



5.10.2017

PARECER

da Comissão dos Assuntos Jurídicos

dirigido à Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

sobre a 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)
(COM(2017)0010 – C8-0009/2017 – 2017/0003(COD))

Relator de parecer: Pavel Svoboda

PA_Legam

JUSTIFICAÇÃO SUCINTA

O relator **não** acolhe com satisfação a proposta relativa ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas (a seguir designado «Regulamento Privacidade e Comunicações Eletrónicas»).

A proposta não contribuirá para a realização dos objetivos da criação de um mercado único digital (crescimento, promoção da inovação, incentivo a uma economia europeia de dados, livre circulação de dados e apoio às PME), podendo até ter um efeito totalmente oposto ao pretendido. Muitos dos atuais modelos de negócio deixariam de ser viáveis.

A proposta suscita forte incoerência jurídica em relação ao Regulamento (UE) 2016/679 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 (a seguir designada RGPD) e em relação à proposta relativa ao Código Europeu das Comunicações Eletrónicas (a seguir designado CECE), bem como extrema incerteza jurídica no que respeita ao tratamento de dados e incoerências no tratamento de dados de caráter pessoal.

A falta de coragem e de criatividade, bem como a recusa em abandonar estruturas e convicções antigas, não são condições ideais para a construção de um futuro digital bem-sucedido.

A proposta deveria:

- 1) incidir principalmente na confidencialidade das comunicações;
- 2) estabelecer condições de concorrência equitativas a) no setor da comunicação e b) adaptar-se ao contexto global;
- 3) ser um complemento do RGPD e não uma *lex specialis* do mesmo;
- 4) evitar a duplicação de estruturas com o RGPD (por exemplo, o consentimento, a transferência de dados pessoais para países terceiros, sanções, CEPD, etc.). Os dados pessoais devem ser abrangidos apenas por um regime jurídico. Os dados de comunicações considerados dados pessoais não devem ser, de modo algum, objeto de tratamento em separado. Os dados idênticos devem estar sujeitos às mesmas disposições e aos mesmos princípios. O artigo 6.º do RGPD deve ser aplicável da mesma forma;
- 5) ser orientada para o futuro e estar em conformidade com o CECE.
- 6) abster-se de atribuir uma importância excessiva ao consentimento, uma vez que este já não é o instrumento ideal. Seria preferível recorrer à transparência, à soberania de dados, a soluções de exclusão, à possibilidade de se opor ao tratamento de dados, à criação de uma nova categoria de dados (por exemplo, dados sob pseudónimo) ou, pelo menos, à melhoria da diferenciação entre dados anonimizados, pseudonimizados e codificados. Além disso, o equilíbrio entre a proteção da vida privada e as novas tecnologias que se alcançou graças ao RGPD poderá ficar novamente comprometido dado que, em muitos domínios, os tratamentos de dados ainda autorizados pelo RGPD seriam sujeitos a uma forma ainda mais estrita de autorização ou, até mesmo, proibidos. Tal é absolutamente contraproducente.

É de louvar o facto de:

- o Regulamento Privacidade e Comunicações Eletrónicas estar adaptado à realidade técnica e aos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da UE;

- a Comissão ter integrado os serviços de comunicações suplementares através da Internet no âmbito de aplicação;
- a Comissão pretender sincronizar a data de entrada em vigor com a do RGPD. Na verdade, será impossível atingir esse objetivo, nomeadamente se se mantiverem as complexas estruturas duplas.

Mais concretamente:

- O artigo 4.º, em particular, tem por base o CECE. Por conseguinte, o Regulamento Privacidade e Comunicações Eletrónicas não pode ser aplicado antes da adoção do CECE. Trata-se de um erro sistémico que deve ser corrigido.
- A proposta não estabelece uma distinção nítida entre conteúdos, dados e informações.
- A fronteira entre o Regulamento Privacidade e Comunicações Eletrónicas e o RGPD não é clara. Por motivos de segurança jurídica, é conveniente clarificar quando é que se aplica um regulamento e quando é que se aplica o outro, a fim de criar um regime jurídico perceptível para os responsáveis. Por conseguinte, é conveniente limitar a aplicação do Regulamento Privacidade e Comunicações Eletrónicas aos dados de carácter pessoal no contexto da comunicação, como previsto na Diretiva 2002/58/CE. Em todos os restantes casos, aplicar-se-á então o RGPD. Como tal, é necessária uma clarificação de ordem jurídica quanto ao que se considera «fim de uma comunicação».
- É conveniente estabelecer uma distinção clara entre a confidencialidade do conteúdo das comunicações e o tratamento dos dados (proteção de dados), uma vez que o âmbito de aplicação do Regulamento Privacidade e Comunicações Eletrónicas inclui as máquinas e os dispositivos conectados. A proposta revela falta de clareza no que respeita às definições e ao âmbito de aplicação. Tal gera incertezas imprevisíveis e sem qualquer lógica quanto às repercussões para as comunicações máquina-máquina (por exemplo, no setor automóvel, no setor da logística ou das casas inteligentes). A fronteira entre a transmissão de comunicações no âmbito do Regulamento Privacidade e Comunicações Eletrónicas e a transmissão de dados nos termos do RGPD não é clara. Além disso, a relação entre o consentimento e as comunicações máquina-máquina também não é clara.
- A proposta condiciona o tratamento de dados, inclusivamente de dados anónimos, ao consentimento, o que é ilógico e completamente impossível de um ponto de vista técnico. Neste contexto, teria sido possível desenvolver o conceito de «pseudonimização» referido no RGPD.
- Igualmente difícil de compreender é a razão pela qual os metadados (Regulamento Privacidade e Comunicações Eletrónicas) devem ser mais bem protegidos do que os dados relativos à saúde (RGPD).
- Igualmente incompreensível é a entrada em vigor de dois sistemas de sanções na mesma data.
- É conveniente analisar a eventual necessidade de uma exceção no quadro das atividades domésticas.
- A regulamentação proposta relativamente aos testemunhos de conexão favorece as grandes empresas em detrimento das PME (europeias). O mais adequado seria exatamente o oposto.

