Parlamento Europeu
2014-2019

Comissão do Mercado Interno e da Proteção dos Consumidores

2017/0003(COD)

3.7.2017

ALTERAÇÕES
44 - 180

Draft opinion
Eva Maydell
(PE604.857v01-00)

Rrespeito 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)

Proposta de regulamento
(COM(2017)0010 – C8-0009/2017 – 2017/0003(COD))

AM_Com_LegOpinion

Alteração 44
Jan Philipp Albrecht

Proposta de regulamento
Considerando 1

Texto da Comissão	*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 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.	(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 ***comunicantes***. 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 ***interpessoais*** nas redes sociais. ***Deve ser, igualmente, aplicável quando a confidencialidade das comunicações eletrónicas convergir com a privacidade do ambiente físico, ou seja, quando os aparelhos terminais de comunicações eletrónicas tenham a capacidade de ouvir o seu ambiente físico ou de utilizar outros canais de entrada, como, por exemplo, a sinalização por Bluetooth ou detetores de movimento.***

Or. en

Alteração 45
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Liisa Jaakonsaari, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 1

Texto da Comissão	*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 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.	(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 ***em plataformas entre utilizadores de*** redes sociais ***e qualquer sistema de mensagens privadas em linha***.

Or. en

Alteração 46
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 2

Texto da Comissão	*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***	(2) O conteúdo das comunicações eletrónicas pode revelar informações altamente sensíveis acerca das pessoas singulares envolvidas na comunicação. De igual modo, os metadados derivados de

condições de saúde, preferências sexuais e opiniões políticas, cuja divulgação poderia resultar em danos pessoais e sociais, prejuízos económicos ou constrangimento. De igual modo, os metadados derivados de comunicações eletrónicas podem também revelar informações muito sensíveis e 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.***.

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 relativas à vida privada das pessoas envolvidas na comunicação eletrónica.

Or. en

Alteração 47
Inese Vaidere

Proposta de regulamento
Considerando 2

Texto da Comissão	*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***. De igual modo, 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	(2) O conteúdo das comunicações eletrónicas pode revelar informações altamente sensíveis ***sobre as*** pessoas singulares envolvidas na comunicação. De igual modo, 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.

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.

Or. en

Alteração 48
Curzio Maltese

Proposta de regulamento
Considerando 2

Texto da Comissão	*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. ***De igual modo, 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.	(2) ***As*** comunicações eletrónicas ***podem*** 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. ***Estes dados incluem texto, voz, vídeos, imagens, sons, o endereço IP*** e ***MAC dos utilizadores finais,*** 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.

Or. en

Justificação

Em princípio, os conteúdos e os metadados devem beneficiar do mesmo nível de proteção. Foi demonstrado em diversas ocasiões que os metadados facultam tanta informação relevante como os dados relacionados com a vida privada dos utilizadores finais (ver: https://techcrunch.com/2016/05/17/stanford-quantifies-the-privacy-stripping-power-of-

metadata/ ou https://www.privacyinternational.org/node/53). Deixa de existir justificação para fazer uma diferenciação entre níveis de proteção de metadados e de conteúdos.

Alteração 49
Jan Philipp Albrecht

Proposta de regulamento
Considerando 2

Texto da Comissão	*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. ***De igual modo,*** 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.	(2) ***Os dados de*** comunicações eletrónicas ***podem*** 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.***

Or. en

Justificação

A presente alteração visa salientar a importância deste diploma específico.

Alteração 50
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 3

Texto da Comissão	*Alteração*
(3) Os dados das comunicações eletrónicas podem também revelar informações sobre pessoas coletivas, tais como os seus segredos comerciais ou outras informações sensíveis com valor económico. Por conseguinte, as disposições do presente regulamento devem aplicar-se tanto a pessoas singulares como coletivas. Além disso, o presente regulamento deve assegurar que as disposições do Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho***[21]*** são igualmente aplicáveis a utilizadores finais que sejam pessoas coletivas. ***Tal inclui a definição de consentimento que consta do Regulamento (UE) n.º 2016/679. Quando é feita referência ao consentimento por parte de um utilizador final, incluindo pessoas coletivas, aplica-se esta definição. Além disso, as pessoas coletivas devem ter os mesmos direitos que os utilizadores finais que são pessoas singulares no que respeita às autoridades de controlo; ademais, as autoridades de controlo ao abrigo do presente regulamento devem ser responsáveis pelo acompanhamento da aplicação do mesmo às pessoas coletivas.***	***Suprimido***

_____

[21] Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral

sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1-88).

Or. en

Alteração 51
Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 3

Texto da Comissão	*Alteração*
(3) Os dados das comunicações eletrónicas podem também revelar informações sobre pessoas coletivas, tais como os seus segredos comerciais ou outras informações sensíveis com valor económico. Por conseguinte, as disposições do presente regulamento devem aplicar-se tanto a pessoas singulares como coletivas. Além disso, o presente regulamento deve assegurar que as disposições do Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho[21] são igualmente aplicáveis a utilizadores finais que sejam pessoas coletivas. Tal inclui a definição de consentimento que consta do Regulamento (UE) n.º 2016/679. Quando é feita referência ao consentimento por parte de um utilizador final, incluindo pessoas coletivas, aplica-se esta definição. Além disso, as pessoas coletivas devem ter os mesmos direitos que os utilizadores finais que são pessoas singulares no que respeita às autoridades de controlo; ademais, as autoridades de controlo ao abrigo do presente regulamento devem ser responsáveis pelo acompanhamento da aplicação do mesmo às pessoas coletivas.	***Suprimido***

[21] Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das

pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1-88).

Or. en

Alteração 52
Inese Vaidere

Proposta de regulamento
Considerando 3

Texto da Comissão	*Alteração*
(3) Os dados das comunicações eletrónicas podem também revelar informações sobre pessoas coletivas, tais como os seus segredos comerciais ou outras informações sensíveis com valor económico. Por conseguinte, as disposições do presente regulamento devem aplicar-se tanto a pessoas singulares como coletivas. Além disso, o presente regulamento deve assegurar que as disposições do Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho[21] são igualmente aplicáveis a utilizadores finais que sejam pessoas coletivas. Tal inclui a definição de consentimento que consta do Regulamento (UE) n.º 2016/679. Quando é feita referência ao consentimento por parte de um utilizador final, incluindo pessoas coletivas, aplica-se esta definição. Além disso, as pessoas coletivas devem ter os mesmos direitos que os utilizadores finais que são pessoas singulares no que respeita às autoridades de controlo; ademais, as autoridades de controlo ao abrigo do presente regulamento devem ser responsáveis pelo acompanhamento da aplicação do mesmo às pessoas coletivas.	(3) Os dados das comunicações eletrónicas podem também revelar informações sobre pessoas coletivas, tais como os seus segredos comerciais ou outras informações sensíveis com valor económico. Por conseguinte, as disposições do presente regulamento devem aplicar-se tanto a pessoas singulares como coletivas***, para além das disposições previstas na Diretiva 2016/943/UE***. Além disso, o presente regulamento deve assegurar que as disposições do Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho[21] são igualmente aplicáveis a utilizadores finais que sejam pessoas coletivas. Tal inclui a definição de consentimento que consta do Regulamento (UE) n.º 2016/679. Quando é feita referência ao consentimento por parte de um utilizador final, incluindo pessoas coletivas, aplica-se esta definição. Além disso, as pessoas coletivas devem ter os mesmos direitos que os utilizadores finais que são pessoas singulares no que respeita às autoridades de controlo; ademais, as autoridades de controlo ao abrigo do presente regulamento devem ser responsáveis pelo acompanhamento da aplicação do mesmo às pessoas coletivas.

[21] Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1-88).

[21] Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1-88).

Or. en

Alteração 53
Jan Philipp Albrecht

Proposta de regulamento
Considerando 3

Texto da Comissão	*Alteração*
(3) Os dados das comunicações eletrónicas podem também revelar informações sobre pessoas coletivas, tais como os seus segredos comerciais ou outras informações sensíveis com valor económico. Por conseguinte, as disposições do presente regulamento devem aplicar-se tanto a pessoas singulares como coletivas. Além disso, o presente regulamento deve assegurar que ***as*** disposições do Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho[21] são igualmente aplicáveis a utilizadores finais que sejam pessoas coletivas. Tal inclui a definição de consentimento que consta do Regulamento (UE) n.º 2016/679. Quando é feita referência ao consentimento por parte de um utilizador final, incluindo pessoas coletivas, aplica-se esta definição. Além disso, as pessoas coletivas devem ter os mesmos direitos que os utilizadores finais que são pessoas singulares no que respeita às autoridades de controlo; ademais, as autoridades de controlo ao abrigo do	(3) Os dados das comunicações eletrónicas podem também revelar informações sobre pessoas coletivas, tais como os seus segredos comerciais ou outras informações sensíveis com valor económico. Por conseguinte, as disposições do presente regulamento devem aplicar-se tanto a pessoas singulares como coletivas. Além disso, o presente regulamento deve assegurar que ***determinadas*** disposições do Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho***[21]*** são igualmente aplicáveis a utilizadores finais que sejam pessoas coletivas. Tal inclui a definição de consentimento que consta do Regulamento (UE) n.º 2016/679. Quando é feita referência ao consentimento por parte de um utilizador final, incluindo pessoas coletivas, aplica-se esta definição. Além disso, as pessoas coletivas devem ter os mesmos direitos que os utilizadores finais que são pessoas singulares no que respeita às autoridades de controlo; ademais, as autoridades de controlo ao abrigo do

presente regulamento devem ser responsáveis pelo acompanhamento da aplicação do mesmo às pessoas coletivas.	presente regulamento devem ser responsáveis pelo acompanhamento da aplicação do mesmo às pessoas coletivas.
_____	_____
[21] Regulamento (UE) n.º2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1-88).	[21] Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1-88).
	Or. en

Alteração 54
Jan Philipp Albrecht

Proposta de regulamento
Considerando 4

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

Alteração 55

Curzio Maltese

Proposta de regulamento
Considerando 4

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

Or. en

Justificação

Esta alteração explica quais os dados de comunicações eletrónicas que são dados pessoais.

Alteração 56
Jan Philipp Albrecht

Proposta de regulamento
Considerando 5

Texto da Comissão	*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) n.º 2016/679. ***O***	(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) n.º 2016/679. ***Pelo***

tratamento de ***dados*** das comunicações ***eletrónicas pelos prestadores*** de ***serviços de*** comunicações eletrónicas deve apenas ser permitido em conformidade com o presente regulamento.	***contrário, pretende proporcionar salvaguardas adicionais e complementares, que tomem em consideração a necessidade de proteção adicional quanto à confidencialidade das comunicações. 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***.

Or. en

Justificação

A Autoridade Europeia para a Proteção de Dados incentiva esta clarificação.

Alteração 57
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 5

Texto da Comissão	*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) n.º 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.	(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***, sem ir além, nem contradizer, o elevado nível de proteção previsto no Regulamento (UE) n.º 2016/679***. O presente regulamento, por conseguinte, não baixa o nível de proteção de que beneficiam as pessoas singulares ao abrigo do Regulamento (UE) n.º 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.

Or. en

Alteração 58
Curzio Maltese

Proposta de regulamento
Considerando 5

Texto da Comissão	*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) n.º 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.	(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) n.º 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. ***Sempre que o presente regulamento e o Regulamento (UE) n.º 2016/679 possam ser aplicados ao mesmo tratamento, deve ser somente aplicado o presente regulamento.***

Or. en

Justificação

A presente alteração especifica a forma como estes dois regulamentos devem ser aplicados em conjunto.

Alteração 59
Inese Vaidere

Proposta de regulamento
Considerando 6

Texto da Comissão	*Alteração*
(6) Embora os princípios e as principais disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho[22] 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.	(6) Embora os princípios e as principais disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho[22] permaneçam, de um modo geral, adequados, esta diretiva não acompanhou plenamente a evolução da realidade tecnológica e do mercado, o que resultou numa ***clareza*** insuficiente ***e numa aplicação*** 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.
_____	_____
[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).

Or. en

Alteração 60
Jan Philipp Albrecht

Proposta de regulamento
Considerando 6

Texto da Comissão	*Alteração*
(6) Embora os princípios e as principais disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho[22] 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.	(6) Embora os princípios e as principais disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho[22] 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 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).

Or. en

Alteração 61
Jan Philipp Albrecht

Proposta de regulamento
Considerando 7

Texto da Comissão	*Alteração*
(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.	***Suprimido***

Or. en

Justificação

Este considerando prejudicaria a abordagem de harmonização do mercado único digital, por meio de um regulamento.

Alteração 62
Kaja Kallas, Dita Charanzová

Proposta de regulamento
Considerando 7

Texto da Comissão	*Alteração*
(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	(7) ***O Comité Europeu para a Proteção de Dados deve, quando necessário***, ***formular orientações e pareceres*** dentro dos limites do presente regulamento para especificar e clarificar a aplicação das regras do presente regulamento, a fim de assegurar uma aplicação e interpretação eficazes das referidas regras. ***É essencial assegurar*** a ***cooperação e a coerência entre*** os Estados-Membros***, em particular entre as autoridades nacionais responsáveis pela proteção de dados, por forma a*** manter um

pessoais e a livre circulação de dados de comunicações eletrónicas.	equilíbrio entre a proteção da vida privada e dos dados pessoais e a livre circulação de dados de comunicações eletrónicas ***na União***.

Or. en

Alteração 63
Curzio Maltese

Proposta de regulamento
Considerando 7

Texto da Comissão	*Alteração*
(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.	(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, os Estados-Membros ***devem introduzir disposições no sentido de aumentar*** a ***privacidade*** dos ***utilizadores finais, sem comprometer*** a livre circulação ***das*** comunicações eletrónicas.

Or. en

Alteração 64
Christel Schaldemose, Lucy Anderson, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 8

Texto da Comissão	*Alteração*
(8) O presente regulamento deve aplicar-se aos prestadores de serviços de comunicações eletrónicas, aos	(8) O presente regulamento deve aplicar-se aos prestadores de serviços de comunicações eletrónicas, aos

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

Or. en

Alteração 65
Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 8

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

Or. en

Alteração 66
Jan Philipp Albrecht

Proposta de regulamento
Considerando 8

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

Or. en

Justificação

Alinhamento com o Regulamento Geral sobre a Proteção de Dados.

Alteração 67
Curzio Maltese

Proposta de regulamento
Considerando 8

Texto da Comissão	*Alteração*
(8) O presente regulamento deve aplicar-se aos prestadores de serviços de comunicações eletrónicas, aos fornecedores de listas acessíveis ao público e aos fornecedores de software que permita comunicações eletrónicas, incluindo a recuperação e a apresentação de informações na Internet. Deve aplicar-se igualmente às pessoas singulares e coletivas que utilizam serviços de comunicações eletrónicas para enviar comunicações comerciais diretas ou	(8) O presente regulamento deve aplicar-se aos prestadores de serviços de comunicações eletrónicas, aos fornecedores de listas acessíveis ao público e aos fornecedores de software que permita comunicações eletrónicas, incluindo a recuperação e a apresentação de informações na Internet. Deve aplicar-se igualmente às pessoas singulares e coletivas que utilizam serviços de comunicações eletrónicas para enviar comunicações comerciais diretas ou

recolher informações relacionadas com equipamentos terminais dos utilizadores finais ou neles armazenadas.	recolher informações relacionadas com equipamentos terminais dos utilizadores finais ou neles armazenadas***, ou para utilizar as capacidades de tratamento desses equipamentos terminais***.

Or. en

Justificação

O amplo âmbito de aplicação do presente regulamento deve incluir claramente uma limitação da forma como as capacidades de tratamento dos equipamentos terminais dos utilizadores finais podem ser utilizadas. A presente formulação do considerando não é clara sobre este ponto.

Alteração 68
Inese Vaidere

Proposta de regulamento
Considerando 8

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

Or. en

Alteração 69
Jan Philipp Albrecht

Proposta de regulamento
Considerando 9

Texto da Comissão	*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.	(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. ***Tal deve acontecer independentemente de as comunicações eletrónicas estarem ou não associadas a um pagamento.***

Or. en

Justificação

Alinhamento com o Regulamento Geral sobre a Proteção de Dados.

Alteração 70
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Liisa Jaakonsaari, Kerstin Westphal, Marc Tarabella, Josef Weidenholzer

Proposta de regulamento
Considerando 9

Texto da Comissão	*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	(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.

