outras organizações similares, têm interesse em garantir o anonimato de quem faz as chamadas. No que se refere à identificação da linha conectada, é necessário proteger o direito e os legítimos interesses da parte destinatária de impedir a apresentação da identificação da linha à qual a parte chamadora se encontra efetivamente ligada.

(28) Em casos específicos, justifica-se impedir que a apresentação da identificação da linha chamadora seja suprimida. Deve restringir-se os direitos à privacidade dos utilizadores finais no que respeita à identificação da linha chamadora sempre que tal for necessário para detetar chamadas inoportunas e, no que respeita à identificação da linha chamadora e aos dados de localização, sempre que tal for necessário para possibilitar que os serviços de emergência desempenhem as suas missões de forma tão eficaz quanto possível.

(29) Existe tecnologia que permite que os prestadores de serviços de comunicações eletrónicas limitem, de diferentes maneiras, a receção de chamadas não desejadas pelos utilizadores finais, designadamente pelo bloqueio de chamadas silenciosas e outras chamadas fraudulentas e incomodativas. Os prestadores de serviços de comunicações interpessoais com base no número acessíveis ao público devem utilizar esta tecnologia e proteger os utilizadores finais contra chamadas incomodativas, de forma gratuita. Os fornecedores devem assegurar que os utilizadores finais têm conhecimento da existência de tais funcionalidades publicitando o facto no seu sítio web, por exemplo.

(30) As listas acessíveis ao público de utilizadores finais de serviços de comunicações eletrónicas são amplamente distribuídas. listas acessíveis ao público significa qualquer lista ou serviço que contenha informações sobre os utilizadores finais, tais como números de telefone (incluindo os números de telefone móvel), endereço de correio eletrónico e inclui os serviços informativos. O direito à privacidade e à proteção dos dados pessoais de uma pessoa singular exige que os utilizadores finais que são pessoas singulares, dêem o seu consentimento antes dos seus dados pessoais serem incluídos numa lista. O interesse legítimo das pessoas coletivas exige que os utilizadores finais que são pessoas coletivas tenham o direito de se opor à inclusão numa lista de dados com eles relacionados.

(31) Se os utilizadores finais que são pessoas singulares consentirem que os seus dados sejam incluídos em tais listas, devem poder determinar, com base no consentimento,

que categorias de dados pessoais devem figurar na lista (por exemplo, nome e apelido, endereço de correio eletrónico, endereço postal, nome de utilizador, número de telefone). Além disso, os fornecedores de listas acessíveis ao público devem informar os utilizadores finais da finalidade da lista e das suas funções de procura, antes de os incluir na mesma. Os utilizadores finais devem poder determinar, mediante consentimento, as categorias de dados pessoais que podem servir de base para procurar os seus dados de contacto. As categorias de dados pessoais incluídas na lista e as categorias de dados pessoais com base nas quais os dados de contacto do utilizador final podem ser procurados não devem ser necessariamente as mesmas.

(32) No presente regulamento, «marketing direto» refere-se a qualquer forma de publicidade através da qual uma pessoa singular ou coletiva envia diretamente comunicações comerciais diretas a um ou mais utilizadores finais identificados ou identificáveis através da utilização de serviços de comunicações eletrónicas. Para além da oferta de produtos e de serviços para fins comerciais, deve incluir igualmente as mensagens enviadas pelos partidos políticos que contactam pessoas singulares através de serviços de comunicações eletrónicas para promover os seus partidos. O mesmo deverá aplicar-se às mensagens enviadas por outras organizações sem fins lucrativos para apoiar os objetivos da organização.

(33) Há que prever salvaguardas para proteger os utilizadores finais contra comunicações não solicitadas para fins de marketing direto, que invadem a vida privada dos utilizadores finais. O grau de invasão da privacidade e de incómodo é considerado relativamente semelhante, independentemente do amplo leque de tecnologias e meios utilizados para efetuar essas comunicações eletrónicas, quer utilizando sistemas de chamada e de comunicação automatizados, aplicações de mensagens instantâneas, mensagens de correio eletrónico, SMS, MMS, Bluetooth, etc. Por conseguinte, justifica-se exigir a obtenção do consentimento do utilizador final antes lhe enviar comunicações eletrónicas comerciais para fins de marketing direto, a fim de proteger eficazmente os indivíduos contra a intrusão na sua vida privada, assim como os interesses legítimos das pessoas coletivas. A segurança jurídica e a necessidade de assegurar que as regras de proteção contra as comunicações eletrónicas não solicitadas permanecem orientadas para o futuro justificam a necessidade de definir um conjunto único de regras que não variam em função da tecnologia utilizada para enviar estas comunicações não solicitadas, garantindo ao mesmo tempo um nível equivalente de proteção para todos os cidadãos em toda a União. No entanto, é razoável permitir a utilização de contactos de correio eletrónico no contexto de uma relação existente entre o cliente e o fornecedor para a oferta de produtos ou serviços similares. Essa possibilidade deve aplicar-se apenas à mesma empresa que obteve as coordenadas eletrónicas de contacto em conformidade com o Regulamento (UE) 2016/679.

(34) Quando os utilizadores finais tiverem consentido receber comunicações não solicitadas para fins de marketing direto, devem poder retirar facilmente o seu consentimento a qualquer momento. Para facilitar a aplicação eficaz das regras da União relativas às mensagens não solicitadas para fins de marketing direto, é necessário proibir a ocultação da identidade e a utilização de falsas identidades, falsos endereços ou números quando se enviam comunicações comerciais não solicitadas para fins de marketing direto. As comunicações comerciais não solicitadas devem, por conseguinte, ser claramente identificáveis como tal e indicar a identidade da pessoa singular ou coletiva que transmite a comunicação, ou por conta de quem a comunicação é transmitida, e fornecer as informações necessárias para que os

destinatários exerçam o seu direito de se oporem à receção de novas mensagens comerciais escritas e/ou orais.