- A formulação do artigo 5.º da proposta poderia comprometer o futuro do correio eletrónico.

Existe margem para melhorias em muitos aspetos. Por conseguinte, a Comissão dos Assuntos Jurídicos insta a Comissão das Liberdades Cívicas a ter em conta as alterações que se seguem.

ALTERAÇÕES

A Comissão dos Assuntos Jurídicos insta a Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos, competente quanto à matéria de fundo, a ter em conta as seguintes alterações:

Alteração 1

Proposta de regulamento Considerando 1

Proposta da Comissão

(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.

Alteração

(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 ***dessas comunicações***, nomeadamente ***as informações relativas a*** quando a informação foi enviada, a partir de onde e a quem, não sejam revelados a uma pessoa distinta das partes ***nessa*** comunicação. O princípio da confidencialidade deve ser aplicável às formas de comunicação atuais e futuras, incluindo chamadas, acesso à Internet, mensagens instantâneas, ***mensagens em plataformas trocadas entre utilizadores de uma rede social***, correio eletrónico, chamadas telefónicas pela Internet e mensagens pessoais nas redes sociais.

Alteração 2

Proposta de regulamento Considerando 2

Proposta da Comissão

(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. Os metadados derivados de comunicações eletrónicas podem também revelar informações muito sensíveis e 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.

Alteração

(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. Os metadados derivados de comunicações eletrónicas podem também revelar informações muito sensíveis e 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.
A proteção da confidencialidade das comunicações constitui uma condição essencial para o respeito de outros direitos e liberdades fundamentais conexos, como a proteção da liberdade de pensamento, de consciência e de religião e a liberdade de expressão e de informação.

Alteração 3

Proposta de regulamento Considerando 5

Proposta da Comissão

(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

Alteração

(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.

Alteração 4

Proposta de regulamento Considerando 6

Proposta da Comissão

(6) Embora os princípios e as principais disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho²² 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 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.

dados de comunicações eletrónicas que possam ser considerados dados pessoais. O presente regulamento **não pode**, por conseguinte, **baixar** o nível de proteção de que beneficiam as pessoas singulares ao abrigo do Regulamento (UE) 2016/679. O tratamento de dados das comunicações eletrónicas deve apenas ser permitido em conformidade com o presente regulamento, **e com base num fundamento jurídico especificamente previsto no mesmo.**

Alteração

(6) Embora os princípios e as principais disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho 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 **nas** comunicações eletrónicas **que utilizam os novos meios de comunicação**. Esses desenvolvimentos incluem a entrada no mercado de serviços de comunicações eletrónicas **(tais como os novos serviços de comunicações interpessoais baseados na Internet, por exemplo telefone via Internet, mensagens instantâneas e serviços de correio eletrónico com base na web)** que, na perspetiva de um consumidor, são alternativas aos serviços tradicionais, mas que não têm de cumprir o mesmo conjunto de regras. Outro 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.

²² 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).

²² 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).

Alteração 5

Proposta de regulamento Considerando 7

Proposta da Comissão

(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.

Alteração

Suprimido

Alteração 6

Proposta de regulamento Considerando 9

Proposta da Comissão

(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,

Alteração

(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.

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. ***Tal deve suceder independentemente de as comunicações eletrónicas estarem ou não vinculadas a um pagamento.***

Alteração 7

Proposta de regulamento Considerando 11

Proposta da Comissão

(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 Comunicações Eletrónicas²⁴]. 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

Alteração

(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 Comunicações Eletrónicas²⁴]. 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.

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, *como é o caso das mensagens internas, fontes de notícias («newsfeeds»), cronologias e funções semelhantes nos serviços em linha, cujas mensagens sejam trocadas com outros utilizadores dentro ou fora desse serviço (ou seja, fontes de notícias e cronologias acessíveis ao público ou privadas)*; por conseguinte, este tipo de serviços que também possuem uma funcionalidade de comunicação devem ser abrangidos pelo presente regulamento.

²⁴ 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)).

²⁴ 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)).

Alteração 8

Proposta de regulamento Considerando 13

Proposta da Comissão

(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

Alteração

(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, *aeroportos, hotéis, pousadas, hospitais e outros pontos semelhantes de acesso à Internet*. Uma vez que essas redes de comunicações são disponibilizadas a um grupo indefinido de utilizadores finais, a confidencialidade das comunicações transmitidas através dessas

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.

redes deve ser *devidamente* 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.

Alteração 9

Proposta de regulamento Considerando 14

Proposta da Comissão

(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 devem ser considerados metadados de

Alteração

(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. ***Devem incluir ainda dados de localização, como, por exemplo, a localização real ou deduzida do equipamento terminal, a localização do equipamento terminal a partir do qual foi realizada ou recebida uma chamada telefónica ou uma ligação à Internet, ou o acesso a uma zona de Internet sem fios a que um dispositivo esteja ligado, bem***

comunicações eletrônicas e, por conseguinte, ser sujeitos às disposições do presente regulamento. Os metadados de comunicações eletrônicas 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 eletrônicas.

como os dados necessários para identificar os equipamentos terminais dos utilizadores finais. 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 devem ser considerados metadados de comunicações eletrônicas e, por conseguinte, ser sujeitos às disposições do presente regulamento. Os metadados de comunicações eletrônicas 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 eletrônicas.

Alteração 10

Proposta de regulamento Considerando 14-A (novo)

Proposta da Comissão

Alteração

(14-A) Os dados de localização de equipamento incluem os dados transmitidos ou armazenados em equipamentos terminais gerados por acelerómetros, barómetros, bússolas, sistemas de identificação de posição por satélite ou sensores, e dispositivos semelhantes.

Alteração 11

Proposta de regulamento Considerando 15

Proposta da Comissão

Alteração

(15) Os dados das comunicações eletrônicas devem ser tratados como dados confidenciais. Isto significa que qualquer

(15) Os dados das comunicações eletrônicas 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.