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 acontecer independentemente de as comunicações eletrónicas estarem ou não associadas a um pagamento.***

Or. en

Alteração 71
Jan Philipp Albrecht

Proposta de regulamento
Considerando 11

Texto da Comissão	*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 Eletrónicas[24]]***. 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	(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. ***O presente regulamento visa*** assegurar uma proteção eficaz e equitativa dos utilizadores finais aquando da utilização de serviços funcionalmente equivalentes, ***a fim de garantir*** a ***confidencialidade das suas*** comunicações***, independentemente*** do ***meio tecnológico escolhido***. 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

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, por exemplo, as mensagens internas, os fluxos de notícias, os prazos e outras funções similares dos serviços em linha, através dos quais são trocadas mensagens com outros utilizadores dentro ou fora do âmbito desse*** serviço; 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)].

Or. en

Alteração 72
Eva Maydell

Proposta de regulamento
Considerando 11

Texto da Comissão	*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	(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 Eletrónicas[24]]. 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.***	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 Eletrónicas[24]]. 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.
[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)].

Or. en

Alteração 73
Sabine Verheyen

Proposta de regulamento
Considerando 12

Texto da Comissão	*Alteração*
(12) As máquinas e dispositivos conectados comunicam cada vez mais entre si mediante a utilização de redes de comunicações eletrónicas (Internet das	***Suprimido***

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

Or. de

Alteração 74
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 12

Texto da Comissão	*Alteração*
(12) As máquinas e dispositivos conectados comunicam cada vez mais entre si mediante a utilização de redes de comunicações eletrónicas (Internet das Coisas). A transmissão de comunicações máquina-máquina implica o envio de sinais através de uma rede e, por conseguinte, constitui normalmente um serviço de comunicações eletrónicas. A fim de assegurar a plena proteção dos direitos à privacidade e à confidencialidade das comunicações, e para promover uma Internet das Coisas segura e de confiança no mercado único	***Suprimido***

digital, é necessário esclarecer que o presente regulamento deve aplicar-se à transmissão de comunicações máquina-máquina. Por conseguinte, o princípio da confidencialidade consagrado no presente regulamento deve aplicar-se igualmente à transmissão de comunicações deste tipo. Podem também ser adotadas salvaguardas específicas ao abrigo da legislação setorial, como por exemplo a Diretiva 2014/53/UE.

Or. en

Alteração 75
Eva Maydell, Antonio López-Istúriz White, Antanas Guoga

Proposta de regulamento
Considerando 12

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

se deve aplicar às comunicações máquina-máquina que não são oferecidas como um serviço que é dirigido ao público em geral. Ademais, o fornecimento de plataformas máquina-máquina não deve ser considerado um serviço de comunicações eletrónicas somente pela inclusão de outro serviço que não seja a simples transmissão de dados de comunicação (por exemplo, a recolha e disponibilização de dados máquina-máquina para os utilizadores finais, através de (i) uma plataforma, (ii) de uma oferta de funções para analisar os dados máquina-máquina a partir da plataforma, ou (iii) de uma transferência de sinais para fazer funcionar e controlar as máquinas a partir da plataforma).

Or. en

Alteração 76
Jan Philipp Albrecht

Proposta de regulamento
Considerando 12

Texto da Comissão	*Alteração*
(12) As máquinas e dispositivos conectados comunicam cada vez mais entre si mediante a utilização de redes de comunicações eletrónicas (Internet das Coisas). A transmissão de comunicações máquina-máquina implica o envio de sinais através de uma rede e, por conseguinte, constitui normalmente um serviço de comunicações eletrónicas. A fim de assegurar a plena proteção dos direitos à privacidade e à confidencialidade das comunicações, e para promover uma Internet das Coisas segura e de confiança no mercado único digital, é necessário esclarecer que o presente regulamento deve aplicar-se à transmissão de comunicações máquina-máquina. Por conseguinte, o	(12) As máquinas e dispositivos conectados comunicam cada vez mais entre si mediante a utilização de redes de comunicações eletrónicas (Internet das Coisas). A transmissão de comunicações máquina-máquina implica o envio de sinais através de uma rede e, por conseguinte, constitui normalmente um serviço de comunicações eletrónicas. A fim de assegurar a plena proteção dos direitos à privacidade e à confidencialidade das comunicações, e para promover uma Internet das Coisas segura e de confiança no mercado único digital, é necessário esclarecer que o presente regulamento deve aplicar-se à transmissão de comunicações máquina-máquina. ***No âmbito das cadeias***

princípio da confidencialidade consagrado no presente regulamento deve aplicar-se igualmente à transmissão de comunicações deste tipo. Podem também ser adotadas salvaguardas específicas ao abrigo da legislação setorial, como por exemplo a Diretiva 2014/53/UE.

de abastecimento automatizado e em qualquer outro ponto do contexto industrial e de produção, a comunicação por parte das máquinas envolvidas pode não ser interpessoal e pode não envolver pessoas singulares. Porém, continua a ser necessário proteger a sua confidencialidade, no sentido de proteger as informações comerciais internas. Por conseguinte, o princípio da confidencialidade consagrado no presente regulamento deve aplicar-se igualmente à transmissão de comunicações deste tipo. Podem também ser adotadas salvaguardas específicas ao abrigo da legislação setorial, como por exemplo a Diretiva 2014/53/UE.

Or. en

Alteração 77
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 13

Texto da Comissão	*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 e hospitais. Uma vez que essas redes de comunicações são disponibilizadas ***a um grupo indefinido de*** utilizadores ***finais***, a confidencialidade das comunicações transmitidas através dessas redes deve ser protegida. O facto de os serviços de comunicações eletrónicas sem fios poderem ser acessórios de outros serviços não deve impedir a proteção da confidencialidade dos dados das	(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, ***por exemplo, em*** grandes armazéns, centros comerciais e hospitais***, bem como aeroportos, transportes públicos, hotéis e restaurantes. Essas zonas de Internet sem fios podem exigir um início de sessão ou uma senha, podendo igualmente ser fornecidas pelas administrações públicas***. Uma vez que essas redes de comunicações são disponibilizadas ***aos*** utilizadores, a confidencialidade das comunicações

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***.

transmitidas através dessas redes deve ser protegida. O facto de os serviços de comunicações eletrónicas sem fios poderem ser acessórios de outros serviços não deve impedir a proteção da confidencialidade dos dados das comunicações e a aplicação do presente regulamento. Por conseguinte, o presente regulamento deve aplicar-se aos dados de comunicações eletrónicas que utilizam serviços de comunicações eletrónicas e redes de comunicações públicas. ***Além disso, o presente regulamento deve aplicar-se aos perfis privados de redes sociais e aos grupos que o utilizador tenha restringido ou definido como privados.*** Em contrapartida, não deve ser aplicável a grupos fechados de utilizadores finais, tais como redes ***intranet*** de empresas, cujo acesso é limitado aos membros ***de uma organização***.

Or. en

Alteração 78
Jan Philipp Albrecht

Proposta de regulamento
Considerando 13

Texto da Comissão	*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 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	(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 ***acesso à*** Internet sem fios situadas em locais diferentes de uma cidade, grandes armazéns, centros comerciais***, hospitais, aeroportos, hotéis*** e ***restaurantes. Essas zonas de acesso á Internet podem exigir um início de sessão ou providenciar uma senha, podendo igualmente ser fornecidas pelas administrações públicas, incluindo***

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***.

órgãos e agências da União Europeia. Uma vez que essas redes de comunicações são disponibilizadas ***aos*** utilizadores, a confidencialidade das comunicações transmitidas através dessas redes deve ser protegida. O facto de os serviços de comunicações eletrónicas sem fios poderem ser acessórios de outros serviços não deve impedir a proteção da confidencialidade dos dados das comunicações e a aplicação do presente regulamento. Por conseguinte, o presente regulamento deve aplicar-se aos dados de comunicações eletrónicas que utilizam serviços de comunicações eletrónicas e redes de comunicações públicas. ***O presente regulamento deve aplicar-se igualmente aos perfis privados de redes sociais e aos grupos que os utilizadores tenham definido como privados.*** Em contrapartida, não deve ser aplicável a grupos fechados de utilizadores finais, tais como redes de empresas, cujo acesso é limitado aos membros da ***organização***.

Or. en

Alteração 79
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 13

Texto da Comissão	*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 e hospitais. Uma vez que essas redes de comunicações são disponibilizadas a um grupo indefinido de	(13) O desenvolvimento de tecnologias sem fios rápidas e eficientes permitiu que o público dispusesse de um acesso crescente à Internet através de redes sem fios abertas a todos em espaços públicos e semiprivados, como zonas de Internet sem fios situadas em locais diferentes de uma cidade, grandes armazéns, centros comerciais e hospitais. Uma vez que essas redes de comunicações são disponibilizadas a um grupo indefinido de

utilizadores finais, a confidencialidade das comunicações transmitidas através dessas redes deve ser protegida. O ***facto*** de ***os*** serviços de comunicações eletrónicas ***sem fios poderem ser acessórios*** de ***outros*** serviços não deve ***impedir*** a ***proteção da confidencialidade dos dados das comunicações e*** a ***aplicação*** do ***presente regulamento. Por conseguinte, o presente regulamento deve aplicar-se aos dados de comunicações eletrónicas que utilizam serviços de comunicações eletrónicas e redes de comunicações públicas. Em contrapartida,*** não deve ser aplicável a grupos fechados de utilizadores finais, tais como redes de empresas, cujo acesso é limitado aos membros da sociedade.

utilizadores finais, a confidencialidade das comunicações transmitidas através dessas redes deve ser protegida. O ***presente regulamento deve aplicar-se aos dados*** de ***comunicações eletrónicas que utilizam*** serviços de comunicações eletrónicas ***acessíveis ao público e redes*** de ***comunicações públicas. Neste contexto, «acessíveis ao público» refere-se somente aos*** serviços ***destinados aos consumidores.*** Não deve ***incluir serviços destinados*** a ***utilizadores empresariais, nem os meios utilizados para*** a ***prestação*** do ***serviço em questão***, ***quer seja ou não através da rede*** de ***Internet pública, devem ter qualquer influência sobre a determinação*** de ***o serviço ser acessível ou não ao público***. ***O presente regulamento*** não deve ser aplicável a grupos fechados de utilizadores finais, tais como redes de empresas, cujo acesso é limitado aos membros da sociedade.

Or. en

Alteração 80
Curzio Maltese

Proposta de regulamento
Considerando 13

Texto da Comissão	*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 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	(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 ***aos*** utilizadores finais, a confidencialidade das comunicações transmitidas através dessas redes deve ser

redes deve ser protegida. O facto de os serviços de comunicações eletrónicas sem fios poderem ser acessórios de outros serviços não deve impedir a proteção da confidencialidade dos dados das comunicações e a aplicação do presente regulamento. Por conseguinte, o presente regulamento deve aplicar-se aos dados de comunicações eletrónicas que utilizam serviços de comunicações eletrónicas e redes de comunicações públicas***. Em contrapartida***, ***não deve ser aplicável a grupos fechados*** de ***utilizadores finais, tais como*** redes ***de empresas, cujo acesso é limitado aos membros da sociedade***.	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, ***independentemente do facto*** de ***estes serviços e*** redes ***se encontrarem ou não acessíveis ao público***.

Or. en

Justificação

Services not publicly available are excluded from the scope of telecommunications regulations for reasons specific to such regulations (for instance, it would be unjustified to impose access obligations on networks not publicly available). However, this distinction is irrelevant as regards the confidentiality of communications: all communications should be protected equally irrespective of end-users' location. Therefore, electronic communications services which are not publicly available should remain within the scope of this regulation.

Otherwise, excluding them from this scope would allow companies to monitor how their employees are using their access to the network, which is unacceptable: companies only need to assess the work done by their employees, not to monitor each of their actions.

Alteração 81
Kaja Kallas, Dita Charanzová

Proposta de regulamento
Considerando 13

Texto da Comissão	*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	(13) O desenvolvimento de tecnologias sem fios rápidas e eficientes permitiu que o público dispusesse de um acesso crescente à Internet através de redes sem fios abertas a todos em espaços públicos e semiprivados, como zonas de Internet sem fios situadas em locais diferentes de uma

cidade, grandes armazéns, centros comerciais e hospitais. Uma vez que essas redes de comunicações são disponibilizadas a um grupo indefinido de utilizadores finais, a confidencialidade das comunicações transmitidas através dessas redes deve ser protegida. O facto de os serviços de comunicações eletrónicas sem fios poderem ser acessórios de outros serviços não deve impedir a proteção da confidencialidade dos dados das comunicações e a aplicação do presente regulamento. Por conseguinte, o presente regulamento deve aplicar-se aos dados de comunicações eletrónicas que utilizam serviços de comunicações eletrónicas e redes de comunicações públicas. Em contrapartida, não deve ser aplicável a grupos fechados de utilizadores finais, tais como redes de empresas, cujo acesso é limitado aos membros da sociedade.	cidade, grandes armazéns, centros comerciais e hospitais. Uma vez que essas redes de comunicações são disponibilizadas a um grupo indefinido de utilizadores finais, a confidencialidade das comunicações transmitidas através dessas redes deve ser protegida. O facto de os serviços de comunicações eletrónicas sem fios poderem ser acessórios de outros serviços não deve impedir a proteção da confidencialidade dos dados das comunicações e a aplicação do presente regulamento. Por conseguinte, o presente regulamento deve aplicar-se aos dados de comunicações eletrónicas que utilizam serviços de comunicações eletrónicas e redes de comunicações públicas. Em contrapartida, não deve ser aplicável a grupos fechados de utilizadores finais, tais como redes de empresas, cujo acesso é limitado aos membros da sociedade. ***Não se deve considerar que o mero pedido de introdução de uma palavra-passe permite o acesso a um grupo fechado de utilizadores finais quando se trata de disponibilizar o acesso a um grupo indefinido de utilizadores finais.***
	Or. en

Alteração 82
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 14

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

Or. en

Alteração 83
Jan Philipp Albrecht

Proposta de regulamento
Considerando 14

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

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 específicos, como, por exemplo, a localização do equipamento terminal a partir do qual foi realizada uma chamada telefónica ou uma ligação à Internet ou o acesso a uma zona de Internet sem fios a que um dispositivo esteja conectado. Deverá igualmente incluir os dados necessários para identificar os equipamentos terminais dos utilizadores e os dados emitidos por equipamentos terminais na procura de pontos de acesso ou de outros equipamentos.*** 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 eletrónicas e, por conseguinte, ser sujeitos às disposições do presente regulamento. Os metadados de comunicações eletrónicas podem incluir informações que façam parte da subscrição do serviço se essas informações forem tratadas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas. ***A exclusão de serviços de fornecimento de «conteúdos transmitidos através de redes de comunicações eletrónicas» da definição de «serviço de comunicações eletrónicas», constante do artigo 4.º do presente regulamento, não significa que os fornecedores de serviços que disponibilizam serviços de comunicações eletrónicas e serviços de conteúdos estejam fora do âmbito de aplicação das disposições do regulamento que se aplica***

aos fornecedores de serviços de comunicações eletrónicas.

Or. en

Alteração 84
Curzio Maltese

Proposta de regulamento
Considerando 14

Texto da Comissão	*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. 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 eletrónicas e, por conseguinte, ser sujeitos às disposições do presente regulamento. Os metadados de comunicações eletrónicas podem incluir informações que façam parte da subscrição do serviço se essas informações forem tratadas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas.	(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 comunicações eletrónicas***, do ponto de vista dos fornecedores de acesso à Internet*** e, por conseguinte, ser sujeitos às disposições do presente regulamento***. Os dados gerados, tratados ou transmitidos por serviços de comunicações interpessoais para fins de envio, transmissão ou receção de tais comunicações devem ser considerados***

metadados de comunicações eletrónicas, do ponto de vista dos fornecedores desses serviços, mas devem também ser considerados conteúdos de comunicações eletrónicas, do ponto de vista dos fornecedores de acesso à Internet. Os metadados de comunicações eletrónicas podem incluir informações que façam parte da subscrição do serviço se essas informações forem tratadas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas.

Or. en

Justificação

A definição de «metadados» depende do nível da rede em que é considerado. No terceiro nível («transmissão» — ver o modelo OSI https://en.wikipedia.org/wiki/OSI_model), os metadados e os conteúdos tratados por OTT num nível superior («pedido» e «conteúdo») são transmitidos em conjunto em pacotes TCP/IP. Os operadores de telecomunicações não estabelecem qualquer distinção entre os metadados e os conteúdos tratados por serviços OTT. Do ponto de vista dos operadores, estes dados representam o «conteúdo» transmitidos na rede.

O considerando deve proceder a este esclarecimento técnico.