(35) A fim de facilitar a retirada do consentimento, as pessoas singulares ou coletivas que efetuam comunicações de marketing direto por correio eletrónico devem apresentar uma ligação, ou um endereço de correio eletrónico válido, que possa ser facilmente utilizado pelos utilizadores finais para retirarem o seu consentimento. As pessoas singulares ou coletivas que efetuam comunicações de marketing direto através de chamadas vocais e de chamadas por sistemas de chamada e de comunicação automatizados devem exibir a identidade da linha para a qual a empresa pode ser contactada ou apresentar um código específico que indique que se trata de uma chamada promocional.

(36) As chamadas vocais de marketing direto que não envolvem a utilização de sistemas de chamada e de comunicação automatizados são mais onerosos para o emissor e não implicam quaisquer custos financeiros para os utilizadores finais. Os Estados-Membros devem, pois, poder estabelecer e/ou manter sistemas nacionais que permitam essas chamadas apenas para os utilizadores finais que não tenham levantado objeções.

(37) Os prestadores de serviços que disponibilizam serviços de comunicações eletrónicas devem informar os seus utilizadores finais das medidas que podem tomar para proteger a segurança das suas comunicações, tais como, o recurso a tipos específicos de *software* ou tecnologias de encriptação. O requisito de informar os utilizadores finais de riscos de segurança específicos não isenta os fornecedores de serviços da obrigação de, a expensas suas, adotarem medidas imediatas e necessárias para remediar quaisquer riscos de segurança novos e imprevistos e restabelecer o nível normal de segurança do serviço. A prestação de informações sobre os riscos de segurança para o assinante deve ser gratuita. A segurança é avaliada em função do disposto no artigo 32.º do Regulamento (UE) 2016/679.

(38) A fim de assegurar a plena conformidade com o Regulamento (UE) 2016/679, a execução das disposições do presente regulamento deve ser confiada às mesmas autoridades responsáveis pela execução das disposições do Regulamento (UE) 2016/679 e o presente regulamento recorre ao procedimento de controlo da coerência previsto naquele regulamento. Os Estados-Membros devem poder ter mais do que uma autoridade de controlo, de modo a refletir a sua estrutura constitucional, organizacional e administrativa. As autoridades de controlo devem também ser responsáveis pelo controlo da aplicação do presente regulamento no que se refere aos dados de comunicações eletrónicas relativos a pessoas coletivas. Essas funções adicionais não devem comprometer a capacidade da autoridade de controlo para desempenhar as funções respeitantes à proteção dos dados pessoais ao abrigo do Regulamento (UE) 2016/679 e do presente regulamento. Cada autoridade de controlo deve dispor dos recursos humanos e financeiros, instalações e infraestruturas suplementares necessários ao bom desempenho das funções previstas no presente regulamento.

(39) Cada autoridade de controlo deverá ser competente no território do seu Estado-Membro para exercer os poderes e para desempenhar as funções estabelecidas no presente regulamento. A fim de assegurar o controlo e a aplicação coerente do presente regulamento em toda a União, as autoridades de controlo devem ter as mesmas atribuições e poderes efetivos em cada Estado-Membro, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal ao abrigo do direito do Estado-Membro, para levar as infrações ao presente regulamento ao

conhecimento das autoridades judiciais e para intentar processos judiciais. Os Estados-Membros e as suas autoridades de controlo são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas na aplicação do presente regulamento.

(40) A fim de reforçar a aplicação das disposições do presente regulamento, cada autoridade de controlo deve dispor de poderes para impor sanções, incluindo coimas por qualquer infração ao presente regulamento, para além de, ou em vez de, quaisquer outras medidas adequadas nos termos do presente regulamento. O presente regulamento deverá definir as infrações e o montante máximo e o critério de fixação do valor das coimas daí decorrentes, que deverá ser determinado pela autoridade de controlo competente, em cada caso individual, tendo em conta todas as circunstâncias relevantes da situação específica, ponderando devidamente, em particular, a natureza, a gravidade e a duração da infração e das suas consequências e as medidas tomadas para garantir o cumprimento das obrigações constantes do presente regulamento e para prevenir ou atenuar as consequências da infração. Para efeitos da fixação de uma coima ao abrigo do presente regulamento, uma empresa deve ser entendida como uma empresa na aceção dos artigos 101.º e 102.º do Tratado.

(41) A fim de cumprir os objetivos do presente regulamento, nomeadamente proteger os direitos e liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais, e assegurar a livre circulação desses dados na União, o poder de adotar atos em conformidade com o artigo 290.º do Tratado sobre o Funcionamento da União Europeia deve ser delegado na Comissão para complementar o presente regulamento. Em especial, convém adotar atos delegados no que respeita à informação a apresentar, nomeadamente por meio de ícones normalizados, que ofereçam uma perspetiva geral inteligível e facilmente visível da recolha das informações emitidas pelo equipamento terminal, o seu objetivo, a pessoa responsável por ela e qualquer medida que o utilizador final dos equipamentos terminais pode tomar para minimizar a recolha de dados. São igualmente necessários atos delegados para especificar um código de identificação de chamadas de marketing direto, incluindo as efetuadas através de sistemas de chamada e de comunicação automatizados. É particularmente importante que a Comissão proceda a consultas adequadas e que essas consultas sejam realizadas em conformidade com os princípios estabelecidos no Acordo Interinstitucional «Legislar Melhor», de 13 de abril de 2016[8]. Em especial, a fim de assegurar a igualdade de participação na preparação de atos delegados, o Parlamento Europeu e o Conselho devem receber todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os seus peritos devem ter sistematicamente acesso às reuniões dos grupos de peritos da Comissão incumbidos da elaboração dos atos delegados. Além disso, para assegurar condições uniformes de execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão nos casos previstos no presente regulamento. Essas competências devem ser exercidas em conformidade com o Regulamento (UE) n.º 182/2011.