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 igualmente aplicável durante o seu envio, ou seja, até à receção do conteúdo da comunicação eletrónica pelo destinatário desejado *e aquando do armazenamento*. 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, *injetando publicidade ou outros conteúdos, e a análise dos dados de tráfego dos clientes*, incluindo os hábitos de navegação na Internet, sem o consentimento dos utilizadores finais.

Alteração 12

Proposta de regulamento Considerando 16

Proposta da Comissão

(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.

Alteração

(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.
Sempre que um tipo de tratamento dos dados de comunicações eletrónicas para estes fins seja suscetível de gerar um elevado risco para os direitos e liberdades das pessoas singulares, deve realizar-se uma avaliação de impacto da 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.

Alteração 13

Proposta de regulamento Considerando 17

Proposta da Comissão

(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

Alteração

(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 omitido 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***

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. ***Isso deve ser realizado em conformidade com o artigo 25.º do Regulamento (UE) 2016/679.*** Para apresentar os movimentos de tráfego em certas direções durante um determinado período de tempo ***pode ser*** necessário um identificador para estabelecer a ligação entre as posições das pessoas em certos intervalos de tempo. ***Aquando do*** tratamento de metadados de comunicações eletrónicas, deve realizar-se uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) 2016/679.

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**. 2016/679.

Alteração 14

Proposta de regulamento Considerando 20

Proposta da Comissão

(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 espíões, os pixels espíões, os identificadores ocultos, os testemunhos persistentes e outros

Alteração

(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 espíões, os pixels espíões, 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.

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, ***rastrear atividades*** ou ***desencadear determinadas operações ou tarefas técnicas, muitas vezes sem o conhecimento do utilizador***. 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. ***É necessário assegurar um nível de proteção elevado e equitativo da esfera privada dos utilizadores no que diz respeito à privacidade e confidencialidade do conteúdo, do funcionamento e da utilização do respetivo equipamento terminal***. Por conseguinte, as interferências com o equipamento terminal do utilizador final só devem ser permitidas com o consentimento deste último e para fins específicos, ***limitados*** e transparentes.

Alteração 15

Proposta de regulamento Considerando 21

Proposta da Comissão

(21) As exceções à obrigação de obter o consentimento para utilizar as capacidades

Alteração

(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.***

Alteração 16

Proposta de regulamento Considerando 21-A (novo)

Proposta da Comissão

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 ***pela pessoa singular ou pessoa coletiva responsável pelo sítio web («análises de origem»).***

Alteração

(21-A) Os dados de localização do equipamento podem dar uma perspetiva muito pormenorizada e invasiva da vida pessoal de um indivíduo ou dos negócios e das atividades de uma organização. O tratamento dos dados de localização de qualquer fonte, sejam eles metadados de

comunicações eletrónicas ou dados de localização do equipamento, deve ser realizado com base em regras claras.

Alteração 17

Proposta de regulamento Considerando 22

Proposta da Comissão

(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

Alteração

(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, ***impedir a utilização das chamadas «barreiras de testemunhos de conexão» e «mensagens de testemunhos de conexão» que não ajudem os utilizadores a manter o controlo sobre as suas informações pessoais e a sua privacidade ou a informar-se sobre os seus direitos. O presente regulamento deve*** prever a possibilidade de expressar o consentimento ***através de especificações técnicas, por exemplo,*** utilizando as predefinições adequadas do programa de navegação ou outra aplicação. ***Essas predefinições devem incluir escolhas relativas ao armazenamento de informações no equipamento terminal do utilizador, bem como um sinal enviado pelo programa de navegação ou outra aplicação a outras partes indicando as preferências do***

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.

utilizador. As escolhas efetuadas pelos utilizadores 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 a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente, os programas de navegação, **as aplicações ou os sistemas operativos móveis** podem ser utilizados como **executores das escolhas de um utilizador final**, 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.

Alteração 18

Proposta de regulamento Considerando 23

Proposta da Comissão

(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

Alteração

(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.

apresentação de informações da Internet devem ser obrigados a configurar o software de modo a que ofereça a possibilidade de impedir **o rastreio por defeito entre domínios e o armazenamento de** informações **por terceiros** nos equipamentos terminais; este procedimento é frequentemente apresentado como «rejeitar **rastreadores e** testemunhos de conexão de terceiros». Os utilizadores devem dispor, **por defeito**, da configuração que lhes permita escolher entre diferentes níveis um conjunto de opções de privacidade, desde o nível mais elevado (por exemplo, «nunca aceitar **rastreadores nem** testemunhos de conexão») **até** ao nível mais baixo (por exemplo, «aceitar sempre **rastreadores e** testemunhos de conexão»), passando pelo nível intermédio (por exemplo, «rejeitar **todos os rastreadores e** testemunhos de conexão **que não sejam estritamente necessários para fornecer o serviço explicitamente solicitado pelo utilizador**» ou «rejeitar **todos os rastreios entre domínios**»). **Estas opções podem também ser mais precisas. As predefinições de privacidade devem incluir igualmente opções que permitam ao utilizador decidir, por exemplo, se Flash, JavaScript ou outro software similar pode ser executado, ou se um sítio web pode recolher os dados de localização geográfica do utilizador ou aceder a hardware específico, como uma webcam ou um microfone.** Essas predefinições de privacidade devem ser apresentadas de uma forma compreensível, **objetiva e** facilmente visível.

Alteração 19

Proposta de regulamento Considerando 24

Proposta da Comissão

(24) Para obter o consentimento dos utilizadores finais, na aceção do

Alteração

Suprimido

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).

Alteração 20

Proposta de regulamento Considerando 25

Proposta da Comissão

(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

Alteração

(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.

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. ***Além disso, esses fornecedores devem obter o consentimento junto do utilizador final ou anonimizar os dados imediatamente, limitando a finalidade à mera contagem estatística limitada no tempo e no espaço, e oferecendo possibilidades efetivas de retirada.***

Alteração 21

Proposta de regulamento Considerando 26

Proposta da Comissão

(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

Alteração

(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 **a título temporário**, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar interesses públicos específicos, **incluindo** a segurança nacional (**isto é, a segurança do Estado**), 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

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.