Alteração 85
Jan Philipp Albrecht

Proposta de regulamento
Considerando 14-A (novo)

Texto da Comissão	*Alteração*
	1(4-A) Os serviços modernos de comunicações eletrónicas, nomeadamente a Internet e os serviços que funcionam com base nela, funcionam de acordo com uma lógica de separação de níveis de protocolos e de serviços, tal como definido pelo modelo OSI (Open Systems Interconnection, ISO/IEC 7498-1). Por exemplo, um pacote de dados Internet (TCP/IP) está integrado num pacote subjacente de dados Ethernet ou sem fios

para o encaminhamento local. Num nível superior, uma mensagem de correio eletrónico, incluindo o conteúdo e os metadados, está integrada num ou em diversos pacotes de dados TCP/IP. A mensagem de correio eletrónico, por sua vez, é composta por metadados que utilizam o protocolo SMTP e por dados de conteúdo no corpo da mensagem. Isto significa que os metadados num nível de protocolo representam geralmente dados de conteúdo para os níveis inferiores. Nos casos em que o presente regulamento estabeleça normas distintas para o tratamento de conteúdos e de metadados, tal deve ser entendido para o serviço respetivo de comunicações eletrónicas e o nível de protocolo em que se encontra a funcionar. Um fornecedor de acesso à Internet, por exemplo, não deve, por conseguinte, analisar o conteúdo dos pacotes TCP/IP encaminhados, no sentido de detetar remetentes de mensagens de correio eletrónico ou de anexos maliciosos, porque, para o nível de Internet, as mensagens de correio eletrónico são constituídas inteiramente por conteúdo. Porém, a análise de mensagens de correio eletrónico pode ser feita pelo fornecedor do serviço de correio eletrónico se tal for necessário para a segurança do serviço ou se o utilizador o solicitar expressamente.

Or. en

Justificação

Esta alteração explica o aditamento às definições de «conteúdos» e «metadados» no artigo 4.º.

Alteração 86
Jan Philipp Albrecht

Proposta de regulamento
Considerando 15

Texto da Comissão	*Alteração*
(15) Os dados das comunicações eletrónicas devem ser tratados como dados confidenciais. Isto significa que qualquer interferência com a transmissão de dados de comunicações eletrónicas, seja diretamente por intervenção humana ou através de tratamento automatizado por máquinas, sem o consentimento de todas as partes comunicantes deve ser proibida. A proibição ***da interceção*** de dados de comunicações deve ser aplicável durante o seu envio, ***ou seja***, ***até à receção*** do ***conteúdo da comunicação eletrónica pelo destinatário desejado***. A interceção de dados de comunicações eletrónicas pode ocorrer, por exemplo, quando alguém, que não as partes comunicantes, ouve as chamadas, lê, digitaliza ou armazena o conteúdo das comunicações eletrónicas, ou os metadados associados, para fins que não a troca de comunicações. A interceção ocorre também quando terceiros controlam os sítios web visitados, o calendário das visitas, a interação com outros, etc., sem o consentimento do utilizador ***final*** em causa. À medida que a tecnologia evoluiu, os meios técnicos para proceder à interceção também multiplicaram. Esses meios podem incluir desde a instalação de equipamento que reúne dados provenientes de equipamentos terminais em zonas específicas, tais como os chamados intercetores de IMSI (Identidade Internacional de Assinante Móvel), aos programas e técnicas que, por exemplo, monitorizam sub-repticiamente os hábitos de navegação na Internet para criar perfis de utilizador final. Outros exemplos de interceção incluem a captação de dados sobre a carga útil ou o conteúdo provenientes de redes sem fios não encriptadas e roteadores, incluindo os hábitos de navegação na Internet, sem o consentimento dos utilizadores ***finais***.	(15) Os dados das comunicações eletrónicas devem ser tratados como dados confidenciais. Isto significa que qualquer ***tratamento dos dados das comunicações eletrónicas ou 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. ***Quando o tratamento é permitido no âmbito do presente regulamento, qualquer outro tratamento com base no artigo 6.º do Regulamento (UE) n.º 2016/679 deve ser considerado proibido, incluindo o tratamento para outros fins com base no artigo 6.º, n.º 4, do referido regulamento. Tal não deve impedir eventuais pedidos de consentimento adicional para novas operações de tratamento.*** A proibição ***do tratamento*** de dados de comunicações deve ser aplicável durante o seu envio ***e no momento em que são posteriormente armazenados***, ***a fim de refletir a tendência crescente de que os utilizadores finais não armazenam todos os dados das comunicações no seu próprio equipamento terminal, mas recorrem a espaço de armazenamento com base na nuvem,*** do ***prestador de serviços de comunicações ou de outras partes***. 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 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, ***assim como a análise dos dados relativos ao tráfego dos clientes,*** incluindo os hábitos de navegação na Internet, sem o consentimento dos utilizadores.

Or. en

Alteração 87
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Josef Weidenholzer

Proposta de regulamento
Considerando 15

Texto da Comissão	*Alteração*
(15) ***Os dados das*** comunicações eletrónicas devem ser ***tratados*** como ***dados*** confidenciais. Isto significa que qualquer interferência com ***a transmissão de dados de*** comunicações eletrónicas, seja diretamente por intervenção humana ou através de tratamento automatizado por máquinas, sem o consentimento de todas as partes comunicantes deve ser proibida. A proibição da interceção de ***dados de*** comunicações deve ser aplicável durante o seu envio, ou seja, até à receção do conteúdo da comunicação eletrónica pelo destinatário desejado. A interceção de	(15) ***As*** comunicações eletrónicas devem ser ***tratadas*** como confidenciais. Isto significa que qualquer interferência com ***as*** 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. ***Quando o tratamento é permitido mediante exceção às proibições previstas no presente regulamento, qualquer outro tratamento nos termos do artigo 6.º do Regulamento (UE) n.º 2016/679 deve ser considerado proibido, incluindo o tratamento para***

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***.

outros fins nos termos do artigo 6.º, n.º 4, do referido regulamento. Isso não deve impedir eventuais pedidos de consentimento adicional para novas operações de tratamento. A proibição da interceção de comunicações deve ser ***igualmente*** aplicável durante o seu envio, ou seja, até à receção do conteúdo da comunicação eletrónica pelo destinatário desejado***, e a quaisquer ficheiros temporários na rede após a receção***. 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 ***outra parte controla*** os sítios web visitados, o calendário das visitas, a interação com outros, etc., sem o consentimento do utilizador em causa. À medida que a tecnologia evoluiu, os meios técnicos para proceder à interceção também ***se*** 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. 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, ***assim como a análise dos dados relativos ao tráfego dos utilizadores,*** incluindo os hábitos de navegação na Internet, sem o consentimento dos utilizadores.

Or. en

Alteração 88
Curzio Maltese

Proposta de regulamento
Considerando 15

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

provenientes de redes sem fios não encriptadas e roteadores, incluindo os hábitos de navegação na Internet, sem o consentimento dos utilizadores finais.	de utilizador final. Outros exemplos de ***interferência*** 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.

Or. en

Justificação

Na sua versão atual, o presente considerando pode limitar o âmbito de aplicação do artigo 5.º às interferências que ocorrem apenas durante a transmissão das comunicações. Esta seria uma forma de impedir a proteção dos dados de comunicações antes e após a transmissão. Assim, este considerando carece de clarificação.

Alteração 89
Jan Philipp Albrecht

Proposta de regulamento
Considerando 16

Texto da Comissão	*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.	(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. 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 ***relacionadas com o respetivo serviço ou*** o tratamento dos metadados ***do serviço em causa*** para assegurar a necessária qualidade dos serviços, em termos de controlo de latência, instabilidade, etc.

Or. en

Alteração 90
Eva Maydell, Antonio López-Istúriz White, Antanas Guoga, Roberta Metsola

Proposta de regulamento
Considerando 16

Texto da Comissão	*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.	(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. ***Deve ser incentivado o tratamento de dados anónimos pelos prestadores e a respetiva anonimização, já que este último ato reduz consideravelmente o risco contra a privacidade e a segurança associado ao processamento de dados relacionados com a transmissão. O presente regulamento também*** não deve proibir o tratamento de dados de comunicações eletrónicas para garantir a segurança***, confidencialidade, integridade, disponibilidade, autenticidade*** e continuidade dos serviços ***e das redes*** de comunicações eletrónicas, incluindo a verificação das ameaças à segurança, tais como a presença de programas maliciosos, ***ou*** o tratamento dos metadados para assegurar a necessária qualidade dos serviços, em termos de controlo de latência, instabilidade, etc.

Or. en

Alteração 91
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 16

Texto da Comissão	*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.	(16) A proibição de armazenamento das comunicações ***durante a transmissão*** 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. ***Deve ser incentivado o tratamento de dados sob pseudónimo, já que este último ato reduz consideravelmente o risco contra a privacidade e segurança associado ao processamento de dados relacionados com a transmissão.*** 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 ***devida*** qualidade dos serviços, em termos de controlo de latência, instabilidade, etc.
	Or. en

Alteração 92
Sabine Verheyen

Proposta de regulamento
Considerando 16

Texto da Comissão	*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	(16) A proibição de armazenamento das comunicações ***durante o envio*** 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.	dos metadados para assegurar a necessária qualidade dos serviços, em termos de controlo de latência, instabilidade, etc.

Or. de

Alteração 93
Eva Maydell, Pascal Arimont, Antanas Guoga, Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 16-A (novo)

Texto da Comissão	*Alteração*
	(16-A) O Regulamento n.º 2016/679 reconhece explicitamente a necessidade de dispensar uma proteção adicional às crianças, já que estas podem estar menos cientes dos riscos e consequências associados ao tratamento dos seus dados pessoais. O presente regulamento deve igualmente conceder especial atenção à proteção da privacidade das crianças. Elas contam-se entre os utilizadores mais ativos da Internet e deve ser proibida a sua exposição à definição de perfis e técnicas de publicidade comportamental direcionada.

Or. en

Alteração 94
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Josef Weidenholzer

Proposta de regulamento
Considerando 17

Texto da Comissão	*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,***	(17) O tratamento dos dados de comunicações eletrónicas pode ser útil para as empresas, consumidores e sociedade em geral. Os exemplos de ***tais utilizações*** dos

o presente regulamento alarga as possibilidades de tratamento de metadados das comunicações eletrónicas pelos prestadores de serviços de comunicações eletrónicas, com base no consentimento do utilizador final. No entanto, os utilizadores finais conferem grande importância à confidencialidade das suas comunicações, incluindo as suas atividades em linha, e desejam controlar a utilização dos dados das comunicações eletrónicas para fins diferentes do envio de comunicação. Por conseguinte, o presente regulamento deve exigir que os prestadores de serviços de comunicações eletrónicas obtenham o consentimento dos utilizadores finais para procederem ao tratamento dos metadados de comunicações eletrónicas. Os dados de localização que são gerados fora do contexto de uma comunicação não devem ser considerados metadados. Os exemplos de ***utilizações comerciais*** dos metadados das comunicações eletrónicas por prestadores de serviços de comunicações eletrónicas podem incluir o fornecimento de mapas térmicos (heatmaps); uma representação gráfica dos dados utilizando cores para indicar a presença de pessoas. Para apresentar os movimentos de tráfego em certas direções durante um determinado período de tempo é necessário um identificador para estabelecer a ligação entre as posições das pessoas em certos intervalos de tempo***. Este identificador seria omisso se fossem utilizados dados anónimos e esse movimento não poderia ser visto***. Essa utilização de metadados de comunicações eletrónicas pode, por exemplo, ajudar as autoridades públicas e os operadores de transporte coletivo a definirem onde desenvolver novas infraestruturas, com base na utilização e na pressão sobre a estrutura existente. ***Sempre que um tipo de tratamento de metadados de comunicações eletrónicas, nomeadamente que utilize novas tecnologias, e tendo em conta a natureza,***

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***, desde que os dados sejam imediatamente anonimizados ou sejam utilizadas técnicas de anonimização em que o utilizador é misturado com outros***. 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.

o âmbito de aplicação, o contexto e as finalidades do tratamento, seja suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares, deve realizar-se uma avaliação de impacto sobre a proteção dos dados e, se for caso disso, uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) n.º 2016/679.

Or. en

Alteração 95
Curzio Maltese

Proposta de regulamento
Considerando 17

Texto da Comissão	*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***	(17) O tratamento dos dados de comunicações eletrónicas pode ser útil para as empresas, consumidores e sociedade em geral. 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 ***das*** comunicações eletrónicas***,*** que devem incluir dados ***sobre*** a ***localização do dispositivo gerados*** para ***fins*** de ***concessão*** e ***manutenção*** de ***acesso*** e de ***ligação ao serviço***. 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

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

finalidades do tratamento, seja suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares, deve realizar-se uma avaliação de impacto sobre a proteção dos dados e, se for caso disso, uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) n.º 2016/679.

Or. en

Justificação

Os dados de localização são altamente sensíveis, em especial porque permitem uma das maiores formas de vigilância. Devem beneficiar do nível de proteção mais elevado.

Alteração 96

Jan Philipp Albrecht

Proposta de regulamento
Considerando 17

Texto da Comissão	*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 omisso se fossem utilizados dados anónimos e esse movimento não poderia ser visto.*** Essa	(17) O tratamento dos dados de comunicações eletrónicas pode ser útil para as empresas, consumidores e sociedade em geral. 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 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 ***pode ser*** necessário um identificador para estabelecer a ligação entre as posições das pessoas em certos intervalos de tempo. 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 ***seja previsto o*** tratamento de ***dados*** de comunicações eletrónicas, 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

utilização de metadados de comunicações eletrónicas pode, por exemplo, ajudar as autoridades públicas e os operadores de transporte coletivo a definirem onde desenvolver novas infraestruturas, com base na utilização e na pressão sobre a estrutura existente. Sempre que ***um tipo de*** tratamento de ***metadados*** de comunicações eletrónicas***, nomeadamente que utilize novas tecnologias, e tendo em conta a natureza, o âmbito de aplicação, o contexto e as finalidades do tratamento, seja suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares***, deve realizar-se uma avaliação de impacto sobre a proteção dos dados e, se for caso disso, uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) n.º 2016/679.

conformidade com os artigos 35.º e 36.º do Regulamento (UE) n.º 2016/679.

Or. en

Alteração 97
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 17

Texto da Comissão	*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	(17) O tratamento dos ***metadados*** 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, ***em conformidade*** com ***o artigo 6.°, n.° 1 e n.° 4,*** do ***Regulamento (UE) n.º 2016/679***. 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

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

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 ***respeitem*** o ***Regulamento (UE) n.° 2016/679 ao procederem ao tratamento dos metadados de comunicações eletrónicas, que deve incluir dados sobre a localização do dispositivo. A título de exceção à obtenção do*** consentimento dos utilizadores finais***, o*** tratamento ***de*** metadados de comunicações eletrónicas ***para outros fins que não aqueles para os quais os dados pessoais foram inicialmente recolhidos, deve ser permitido nos casos em que o tratamento posterior seja compatível, em conformidade com o artigo 6.º, n.º 4, do Regulamento (UE) n.º 2016/679***. Os dados de localização que são gerados fora do contexto de uma comunicação não devem ser considerados metadados. Os exemplos de utilizações comerciais dos metadados das comunicações eletrónicas por prestadores de serviços de comunicações eletrónicas podem incluir o fornecimento de mapas térmicos (heatmaps); uma representação gráfica dos dados utilizando cores para indicar a presença de pessoas. Para apresentar os movimentos de tráfego em certas direções durante um determinado período de tempo é necessário um identificador para estabelecer a ligação entre as posições das pessoas em certos intervalos de tempo. Este identificador seria omisso se fossem utilizados dados anónimos e esse movimento não poderia ser visto***. Por conseguinte, sempre que não se possa alcançar a(s) finalidade(s) do tratamento posterior dos dados através do tratamento de dados que é feita de forma anónima, deve ser permitida a apresentação de dados sob pseudónimo***. Essa utilização de metadados de comunicações eletrónicas pode, por exemplo, ajudar as autoridades públicas e os operadores de transporte coletivo a definirem onde desenvolver novas

infraestruturas, com base na utilização e na pressão sobre a estrutura existente. Sempre que um tipo de tratamento de metadados de comunicações eletrónicas, nomeadamente que utilize novas tecnologias, e tendo em conta a natureza, o âmbito de aplicação, o contexto e as finalidades do tratamento, seja suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares, deve realizar-se uma avaliação de impacto sobre a proteção dos dados e, se for caso disso, uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) n.º 2016/679.