(42) Uma vez que o objetivo do presente regulamento, a saber, assegurar um nível equivalente de proteção das pessoas singulares e coletivas e a livre circulação de dados de comunicações eletrónicas na União, não pode ser suficientemente alcançado pelos Estados-Membros e pode, devido à dimensão ou aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode adotar medidas em conformidade com o

[8] Acordo Interinstitucional entre o Parlamento Europeu, o Conselho da União Europeia e a Comissão Europeia sobre legislar melhor, de 13 de abril de 2016 (JO L 123 de 12.5.2016, p. 1-14).

princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para atingir aquele objetivo.

(43) A Diretiva 2002/58/CE deverá ser revogada.

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto

1. O presente regulamento estabelece as normas respeitantes à proteção dos direitos e liberdades fundamentais das pessoas singulares e coletivas aquando da prestação e utilização de serviços de comunicações eletrónicas, e, nomeadamente, os direitos ao respeito pela vida privada e pelas comunicações e à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

2. O presente regulamento assegura a livre circulação de dados de comunicações eletrónicas e de serviços de comunicações eletrónicas na União, que não deve ser restringida nem proibida por motivos relacionados com o respeito pela vida privada e pelas comunicações de pessoas singulares e coletivas e com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

3. As disposições do presente Regulamento precisam e completam o Regulamento (UE) n.º 2016/679, estabelecendo normass específicas para os fins mencionados nos n.^{os} 1 e 2.

Artigo 2.º
Âmbito de aplicação material

1. O presente regulamento aplica-se ao tratamento de dados de comunicações eletrónicas efetuado no contexto da prestação e da utilização de serviços de comunicações eletrónicas e às informações relativas ao equipamento terminal dos utilizadores finais.

2. O presente regulamento não se aplica a:

a) Atividades não abrangidas pelo âmbito de aplicação do direito da União;

b) Atividades dos Estados-Membros abrangidas pelo âmbito de aplicação do título V, do capítulo 2, do Tratado da União Europeia;

c) Serviços de comunicações eletrónicas não acessíveis ao público;

d) Atividades das autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a a proteção contra ameaças à segurança pública e a prevenção de tais ameaças;

e) Instituições, órgãos, organismos e agências da União.

3. O tratamento de dados de comunicações eletrónicas pelas instituições, órgãos, organismos e agências da União é regido pelo Regulamento (UE) 00/0000 [novo regulamento que substitui o Regulamento n.º 45/2001]

4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE[9], nomeadamente as regras em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos artigos 12.º a 15.º dessa diretiva.

5. O presente regulamento não prejudica as disposições da Diretiva 2014/53/UE.

Artigo 3.º
Âmbito de aplicação territorial e representante

1. O presente regulamento aplica-se:

a) À prestação de serviços de comunicações eletrónicas a utilizadores finais na União, independentemente da exigência de o utilizador final proceder a um pagamento;

b) À utilização desses serviços;

c) À proteção das informações relativas ao equipamento terminal dos utilizadores finais localizados na União.

2. Sempre que o prestador de um serviço de comunicações eletrónicas não estiver estabelecido na União deve designar, por escrito, um representante na União.

3. O representante deve estar estabelecido num dos Estados-Membros onde estão localizados os utilizadores finais desses serviços de comunicações eletrónicas.

4. O representante deve estar habilitado a responder às perguntas e facultar informações complementares ou em substituição do fornecedor que representa, nomeadamente às autoridades de controlo e aos utilizadores finais, sobre todas as questões relativas ao tratamento de dados de comunicações eletrónicas para efeitos de garantir a conformidade com o presente regulamento.

5. A designação de um representante nos termos do n.º 2 não prejudica as ações judiciais que podem vir a ser intentadas contra a pessoa singular ou coletiva que trata os dados das comunicações eletrónicas no contexto da prestação de serviços de comunicações eletrónicas de fora da União a utilizadores finais na União.

Artigo 4.º
Definições

1. Para efeitos do presente regulamento, aplicam-se as seguintes definições:

a) As definições constantes do Regulamento (UE) 2016/679;

b) As definições de «rede de comunicações eletrónicas», «serviço de comunicações eletrónicas», «serviço de comunicações interpessoais», «serviço de comunicações interpessoais com base no número», «serviço de comunicações interpessoais independentes do número», «utilizador final» e «chamada» que constam do artigo 2.º, pontos 1, 4, 5, 6, 7, 14 e 21, respetivamente, da [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas];

c) A definição de «equipamento terminal» que consta do artigo 1.º, n.º 1, da Diretiva 2008/63/CE da Comissão[10].

[9] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1-16).

2. Para efeitos do n.º 1, alínea b), a definição de «serviço de comunicações interpessoais» inclui os serviços de comunicação interpessoal e interativa que funcionam de modo acessório e que estejam intrinsecamente ligados a outro serviço.