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. *A encriptação e outras medidas de segurança são fundamentais para garantir a confidencialidade e a integridade das comunicações eletrónicas e a segurança e a integridade das infraestruturas das comunicações eletrónicas no seu conjunto. As medidas tomadas pelos Estados-Membros não devem comportar quaisquer obrigações para os fornecedores de redes ou de serviços de comunicações eletrónicas que enfraqueçam a segurança e a encriptação das respetivas redes ou serviços.* 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.

Alteração 22

Proposta de regulamento

Considerando 32-A (novo)

Proposta da Comissão

Alteração

(32-A) As comunicações destinadas aos representantes eleitos ou às autoridades públicas sobre questões relativas a políticas públicas, legislação ou a outras atividades de instituições democráticas não devem ser consideradas, para efeitos do presente regulamento, marketing direto.

Alteração 23

Proposta de regulamento Considerando 33

Proposta da Comissão

Alteração

(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 de 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

(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 de 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.

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 *e apenas por um período de tempo limitado.*

Alteração 24

Proposta de regulamento Considerando 35

Proposta da Comissão

(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.

Alteração

(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 **e** apresentar um código específico que indique que se trata de uma chamada promocional.

Alteração 25

Proposta de regulamento Considerando 37

Proposta da Comissão

(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.

Alteração

(37) Os prestadores de serviços que disponibilizam serviços de comunicações eletrónicas devem **tratar os dados de comunicações eletrónicas de forma a impedir o acesso, a divulgação ou a alteração não autorizados, garantir que esse acesso, divulgação ou alteração não autorizados possam ser verificados, e garantir também que esses dados de comunicações eletrónicas sejam protegidos através do** recurso a tipos específicos de software **e a** 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. **As obrigações previstas no artigo 40.º do [Código Europeu das Comunicações Eletrónicas] devem aplicar-se a todos os serviços abrangidos pelo presente regulamento no que diz respeito à segurança das redes e dos serviços e às correspondentes obrigações de segurança.**

Alteração 26

Proposta de regulamento Considerando 40

Proposta da Comissão

(40) A fim de reforçar a aplicação das disposições do presente regulamento, cada autoridade de controlo deve dispor de poderes para impor sanções, incluindo

Alteração

(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.

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. ***Deve ser proibida a aplicação de duplas sanções por violação tanto do Regulamento (UE) 2016/279 como do presente regulamento.***

Alteração 27

Proposta de regulamento

Artigo 1

Proposta da Comissão

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

Alteração

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 *normas* específicas para os fins mencionados nos *n.os* 1 e 2.

respeito ao tratamento de dados pessoais.

2. O presente regulamento assegura, *em conformidade com o Regulamento (UE) 2016/679*, 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 com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

3. As disposições do presente Regulamento completam o Regulamento (UE) 2016/679, estabelecendo *as normas* específicas *necessárias* para os fins mencionados nos *n.ºs* 1 e 2. *Aplicam-se as disposições do Regulamento (UE) 2016/679, exceto se o presente regulamento previr disposições especiais.*

Alteração 28

Proposta de regulamento

Artigo 2

Proposta da Comissão

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.*

Alteração

Artigo 2.º

Âmbito de aplicação material

1. O presente regulamento aplica-se:

a) 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, ou processadas por esse mesmo equipamento, independentemente de qualquer

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/CE¹, 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.

pagamento solicitado ao utilizador final.

b) às informações transmitidas ao equipamento terminal dos utilizadores finais, nele armazenadas, reunidas, por ele processadas, ou de outra forma relacionadas com esse equipamento terminal, se não estiverem protegidas pelo Regulamento (UE) 2016/679;

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, **nos termos do artigo 2.º, n.º 2, alínea c), do Regulamento (UE) 2016/679;**
 - 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/CE¹, 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.

¹ 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).

¹ 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).

Alteração 29

Proposta de regulamento

Artigo 3

Proposta da Comissão

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.

Alteração

Artigo 3.º

Âmbito de aplicação territorial e representante

1. O presente regulamento aplica-se *às atividades referidas no artigo 2.º quando o utilizador final se encontre na União:*

2. Sempre que o prestador de um serviço de comunicações eletrónicas, *o fornecedor de uma lista disponível ao público, o fornecedor de software que permita comunicações eletrónicas ou a pessoa que envie comunicações comerciais para fins de marketing direto ou de recolha de (outras) informações relacionadas com o equipamento terminal dos utilizadores finais ou armazenadas nesse equipamento não estiverem estabelecidos* na União, *devem* designar,

por escrito, um representante na União, **nos termos do artigo 27.º do Regulamento (UE) 2016/679**.

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**.

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

4. O representante **do fornecedor** deve **ser autorizado por este último, que lhe deve além disso transmitir as informações pertinentes**, a responder às perguntas e a facultar informações complementares ou em substituição do fornecedor que representa, nomeadamente às autoridades de controlo, **aos tribunais** e aos utilizadores finais, sobre todas as questões relativas **às atividades a que se refere o artigo 2.º** 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 **executa as atividades referidas no artigo 2.º** de fora da União.

Alteração 30

Proposta de regulamento Artigo 4 – n.º 3 – alínea c)

Proposta da Comissão

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,

Alteração

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, mas não exclusivamente, os dados utilizados para detetar uma comunicação e identificar a sua fonte e destino, a localização do dispositivo no

duração e tipo de comunicação;

contexto da comunicação e a data, hora, duração e tipo de comunicação; *inclui os dados transmitidos ou emitidos pelo equipamento terminal para identificar as comunicações dos utilizadores finais e/ou o equipamento terminal na rede e permitir que este último se ligue a uma rede ou a outro dispositivo.*

Alteração 31

Proposta de regulamento Artigo 4 – n.º 3 – alínea f)

Proposta da Comissão

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.;

Alteração

f) «Comunicações comerciais diretas» qualquer forma de **comunicação comercial**, 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.;

Alteração 32

Proposta de regulamento Capítulo 2 – título

Proposta da Comissão

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

Alteração

PROTEÇÃO DAS COMUNICAÇÕES ELETRÓNICAS DE PESSOAS SINGULARES E COLETIVAS E DAS INFORMAÇÕES **TRATADAS PELOS SEUS EQUIPAMENTOS TERMINAIS E COM ESTES RELACIONADAS**

Alteração 33

Proposta de regulamento Artigo 5

Proposta da Comissão

Artigo 5.º

Confidencialidade dos dados de comunicações eletrónicas

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.