Or. en

Alteração 98
Sabine Verheyen

Proposta de regulamento
Considerando 17

Texto da Comissão	*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	(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, ***em conformidade com o Regulamento (UE) n.º 2016/679***. 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 ***procedam, em conformidade com o Regulamento (UE) n.º 2016/679,*** ao tratamento dos metadados de

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

Or. de

Alteração 99
Andreas Schwab

Proposta de regulamento
Considerando 17

Texto da Comissão	*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 omisso se fossem utilizados dados anónimos e esse movimento não poderia ser visto. Essa utilização de metadados de comunicações eletrónicas pode, por exemplo, ajudar as autoridades públicas e	(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, ***em conformidade com o Regulamento (UE) n.º 2016/679***. 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 ***cumpram os requisitos estabelecidos pelo Regulamento (UE) n.º 2016/679*** para procederem ao tratamento dos metadados de comunicações eletrónicas***, que devem incluir dados sobre a localização do dispositivo gerados para fins de concessão e manutenção de acesso e ligação ao serviço***. Os dados de localização que são gerados fora do contexto ***da prestação*** de ***serviços de*** 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

os operadores de transporte coletivo a definirem onde desenvolver novas infraestruturas, com base na utilização e na pressão sobre a estrutura existente. Sempre que um tipo de tratamento de metadados de comunicações eletrónicas, nomeadamente que utilize novas tecnologias, e tendo em conta a natureza, o âmbito de aplicação, o contexto e as finalidades do tratamento, seja suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares, deve realizar-se uma avaliação de impacto sobre a proteção dos dados e, se for caso disso, uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) n.º 2016/679.	seria omisso se fossem utilizados dados anónimos e esse movimento não poderia ser visto. Essa utilização de metadados de comunicações eletrónicas pode, por exemplo, ajudar as autoridades públicas e os operadores de transporte coletivo a definirem onde desenvolver novas infraestruturas, com base na utilização e na pressão sobre a estrutura existente. Sempre que um tipo de tratamento de metadados de comunicações eletrónicas, nomeadamente que utilize novas tecnologias, e tendo em conta a natureza, o âmbito de aplicação, o contexto e as finalidades do tratamento, seja suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares, deve realizar-se uma avaliação de impacto sobre a proteção dos dados e, se for caso disso, uma consulta da autoridade de controlo antes do tratamento, em conformidade com os artigos 35.º e 36.º do Regulamento (UE) n.º 2016/679.
	Or. de

Alteração 100
Jan Philipp Albrecht

Proposta de regulamento
Considerando 17-A (novo)

Texto da Comissão	*Alteração*
	(17-A) O presente regulamento alarga as possibilidades de tratamento de metadados das comunicações eletrónicas pelos prestadores de serviços de comunicações eletrónicas, com base no consentimento informado dos utilizadores. No entanto, os utilizadores conferem grande importância à confidencialidade das suas comunicações, incluindo as suas atividades em linha, e desejam controlar a utilização dos seus dados das comunicações eletrónicas para

fins diferentes do envio de comunicação. Por conseguinte, o presente regulamento deve exigir aos prestadores de serviços de comunicações eletrónicas que obtenham o consentimento dos utilizadores finais para procederem ao tratamento dos dados de comunicações eletrónicas. Para efeitos do presente regulamento, o consentimento de um utilizador final deve ter o mesmo significado e estar subordinado às mesmas condições que o consentimento do titular de dados ao abrigo do Regulamento (UE) n.º 2016/679.

Or. en

Alteração 101
Jan Philipp Albrecht

Proposta de regulamento
Considerando 18

Texto da Comissão	*Alteração*
(18) Os utilizadores finais podem consentir o tratamento dos seus ***metadados*** a fim de receberem serviços específicos***, tais*** como serviços de proteção contra ***atividades fraudulentas (através da análise dos dados de utilização**, **da localização e da conta de cliente em tempo real)**. **Na economia digital, os serviços são frequentemente prestados em troca*** de ***uma contrapartida que*** não ***dinheiro, por exemplo, mediante a exposição*** dos ***utilizadores finais a anúncios. Para efeitos do presente regulamento, o consentimento*** de ***um utilizador final, independentemente de este ser uma pessoa singular ou coletiva, deve ter*** o ***mesmo significado e estar subordinado às mesmas condições que o consentimento do titular de dados ao abrigo*** do Regulamento (UE) n.º 2016/679***. Os serviços de acesso à Internet de banda larga básica e de comunicações de voz***	(18) Os utilizadores finais podem consentir o tratamento dos seus ***dados de comunicações eletrónicas*** a fim de receberem serviços específicos ***por eles solicitados,*** como***, por exemplo,*** serviços de proteção contra ***software mal-intencionado, comunicações não solicitadas**, **ou atividades fraudulentas**. **O consentimento para o tratamento de dados de comunicações eletrónicas não será válido se o titular dos dados não dispuser de uma escolha verdadeira e livre, ou não puder recusar nem retirar o consentimento sem ser prejudicado. Tal como prevê o artigo 7.º*** do Regulamento (UE) n.º 2016/679***, o consentimento não é dado*** de ***livre vontade se for exigido*** para ***aceder a qualquer serviço ou for obtido através de pedidos insistentes e reiterados**. **A fim*** de ***impedir tais pedidos abusivos, os utilizadores finais devem poder obrigar os***

devem ser considerados serviços essenciais para que as pessoas sejam capazes de comunicar e participar nos benefícios da economia digital. O consentimento para o tratamento de ***dados provenientes da Internet ou da utilização de comunicações de voz não será válido se o titular dos dados não dispuser*** de ***uma escolha verdadeira ou livre ou*** não ***puder recusar nem retirar o*** consentimento ***sem ser prejudicado.***

prestadores de serviços a memorizar a sua opção de não ***dar*** consentimento***.***

Or. en

Alteração 102
Curzio Maltese

Proposta de regulamento
Considerando 18

Texto da Comissão	*Alteração*
(18) Os utilizadores finais podem consentir o tratamento dos seus ***metadados*** a fim de receberem serviços específicos***, tais como serviços de proteção contra atividades fraudulentas (através da análise dos dados de utilização, da localização e da conta de cliente em tempo real).*** Na economia digital, os serviços são frequentemente prestados em troca de uma contrapartida que não dinheiro, por exemplo, mediante a exposição dos utilizadores finais a anúncios. Para efeitos do presente regulamento, o consentimento de um utilizador final, independentemente de este ser uma pessoa singular ou coletiva, deve ter o mesmo significado e estar subordinado às mesmas condições que o consentimento do titular de dados ao abrigo do Regulamento (UE) n.º 2016/679. ***Os serviços*** de ***acesso à Internet de banda larga básica e de comunicações*** de ***voz devem ser considerados serviços essenciais para que as pessoas sejam capazes de comunicar e participar nos***	(18) Os utilizadores finais podem consentir o tratamento dos seus ***dados*** a fim de receberem serviços específicos Na economia digital, os serviços são frequentemente prestados em troca de uma contrapartida que não dinheiro, por exemplo, mediante a exposição dos utilizadores finais a anúncios. Para efeitos do presente regulamento, o consentimento de um utilizador final, independentemente de este ser uma pessoa singular ou coletiva, deve ter o mesmo significado e estar subordinado às mesmas condições que o consentimento do titular de dados ao abrigo do Regulamento (UE) n.º 2016/679. ***O consentimento para o tratamento de dados não será válido se o titular dos dados não dispuser de uma escolha verdadeira e livre ou não puder recusar nem retirar o consentimento sem ser prejudicado. Tal como previsto no artigo 7.º do Regulamento (UE) n.º 2016/679,*** o consentimento ***não é dado*** de ***livre vontade, se for exigido para aceder a***

benefícios da economia digital. O consentimento ***para o tratamento*** de ***dados provenientes da Internet ou da utilização de comunicações*** de ***voz não será válido se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado***.

qualquer serviço ou se for obtido através de ***pedidos insistentes e reiterados. A fim de impedir tais pedidos abusivos, os utilizadores devem poder obrigar os prestadores de serviços a memorizar a sua opção de não dar consentimento***.

Or. en

Justificação

O consentimento deve ser dado livremente para qualquer tipo de tratamento. O Regulamento geral sobre a proteção de dados não estabelece qualquer distinção entre tratamento de dados. O presente regulamento também não o deve fazer.

Além disso, os utilizadores finais devem ser protegidos contra pedidos intimidatórios conducentes à fadiga e ao consentimento dado de forma não livre.

Alteração 103
Inese Vaidere

Proposta de regulamento
Considerando 18

Texto da Comissão	*Alteração*
(18) Os utilizadores finais podem consentir o tratamento dos seus metadados a fim de receberem serviços específicos, tais como serviços de proteção contra atividades fraudulentas (através da análise dos dados de utilização, da localização e da conta de cliente em tempo real). Na economia digital, os serviços são frequentemente prestados em troca de uma contrapartida que não dinheiro, por exemplo, mediante a exposição dos utilizadores finais a anúncios. Para efeitos do presente regulamento, o consentimento de um utilizador final, independentemente de este ser uma pessoa singular ou coletiva, deve ter o mesmo significado e estar subordinado às mesmas condições que o consentimento do titular de dados ao	(18) Os utilizadores finais podem consentir o tratamento dos seus metadados a fim de receberem serviços específicos, tais como serviços de proteção contra atividades fraudulentas (através da análise dos dados de utilização, da localização e da conta de cliente em tempo real). Na economia digital, os serviços são frequentemente prestados em troca de uma contrapartida que não dinheiro, por exemplo, mediante a exposição dos utilizadores finais a anúncios. Para efeitos do presente regulamento, o consentimento de um utilizador final, independentemente de este ser uma pessoa singular ou coletiva, deve ter o mesmo significado e estar subordinado às mesmas condições que o consentimento do titular de dados ao

abrigo do Regulamento (UE) n.º 2016/679. Os serviços de acesso à Internet de banda larga básica e de comunicações de voz devem ser considerados serviços essenciais para que as pessoas sejam capazes de comunicar e participar nos benefícios da economia digital. O consentimento para o tratamento de dados provenientes da Internet ou da utilização de comunicações de voz não será válido se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.

abrigo do Regulamento (UE) n.º 2016/679. ***O utilizador final deve ser informado sobre a eventual utilização posterior dos seus dados pessoais por terceiros.*** Os serviços de acesso à Internet de banda larga básica e de comunicações de voz devem ser considerados serviços essenciais para que as pessoas sejam capazes de comunicar e participar nos benefícios da economia digital. O consentimento para o tratamento de dados provenientes da Internet ou da utilização de comunicações de voz não será válido se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.

Or. en

Alteração 104
Curzio Maltese

Proposta de regulamento
Considerando 19

Texto da Comissão	*Alteração*
(19) ***O conteúdo*** das comunicações eletrónicas ***inscreve-se*** na essência do direito fundamental ***ao*** respeito pela vida privada e familiar, pelo domicílio e pelas comunicações protegido pelo artigo 7.º da Carta. Qualquer interferência ***no conteúdo*** das comunicações eletrónicas deve ser permitida apenas sob condições muito claramente definidas, para fins específicos e mediante garantias adequadas contra abusos. O presente regulamento prevê a possibilidade de os prestadores de serviços de comunicações eletrónicas tratarem os dados de comunicações eletrónicas em trânsito, com o consentimento informado de todos os utilizadores finais em causa. Por exemplo, os prestadores podem oferecer serviços que impliquem a digitalização das mensagens de correio	(19) ***Os dados*** das comunicações eletrónicas ***inscrevem-se*** na essência do direito fundamental ***do*** respeito pela vida privada e familiar, pelo domicílio e pelas comunicações**,** protegido pelo artigo 7.º da Carta. Qualquer interferência ***nos dados*** das comunicações eletrónicas deve ser permitida apenas sob condições muito claramente definidas, para fins específicos e mediante garantias adequadas contra abusos. O presente regulamento prevê a possibilidade de os prestadores de serviços de comunicações eletrónicas tratarem os dados de comunicações eletrónicas em trânsito, com o consentimento informado de todos os utilizadores finais em causa. Por exemplo, os prestadores podem oferecer serviços que impliquem a digitalização das mensagens de correio

eletrónico para a eliminação de certos materiais pré-definidos. Dado o caráter sensível ***do conteúdo*** das comunicações, o presente regulamento estabelece uma presunção de que o tratamento desses dados ***de conteúdo*** terá como resultado um elevado risco para os direitos e liberdades das pessoas singulares. Aquando do tratamento deste tipo de dados, o prestador do serviço de comunicações eletrónicas deve consultar sempre a autoridade de controlo antes do tratamento. Tal consulta deve estar em conformidade com o artigo 36.º, n.ºs 2 e 3, do Regulamento (UE) n.º 2016/679. ***A presunção não abrange o tratamento de dados de conteúdo para a prestação de um serviço solicitado pelo utilizador final quando este consentiu tal tratamento e o tratamento for efetuado para os fins e duração estritamente necessários e proporcionados para esse serviço. Após o conteúdo*** das comunicações eletrónicas ***ter*** sido ***enviado*** pelo utilizador final e ***recebido*** pelo ou pelos utilizadores finais destinatários, ***pode*** ser ***registado*** ou ***armazenado*** pelo utilizador final, utilizadores finais ou por um terceiro por eles mandatado para registar ou armazenar esses dados. Qualquer tratamento desses dados deve ser conforme com o Regulamento (UE) n.º 2016/679.	eletrónico para a eliminação de certos materiais pré-definidos. Dado o caráter sensível ***dos dados*** das comunicações ***eletrónicas***, o presente regulamento estabelece uma presunção de que o tratamento desses dados terá como resultado um elevado risco para os direitos e liberdades das pessoas singulares. Aquando do tratamento deste tipo de dados, o prestador do serviço de comunicações eletrónicas deve consultar sempre a autoridade de controlo antes do tratamento. Tal consulta deve estar em conformidade com o artigo 36.º, n.ºs 2 e 3, do Regulamento (UE) n.º 2016/679. ***Depois de os*** dados das comunicações eletrónicas ***terem*** sido ***enviados*** pelo utilizador final e ***recebidos*** pelo ou pelos utilizadores finais destinatários, ***podem*** ser ***registados*** ou ***armazenados*** pelo utilizador final, utilizadores finais ou por um terceiro por eles mandatado para registar ou armazenar esses dados. Qualquer tratamento desses dados deve ser conforme com o Regulamento (UE) n.º 2016/679. ***Sempre que os dados das comunicações forem conservados por um terceiro, este último deve encriptar de extremo a extremo qualquer informação cujo tratamento não seja necessário para prestar o serviço solicitado pelo utilizador final.***

Or. en

Justificação

Os conteúdos e os metadados devem beneficiar do mesmo nível de proteção.

Os prestadores devem encriptar as comunicações de extremo a extremo sempre que isso seja tecnicamente viável.

Alteração 105
Jan Philipp Albrecht

Proposta de regulamento

Considerando 19

Texto da Comissão	*Alteração*
(19) O conteúdo das comunicações eletrónicas inscreve-se na essência do direito fundamental ao respeito pela vida privada e familiar, pelo domicílio e pelas comunicações protegido pelo artigo 7.º da Carta. ***Qualquer interferência no*** conteúdo das comunicações eletrónicas deve ser ***permitida*** apenas sob condições muito claramente ***definidas***, para fins específicos e mediante garantias adequadas contra abusos. O presente regulamento prevê a possibilidade de os prestadores de serviços de comunicações eletrónicas tratarem os dados de comunicações eletrónicas em trânsito, com o consentimento informado de todos os utilizadores finais em causa. Por exemplo, os prestadores podem oferecer serviços que impliquem a digitalização das mensagens de correio eletrónico para a eliminação de certos materiais pré-definidos. Dado o caráter sensível ***do conteúdo*** das comunicações, o presente regulamento estabelece uma presunção de que o tratamento desses dados de conteúdo terá como resultado um elevado risco para os direitos e liberdades das pessoas singulares. Aquando do tratamento deste tipo de dados, o prestador do serviço de comunicações eletrónicas deve ***consultar*** sempre a ***autoridade*** de ***controlo antes do tratamento.*** Tal ***consulta deve estar em conformidade com o artigo 36.º, n.ºs 2 e 3, do*** Regulamento (UE) n.º 2016/679***. A presunção não abrange o tratamento de dados de conteúdo para*** a ***prestação*** de ***um serviço solicitado pelo utilizador final quando este consentiu tal tratamento e o*** tratamento ***for efetuado para os fins e duração estritamente necessários e proporcionados para esse serviço***. Após o conteúdo das comunicações eletrónicas ter sido enviado pelo utilizador final e recebido pelo ou pelos utilizadores finais destinatários, pode	(19) O conteúdo das comunicações eletrónicas inscreve-se na essência do direito fundamental ao respeito pela vida privada e familiar, pelo domicílio e pelas comunicações protegido pelo artigo 7.º da Carta. ***Todo o tratamento do*** conteúdo das comunicações eletrónicas deve ser ***permitido*** apenas sob condições ***definidas*** muito claramente, para fins específicos e mediante garantias adequadas contra abusos. O presente regulamento prevê a possibilidade de os prestadores de serviços de comunicações eletrónicas tratarem os dados de comunicações eletrónicas em trânsito, com o consentimento informado de todos os utilizadores finais em causa. Por exemplo, os prestadores podem oferecer serviços que impliquem a digitalização das mensagens de correio eletrónico para a eliminação de certos materiais pré-definidos. Dado o caráter sensível ***dos dados*** das comunicações ***eletrónicas***, o presente regulamento estabelece uma presunção de que o tratamento desses dados de conteúdo terá como resultado um elevado risco para os direitos e liberdades das pessoas singulares. Aquando do tratamento deste tipo de dados, o prestador do serviço de comunicações eletrónicas deve ***proceder*** sempre a ***uma avaliação*** de ***impacto,*** tal ***como previsto no*** Regulamento (UE) n.º 2016/679 ***e, se necessário, consultar, ao abrigo desse regulamento,*** a ***autoridade*** de ***controlo previamente à operação de*** tratamento. Após o conteúdo das comunicações eletrónicas ter sido enviado pelo utilizador final e recebido pelo ou pelos utilizadores finais destinatários, pode ser registado ou armazenado pelo utilizador final, utilizadores finais ou por ***outra parte*** por eles ***mandatada*** para registar ou armazenar esses dados***, que poderia ser o prestador de comunicações eletrónicas***.

ser registado ou armazenado pelo utilizador final, utilizadores finais ou por ***um terceiro*** por eles ***mandatado*** para registar ou armazenar esses dados. Qualquer tratamento desses dados deve ser conforme com o Regulamento (UE) n.º 2016/679.	Qualquer tratamento em nome do utilizador final desses dados ***das comunicações armazenados no respetivo local de armazenamento deve respeitar o disposto no presente regulamento. O utilizador final pode prosseguir o tratamento dos dados e, se contém dados pessoais, esse tratamento*** deve ser conforme com o Regulamento (UE) n.º 2016/679.