3. Além disso, para efeitos do presente regulamento, entende-se por:

a) «Dados de comunicações eletrónicas», o conteúdo das comunicações eletrónicas e os metadados das comunicações eletrónicas;

b) «Conteúdo das comunicações eletrónicas», o conteúdo trocado através de serviços de comunicações eletrónicas, sob a forma de texto, voz, vídeos, imagens e som;

c) «Metadados das comunicações eletrónicas», os dados tratados numa rede de comunicações eletrónicas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas, incluindo os dados utilizados para detetar uma comunicação e identificar a sua fonte e destino, a localização do dispositivo no contexto da comunicação e a data, hora, duração e tipo de comunicação;

d) «Listas acessíveis ao público», as listas de utilizadores finais de serviços de comunicações eletrónicas, sob forma impressa ou eletrónica, publicadas ou colocadas à disposição do público ou de uma parte do público, incluindo por meio de um serviço de informações sobre listas;

e) «Correio eletrónico», qualquer mensagem eletrónica que contenha informações sob a forma de texto, voz, vídeo, som ou imagem, enviada através de uma rede de comunicações eletrónicas, que possa ser armazenada na rede ou em centros de computação conexos, ou no equipamento terminal do seu destinatário;

f) «Comunicações comerciais diretas» qualquer forma de publicidade, oral ou escrita, enviada a um ou mais utilizadores finais identificados ou identificáveis de serviços de comunicações eletrónicas, incluindo a utilização de sistemas de chamada e de comunicação automatizados, com ou sem interação humana, de correio eletrónico, SMS, etc.;

g) «Chamadas de televendas», chamadas em direto que não implicam a utilização de sistemas de chamada e de comunicação automatizados;

h) «Sistemas de chamada e de comunicação automatizados», sistemas que podem iniciar automaticamente chamadas para um ou mais destinatários, em conformidade com as instruções estabelecidas, e de transmitir sons que não emitidos em direto, incluindo chamadas efetuadas com recurso a sistemas de chamada e de comunicação automatizados que ligam a pessoa chamada a outra pessoa.

---

[10] Diretiva 2008/63/CE da Comissão, de 20 de junho de 2008, relativa à concorrência nos mercados de equipamentos terminais de telecomunicações (JO L 162 de 21.6.2008, p. 20-26).

CAPÍTULO II
PROTEÇÃO DAS COMUNICAÇÕES ELETRÓNICAS DE PESSOAS SINGULARES E COLETIVAS E DAS INFORMAÇÕES ARMAZENADAS NOS SEUS EQUIPAMENTOS TERMINAIS

Artigo 5.º
Confidencialidade dos dados de comunicações eletrónicas

Os dados das comunicações eletrónicas devem ser confidenciais. Salvo quando permitido pelo presente regulamento, é proibida qualquer interferência com os dados das comunicações eletrónicas, por escuta, instalação de dispositivos de escuta, armazenamento, controlo, digitalização ou outras formas de interceção, vigilância ou tratamento de dados de comunicações eletrónicas, por outras pessoas que não os utilizadores finais.

Artigo 6.º
Tratamento permitido de dados de comunicações eletrónicas

1. Os fornecedores de redes e de serviços de comunicações eletrónicas podem tratar dados de comunicações eletrónicas:

a) Se tal for necessário para assegurar a transmissão da comunicação, durante o período necessário para esse efeito; ou

b) Se tal for necessário para manter ou restabelecer a segurança das redes e serviços de comunicações eletrónicas, ou detetar falhas técnicas e/ou erros na transmissão das comunicações eletrónicas, durante o período necessário para esse efeito.

2. Os prestadores de serviços de comunicações eletrónicas podem tratar metadados de comunicações eletrónicas:

a) Se tal for necessário para cumprir as obrigações em matéria de qualidade do serviço previstas na [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas] ou no Regulamento (UE) 2015/2120[11] durante o período necessário para esse efeito; ou

b) Se tal for necessário para proceder à faturação, calcular o pagamento das interligações, detetar ou impedir a utilização abusiva ou fraudulenta de serviços de comunicações eletrónicas ou a subscrição desses serviços; ou

c) Se o utilizador final em causa tiver consentido o tratamento dos metadados das suas comunicações para uma ou várias finalidades específicas, incluindo a prestação de serviços específicos a esses utilizadores finais, desde que a finalidade ou finalidades em causa não possam ser atingidas através do tratamento de informações tornadas anónimas.

[11] Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que estabelece medidas respeitantes ao acesso à Internet aberta e que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (UE) n.º 531/2012 relativo à itinerância nas redes de comunicações móveis públicas da União (JO L 310 de 26.11.2015, p. 1-18).

3. Os prestadores de serviços de comunicações eletrónicas podem tratar o conteúdo das comunicações eletrónicas:

a) Exclusivamente para efeitos da prestação de um serviço específico a um utilizador final, se o utilizador final ou utilizadores finais em causa tiverem dado o seu consentimento para o tratamento do conteúdo das suas comunicações eletrónicas e a prestação desse serviço não puder ser efetuada sem o tratamento desse conteúdo; ou

b) Se todos os utilizadores finais em causa tiverem dado o seu consentimento para o tratamento do conteúdo das suas comunicações eletrónicas para uma ou mais finalidades específicas que não possam ser atingidas através do tratamento de informações tornadas anónimas e o fornecedor tiver consultado a autoridade de controlo. O disposto no artigo 36.º, n.os 2 e 3, do Regulamento (UE) 2016/679 aplica-se à consulta da autoridade de controlo.