Alteração

Artigo 5.º

Confidencialidade dos dados de comunicações eletrónicas

Confidencialidade dos dados de comunicações eletrónicas

1. 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 qualquer tratamento de dados de comunicações eletrónicas, independentemente de os dados se encontrarem em trânsito ou armazenados, por outras pessoas que não os utilizadores finais.

1-A. *Para efeitos da aplicação do n.º 1, os fornecedores de redes e de serviços de comunicações eletrónicas devem tomar medidas técnicas e organizativas, conforme disposto no artigo 32.º do Regulamento (UE) 2016/679. Além disso, para proteger a integridade do equipamento terminal e a segurança e a privacidade dos utilizadores, os fornecedores de redes e serviços de comunicações eletrónicas devem tomar as medidas adequadas, baseadas no risco e nas técnicas mais recentes, para prevenir de forma razoável a distribuição de programas maliciosos através das suas redes ou serviços, tal como referido no artigo 7.º, alínea a), da Diretiva 2013/40/UE.*

1-B. *A confidencialidade dos dados das comunicações eletrónicas deve também englobar os equipamentos terminais e as comunicações máquina-máquina quando relacionadas com um utilizador.*

Alteração 34

Proposta de regulamento

Artigo 6

Proposta da Comissão

Artigo 6.º

Tratamento permitido de dados de comunicações eletrónicas

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

Alteração

Artigo 6.º

Tratamento permitido de dados de comunicações eletrónicas

Tratamento *legal* de dados de comunicações eletrónicas

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

a) Se tal for necessário para assegurar a transmissão da comunicação, durante o período necessário para esse efeito, *e se os dados forem armazenados em formato binário*; ou

b) Se tal for *estritamente* necessário *em termos técnicos* para manter ou restabelecer a *disponibilidade, integridade, confidencialidade e a* segurança das redes *ou dos* serviços de comunicações eletrónicas, ou *para* detetar falhas técnicas e/ou erros na transmissão das comunicações eletrónicas, durante o período necessário para esse efeito; *ou*

b-A) Se esse tratamento produzir apenas efeitos para o utilizador que solicitou o serviço e não prejudicar os direitos fundamentais de outro utilizador ou utilizadores, se o utilizador em causa tiver dado o seu consentimento para o tratamento dos respetivos dados de comunicações eletrónicas, e desde que a finalidade em causa não possa ser atingida sem o tratamento desses metadados.

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) 2015/2120¹ 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*.

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

metadados de comunicações eletrónicas *apenas*:

- a) Se tal for *estritamente* 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) 2015/2120¹¹ durante o período *tecnicamente* necessário para esse efeito; ou
- b) Se tal for *estritamente* necessário para proceder à faturação, calcular o pagamento das interligações, detetar ou impedir a utilização *ilegal*, abusiva ou fraudulenta de serviços de comunicações eletrónicas ou a subscrição desses serviços; ou
- c) Se o utilizador final em causa, *depois de receber todas as informações relevantes sobre o tratamento previsto numa linguagem clara e facilmente compreensível, fornecidas em separado dos termos e condições do prestador*, 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 *sem o* tratamento *desses metadados*.

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 *solicitado pelo* utilizador final, se o utilizador final em causa *tiver* dado o seu consentimento *prévio* para o tratamento do conteúdo das suas comunicações eletrónicas, e a prestação desse serviço não puder ser efetuada sem o tratamento desse conteúdo *pelo fornecedor, e o consentimento não tiver condicionado o acesso ao serviço ou a sua utilização*; 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.

causa tiverem dado o seu consentimento **prévio** 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.

3-A. Para efeitos da prestação de um serviço explicitamente solicitado pelo utilizador final de um serviço de comunicações eletrónicas para utilização exclusivamente individual ou utilização individual relacionada com o trabalho, o prestador do serviço de comunicações eletrónicas só pode tratar os dados das comunicações eletrónicas para efeitos da prestação do serviço explicitamente solicitado e sem o consentimento de todos os utilizadores, se esse tratamento apenas produzir efeitos para o utilizador final que solicitou o serviço e não prejudicar os direitos fundamentais de outro utilizador ou utilizadores. Esse consentimento específico do utilizador final impede o prestador do serviço de tratar esses dados para qualquer outra finalidade.

¹ 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).

¹ 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).

Alteração 35

Proposta de regulamento

Artigo 7

Proposta da Comissão

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.

Alteração

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), **no artigo 6.º, n.º 2, alíneas a) e c)** 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 **um terceiro específico** por ele **designado** 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 **dados estritamente necessários** 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.