Or. en

Alteração 106
Kaja Kallas, Dita Charanzová

Proposta de regulamento
Considerando 19

Texto da Comissão	*Alteração*
(19) O conteúdo das comunicações eletrónicas inscreve-se na essência do direito fundamental ao respeito pela vida privada e familiar, pelo domicílio e pelas comunicações protegido pelo artigo 7.º da Carta. Qualquer interferência no conteúdo das comunicações eletrónicas deve ser permitida apenas sob condições muito claramente definidas, para fins específicos e mediante garantias adequadas contra abusos. O presente regulamento prevê a possibilidade de os prestadores de serviços de comunicações eletrónicas tratarem os dados de comunicações eletrónicas em trânsito, com o consentimento informado de todos os utilizadores finais em causa. Por exemplo, os prestadores podem oferecer serviços que impliquem a digitalização das mensagens de correio eletrónico para a eliminação de certos materiais pré-definidos. Dado o caráter sensível do conteúdo das comunicações, o presente regulamento estabelece uma presunção de que o tratamento desses dados de conteúdo terá como resultado um	(19) O conteúdo das comunicações eletrónicas inscreve-se na essência do direito fundamental ao respeito pela vida privada e familiar, pelo domicílio e pelas comunicações protegido pelo artigo 7.º da Carta. Qualquer interferência no conteúdo das comunicações eletrónicas deve ser permitida apenas sob condições muito claramente definidas, para fins específicos e mediante garantias adequadas contra abusos. O presente regulamento prevê a possibilidade de os prestadores de serviços de comunicações eletrónicas tratarem os dados de comunicações eletrónicas em trânsito, com o consentimento informado de todos os utilizadores finais em causa. Por exemplo, os prestadores podem oferecer serviços que impliquem a digitalização das mensagens de correio eletrónico para a eliminação de certos materiais pré-definidos. ***No caso dos serviços prestados a utilizadores que realizem atividades exclusivamente pessoais ou domésticas, deve ser suficiente o consentimento do utilizador***

elevado risco para os direitos e liberdades das pessoas singulares. Aquando do tratamento deste tipo de dados, o prestador do serviço de comunicações eletrónicas deve consultar sempre a autoridade de controlo antes do tratamento. Tal consulta deve estar em conformidade com o artigo 36.º, n.ºs 2 e 3, do Regulamento (UE) n.º 2016/679. A presunção não abrange o tratamento de dados de conteúdo para a prestação de um serviço solicitado pelo utilizador final quando este consentiu tal tratamento e o tratamento for efetuado para os fins e duração estritamente necessários e proporcionados para esse serviço. Após o conteúdo das comunicações eletrónicas ter sido enviado pelo utilizador final e recebido pelo ou pelos utilizadores finais destinatários, pode ser registado ou armazenado pelo utilizador final, utilizadores finais ou por um terceiro por eles mandatado para registar ou armazenar esses dados. Qualquer tratamento desses dados deve ser conforme com o Regulamento (UE) n.º 2016/679.

final que solicita o serviço. Dado o caráter sensível do conteúdo das comunicações, o presente regulamento estabelece uma presunção de que o tratamento desses dados de conteúdo terá como resultado um elevado risco para os direitos e liberdades das pessoas singulares. Aquando do tratamento deste tipo de dados, o prestador do serviço de comunicações eletrónicas deve consultar sempre a autoridade de controlo antes do tratamento. Tal consulta deve estar em conformidade com o artigo 36.º, n.ºs 2 e 3, do Regulamento (UE) n.º 2016/679. A presunção não abrange o tratamento de dados de conteúdo para a prestação de um serviço solicitado pelo utilizador final quando este consentiu tal tratamento e o tratamento for efetuado para os fins e duração estritamente necessários e proporcionados para esse serviço. Após o conteúdo das comunicações eletrónicas ter sido enviado pelo utilizador final e recebido pelo ou pelos utilizadores finais destinatários, pode ser registado ou armazenado pelo utilizador final, utilizadores finais ou por um terceiro por eles mandatado para registar ou armazenar esses dados. Qualquer tratamento desses dados deve ser conforme com o Regulamento (UE) n.º 2016/679.

Or. en

Alteração 107
Jan Philipp Albrecht

Proposta de regulamento
Considerando 19-A (novo)

Texto da Comissão	*Alteração*
	(19-A) Deve ser possível tratar os dados das comunicações eletrónicas para efeitos da prestação dos serviços explicitamente solicitados por um utilizador para fins pessoais, ou pessoais relacionados com o

trabalho, tais como funcionalidades de pesquisa ou de indexação de palavras-chave, motores de texto-palavra e serviços de tradução, incluindo o tratamento de imagem para voz, ou outros tratamentos automatizados de conteúdos utilizados como ferramentas de acessibilidade por pessoas com deficiência. Tal deve ser possível sem o consentimento de todos os utilizadores que façam parte da comunicação, mas só pode ocorrer com o consentimento do utilizador que solicita o serviço. Esse consentimento específico também impede o prestador de tratar esses dados para fins diferentes.

Or. en

Alteração 108
Jan Philipp Albrecht

Proposta de regulamento
Considerando 20

Texto da Comissão	*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	(20) Os equipamentos terminais dos utilizadores 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, 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 ***dados muito sensíveis,*** suscetíveis de revelar pormenores sobre ***o comportamento,*** as ***características psicológicas***, ***a condição emocional e as convicções*** políticas***, as crenças religiosas***

comunicações, imagens, a localização das pessoas através do acesso às capacidades de GPS do dispositivo, listas de contactos, bem como outras informações já armazenadas no dispositivo, as informações ***relacionadas com o*** referido equipamento exigem uma proteção da privacidade ***reforçada***. Além disso, os denominados programas espiões, os pixels espiões, os identificadores ocultos, os testemunhos persistentes e outros dispositivos de rastreio ***indesejado*** análogos podem introduzir-se nos equipamentos terminais dos utilizadores finais, sem o seu conhecimento, a fim de aceder a informações, armazenar informações ocultas ***ou rastrear atividades. As informações relacionadas com o dispositivo do utilizador final podem igualmente ser recolhidas à distância para efeitos*** de ***identificação*** e ***rastreio***, ***recorrendo a técnicas*** como ***a recolha da «impressão digital do aparelho», muitas vezes sem o conhecimento do utilizador final***, e ***podem constituir uma grave intrusão na privacidade desses utilizadores finais***. As técnicas que controlam sub-repticiamente as ações dos utilizadores ***finais***, mediante o rastreio das suas atividades em linha ou a localização do seu equipamento terminal, por exemplo, ou que alteram o funcionamento do equipamento terminal dos utilizadores ***finais***, representam uma séria ameaça à privacidade destes utilizadores. Por conseguinte, as interferências com o equipamento terminal do utilizador ***final*** só devem ser permitidas com o consentimento deste último e para fins específicos e transparentes.

e ***as complexidades*** sociais de ***um indivíduo***, incluindo o conteúdo das comunicações, imagens, a localização das pessoas através do acesso às capacidades de GPS do ***seu*** dispositivo, listas de contactos, bem como outras informações já armazenadas no dispositivo, as informações ***tratadas pelo*** referido equipamento***, ou com ele relacionadas,*** exigem uma proteção ***reforçada*** da privacidade***. As informações relacionadas com o dispositivo do utilizador podem ser igualmente 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, e podem constituir uma grave intrusão na privacidade desses utilizadores.*** Além disso, os denominados programas espiões, os pixels espiões, os identificadores ocultos, os testemunhos persistentes e outros dispositivos de rastreio análogos podem introduzir-se nos equipamentos terminais dos utilizadores finais, sem o seu conhecimento, a fim de aceder a informações, armazenar informações ocultas***, proceder ao tratamento de dados e utilizar funcionalidades*** de ***entrada*** e ***saída***, ***tais*** como ***sensores***, e ***rastrear atividades***. As técnicas que controlam sub-repticiamente as ações dos utilizadores, 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, representam uma séria ameaça à privacidade destes utilizadores. Por conseguinte, as interferências com o equipamento terminal do utilizador só devem ser permitidas com o consentimento deste último e para fins específicos e transparentes.

Or. en

Alteração 109
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Kerstin Westphal, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 20

Texto da Comissão	*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 espiões, os pixels espiões, os identificadores ocultos, os testemunhos persistentes e outros dispositivos de rastreio indesejado análogos podem introduzir-se nos equipamentos terminais dos utilizadores finais, sem o seu conhecimento, a fim de aceder a informações, armazenar informações ocultas ou rastrear atividades. As informações relacionadas com o dispositivo do utilizador ***final*** podem	(20) Os equipamentos terminais dos utilizadores 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, 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 ***sensíveis,*** suscetíveis de revelar pormenores sobre as complexidades emocionais, políticas e sociais de uma pessoa singular, incluindo o conteúdo das comunicações, imagens, a localização das pessoas através do acesso às capacidades de GPS do dispositivo, listas de contactos, bem como outras informações já armazenadas no dispositivo, as informações relacionadas com o referido equipamento exigem uma proteção da privacidade reforçada. Além disso, os denominados programas espiões, os pixels espiões, os identificadores ocultos, os testemunhos persistentes e outros dispositivos de rastreio indesejado análogos podem introduzir-se nos equipamentos terminais dos utilizadores finais, sem o seu conhecimento, a fim de aceder a informações, armazenar informações ocultas ou rastrear atividades. As informações relacionadas com o dispositivo do utilizador podem igualmente ser recolhidas à distância para efeitos de

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***.	identificação e rastreio, recorrendo a técnicas como a recolha da «impressão digital do aparelho», muitas vezes sem o conhecimento do utilizador, e podem constituir uma grave intrusão na ***respetiva*** privacidade***. Por conseguinte, as interferências com o equipamento terminal do utilizador só devem ser permitidas com o consentimento deste último, e para fins específicos e transparentes. A utilização de tecnologias e de*** técnicas ***excecionalmente invasivas da privacidade*** que controlam sub-repticiamente as ações dos utilizadores, mediante o rastreio das suas atividades em linha ou a localização do seu equipamento terminal, por exemplo, ***sem o conhecimento dos utilizadores,*** ou que alteram o funcionamento do equipamento terminal dos utilizadores, representam uma séria ameaça à privacidade destes utilizadores, ***e*** devem ser ***proibidas***.

Or. en

Alteração 110
Sabine Verheyen

Proposta de regulamento
Considerando 20

Texto da Comissão	*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	(20) Os equipamentos terminais dos utilizadores finais de redes de comunicações eletrónicas e quaisquer informações relativas à utilização de tais equipamentos terminais, em especial as armazenadas ou emitidas por tais equipamentos, solicitadas ou tratadas para permitir a sua ligação a outro dispositivo e/ou equipamento de rede, fazem parte da esfera privada dos utilizadores finais, que deve ser protegida por força da Carta dos Direitos Fundamentais da União Europeia e da Convenção Europeia para a Proteção

dos Direitos do Homem e das Liberdades Fundamentais. Tendo em conta que esses equipamentos contêm ou tratam informações suscetíveis de revelar pormenores sobre as complexidades emocionais, políticas e sociais de uma pessoa singular, incluindo o conteúdo das comunicações, imagens, a localização das pessoas através do acesso às capacidades de GPS do dispositivo, listas de contactos, bem como outras informações já armazenadas no dispositivo, as informações relacionadas com o referido equipamento exigem uma proteção da privacidade reforçada. Além disso, os denominados programas espiões, os pixels espiões, os identificadores ocultos***, os testemunhos persistentes*** e outros dispositivos de rastreio 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***, 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***

dos Direitos do Homem e das Liberdades Fundamentais. Tendo em conta que esses equipamentos contêm ou tratam informações suscetíveis de revelar pormenores sobre as complexidades emocionais, políticas e sociais de uma pessoa singular, incluindo o conteúdo das comunicações, imagens, a localização das pessoas através do acesso às capacidades de GPS do dispositivo, listas de contactos, bem como outras informações já armazenadas no dispositivo, as informações relacionadas com o referido equipamento exigem uma proteção da privacidade reforçada. Além disso, os denominados programas espiões, os pixels espiões, os identificadores ocultos e outros dispositivos de rastreio análogos persistentes 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.

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.

Or. de

Alteração 111
Inese Vaidere

Proposta de regulamento
Considerando 20

Texto da Comissão	*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 espiões, os pixels espiões, os identificadores ocultos, os testemunhos persistentes e outros dispositivos de rastreio indesejado	(20) Os equipamentos terminais dos utilizadores finais de redes de comunicações eletrónicas e quaisquer informações relativas à utilização de tais equipamentos terminais, em especial as armazenadas ou emitidas por tais equipamentos, solicitadas ou tratadas para permitir a sua ligação a outro dispositivo e/ou equipamento de rede, fazem parte da esfera privada dos utilizadores finais, que deve ser protegida por força da Carta dos Direitos Fundamentais da União Europeia e da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Tendo em conta que esses equipamentos contêm ou tratam informações suscetíveis de revelar pormenores sobre as complexidades emocionais, políticas e sociais de uma pessoa singular, incluindo o conteúdo das comunicações, imagens, a localização das pessoas através do acesso às capacidades de GPS do dispositivo, listas de contactos, bem como outras informações já armazenadas no dispositivo, as informações relacionadas com o referido equipamento exigem uma proteção da privacidade reforçada. Além disso, os denominados programas espiões, os pixels espiões, os identificadores ocultos, os testemunhos persistentes e outros dispositivos de rastreio indesejado

análogos podem introduzir-se nos equipamentos terminais dos utilizadores finais, sem o seu conhecimento, a fim de aceder a informações, armazenar informações ocultas ou rastrear atividades. As informações relacionadas com o dispositivo do utilizador final podem igualmente ser recolhidas à distância para efeitos de identificação e rastreio, recorrendo a técnicas como a recolha da «impressão digital do aparelho», muitas vezes sem o conhecimento do utilizador final, e podem constituir uma grave intrusão na privacidade desses utilizadores finais. As técnicas que controlam sub-repticiamente as ações dos utilizadores finais, mediante o rastreio das suas atividades em linha ou a localização do seu equipamento terminal, por exemplo, ou que alteram o funcionamento do equipamento terminal dos utilizadores finais, representam uma séria ameaça à privacidade destes utilizadores. Por conseguinte, as interferências com o equipamento terminal do utilizador final só devem ser permitidas com o consentimento deste último e para fins específicos e transparentes.

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. ***A recusa dos utilizadores finais em dar consentimento à colocação de ferramentas de rastreio no seu equipamento terminal não pode servir de motivo para recusar o acesso aos conteúdos, se não for necessário para o funcionamento do serviço ou durante a prestação do mesmo.***

Or. en

Alteração 112
Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 21

Texto da Comissão	*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 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.