Artigo 7.º
Armazenagem e apagamento dos dados de comunicações eletrónicas

1. Sem prejuízo do disposto no artigo 6.º, n.º 1, alínea b), e no artigo 6.º, n.º 3, alíneas a) e b), o prestador do serviço de comunicações eletrónicas deve apagar o conteúdo das comunicações eletrónicas ou tornar esses dados anónimos após a receção do conteúdo das comunicações eletrónicas pelo destinatário ou destinatários. Esses dados podem ser registados ou armazenados pelo utilizador final ou por terceiros por ele designados para registar, armazenar ou de outra forma tratar esses dados, em conformidade com o Regulamento (UE) 2016/679.

2. Sem prejuízo do disposto no artigo 6.º, n.º 1, alínea b), e no artigo 6.º, n.º 3, alíneas a) e b), o prestador do serviço de comunicações eletrónicas deve apagar os metadados das comunicações eletrónicas ou tornar esses dados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.

3. Quando o tratamento dos metadados das comunicações eletrónicas ocorrer para efeitos de faturação, em conformidade com o artigo 6.º, n.º 2, alínea b), os metadados em causa podem ser conservados até ao final do período durante o qual uma fatura pode ser contestada judicialmente ou exigido o seu pagamento em conformidade com o direito nacional.

Artigo 8.º
Proteção das informações armazenadas nos equipamentos terminais dos utilizadores finais e relacionadas com esses equipamentos

1. A utilização das capacidades de tratamento e de armazenamento dos equipamentos terminais e a recolha de informações provenientes dos equipamentos terminais dos utilizadores finais, incluindo sobre o seu *software* e *hardware*, que não sejam efetuadas pelo utilizador final em causa são proibidas, exceto pelos seguintes motivos:

a) Se forem necessárias exclusivamente para assegurar a transmissão de uma comunicação eletrónica através de uma rede de comunicações eletrónicas; ou

b) Se o utilizador final tiver dado o seu consentimento; ou

c) Se forem necessárias para prestar um serviço da sociedade de informação solicitado pelo utilizador final; ou

d) Se forem necessárias para uma medição de audiência da web, desde que tal medição seja efetuada pelo prestador do serviço da sociedade de informação solicitado pelo utilizador final.

2. A recolha de informações emitidas pelos equipamentos terminais para permitir a sua ligação a outro dispositivo e/ou equipamento de rede é proibida, exceto se:

a) For exclusivamente efetuada para estabelecer uma ligação e durante o tempo necessário para o efeito; ou

b) For afixado um aviso claro e visível contendo, no mínimo, informações sobre as modalidades da recolha, o seu objetivo, a pessoa responsável e as outras informações exigidas ao abrigo do artigo 13.º do Regulamento (UE) 2016/679, quando forem recolhidos dados de caráter pessoal, bem como qualquer medida que o utilizador final dos equipamentos terminais pode tomar para reduzir ao mínimo ou fazer cessar a recolha.

c) A recolha dessas informações deve ser subordinada à aplicação de medidas técnicas e organizativas adequadas para garantir um nível de segurança adequado aos riscos, tal como estabelecido no artigo 32.º do Regulamento (UE) 2016/679.

3. As informações a fornecer nos termos do n.º 2, alínea b), podem ser associadas a ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível uma útil perspetiva geral da recolha.

4. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 27.º que determinem as informações a fornecer por meio dos ícones normalizados e os procedimentos aplicáveis ao fornecimento de ícones normalizados.

Artigo 9.º
Consentimento

1. São aplicáveis a definição e as condições do consentimento previstas no artigo 4.º, n.º 11, e no artigo 7.º do Regulamento (UE) 2016/679/UE.

2. Sem prejuízo do disposto no n.º 1, sempre que for tecnicamente possível e exequível, para efeitos do artigo 8.º, n.º 1, alínea b), o consentimento pode ser expresso utilizando as definições técnicas adequadas de uma aplicação de *software* que permita o acesso à Internet.

3. Os utilizadores finais que tenham consentido o tratamento de dados de comunicações eletrónicas, tal como estabelecido no artigo 6.º, n.º 2, alínea c), e no artigo 6.º, n.º 3, alíneas a) e b), devem ter a possibilidade de retirar o seu consentimento em qualquer momento, tal como estabelecido no artigo 7.º, n.º 3, do Regulamento (UE) 2016/679, e serem recordados desta possibilidade a intervalos regulares de 6 meses, enquanto o tratamento continuar.

Artigo 10.º
Informações e opções de predefinições de privacidade a fornecer

1. O *software* colocado no mercado que permite efetuar comunicações eletrónicas, incluindo a recuperação e a apresentação de informações da Internet, deve oferecer a possibilidade de impedir que terceiros armazenem informações no equipamento terminal de um utilizador final ou tratem as informações já armazenadas nesse equipamento.

2. Aquando da instalação, o *software* deve informar o utilizador final acerca das opções relativas às predefinições de privacidade e, para prosseguir a instalação, exigir que o utilizador final dê o seu consentimento relativamente a uma predefinição.

3. No caso de *software* instalado até 25 de maio de 2018, os requisitos previstos nos n.os 1 e 2 devem ser respeitados no momento da primeira atualização do *software*, o mais tardar até 25 de agosto de 2018.

Artigo 11.º
Restrições

1. O direito da União ou o direito dos Estados-Membros podem restringir, através de medidas legislativas, o âmbito das obrigações e dos direitos previstos nos artigos 5.º a 8.º, sempre que tal restrição respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária, adequada e proporcionada, numa sociedade democrática, para salvaguardar um ou mais dos interesses públicos gerais a que se refere o artigo 23.º, n.º 1, alíneas a) a e), do Regulamento (UE) 2016/679 ou uma função de controlo, de inspeção ou de regulamentação associada ao exercício da autoridade pública relativamente a esses interesses.