Alteração 36

Proposta de regulamento

Artigo 8

Proposta da Comissão

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

Alteração

Artigo 8.º

Proteção das informações armazenadas nos equipamentos terminais dos utilizadores finais, relacionadas com esses equipamentos ***e por eles tratadas***

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, ***ou a disponibilização de informações através dos equipamentos terminais***, incluindo ***informações*** sobre o seu software e ***hardware*** ***ou por estes geradas, bem como quaisquer outros dados de comunicações eletrónicas que identifiquem os utilizadores finais*** 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 ***em que os dados estejam armazenados em formato binário***; ou
- b) Se o utilizador final tiver dado o seu consentimento ***específico, o qual não deve ser obrigatório para aceder ao serviço***;
- c) Se forem ***estritamente*** necessárias para prestar um serviço da sociedade de informação solicitado pelo utilizador final, ***durante o período necessário para a respetiva prestação do serviço, desde que a prestação desse serviço específico não possa ser efetuada sem o tratamento desse***

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.

conteúdo pelo prestador; ou

d) Se forem **estritamente** necessárias **em termos técnicos** para uma medição de audiência da web **do serviço da sociedade de informação solicitado pelo utilizador final**, desde que tal medição seja efetuada pelo prestador, **ou em nome deste, ou por uma agência independente de análises de rede que atue no interesse público ou para fins científicos; e, além disso, desde que nenhum dado pessoal seja tornado acessível a qualquer outra parte, que essa medição de audiência da web não implique o rastreio do utilizador final em diferentes serviços** da sociedade de informação **e que respeite os direitos fundamentais do** utilizador final.

d-A) Se os dados forem suprimidos sem demora injustificada assim que a finalidade da recolha deixar de existir.

d-AA) Se forem necessárias do ponto de vista estritamente técnico para uma atualização de segurança, desde que:

i) estas atualizações não alterem, de modo algum, a funcionalidade do hardware ou software, nem os parâmetros de privacidade escolhidos pelo utilizador;

ii) o utilizador seja informado previamente da instalação de cada atualização; e

iii) o utilizador tenha a possibilidade de adiar ou desligar a instalação automática destas atualizações;

d-B) Se forem úteis para a personalização dos serviços de comunicações eletrónicas prestados aos utilizadores finais e por estes explicitamente solicitadas.

O disposto nas alíneas a), c) e d) deve ser limitado a situações que não envolvam qualquer intrusão, ou apenas uma intrusão muito limitada, na privacidade ou relacionada com os direitos fundamentais.

Não deve ser recusado ao utilizador final o acesso a qualquer serviço ou funcionalidade da sociedade de informação, independentemente de ser remunerado ou não, em virtude de não ter dado o seu consentimento nos termos do artigo 8.º, n.º 1, alínea b), ou do artigo 8.º, n.º 2, alínea b), ao tratamento de quaisquer dados que não sejam estritamente necessários para a funcionalidade solicitada 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.***

A recolha dessas informações deve ser subordinada à aplicação de medidas

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 ***solicitada pelo utilizador final*** e durante o tempo necessário para o efeito; ou

a-A) Se o utilizador final tiver dado o seu consentimento; ou

a-B) Os dados forem anonimizados e os riscos adequadamente atenuados.

b) ***Todas as informações pertinentes sobre o tratamento previsto forem transmitidas num aviso claro e facilmente compreensível, separadamente dos termos e condições do fornecedor, e que indiquem, pelo menos, pormenorizadamente o modo como as informações serão recolhidas, a finalidade da recolha, a pessoa responsável pela mesma, e outras informações exigidas nos termos do artigo 13.º do Regulamento (UE) 2016/679, sempre que forem recolhidos dados pessoais. 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.***

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.

Alteração 37

Proposta de regulamento

Artigo 9

Proposta da Comissão

Artigo 9.º

Consentimento

1. São aplicáveis a definição e as condições do consentimento previstas no

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.

2-A. Para efeitos da aplicação do n.º 2, alínea a-B), são executados os seguintes controlos a fim de atenuar os riscos:

a) A finalidade da recolha de dados do equipamento terminal deve ser limitada à mera contagem estatística;

b) O rastreio deve ser limitado no tempo e no espaço na medida estritamente necessária para essa finalidade;

c) Os dados devem ser suprimidos ou anonimizados imediatamente após atingida essa finalidade; e

d) Devem ser oferecidas aos utilizadores finais possibilidades efetivas de retirada.

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.

Alteração

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 4.º, n.º 11, e no artigo 7.º, **n.ºs 1, 2 e 3**, do Regulamento (UE) 2016/679/UE.

2. Sem prejuízo do disposto no n.º 1, sempre que for tecnicamente possível e exequível, **em particular** para efeitos do artigo 8.º, n.º 1, alínea b), o consentimento pode ser expresso utilizando as **especificações técnicas dos serviços de comunicações eletrónicas. Sempre que essas especificações técnicas forem utilizadas pelo utilizador final, devem ser vinculativas e aplicáveis a qualquer outra parte.**

3. Os utilizadores finais que tenham **dado o seu consentimento ao** tratamento de dados de comunicações eletrónicas, tal como estabelecido no artigo 6.º, n.º 2, alínea c), no artigo 6.º, n.º 3, alíneas a) e b), **no artigo 8.º, n.º 1, alínea b), e no artigo 8.º, n.º 2, alínea a-A)**, 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. **Retirar o consentimento deve ser tão fácil como dá-lo, e, além disso, o utilizador final deve ser recordado** desta possibilidade a intervalos regulares de 6 meses, enquanto o tratamento continuar.

Alteração 38

Proposta de regulamento Artigo 10

Proposta da Comissão

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,

Alteração

Artigo 10.º

Informações e opções de predefinições de privacidade a fornecer - **privacidade desde a conceção e por defeito**

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

deve:

1-A. oferecer a possibilidade de impedir que terceiros armazenem informações no equipamento terminal de um utilizador final ou que tratem informações já armazenadas nesse equipamento.

1-A. Por defeito, oferecer predefinições de proteção de privacidade para evitar que terceiros armazenem informações no equipamento terminal de um utilizador e tratem informações já armazenadas nesse equipamento;

1-B. Após a instalação, informar e oferecer ao utilizador a possibilidade de alterar ou confirmar as opções de predefinições de privacidade definidas na alínea a), exigindo o consentimento do utilizador para uma predefinição;

1-C. Tornar a predefinição estabelecida nas alíneas a) e b) facilmente acessível durante a utilização do software; e

1-D. Oferecer ao utilizador a possibilidade de expressar consentimento específico através das predefinições após a instalação do software.