(21) As exceções à obrigação de obter o consentimento para ***armazenar informação em*** equipamento terminal ou para aceder à informação armazenada no equipamento terminal devem ser limitadas a situações que ***respeitem todas as obrigações estabelecidas no Regulamento (UE) n.º 2016/679***. Por exemplo, o armazenamento técnico ou ***o*** acesso que sejam estritamente necessários e proporcionados para o objetivo legítimo de permitir a utilização de um serviço solicitado pelo utilizador. 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 ***consumidor*** 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. ***Do mesmo modo, os fornecedores do equipamento terminal e do software necessário à exploração desse equipamento necessitam de aceder regularmente à configuração e a outras informações do dispositivo, bem como às capacidades de tratamento e de armazenamento, a fim de manterem o equipamento, prevenirem vulnerabilidades de segurança ou a sua exploração, e corrigirem problemas relacionados com o funcionamento do equipamento.*** O facto de ***os prestadores*** de serviços da sociedade da informação ***e de comunicações eletrónicas verificarem*** a configuração para ***prestarem*** o serviço em conformidade com as predefinições do ***consumidor*** e o mero registo do facto de o dispositivo do ***consumidor*** não permitir receber o conteúdo solicitado pelo ***consumidor*** não devem ser considerados um acesso ao referido dispositivo nem uma utilização das capacidades de tratamento do dispositivo.

Or. en

Alteração 113
Jan Philipp Albrecht

Proposta de regulamento
Considerando 21

Texto da Comissão	*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 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***.	(21) As exceções à obrigação de obter o consentimento para utilizar as capacidades de ***entrada, saída,*** 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 ou acesso que sejam estritamente necessários e proporcionados para o objetivo legítimo de permitir a utilização de um serviço específico explicitamente solicitado pelo utilizador***. Tal pode incluir o armazenamento de informações (como testemunhos de conexão e identificadores)*** 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 ***prestadores*** de serviços da sociedade da informação ***poderiam*** verificar a configuração***, a fim de*** prestar o serviço em conformidade com as predefinições do utilizador e o mero registo do facto de o dispositivo do utilizador não permitir receber o conteúdo solicitado pelo utilizador não ***deve configurar*** um acesso ***ilegítimo***.

Or. en

Alteração 114
Curzio Maltese

Proposta de regulamento
Considerando 21

Texto da Comissão	*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.	(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 ***ou emitida pelo mesmo*** 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 ou ***o*** acesso que sejam estritamente necessários e proporcionados para o objetivo legítimo de ***recordar a opção de os utilizadores finais não darem consentimento a outro tratamento ou para*** 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. 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.

Or. en

Alteração 115
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 21

Texto da Comissão	*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 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***.	(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 ou acesso que sejam estritamente necessários e proporcionados para o objetivo legítimo de permitir a utilização de um serviço específico explicitamente solicitado pelo utilizador. Tal pode incluir o armazenamento de ***informações (como*** testemunhos de conexão ***e identificadores)*** 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. ***As técnicas de rastreio, quando aplicadas em conjunto com as adequadas salvaguardas*** de ***privacidade,*** também podem ser um instrumento legítimo e útil, nomeadamente para medir o tráfego de um sítio web. ***Os prestadores*** de serviços da sociedade da informação ***poderiam*** verificar a configuração ***a fim de*** prestar o serviço em conformidade com as predefinições do utilizador e o mero registo do facto de o dispositivo do utilizador não permitir receber o conteúdo solicitado pelo utilizador não ***deve configurar*** um acesso ***ilegítimo***.

Or. en

Alteração 116
Eva Maydell, Antanas Guoga

Proposta de regulamento
Considerando 21

Texto da Comissão	*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 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.	(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 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. ***O consentimento também não deve ser necessário se a informação tratada ou armazenada for necessária para proteger a privacidade, a segurança do utilizador final, ou para proteger a confidencialidade, integridade, disponibilidade e autenticidade do equipamento terminal.*** 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. ***A título de isenção da obtenção do consentimento do utilizador final, o tratamento das informações e dos dados sob pseudónimo ou tornados anónimos deve ser autorizado para outros fins que não aqueles para os quais foram recolhidos inicialmente, nos casos em que o tratamento seja compatível e esteja sujeito a garantias específicas, nomeadamente a pseudonimização, tal como estabelecido artigo 6.º, n.° 4, do Regulamento (UE) n.º 2016/679.***

Or. en

Alteração 117
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 21

Texto da Comissão	*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 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	(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 ou acesso que sejam 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

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.

determinada num sítio web, a fim de conservar os dados do utilizador final aquando do preenchimento de formulários em linha de várias páginas***. Isto pode abranger igualmente situações em que os utilizadores finais utilizam um serviço entre dispositivos para fins de personalização de serviços e de recomendação de conteúdos***. 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.

Or. en

Alteração 118
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 22

Texto da Comissão	*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	(22) Os métodos utilizados para a prestação de informações e a obtenção do consentimento do utilizador final deverão ser tão conviviais quanto possível. Atendendo à utilização omnipresente de testemunhos persistentes e outras técnicas de rastreio, os utilizadores finais são cada vez mais convidados a dar o seu consentimento para o armazenamento de tais testemunhos persistentes no seu equipamento terminal. Em consequência, os utilizadores finais são sobrecarregados

com pedidos de consentimento. A utilização de meios técnicos para expressar o consentimento, nomeadamente, através de predefinições transparentes e de fácil utilização, pode resolver este problema. O presente regulamento deverá***, pois,*** prever a possibilidade de expressar o consentimento utilizando as predefinições ***adequadas do programa de navegação ou outra aplicação. As escolhas efetuadas pelos utilizadores finais quando estabelecem as suas predefinições gerais de privacidade de um programa de navegação ou de outra aplicação devem ser vinculativas e aplicáveis a quaisquer terceiros. Os navegadores web são um tipo de aplicação de software que permite a recuperação e a apresentação de informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente, os programas de navegação podem ser utilizados como filtro, ajudando assim os utilizadores finais a impedir o acesso a informações provenientes do seu equipamento terminal (por exemplo, telemóvel inteligente, tablete ou computador) ou o armazenamento dessas informações***.	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 prever a possibilidade de expressar o consentimento utilizando as predefinições ***técnicas adequadas***.

Or. en

Alteração 119
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Liisa Jaakonsaari, Marc Tarabella, Josef Weidenholzer

Proposta de regulamento

Considerando 22

Texto da Comissão	*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, prever a possibilidade de expressar o consentimento utilizando as predefinições adequadas do programa de navegação ou outra aplicação. ***As escolhas efetuadas pelos utilizadores finais quando estabelecem as suas predefinições gerais de privacidade de um programa de navegação ou de outra aplicação devem ser vinculativas e aplicáveis a quaisquer terceiros. Os navegadores web são um tipo de aplicação de software que permite a recuperação e a apresentação de informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente, os programas de navegação podem ser utilizados como***	(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 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 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 deverá*** prever a possibilidade de expressar o consentimento ***através de especificações técnicas, nomeadamente,*** 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 que indique as preferências do utilizador a outras partes.*** 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. ***Neste sentido, as predefinições***

***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**.*

devem ser suficientemente pormenorizadas para controlar todo o processamento de dados a que o utilizador tenha dado consentimento e para englobar todas as funcionalidades importantes (por exemplo, se os sítios Web ou as aplicações móveis podem recolher dados de localização do utilizador ou podem ter acesso a equipamento específico, como uma webcam ou microfone). Os dispositivos e as aplicações de software que permitam as comunicações eletrónicas devem implementar mecanismos técnicos como a norma «Do Not Track», a fim de garantir a proteção por defeito da privacidade dos utilizadores e que os utilizadores disponham de uma verdadeira escolha e controlo.

Or. en

Alteração 120
Jan Philipp Albrecht

Proposta de regulamento
Considerando 22

Texto da Comissão	*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	(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 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 são sobrecarregados com pedidos de consentimento. ***O presente regulamento deve impedir a utilização das chamadas «barreiras de testemunhos de conexão» e «mensagens de testemunhos de conexão»***

utilização, pode resolver este problema. O presente regulamento deverá, pois, prever a possibilidade de expressar o consentimento ***utilizando as*** predefinições ***adequadas*** do programa de navegação ou outra aplicação. As escolhas efetuadas pelos utilizadores ***finais*** quando estabelecem as suas predefinições gerais de privacidade de um ***programa de navegação*** ou de ***outra aplicação*** devem ser vinculativas e aplicáveis a quaisquer terceiros. Os navegadores web são um tipo de aplicação de software que permite a recuperação e a apresentação de informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação ***atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente***, ***os programas de navegação podem ser utilizados como filtro***, ***ajudando assim os utilizadores finais a impedir o acesso*** a ***informações provenientes do seu equipamento terminal (por exemplo, telemóvel inteligente, tablete ou computador)*** ou ***o armazenamento dessas informações***.

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. 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 ***e negar*** o consentimento ***através de especificações técnicas, por meios automatizados, como a configuração adequada do equipamento ou de software que permita recuperar e apresentar informação na Internet. 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 ***que indique as preferências do utilizador a outras partes***. As escolhas efetuadas pelos utilizadores quando estabelecem as suas predefinições gerais de privacidade de um ***equipamento*** ou de ***software*** 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. ***Mais especificamente,*** os programas de navegação***, as aplicações ou os sistemas operativos móveis podem ser utilizados como um assistente da privacidade do utilizador*** para ***comunicar as escolhas dos utilizadores***, ajudando ***assim os utilizadores finais*** a ***impedir***em o ***acesso a*** informações ***relativas ao seu equipamento terminal ou dele provenientes (por exemplo***, ***telemóvel inteligente, tablete ou computador) ou o tratamento ou armazenamento dessas informações. Por conseguinte***, ***não devem abusar da sua posição de guardiães e continuar*** a

permitir ao utilizador a possibilidade de dar o seu consentimento a um determinado serviço ou ***prestador de serviços específico***.

Or. en

Alteração 121
Curzio Maltese

Proposta de regulamento
Considerando 22

Texto da Comissão	*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, 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	(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***, sendo porém raramente lembrada pelos prestadores de serviços a sua opção de não dar consentimento***. Em consequência, os utilizadores finais são sobrecarregados com pedidos de consentimento. A ***imposição*** de ***obrigações específicas e limitadas aos prestadores*** de ***serviços*** pode resolver este problema. O presente regulamento deverá, pois, prever a possibilidade de ***os utilizadores finais obrigarem os prestadores de serviços a recordarem-se da sua opção de não dar consentimento e a deixarem de pedir o seu consentimento, depois*** de ***o terem recusado. As escolhas efetuadas pela*** aplicação ***dos utilizadores finais*** devem ser vinculativas e aplicáveis a quaisquer terceiros. ***Além disso,*** os navegadores web são um tipo de aplicação de software que permite a recuperação e a apresentação de informações da Internet.

informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente, os programas de navegação podem ser utilizados como filtro, ajudando assim os utilizadores finais a impedir o acesso a informações provenientes do seu equipamento terminal (por exemplo, telemóvel inteligente, tablete ou computador) ou o armazenamento dessas informações.	Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente, os programas de navegação podem ser utilizados como filtro, ajudando assim os utilizadores finais a impedir o acesso a informações provenientes do seu equipamento terminal (por exemplo, telemóvel inteligente, tablete ou computador) ou o armazenamento dessas informações.

Or. en

Justificação

O consentimento não é dado de livre vontade se os utilizadores finais que já se tenham anteriormente recusado a dá-lo sejam repetidamente instados a fazê-lo, impedindo-os de utilizar o serviço, até por fim o darem.

Alteração 122
Kaja Kallas, Dita Charanzová

Proposta de regulamento
Considerando 22

Texto da Comissão	*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	(22) Os métodos utilizados para a prestação de informações e a obtenção do consentimento do utilizador final deverão ser tão conviviais quanto possível. Atendendo à utilização omnipresente de testemunhos persistentes e outras técnicas de rastreio, os utilizadores finais são cada vez mais convidados a dar o seu consentimento para o armazenamento de

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

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 ***terceiros não autorizados***. Os navegadores web são um tipo de aplicação de software que permite a recuperação e a apresentação de informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. ***Por outro lado***, ***dado o ritmo das inovações, a gama cada vez maior de dispositivos de comunicações,*** a ***utilização crescente dos mesmos e o aumento*** do ***rastreio através de vários dispositivos***, ***é necessário que o presente regulamento mantenha a neutralidade do ponto de vista tecnológico, para poder atingir os seus objetivos***.

Or. en

Alteração 123

Eva Maydell, Antanas Guoga

Proposta de regulamento
Considerando 22

Texto da Comissão	*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, prever a possibilidade de expressar o consentimento utilizando as predefinições adequadas do programa de navegação ou outra aplicação. As escolhas efetuadas pelos utilizadores finais quando estabelecem as suas predefinições gerais de privacidade de um programa de navegação ou de outra aplicação devem ser vinculativas e aplicáveis a quaisquer terceiros. Os navegadores web são um tipo de aplicação de software que permite a recuperação e a apresentação de informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os	(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***, desde que o utilizador final não tenha dado um consentimento específico e distinto***. 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,

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.

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.

Or. en

Alteração 124
Andreas Schwab

Proposta de regulamento
Considerando 22

Texto da Comissão	*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, 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	(22) Os métodos utilizados para a prestação de informações e a obtenção do consentimento do utilizador final deverão ser tão conviviais quanto possível. Atendendo à utilização omnipresente de testemunhos persistentes e outras técnicas de rastreio, os utilizadores finais são cada vez mais convidados a dar o seu consentimento para o armazenamento de tais testemunhos persistentes no seu equipamento terminal. Em consequência, os utilizadores finais são sobrecarregados com pedidos de consentimento. A utilização de meios técnicos para expressar o consentimento, nomeadamente, através de predefinições transparentes e de fácil utilização, pode resolver este problema. O presente regulamento deverá, pois, prever a possibilidade de expressar o consentimento utilizando as predefinições adequadas do programa de navegação ou outra aplicação. As escolhas efetuadas pelos utilizadores finais quando estabelecem as suas predefinições gerais de privacidade de um programa de navegação ou de outra aplicação devem ser vinculativas e

aplicáveis a quaisquer terceiros. Os navegadores web são um tipo de aplicação de software que permite a recuperação e a apresentação de informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente, os programas de navegação podem ser utilizados como filtro, ajudando assim os utilizadores finais a impedir o acesso a informações provenientes do seu equipamento terminal (por exemplo, telemóvel inteligente, tablete ou computador) ou o armazenamento dessas informações.

aplicáveis a quaisquer terceiros. Os navegadores web são um tipo de aplicação de software que permite a recuperação e a apresentação de informações da Internet. Outros tipos de aplicações, como as que permitem chamadas ou mensagens ou que fornecem orientação rodoviária, têm também as mesmas capacidades. Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web. Nesta perspetiva, estão numa posição privilegiada para desempenhar um papel ativo, ajudando o utilizador final a controlar o fluxo de informações de e para os equipamentos terminais. Mais especificamente, os programas de navegação podem ser utilizados como filtro, ajudando assim os utilizadores finais a impedir o acesso a informações provenientes do seu equipamento terminal (por exemplo, telemóvel inteligente, tablete ou computador) ou o armazenamento dessas informações. ***No entanto, é necessário garantir que a função de filtro não seja utilizada de forma abusiva.***

Or. de

Alteração 125
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Kerstin Westphal, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 23

Texto da Comissão	*Alteração*
(23) Os princípios da proteção de dados desde a conceção e por defeito ***foram*** codificados no artigo 25.º do Regulamento (UE) n.º 2016/679. ***Atualmente, a maioria dos programas de navegação estão configurados, por defeito, para «aceitarem todos os testemunhos de conexão». Por conseguinte, os***	(23) Os princípios da proteção de dados desde a conceção e por defeito ***estão*** codificados no artigo 25.º do Regulamento (UE) n.º 2016/679. ***Os fabricantes de equipamento informático e os fornecedores de software que permita comunicações eletrónicas devem ser obrigados a configurar por defeito 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***.

dispositivos e o software de definições, de modo a proporcionarem o mais elevado nível possível de proteção da privacidade, protegendo os utilizadores contra o rastreio através de vários domínios e contra interferências não autorizadas com as suas comunicações e os equipamentos terminais. Os utilizadores devem ser informados sobre as predefinições de privacidade e quaisquer opções disponíveis, com vista a modificar essas predefinições durante a instalação ou primeira utilização do dispositivo ou software, e sempre que procederem a alterações significativas do mesmo. As predefinições de ***privacidade*** devem ser ***apresentadas*** de ***forma objetiva, facilmente visível e compreensível. As predefinições devem ser facilmente acessíveis e modificáveis durante a utilização do dispositivo ou do software. As*** informações ***prestadas não devem incentivar*** os utilizadores ***a selecionar*** um nível de ***proteção da privacidade*** mais baixo ***e*** devem ***incluir informações pertinentes sobre os riscos associados a cada predefinição***.

Or. en

Alteração 126
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 23

Texto da Comissão	*Alteração*
(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 2016/679. ***Atualmente, a maioria dos programas de navegação estão configurados, por defeito, para «aceitarem todos os testemunhos de conexão». Por conseguinte, os***	(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 2016/679. Por ***conseguinte***, os ***fornecedores*** de ***software que permita serviços*** de ***comunicações eletrónicas publicamente disponíveis e*** a recuperação e a apresentação de informações ***na***

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.