2. Os prestadores de serviços de comunicações eletrónicas devem estabelecer procedimentos internos para responder aos pedidos de acesso aos dados de comunicações eletrónicas dos utilizadores finais com base numa medida legislativa adotada nos termos do n.º 1. Devem fornecer à autoridade de controlo competente, a pedido desta, informações sobre esses procedimentos, o número de pedidos recebidos, a justificação jurídica invocada e a resposta dada.

CAPITULO III
DIREITOS DAS PESSOAS SINGULARES E COLETIVAS NO QUE RESPEITA AO CONTROLO DAS COMUNICAÇÕES ELETRÓNICAS

Artigo 12.º
Apresentação e restrição da identificação da linha chamadora e da linha conectada

1. Quando é proposta a apresentação da identificação da linha chamadora e da linha conectada, em conformidade com o artigo [107.º] da [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas], os prestadores de serviços de comunicações interpessoais com base no número acessíveis ao público devem oferecer:

a) Ao utilizador final que efetua a chamada, a possibilidade de impedir a apresentação da identificação da linha chamadora por chamada, por ligação, ou numa base permanente;

b) Ao utilizador final destinatário da chamada, a possibilidade de impedir a apresentação da identificação da linha chamadora das chamadas de entrada;

c) Ao utilizador final destinatário da chamada, a possibilidade de rejeitar chamadas de entrada quando o utilizador final que efetua a chamada tiver impedido a apresentação da identificação da linha chamadora;

d) Ao utilizador final destinatário da chamada, a possibilidade de impedir a apresentação da identificação da linha conectada ao utilizador final que efetua a chamada.

2. Os utilizadores finais devem poder beneficiar das possibilidades referidas no n.º 1, alíneas a), b), c) e d), por meios simples e gratuitos.

3. O n.º 1, alínea a), aplica-se igualmente a chamadas para países terceiros com origem na União. O n.º 1, alíneas b), c) e d) aplica-se igualmente a chamadas de entrada com origem em países terceiros.

4. Sempre que for proposta a apresentação da identificação da linha chamadora e da linha conectada, os prestadores de serviços de comunicações interpessoais com base no número acessíveis ao público devem fornecer informações ao público sobre as opções descritas no n.º 1, alíneas a), b), c) e d).

Artigo 13.º
Exceções relativas à apresentação e à restrição da identificação da linha chamadora e da linha conectada

1. Sempre que for efetuada uma chamada para serviços de emergência, mesmo se o utilizador final que efetua a chamada tiver impedido a apresentação da identificação da linha chamadora, os prestadores de serviços de comunicações interpessoais com base no número acessíveis ao público devem ignorar a eliminação da apresentação da identificação da linha chamadora e a recusa ou a ausência de consentimento do utilizador final quanto ao tratamento dos metadados, por linha, nas chamadas para as organizações que lidam com as comunicações de emergência, incluindo os pontos de atendimento da segurança pública, para efeitos de resposta a essas comunicações.

2. Os Estados-Membros devem estabelecer disposições mais específicas no que diz respeito ao estabelecimento de procedimentos e às circunstâncias em que os prestadores de serviços de comunicações interpessoais com base no número acessíveis ao público devem ignorar temporariamente a eliminação da apresentação da identificação da linha chamadora, sempre que os utilizadores finais solicitarem identificação da origem de chamadas mal intencionadas ou incomodativas.

Artigo 14.º
Bloqueio das chamadas de entrada

Os prestadores de serviços de comunicações interpessoais com base no número acessíveis ao público devem utilizar as técnicas mais avançadas para limitar a receção de chamadas indesejadas pelos utilizadores finais e fornecer também, gratuitamente, ao utilizador final destinatário as seguintes possibilidades:

a) Bloquear chamadas de entrada de números específicos ou de fontes anónimas;

b) Impedir o reencaminhamento automático de chamadas por terceiros para o equipamento terminal do utilizador final.

Artigo 15.º
Listas acessíveis ao público

1. Os fornecedores de listas acessíveis ao público devem obter o consentimento dos utilizadores finais que sejam pessoas singulares para incluir os seus dados pessoais

nas listas e, por conseguinte, devem obter o consentimento destes utilizadores finais para a inclusão de dados por categoria de dados pessoais, na medida em que tais dados sejam pertinentes para a finalidade das listas, tal como determinado pelo fornecedor das listas. Os fornecedores devem dar aos utilizadores finais que sejam pessoas singulares meios para verificar, corrigir e suprimir esses dados.

2. Os fornecedores de listas acessíveis ao público devem informar os utilizadores finais que sejam pessoas singulares e cujos dados pessoais constem da lista acerca das funções de pesquisa de que esta dispõe e obter o consentimento dos utilizadores finais antes de ativarem essas funções de pesquisa em relação aos seus dados pessoais.

3. Os fornecedores de listas acessíveis ao público devem fornecer aos utilizadores finais que sejam pessoas coletivas a possibilidade de se oporem à inclusão dos seus dados na lista. Os fornecedores devem facultarr a esses utilizadores finais que sejam pessoas coletivas os meios para verificar, corrigir e suprimir esses dados.

4. A possibilidade de os utilizadores finais não serem incluídos na lista acessível ao público, ou de verificarem, corrigirem ou suprimirem quaisquer dados que lhes digam respeito deve ser proposta gratuitamente.

Artigo 16.º
Comunicações não solicitadas

1. As pessoas singulares ou coletivas podem utilizar os serviços de comunicações eletrónicas para o envio de comunicações comerciais diretas a utilizadores finais que sejam pessoas singulares que tenham dado o seu consentimento.