2. **Para efeitos da aplicação do n.º 1, alíneas a) e b), as predefinições devem incluir um sinal que é enviado às outras partes para as informar sobre as predefinições de privacidade do utilizador. Essas predefinições devem ser vinculativas e aplicáveis a quaisquer terceiros.**

O Comité Europeu para a Proteção de Dados deve emitir diretrizes destinadas a determinar as especificações técnicas e os métodos de sinalização que cumprem as condições necessárias para expressar o consentimento ou a objeção, nos termos das alíneas a) e b).

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.

2018.

Alteração 39

Proposta de regulamento

Artigo 10-A (novo)

Proposta da Comissão

Alteração

Artigo 10.º-A

Este software deve assegurar que o consentimento dado pelo utilizador final nos termos do artigo 8.º, n.º 1, alínea b), prevaleça sobre as predefinições selecionadas aquando da instalação do software.

O software não pode bloquear um tratamento de dados legalmente autorizado nos termos do artigo 8.º, n.º 1, alíneas a), b), c) ou d), ou do n.º 2, alínea a), independentemente das predefinições do programa de navegação.

Alteração 40

Proposta de regulamento

Artigo 11

Proposta da Comissão

Alteração

Artigo 11.º

Artigo 11.º

Restrições

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,

1. O direito da União ou o direito dos Estados-Membros **a que o fornecedor está sujeito** 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 **os direitos e liberdades fundamentais, em conformidade com a Carta dos Direitos Fundamentais da União Europeia e a Convenção Europeia para a Proteção dos Direitos do Homem e**

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.

das Liberdades Fundamentais, e constitua uma medida necessária, adequada e proporcionada, numa sociedade democrática, para salvaguardar **os** 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 **missão** de controlo, de inspeção ou de regulamentação associada ao exercício da autoridade pública relativamente a **tais** interesses.

1-A. Em particular, qualquer medida legislativa referida no n.º 1 deve incluir disposições específicas, pelo menos, sempre que pertinente, nos termos do artigo 23.º, n.º 2, do Regulamento (UE) 2016/679.

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. **Os prestadores de serviços devem responder aos pedidos de acesso em conformidade com os requisitos legais onde o prestador de serviços tem o seu estabelecimento principal, em conformidade com o Regulamento (UE) 2016/679. No caso de pedidos provenientes de um Estado-Membro em que o prestador de serviços não esteja estabelecido, serão acatados mecanismos transfronteiriços relativos a pedidos ao abrigo de convenções de auxílio judiciário mútuo ou da Diretiva 2014/41/UE do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal. Sem prejuízo de outros requisitos ao abrigo da legislação de um Estado-Membro para fornecer informações às autoridades responsáveis pela aplicação da lei,** 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.

Alteração 41

Proposta de regulamento Artigo 15

Proposta da Comissão

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 facultar 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

Alteração

Artigo 15.º

Listas acessíveis ao público

1. Os fornecedores de listas acessíveis ao público ***ou os prestadores de serviços de comunicações eletrónicas*** devem obter o consentimento ***prévio*** dos utilizadores finais que sejam pessoas singulares para incluir os seus dados pessoais nas listas e ***organizar os dados pessoais*** por categoria, na medida em que tais dados sejam pertinentes para a finalidade das listas. Os fornecedores devem dar aos utilizadores finais que sejam pessoas singulares meios para verificar, corrigir e suprimir esses dados ***ou para retirar o seu consentimento a qualquer momento***.
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 facultar 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.

ao público, ou de verificarem, corrigirem ou suprimirem quaisquer dados que lhes digam respeito deve ser proposta gratuitamente.

Alteração 42

Proposta de regulamento

Artigo 16 – n.º 1

Proposta da Comissão

(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**.

Alteração

(1) **A utilização por** pessoas singulares ou coletivas **de serviços de comunicações eletrónicas, incluindo chamadas vocais, sistemas de chamada e de comunicação automatizados, incluindo sistemas semiautomatizados que ligam a pessoa que efetua a chamada a um indivíduo, fax, endereço de correio eletrónico ou outra utilização de** serviços de comunicações eletrónicas para **efeitos da apresentação** de comunicações **de marketing não solicitadas ou** diretas a utilizadores finais, **só será autorizada no caso de os utilizadores finais terem dado o seu consentimento prévio**.

Alteração 43

Proposta de regulamento

Artigo 16 – n.º 2

Proposta da Comissão

(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

Alteração

(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 **por um período não superior a doze meses**, desde

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. O direito de oposição deve ser oferecido** na data da recolha e sempre que uma mensagem é enviada.

que aos clientes tenha sido dada clara e distintamente a possibilidade de se oporem, de forma gratuita e fácil, a essa utilização. **O cliente deve ser informado do direito de oposição e ter a possibilidade de o exercer facilmente** na data da recolha e sempre que uma mensagem é enviada.

Alteração 44

Proposta de regulamento

Artigo 16 – parágrafo 3 – alínea a)

Proposta da Comissão

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

Alteração

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

Alteração 45

Proposta de regulamento

Artigo 16 – n.º 3-A (novo)

Proposta da Comissão

Alteração

3-A. As comunicações comerciais não solicitadas devem 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. Tais comunicações devem fornecer as informações necessárias para que os destinatários exerçam o seu direito de recusar novas mensagens comerciais escritas ou orais.

Alteração 46

Proposta de regulamento

Artigo 16 – n.º 4

Proposta da Comissão

Alteração

(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.

Suprimido

Alteração 47

**Proposta de regulamento
Artigo 16 – parágrafo 6**

Proposta da Comissão

Alteração

(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.

(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 **o seu consentimento ou o direito de oposição**, de forma **tão fácil como dar** o seu consentimento **e a título gratuito**, em relação à receção de novas comunicações comerciais.

Alteração 48

**Proposta de regulamento
Artigo 17**

Proposta da Comissão

Alteração

Artigo 17.º

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.**

Informações sobre os riscos de segurança detetados

No caso de um risco específico **ou significativo** que possa comprometer a segurança de redes e serviços de comunicações eletrónicas, o prestador de um serviço de comunicações eletrónicas deve **respeitar as obrigações de segurança estabelecidas nos artigos 32.º a 34.º e no artigo 40.º da Diretiva que institui um Código Europeu das Comunicações Eletrónicas.**

Alteração 49

Proposta de regulamento Artigo 21

Proposta da Comissão

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.