Internet devem ser obrigados a configurar o software de modo a ***oferecerem aos*** utilizadores finais um conjunto de opções de privacidade ***para que estes possam selecionar*** de ***forma ativa a opção da sua preferência***, ***depois*** de ***lhes terem sido facultadas as informações necessárias para efetuar essa escolha;*** Essas predefinições de privacidade devem ser apresentadas de uma forma compreensível e facilmente visível.

Or. en

Alteração 127
Pascal Arimont

Proposta de regulamento
Considerando 23

Texto da Comissão	*Alteração*
(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 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	(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 2016/679. Os fornecedores de software que permitam ***as comunicações eletrónicas, incluindo*** a recuperação e a apresentação de informações da Internet***,*** devem ser obrigados a ***definir*** de antemão o software de modo a oferecer ***aos utilizadores finais a máxima proteção da privacidade e, em particular, por forma a impedir que terceiros armazenem***

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.

informações nos equipamentos terminais. Pode ser oferecida aos utilizadores finais ***uma série de opções para definir*** a privacidade, ***que vão*** desde o nível ***intermédio*** ao nível mais baixo***. Estas predefinições*** de ***privacidade devem indicar os riscos associados a uma redução da proteção e*** ser apresentadas de uma forma compreensível e facilmente visível.

Or. de

Alteração 128
Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 23

Texto da Comissão	*Alteração*
(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 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	(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 2016/679. Por ***conseguinte***, os ***fornecedores*** de ***software que permita serviços*** de ***comunicações eletrónicas publicamente disponíveis e*** a recuperação e a apresentação de informações ***na*** Internet devem ser obrigados a configurar o software de modo a que ofereça a possibilidade de impedir que terceiros armazenem informações nos equipamentos terminais; Os ***consumidores*** devem dispor

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.

de um conjunto de opções de privacidade. Essas predefinições de privacidade devem ser apresentadas de uma forma compreensível e facilmente visível.

Or. en

Alteração 129
Eva Maydell, Antanas Guoga

Proposta de regulamento
Considerando 23

Texto da Comissão	*Alteração*
(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 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***	(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 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 ***na*** Internet devem ser obrigados a ***informar*** o ***utilizador final sobre*** a ***possibilidade de assinalar o seu consentimento através de predefinições técnicas adequadas; Os utilizadores finais devem dispor*** de ***múltiplas opções entre as quais optar,***

«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.

inclusive para impedir que terceiros armazenem informações nos equipamentos terminais; ***Os utilizadores finais devem dispor de um conjunto*** de ***opções*** de ***privacidade, desde, por exemplo, rejeitar o rastreio*** que ***não seja necessário para a funcionalidade do sítio Internet ou*** de ***outro software até, por exemplo***, ***aceitar*** o ***rastreio necessário para o funcionamento do sítio Internet ou*** de ***outro software, bem como para outros fins, ou,*** por exemplo, ***aceitar o rastreio necessário para o funcionamento do sítio Internet ou*** de ***outro software e o rastreio para outros fins*** por ***partes que demonstrem cumprir a legislação da UE em matéria*** de ***proteção*** de ***dados e de privacidade, por exemplo, em conformidade com os artigos 40.º e 42.º*** do ***Regulamento (UE***) n.º ***2016/679.*** Essas predefinições de privacidade devem ser apresentadas de uma forma compreensível e facilmente visível.

Or. en

Alteração 130
Kaja Kallas

Proposta de regulamento
Considerando 23

Texto da Comissão	*Alteração*
(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 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***	(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 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 ***aos utilizadores finais*** a possibilidade de

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.

aceitarem ou rejeitarem testemunhos de conexão que ***não sejam necessários à prestação do serviço solicitado pelo utilizador final, depois de informados acerca da função dos*** testemunhos de conexão***, da forma como são utilizados e como a informação recolhida é partilhada. Os utilizadores finais devem dispor de*** um conjunto de opções de privacidade, desde o nível mais elevado (por exemplo, «nunca aceitar testemunhos de conexão») ***até*** ao nível mais baixo (por exemplo, «aceitar sempre testemunhos de conexão»), passando pelo nível intermédio***, em função do tipo de informações que estejam dispostos a partilhar, dos terceiros com quem pretendam partilhar essas informações***, ***do objetivo dos*** testemunhos de conexão***, e da possibilidade*** de ***retirarem o seu consentimento ao rastreio por vários dispositivos. Sempre que o utilizador final aceite*** testemunhos ***de conexão para fins de publicidade orientada, o mesmo deve também ter a possibilidade de corrigir as informações recolhidas a seu respeito para evitar possíveis prejuízos causados por informações incorretas***. ***As*** predefinições de privacidade devem ser apresentadas de uma forma compreensível e facilmente visível.

Or. en

Alteração 131
Jan Philipp Albrecht

Proposta de regulamento
Considerando 23

Texto da Comissão	*Alteração*
(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 2016/679. Atualmente, a maioria	(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 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.

dos programas de navegação estão configurados, por defeito, para «aceitarem todos os testemunhos de conexão». Por conseguinte, os fornecedores de ***equipamento informático ou de*** software que permitam a recuperação e a apresentação de informações da Internet devem ser obrigados a configurar o software de modo a ***oferecer e a ativar*** a possibilidade de impedir***, por defeito, o rastreio através de vários domínios e o armazenamento de*** informações nos equipamentos terminais ***por outras partes***; este procedimento é frequentemente apresentado como «rejeitar ***rastreadores e*** testemunhos de conexão de terceiros». Os utilizadores devem dispor ***de*** 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 rastreamentos entre domínios»). Estas opções podem ser mais esmiuçadas e, entre outros aspetos, refletir a possibilidade*** de ***uma outra parte agir como um processador de dados, na aceção*** do ***Regulamento (UE) n.º 2016/679, para o prestador do serviço. 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 e facilmente visível***, e os utilizadores devem ser informados sobre a possibilidade de***

alterar as predefinições de privacidade de entre várias opções, no momento da instalação ou da primeira utilização. 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 de pessoas singulares e a utilização desses registos para enviar publicidade orientada ou a partilha com outros terceiros. Os produtores de material e de suportes lógicos devem ser instados a proporcionar aos utilizadores meios para alterar facilmente as predefinições de privacidade a qualquer momento durante a utilização e a permitir que o utilizador faça exceções ou dê consentimento a certos serviços da sociedade de informação ou que especifique para que sítios web os testemunhos de conexão são sempre ou nunca consentidos. Caso não haja uma escolha ativa ou ação por parte do utilizador, a configuração será estabelecida por defeito, de modo a rejeitar e a bloquear rastreadores, incluindo testemunhos de conexão, que não sejam estritamente necessários para fornecer o serviço da sociedade de informação expressamente solicitado pelo utilizador.

Or. en

Alteração 132
Curzio Maltese

Proposta de regulamento
Considerando 23

Texto da Comissão	*Alteração*
(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 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.	(23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) n.º 2016/679. Atualmente, a maioria dos programas de navegação estão configurados, por defeito, para «aceitarem todos os testemunhos de ***conexão»», o que impede os utilizadores finais de prestar um consentimento informado e livre, sobrecarregando-o com pedidos***. 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***, por defeito,*** a possibilidade de impedir que terceiros ***solicitem o consentimento dos utilizadores finais para armazenar*** informações nos equipamentos terminais; este procedimento é frequentemente apresentado como «rejeitar testemunhos de conexão de terceiros». Os utilizadores devem dispor ***de*** um conjunto de opções de privacidade, desde o nível mais elevado (por exemplo, «nunca ***perguntar se aceita*** testemunhos de ***conexão, mas rejeitá-los sempre»***) ao nível mais baixo (por exemplo, ***«perguntar*** sempre ***se aceita*** testemunhos de conexão»), passando pelo nível intermédio (por exemplo, «rejeitar***, sem perguntar, os*** testemunhos de conexão de terceiros» ou ***«perguntar*** apenas ***se aceita*** testemunhos ***de conexão*** do sítio ***visitado e rejeita outros testemunhos de conexão»***). Essas predefinições de privacidade devem ser apresentadas de uma forma compreensível e facilmente visível.
	Or. en

Justificação

Os utilizadores finais não devem poder assinalar o seu consentimento utilizando meios automatizados (por exemplo, através de parâmetros técnicos de uma aplicação informática

que permita aceder à Internet), mas, para não serem sobrecarregados com pedidos, devem poder rejeitar automaticamente certas categorias de pedidos.

Alteração 133
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Liisa Jaakonsaari, Kerstin Westphal, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 23-A (novo)

Texto da Comissão	*Alteração*
	(23-A) As crianças merecem proteção especial quanto à sua privacidade em linha. Normalmente, começam a utilizar a Internet em idade precoce, dela se tornando utilizadores muito ativos. No entanto, podem estar menos cientes dos riscos e das consequências inerentes às suas atividades em linha, bem como menos cientes dos seus direitos. São necessárias salvaguardas específicas no que respeita à utilização dos dados de crianças, nomeadamente para efeitos de comercialização e de criação de perfis de personalidade ou de utilizador.

Or. en

Alteração 134
Kaja Kallas

Proposta de regulamento
Considerando 23-A (novo)

Texto da Comissão	*Alteração*
	(23-A) A fim de melhorar a confiança entre os utilizadores finais e os terceiros responsáveis pelo tratamento de informações armazenadas nos equipamentos terminais e de limitar o impacto negativo das técnicas de rastreio na privacidade, importa promover, como alternativa ao rastreio, a capacidade de os

utilizadores finais desenvolverem os próprios perfis, através, por exemplo, de dispositivos elaborados pelos próprios.

Or. en

Alteração 135
Curzio Maltese

Proposta de regulamento
Considerando 24

Texto da Comissão	*Alteração*
(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 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	***Suprimido***

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).

Or. en

Justificação

O consentimento expresso através de meios automatizados (por exemplo, através de definições técnicas de uma aplicação de software que permita o acesso à Internet) nunca poderá ser informado, nem válido.

Alteração 136
Jan Philipp Albrecht

Proposta de regulamento
Considerando 24

Texto da Comissão	*Alteração*
(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 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	***Suprimido***

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).

Or. en

Justificação

Texto integrado no considerando 23 por razões de maior clareza.

Alteração 137
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 24

Texto da Comissão	*Alteração*
(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 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	***Suprimido***

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).

Or. en

Alteração 138
Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 24

Texto da Comissão	*Alteração*
(24) Para obter o consentimento dos ***utilizadores finais***, na aceção do Regulamento (UE) n.º 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	(24) Para obter o consentimento dos ***consumidores***, na aceção do Regulamento (UE) n.º 2016/679, por exemplo, para o armazenamento de testemunhos persistentes de terceiros, ***o software que oferece serviços de comunicação acessíveis ao público e permite efetuar a recuperação e a apresentação*** de ***informações da Internet, deve***, nomeadamente, solicitar ao ***consumidor que utiliza os*** 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 ***consumidores*** 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

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)***.

no contexto dos serviços de comunicações eletrónicas publicamente disponíveis que, no momento da instalação, os ***consumidores*** 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 ***consumidores*** de selecionar as predefinições de privacidade mais elevadas***. Estas obrigações não se verificam nos casos em que o software já se destina a evitar que*** terceiros ***armazenem informações no equipamento terminal*** de ***um utilizador ou tratem informações já armazenadas nesse equipamento***. Os programas de navegação da web são incentivados a proporcionar aos ***consumidores*** meios para alterar facilmente as predefinições de privacidade em qualquer momento durante a utilização.

Or. en

Alteração 139
Kaja Kallas

Proposta de regulamento
Considerando 24

Texto da Comissão	*Alteração*
(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 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	(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 2016/679, por exemplo, para o armazenamento de testemunhos persistentes ***que não sejam necessários à prestação*** de ***um serviço específico solicitado pelo utilizador final***, os programas de navegação ***ou outras aplicações*** devem, nomeadamente, solicitar ao utilizador final dos equipamentos terminais um ato positivo inequívoco a

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)***.

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 testemunhos de conexão ***que processem informações que excedam o necessário para o funcionamento do serviço,*** a fim de confirmar o seu acordo e lhes forem facultadas as informações necessárias para efetuar a escolha. ***O consentimento não deve ser válido no caso do rastreio através de vários dispositivos se o utilizador final não tiver sido informado e se não tiver a possibilidade de retirar o consentimento.*** 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 ***determinados*** testemunhos de conexão 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 ***ou outras aplicações devem*** 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 ***determinadas partes*** ou ***testemunhos de conexão*** que são sempre ou nunca consentidos***. Nos casos em que o modelo de negócio se baseie na publicidade orientada, não se deve considerar que o consentimento tenha***

sido dado de livre vontade se o acesso ao serviço estiver sujeito ao tratamento de dados. O utilizador final deve, por conseguinte, ter a possibilidade de aceitar os testemunhos de conexão ***ou*** de ***optar pelo pagamento do serviço***.

Or. en

Alteração 140
Pascal Arimont

Proposta de regulamento
Considerando 24

Texto da Comissão	*Alteração*
(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 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	(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 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 ***primeira utilização***, ***assegurem que*** os utilizadores finais sejam informados ***de que podem*** escolher ***um nível*** de ***proteção da privacidade inferior ao estabelecido pelas predefinições do software***. As informações prestadas ***aos*** utilizadores finais devem incluir informações sobre os riscos associados à permissão do armazenamento de

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).

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).

Or. de

Alteração 141
Inese Vaidere

Proposta de regulamento
Considerando 24

Texto da Comissão	*Alteração*
(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 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	(24) Para obter o consentimento dos utilizadores finais, na aceção do Regulamento (UE) n.º 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).

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 ***ou apresentar*** 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).

Or. en

Alteração 142
Curzio Maltese

Proposta de regulamento
Considerando 25

Texto da Comissão	*Alteração*
(25) O acesso às redes de comunicações eletrónicas exige o envio regular de determinados pacotes de dados por forma a	(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***

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. ***Em todo o caso, a capacidade para localizar com exatidão as pessoas constitui uma das mais elevadas formas de vigilância e nunca deve ocorrer sem o consentimento dos utilizadores finais. Além disso,*** os ***prestadores de serviços não*** devem ***sequer poder utilizar informações emitidas pelos equipamentos terminais a fim*** de ***solicitar tal consentimento***, ***caso contrário poderiam assediar*** os utilizadores finais ***a fim de obter o seu consentimento e impedi-los*** de ***dar um consentimento livre.*** Em ***vez disso, os fornecedores envolvidos em tais práticas devem afixar avisos visíveis***, ***localizados na extremidade*** da ***zona*** de ***cobertura,*** que ***informem os utilizadores finais de que os podem contactar,*** ou ***descarregar uma aplicação específica no seu equipamento terminal, a fim de***

pessoais em conformidade com o ***artigo 13.º do Regulamento (UE) n.º 2016/679.***	***estarem devidamente informados sobre o tratamento previsto e darem*** o ***seu consentimento***.

Or. en

Justificação

O rastreio dos dispositivos dos utilizadores finais só deve ser autorizado se os utilizadores finais consentirem de forma ativa o seu rastreio. Tal consentimento não se consideraria livre se os fornecedores pudessem enviar automaticamente inúmeros pedidos a todos os utilizadores finais com acesso à zona controlada.

Alteração 143
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 25

Texto da Comissão	*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	(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) n.º 2016/679.

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, por exemplo quando estes entram em lojas, com ofertas personalizadas. Embora algumas destas funcionalidades não ***possam acarretar*** 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. ***A privacidade dos utilizadores deve ser protegida de forma adequada nestas situações. O tratamento das informações emitidas pelos equipamentos terminais dos*** utilizadores ***quando estes se ligam a uma rede ou*** a ***outro dispositivo só deve ser autorizado para fins específicos e transparentes se os utilizadores o tiverem consentido ou se*** o ***tratamento for necessário para fins estatísticos, desde que tais estatísticas sejam efetuadas para fins*** de ***utilidade pública, não existam outros meios para alcançar os fins previstos e as condições estabelecidas nos artigos 35.º e 36***.º do Regulamento (UE) n.º 2016/679 ***estejam preenchidas***.

Or. en

Alteração 144
Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 25

Texto da Comissão	*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	(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) n.º 2016/679.

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 ***consumidores***, por exemplo quando estes entram em lojas, com ofertas personalizadas. ***As informações emitidas por equipamentos terminais devem ser consideradas uma categoria separada dos metadados e das informações emitidas por equipamentos terminais para uso dos consumidores. No entanto, a recolha de tais informações deve estar sujeita a medidas de transparência e a salvaguardas específicas. As organizações que utilizem*** tais ***soluções*** devem afixar ***ou disponibilizar*** 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) n.º 2016/679 ***e o tratamento desses dados pessoais será igualmente abrangido pelo Regulamento***.