2. Se uma pessoa singular ou coletiva obtiver do seu cliente coordenadas eletrónicas de contacto para correio eletrónico, no contexto da venda de um produto ou serviço, em conformidade com o Regulamento (UE) 2016/679, essa pessoa singular ou coletiva pode usar essas coordenadas eletrónicas de contacto para fins de marketing direto dos seus próprios produtos ou serviços análogos, desde que aos clientes tenha sido dada clara e distintamente a possibilidade de se oporem, de forma gratuita e fácil, a essa utilização. O direito de oposição deve ser oferecido na data da recolha e sempre que uma mensagem é enviada.

3. Sem prejuízo dos n.^{os} 1 e 2, as pessoas singulares ou coletivas que utilizam serviços de comunicações eletrónicas para efetuarem chamadas de marketing direto devem:

a) Apresentar a identificação de uma linha na qual podem ser contactados; ou

b) Apresentar um código ou prefixo de identificação específico que indique que se trata de uma chamada comercial.

4. Não obstante o n.º 1, os Estados-Membros podem prever, através de medidas legislativas, que a realização de chamadas vocais de marketing direto para utilizadores finais que sejam pessoas singulares só possa ser permitida em relação aos utilizadores finais que sejam pessoas singulares que não tenham manifestado a sua objeção a receber essas comunicações.

5. Os Estados-Membros devem assegurar, no âmbito do direito da União e do direito nacional aplicável, que os interesses legítimos dos utilizadores finais que são pessoas coletivas são suficientemente protegidos em relação a comunicações não solicitadas enviadas pelos meios indicados no n.º 1.

6. Qualquer pessoa singular ou coletiva que utiliza serviços de comunicações eletrónicas para transmitir comunicações de marketing direta deve informar os utilizadores finais acerca da natureza comercial da comunicação e da identidade da pessoa coletiva ou singular por conta da qual a comunicação é transmitida, facultando aos destinatários as informações necessárias para que estes possam exercer o seu direito de retirar, de forma fácil, o seu consentimento em relação à receção de novas comunicações comerciais.

7. A Comissão fica habilitada a adotar medidas de execução nos termos do artigo 26.º, n.º 2, que especifiquem o código ouprefixo para identificar as chamadas comerciais, nos termos do n.º 3, alínea b).

Artigo 17.º
Informações sobre os riscos de segurança detetados

No caso de um risco específico que possa comprometer a segurança de redes e serviços de comunicações eletrónicas, o prestador de um serviço de comunicações eletrónicas deve informar os utilizadores finais desse risco e, sempre que as medidas que o prestador do serviço pode tomar não permitam evitar esse risco, das soluções possíveis, incluindo uma indicação dos custos prováveis daí decorrentes.

CAPÍTULO IV
AUTORIDADES DE CONTROLO INDEPENDENTES E EXECUÇÃO

Artigo 18.º
Autoridades de controlo independentes

1. A autoridade ou autoridades de controlo independentes responsáveis pelo controlo da aplicação do Regulamento (UE) 2016/679 devem também ser responsáveis pelo controlo da aplicação do presente regulamento. Os capítulos VI e VII do Regulamento (UE) 2016/679 são aplicáveis *mutatis mutandis*. As atribuições e competências das autoridades de controlo são exercidas no que diz respeito aos utilizadores finais.

2. A autoridade ou autoridades de controlo referidas no n.º 1 devem cooperar, sempre que adequado, com as autoridades reguladoras nacionais nos termos da [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas].

Artigo 19.º
Comité Europeu para a Proteção de Dados

O Comité Europeu para a Proteção de Dados, criado pelo artigo 68.º do Regulamento (UE) 2016/679, tem competência para assegurar a aplicação coerente do capítulo II do presente regulamento. Para o efeito, o Comité Europeu para a Proteção de Dados exerce as funções previstas no artigo 70.º do Regulamento (UE) n.º 2016/679. O Comité tem igualmente as seguintes atribuições:

a) Aconselhar a Comissão sobre qualquer proposta de alteração do presente regulamento;

b) Analisar, por iniciativa própria, a pedido de um dos seus membros, ou a pedido da Comissão, qualquer questão relativa à aplicação do presente regulamento e emitir diretrizes, recomendações e melhores práticas, a fim de incentivar a aplicação coerente do presente regulamento.

Artigo 20.º
Procedimentos de cooperação e de coerência

Cada autoridade de controlo deve contribuir para a aplicação coerente do presente regulamento em toda a União. Para o efeito, as autoridades de controlo devem cooperar entre si e com a Comissão, em conformidade com o capítulo VII do Regulamento (UE) 2016/679, relativamente às questões abrangidas pelo capítulo II do presente regulamento.

CAPÍTULO V
VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES

Artigo 21.º
Vias de recurso

1. Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os utilizadores finais de serviços de comunicações eletrónicas dispõem das mesmas vias de recurso previstas nos artigos 77.º, 78.º e 79.º do Regulamento (UE) 2016/679.

2. Qualquer pessoa singular ou coletiva, que não seja utilizador final, afetada negativamente por infrações ao presente regulamento e que tenha um interesse legítimo na cessação ou proibição das alegadas infrações, incluindo um prestador de serviços de comunicações eletrónicas que proteja os seus interesses comerciais legítimos, tem o direito de intentar ações judiciais relativamente a essas infrações.