Alteração

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, 79.º e 80.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.

Alteração 50

Proposta de regulamento

Artigo 22 – n.º 1

Proposta da Comissão

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.

Alteração

É aplicável o artigo 82.º do Regulamento (UE) 2016/679.

Justificação

*O artigo 82.º do Regulamento (UE) n.º 2016/679 já regula a imputação da responsabilidade e o direito de receber uma indemnização. As disposições introduzidas no artigo 22.º da proposta de regulamento constituem uma extensão e uma especificação do artigo 82.º do Regulamento (UE) n.º 2016/679, o que torna a presente proposta uma *lex specialis*.*

Alteração 51

Proposta de regulamento

Artigo 23

Proposta da Comissão

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

Alteração

Suprimido

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;*
 - c) 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.

Justificação

O artigo 83.º do Regulamento (UE) n.º 2016/679 regula as condições gerais para a aplicação de coimas. A especificação introduzida no presente texto modifica o artigo 83.º do Regulamento (UE) n.º 2016/679 e cria um regime duplo. Esta duplicação de estruturas dificulta a correta aplicação do direito pela autoridade de controlo e pelos tribunais, de que resulta uma disparidade de tratamento.

Alteração 52

Proposta de regulamento Artigo 23-A (novo)

Proposta da Comissão

Alteração

Artigo 23.º-A

É aplicável o artigo 83.º do Regulamento (UE) 2016/679.

Justificação

O artigo 83.º do Regulamento (UE) n.º 2016/679 regula as condições gerais para a aplicação de coimas. A especificação introduzida no presente texto modifica o artigo 83.º do Regulamento (UE) n.º 2016/679 e cria um regime duplo. Esta duplicação de estruturas dificulta a correta aplicação do direito pela autoridade de controlo e pelos tribunais, de que resulta uma disparidade de tratamento.

Alteração 53

Proposta de regulamento

Artigo 24

Proposta da Comissão

Alteração

Artigo 24.º

Suprimido

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.

Justificação

O artigo 84.º do Regulamento (UE) n.º 2016/679 regula as sanções. A especificação introduzida no presente texto modifica o artigo 84.º do Regulamento (UE) n.º 2016/679 e cria

um regime duplo. Esta duplicação de estruturas dificulta a correta aplicação do direito pela autoridade de controlo e pelos tribunais, de que resulta uma disparidade de tratamento.

Alteração 54

Proposta de regulamento Artigo 24-A (novo)

Proposta da Comissão

Alteração

Artigo 24.º-A

É aplicável o artigo 84.º do Regulamento (UE) 2016/679.

Justificação

O artigo 84.º do Regulamento (UE) n.º 2016/679 regula as sanções. A especificação introduzida no presente texto modifica o artigo 84.º do Regulamento (UE) n.º 2016/679 e cria um regime duplo. Esta duplicação de estruturas dificulta a correta aplicação do direito pela autoridade de controlo e pelos tribunais, do que resulta uma disparidade de tratamento.

Alteração 55

Proposta de regulamento Artigo 25 – n.º 2

Proposta da Comissão

Alteração

(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].

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

Alteração 56

Proposta de regulamento Artigo 28 – n.º 1

Proposta da Comissão

Alteração

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

Até, o mais tardar, seis meses antes da entrada em vigor do presente regulamento, a Comissão deve estabelecer um programa pormenorizado para

controlar a eficácia do presente
regulamento.

PROCESSO DA COMISSÃO ENCARREGADA DE EMITIR PARECER

Título	Respeito pela vida privada e proteção dos dados pessoais nas comunicações eletrónicas e revogação da Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas)		
Referências	COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)		
Comissão competente quanto ao fundo Data de comunicação em sessão	LIBE 16.2.2017		
Parecer emitido por Data de comunicação em sessão	JURI 16.2.2017		
Relator(a) de parecer Data de designação	Pavel Svoboda 28.2.2017		
Relator(a) de parecer substituído(a)	Axel Voss		
Exame em comissão	29.5.2017	19.6.2017	7.9.2017
Data de aprovação	2.10.2017		
Resultado da votação final	+: -: 0:	11 10 1	
Deputados presentes no momento da votação final	Max Andersson, Joëlle Bergeron, Marie-Christine Boutonnet, Jean-Marie Cavada, Mary Honeyball, Sylvia-Yvonne Kaufmann, Gilles Lebreton, Jiří Maštálka, Emil Radev, Julia Reda, Evelyn Regner, Pavel Svoboda, József Szájer, Axel Voss, Francis Zammit Dimech, Tadeusz Zwiefka		
Suplentes presentes no momento da votação final	Isabella Adinolfi, Angel Dzhambazki, Jens Rohde, Virginie Rozière, Tiemo Wölken		
Suplentes (art. 200.º, n.º 2) presentes no momento da votação final	Arne Lietz		

**VOTAÇÃO NOMINAL FINAL
NA COMISSÃO ENCARREGADA DE EMITIR PARECER**

11	+
ALDE	Jean-Marie Cavada, Jens Rohde
GUE/NGL	Jiří Maštálka
S&D	Mary Honeyball, Sylvia-Yvonne Kaufmann, Arne Lietz, Evelyn Regner, Virginie Rozière, Tiemo Wölken
VERTS/ALE	Max Andersson, Julia Reda

10	-
ECR	Angel Dzhambazki
EFDD	Joëlle Bergeron
ENF	Marie-Christine Boutonnet, Gilles Lebreton
PPE	Emil Radev, Pavel Svoboda, József Szájer, Axel Voss, Francis Zammit Dimech, Tadeusz Zwiefka

1	0
EFDD	Isabella Adinolfi

Legenda dos símbolos utilizados:

+ : votos a favor

- : votos contra

0 : abstenções