Artigo 22.º
Direito de indemnização e responsabilidade

Qualquer utilizador final de serviços de comunicações eletrónicas que tenha sofrido danos materiais ou morais na sequência de uma infração ao presente regulamento tem o direito de receber uma indemnização do infrator pelos danos sofridos, exceto se o infrator provar que não é, de modo algum, responsável pelo evento que deu origem aos danos, em conformidade com o artigo 82.º do Regulamento (UE) 2016/679.

Artigo 23.º
Condições gerais para a aplicação de coimas

1. Para efeitos do presente artigo, o capítulo VII do Regulamento (UE) 2016/679 aplica-se às infrações ao presente regulamento.

2. As infrações às disposições do presente regulamento a seguir enumeradas estão sujeitas, em conformidade com o n.º 1, a coimas até 10 000 000 EUR ou, no caso de uma empresa, até 2 % do seu volume de negócios anual, a nível mundial, no exercício financeiro anterior, consoante o montante que for mais elevado:

a) As obrigações de qualquer pessoa singular ou coletiva que trate dados de comunicações eletrónicas nos termos do artigo 8.º;

b) As obrigações do fornecedor de *software* que permita comunicações eletrónicas, nos termos do artigo 10.º;

c) As obrigações dos prestadores de serviços de listas acessíveis ao público nos termos do artigo 15.º;

d) As obrigações de qualquer pessoa singular ou coletiva que utilize serviços de comunicações eletrónicas nos termos do artigo 16.º.

3. As infrações ao princípio da confidencialidade das comunicações, ao tratamento permitido de dados de comunicações eletrónicas e aos prazos para apagamento nos termos dos artigos 5.º, 6.º e 7.º estão sujeitas, em conformidade com o n.º 1, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual, a nível mundial, no exercício financeiro anterior, consoante o montante que for mais elevado.

4. Os Estados-Membros determinam o regime de sanções aplicáveis às infrações ao disposto nos artigos 12.º, 13.º, 14.º e 17.º.

5. O incumprimento de uma ordem emitida pela autoridade de controlo a que se refere o artigo 18.º está sujeito a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual, a nível mundial, no exercício financeiro anterior, consoante o montante que for mais elevado.

6. Sem prejuízo dos poderes de correção das autoridades de controlo em conformidade com o artigo 18.º, cada Estado-Membro pode prever normas que permitam determinar se e em que medida podem ser aplicadas coimas às autoridades e organismos públicos estabelecidos no seu território.

7. O exercício das competências que lhe são atribuídas pelo presente artigo por parte da autoridade de controlo fica sujeito às garantias processuais adequadas nos termos do direito da União e dos Estados-Membros, incluindo o direito à ação judicial e a um processo equitativo.

8. Quando o sistema jurídico dos Estados-Membros não preveja coimas, pode aplicar-se o presente artigo de modo a que a coima seja proposta pela autoridade de controlo competente e imposta pelos tribunais nacionais competentes, garantindo ao mesmo tempo que estas medidas jurídicas corretivas são eficazes e têm um efeito equivalente às coimas impostas pelas autoridades de controlo. Em todo o caso, as coimas impostas devem ser efetivas, proporcionadas e dissuasivas. Os referidos Estados-Membros notificam a Comissão das disposições de direito interno que adotarem nos termos do presente número até [xxx] e, sem demora, de qualquer alteração subsequente das mesmas.

Artigo 24.º
Sanções

1. Os Estados-Membros estabelecem as regras relativas às outras sanções aplicáveis em caso de infração ao presente regulamento, nomeadamente infrações que não são sujeitas a coimas nos termos do artigo 23.º, e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

2. Os Estados-Membros devem notificar a Comissão das disposições do direito nacional que adotarem nos termos do n.º 1, o mais tardar 18 meses após a data prevista no artigo 29.º, n.º 2, e, sem demora, qualquer alteração subsequente das mesmas.

CAPÍTULO VI
ATOS DELEGADOS E ATOS DE EXECUÇÃO

Artigo 25.º
Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 8.º, n.º 4, é conferido à Comissão por um período indeterminado, a partir de [data de entrada em vigor do presente regulamento].

3. A delegação de poderes referida no artigo 8.º, n.º 4, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no Jornal Oficial da União Europeia ou de uma data posterior nela especificada. Não afeta a validade dos atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão deve consultar os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional «Legislar Melhor», de 13 de abril de 2016.

5. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados nos termos do artigo 8.º, n.º 4, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação desse ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. Esse prazo pode ser prorrogado por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 26.º
Comité

1. A Comissão é assistida pelo Comité das Comunicações criado pelo artigo 110.º da [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas]. O referido comité é um comité na aceção do Regulamento (UE) n.º 182/2011[12].

2. Sempre que se faça referência ao presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

[12] Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13-18).

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Artigo 27.º
Revogação

1. A Diretiva 2002/58/CE é revogada com efeitos a partir de 25 de maio de 2018.
2. As referências à diretiva revogada entendem-se como referências ao presente regulamento.

Artigo 28.º
Cláusula de acompanhamento e avaliação

Até 1 de janeiro de 2018, o mais tardar, a Comissão deve estabelecer um programa pormenorizado para o controlar a eficácia do presente regulamento.

O mais tardar três anos a contar da data de início da aplicação do presente regulamento e, posteriormente, de três em três anos, a Comissão deve proceder a uma avaliação do presente regulamento e apresentar as principais conclusões ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu. A avaliação servirá de base, se adequado, a uma proposta de alteração ou de revogação do presente regulamento à luz da evolução da situação jurídica, técnica ou económica.

Artigo 29.º
Entrada em vigor e aplicação

1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.
2. É aplicável a partir de 25 de maio de 2018.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*