Or. en

Alteração 145
Jan Philipp Albrecht

Proposta de regulamento
Considerando 25

Texto da Comissão	*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	(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 ***os metadados de comunicações eletrónicas*** podem ser ***capturados***. 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, por exemplo quando estes entram em lojas,

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) n.º 2016/679***.

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 ***apenas devem estar autorizados*** a ***tratar esses metadados*** de ***comunicações eletrónicas com base no consentimento*** dos ***utilizadores*** em ***causa***.

Or. en

Alteração 146
Kaja Kallas, Dita Charanzová

Proposta de regulamento
Considerando 25

Texto da Comissão	*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	(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) n.º 2016/679***.	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 ***solicitar o consentimento dos*** utilizadores finais ***em causa***, ***ou nos casos*** em ***que não for possível obter consentimento***, ***essas práticas devem ser limitadas ao estritamente necessário para fins estatísticos, devem ser limitadas no tempo e no espaço e as informações*** devem ser ***tornadas anónimas ou suprimidas assim*** que ***deixarem de ser necessárias para este fim***.
	Or. en

Alteração 147
Eva Maydell, Antonio López-Istúriz White, Antanas Guoga

Proposta de regulamento
Considerando 25

Texto da Comissão	*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	(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 ***solicitar o consentimento dos utilizadores finais ou realizar avaliações de impacto sobre a proteção de dados e, neste caso, os dados recolhidos são ou são tornados pseudónimos ou anónimos.***

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) n.º 2016/679.

Sempre que uma avaliação de impacto sobre a proteção de dados indicar que o tratamento é suscetível de implicar um risco elevado na ausência de medidas por parte do responsável pelo tratamento para atenuar o risco, deve proceder-se à consulta prévia da autoridade de controlo, tal como previsto no artigo 36.º do Regulamento (UE) n.º 2016/679. Os fornecedores 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) n.º 2016/679.

Or. en

Alteração 148
Jan Philipp Albrecht

Proposta de regulamento
Considerando 26

Texto da Comissão	*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, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa	(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 ***se destine a pessoas suspeitas de terem cometido uma infração***

sociedade democrática, para salvaguardar interesses públicos específicos, como a segurança nacional, a defesa e a ***segurança pública e a*** prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais***, incluindo a salvaguarda e a prevenção de ameaças à segurança pública e outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, em especial um interesse económico ou financeiro importante da União ou de um Estado-Membro, ou uma missão de controlo, de inspeção ou de regulamentação associada ao exercício da autoridade pública relativamente a tais interesses***. Por conseguinte, o presente regulamento não deve afetar a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário e proporcionado para salvaguardar os interesses públicos acima referidos, em conformidade com a Carta dos Direitos Fundamentais da União Europeia e a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, segundo a interpretação do Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos do Homem. Os prestadores de serviços de comunicações eletrónicas ***devem estabelecer procedimentos adequados para facilitar pedidos legítimos das*** autoridades competentes***, tendo igualmente em conta, sempre que relevante, o papel do representante designado nos termos do artigo 3.º, n.º 3***.	***penal e*** constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar interesses públicos específicos, como a segurança nacional, a defesa e a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais. 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 ***não devem ser obrigados pelas*** autoridades competentes ***da União ou dos Estados-Membros a atenuar quaisquer medidas que garantam a integridade e a confidencialidade das comunicações eletrónicas***.

Or. en

Alteração 149
Curzio Maltese

Proposta de regulamento
Recital 26

Texto da Comissão	*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, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar ***interesses públicos específicos, como a segurança nacional, a defesa e a segurança pública e*** a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública ***e outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, em especial um interesse económico ou financeiro importante da União ou de um Estado-Membro, ou uma missão de controlo, de inspeção ou de regulamentação associada ao exercício da autoridade pública relativamente a tais interesses***. Por conseguinte, o presente regulamento não deve afetar a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário e proporcionado para salvaguardar os interesses públicos acima referidos, em conformidade com a Carta dos Direitos Fundamentais da União Europeia e a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, segundo a interpretação do Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos do Homem. Os prestadores de serviços de comunicações eletrónicas devem estabelecer procedimentos adequados para facilitar pedidos legítimos das autoridades	(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 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. 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 ***e a luta contra crimes graves, e se tais medidas não puderem ser tomadas sem autorização prévia de um órgão jurisdicional***, 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.

competentes, tendo igualmente em conta, sempre que relevante, o papel do representante designado nos termos do artigo 3.º, n.º 3.

Or. en

Alteração 150
Kaja Kallas

Proposta de regulamento
Considerando 26

Texto da Comissão	*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, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar interesses públicos específicos, como a segurança nacional, a defesa e a segurança pública e a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais***, incluindo a salvaguarda e a prevenção de ameaças à segurança pública e outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, em especial um interesse económico ou financeiro importante da União ou de um Estado-Membro, ou uma missão de controlo, de inspeção ou de regulamentação associada ao exercício da autoridade pública relativamente a tais interesses***. Por conseguinte, o presente regulamento não deve afetar a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou	(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. 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.

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.	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.
	Or. en

Alteração 151
Kaja Kallas

Proposta de regulamento
Considerando 26-A (novo)

Texto da Comissão	*Alteração*
	(26-A) A fim de salvaguardar a segurança e a integridade das redes e dos serviços, a utilização de criptografia de ponta a ponta deve ser promovida e, se necessário, tornada obrigatória, em conformidade com os princípios de segurança e de privacidade desde a conceção. Os Estados-Membros não devem impor qualquer obrigação aos fornecedores de serviços de criptografia, aos prestadores de serviços de comunicações eletrónicas ou a qualquer outra organização (em qualquer nível da cadeia de aprovisionamento) que resultem no enfraquecimento da segurança das suas redes e dos seus serviços, tais como a

criação ou a facilitação da utilização de «funções-alçapão» (backdoors).

Or. en

Alteração 152
Anna Maria Corazza Bildt, Eva Maydell

Proposta de regulamento
Considerando 27

Texto da Comissão	*Alteração*
(27) No que respeita à identificação da linha chamadora, é necessário proteger o direito da parte que efetua a chamada de suprimir a apresentação da identificação da linha da qual a chamada é feita e o direito da parte destinatária de rejeitar chamadas de linhas não identificadas. ***Certos utilizadores finais, em especial as linhas de apoio, e outras organizações similares, têm interesse em garantir o anonimato de quem faz as chamadas.*** No que se refere à identificação da linha conectada, é necessário proteger o direito e os legítimos interesses da parte destinatária de impedir a apresentação da identificação da linha à qual a parte chamadora se encontra efetivamente ligada.	(27) No que respeita à identificação da linha chamadora, é necessário proteger o direito da parte que efetua a chamada de suprimir a apresentação da identificação da linha da qual a chamada é feita e o direito da parte destinatária de rejeitar chamadas de linhas não identificadas. No que se refere à identificação da linha conectada, é necessário proteger o direito e os legítimos interesses da parte destinatária de impedir a apresentação da identificação da linha à qual a parte chamadora se encontra efetivamente ligada. ***Estes requisitos fazem sentido no contexto dos serviços de comunicações bidirecionais realizados a nível individual. Não fazem sentido, nem são tecnicamente viáveis, no contexto de outros serviços de comunicações interpessoais acessíveis ao público, como as aplicações de texto - SMS ou as plataformas de comunicação multilateral e multimédia, que permitem a existência de comunicações concorrentes sob a forma de voz, vídeo, mensagens e partilha de documentos para vários participantes. Uma vez que existem múltiplas partes envolvidas, não é possível que cada uma delas exerça o direito de impedir a identificação de chamadas sem interferir no direito das outras partes a que tal identificação não seja suprimida.***

Or. en

Alteração 153
Anna Maria Corazza Bildt, Eva Maydell

Proposta de regulamento
Considerando 28

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

Or. en

Alteração 154
Anna Maria Corazza Bildt, Eva Maydell

Proposta de regulamento
Considerando 29

Texto da Comissão	*Alteração*
(29) Existe tecnologia que permite que os prestadores de serviços de comunicações eletrónicas limitem, de diferentes maneiras, a receção de chamadas não desejadas pelos ***utilizadores finais***, designadamente pelo bloqueio de chamadas silenciosas e outras chamadas fraudulentas e incomodativas. Os prestadores de serviços de comunicações ***interpessoais com base no número*** acessíveis ao público devem utilizar esta	(29) Existe tecnologia que permite que os prestadores de ***determinados*** serviços de comunicações eletrónicas ***acessíveis ao público*** limitem, de diferentes maneiras, a receção de chamadas não desejadas pelos ***consumidores***, designadamente pelo bloqueio de chamadas silenciosas e outras chamadas fraudulentas e incomodativas. ***Sempre que tal seja tecnicamente possível e economicamente viável,*** os prestadores de serviços de comunicações ***vocais***

tecnologia e proteger os ***utilizadores finais*** contra chamadas incomodativas, de forma gratuita. Os fornecedores devem assegurar que os ***utilizadores finais*** têm conhecimento da existência de tais funcionalidades publicitando o facto no seu sítio web, por exemplo.

acessíveis ao público devem utilizar esta tecnologia e proteger os ***consumidores*** contra chamadas incomodativas, de forma gratuita. Os fornecedores devem assegurar que os ***consumidores*** têm conhecimento da existência de tais funcionalidades publicitando o facto no seu sítio web, por exemplo.

Or. en

Alteração 155
Jan Philipp Albrecht

Proposta de regulamento
Considerando 29

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

Or. en

Alteração 156
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 30

Texto da Comissão	*Alteração*
(30) As listas acessíveis ao público de utilizadores finais de serviços de comunicações eletrónicas são amplamente distribuídas. Listas acessíveis ao público significa qualquer lista ou serviço que contenha informações sobre os utilizadores finais, tais como números de telefone (incluindo os números de telefone móvel), endereço de correio eletrónico e inclui os serviços informativos. O direito à privacidade e à proteção dos dados pessoais de uma pessoa singular exige que os utilizadores finais que são pessoas singulares, ***deem o seu consentimento antes dos seus dados pessoais serem incluídos numa lista***. O interesse legítimo das pessoas coletivas exige que os utilizadores finais que são pessoas coletivas tenham o direito de se opor à inclusão numa lista de dados com eles relacionados.	(30) As listas acessíveis ao público de utilizadores finais de serviços de comunicações eletrónicas são amplamente distribuídas. Listas acessíveis ao público significa qualquer lista ou serviço que contenha informações sobre os utilizadores finais, tais como números de telefone (incluindo os números de telefone móvel), endereço de correio eletrónico e inclui os serviços informativos. O direito à privacidade e à proteção dos dados pessoais de uma pessoa singular ***que não opere a título profissional*** exige que os utilizadores finais que são pessoas singulares ***obtenham, a pedido***, ***informações transparentes sobre os dados incluídos na lista e sobre os meios para verificar, corrigir, atualizar, completar e suprimir os seus dados, de forma gratuita***. O interesse legítimo das pessoas coletivas exige que os utilizadores finais que são pessoas coletivas tenham o direito de se opor à inclusão numa lista de dados com eles relacionados.

Or. en

Alteração 157
Morten Løkkegaard, Gérard Deprez, Jean-Marie Cavada, Fredrick Federley, Pavel Telička

Proposta de regulamento
Considerando 30

Texto da Comissão	*Alteração*
(30) As listas acessíveis ao público de utilizadores finais de serviços de comunicações eletrónicas são amplamente distribuídas. Listas acessíveis ao público	(30) As listas acessíveis ao público de utilizadores finais de serviços de comunicações eletrónicas são amplamente distribuídas. Listas acessíveis ao público

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

Or. en

Justificação

Os serviços de listas publicamente disponíveis baseiam-se atualmente num sistema funcional de autoexclusão. A presente proposta criaria um sistema de participação em que os prestadores seriam forçados a obter o consentimento de todos os utilizadores finais, criando encargos desnecessários para os prestadores. Assegurar o direito de oposição do utilizador final deverá ser suficiente.

Alteração 158
Eva Maydell, Antanas Guoga

Proposta de regulamento
Considerando 30

Texto da Comissão	*Alteração*
(30) As listas acessíveis ao público de utilizadores finais de serviços de comunicações eletrónicas são amplamente distribuídas. Listas acessíveis ao público significa qualquer lista ou serviço que contenha informações sobre os utilizadores finais, tais como números de telefone (incluindo os números de telefone móvel), endereço de correio eletrónico e inclui os serviços informativos. O direito à	(30) As listas acessíveis ao público de utilizadores finais de serviços de comunicações eletrónicas são amplamente distribuídas. Listas acessíveis ao público significa qualquer lista ou serviço que contenha informações sobre os utilizadores finais, tais como números de telefone (incluindo os números de telefone móvel), endereço de correio eletrónico e inclui os serviços informativos. O direito à

privacidade e à proteção dos dados pessoais de uma pessoa singular exige que os utilizadores finais que são pessoas singulares, deem o seu consentimento antes dos seus dados pessoais serem incluídos numa lista. O interesse legítimo das pessoas coletivas exige que os utilizadores finais que são pessoas coletivas tenham o direito de se opor à inclusão numa lista de dados com eles relacionados.

privacidade e à proteção dos dados pessoais de uma pessoa singular exige que os utilizadores finais que são pessoas singulares, deem o seu consentimento antes dos seus dados pessoais serem incluídos numa lista. O interesse legítimo das pessoas coletivas exige que os utilizadores finais que são pessoas coletivas tenham o direito de se opor à inclusão numa lista de dados com eles relacionados. ***O consentimento deve ser obtido pelo prestador de serviços de comunicações eletrónicas no momento da assinatura do contrato relativo a esse serviço.***

Or. en

Alteração 159
Daniel Dalton, Richard Sulík

Proposta de regulamento
Considerando 31

Texto da Comissão	*Alteração*
(31) Se os utilizadores finais que são pessoas singulares ***consentirem que os seus dados sejam incluídos em tais*** listas, devem poder determinar, com base no ***consentimento***, que categorias de dados pessoais devem figurar na lista (por exemplo, nome e apelido, endereço de correio eletrónico, endereço postal, nome de utilizador, número de telefone). Além disso, os fornecedores de listas acessíveis ao público devem informar os utilizadores finais da finalidade da lista e das suas funções de procura***, antes de os incluir na mesma. Os utilizadores finais devem poder determinar, mediante consentimento, as categorias de dados pessoais que podem servir de base para procurar os seus dados de contacto. As categorias de dados pessoais incluídas na lista e as categorias de dados pessoais com base nas quais os dados de contacto do***	(31) Se os utilizadores finais que são pessoas singulares ***não se opuserem à inclusão dos seus dados em*** listas ***públicas por parte de prestadores de serviços de comunicações interpessoais*** com base no ***número e de prestadores de comunicações eletrónicas***, devem poder determinar que categorias de dados pessoais devem figurar na lista (por exemplo, nome e apelido, endereço de correio eletrónico, endereço postal, nome de utilizador, número de telefone). Além disso, os fornecedores de listas acessíveis ao público devem informar os utilizadores finais da finalidade da lista e das suas funções de procura.

utilizador final podem ser procurados não devem ser necessariamente as mesmas.

Or. en

Alteração 160
Morten Løkkegaard, Gérard Deprez, Jean-Marie Cavada, Fredrick Federley, Pavel Telička

Proposta de regulamento
Considerando 31

Texto da Comissão	*Alteração*
(31) Se os utilizadores finais que são pessoas singulares ***consentirem que os seus dados sejam incluídos*** em tais listas, devem poder ***determinar,*** com base ***no consentimento, que*** categorias de dados pessoais devem figurar na lista (por exemplo, nome e apelido, endereço de correio eletrónico, endereço postal, nome de utilizador, número de telefone). Além disso, os fornecedores de listas acessíveis ao público devem ***informar os*** utilizadores finais ***da*** finalidade da lista e ***das*** suas funções de procura, antes de os incluir na mesma. Os utilizadores finais devem poder ***determinar, mediante consentimento, as*** categorias de dados pessoais que podem servir de base para procurar os seus dados de contacto. As categorias de dados pessoais incluídas na lista e as categorias de dados pessoais com base nas quais os dados de contacto do utilizador final podem ser procurados não devem ser necessariamente as mesmas.	(31) Se os utilizadores finais que são pessoas singulares ***não se opuserem à inclusão dos seus dados*** em tais listas, devem poder ***opor-se*** com base ***nas*** categorias de dados pessoais ***que*** devem figurar na lista (por exemplo, nome e apelido, endereço de correio eletrónico, endereço postal, nome de utilizador, número de telefone). Além disso, os fornecedores de listas acessíveis ao público devem ***disponibilizar informações acessíveis aos*** utilizadores finais ***sobre a*** finalidade da lista e ***as*** suas funções de procura, antes de os incluir na mesma. Os utilizadores finais devem poder ***opor-se com base nas*** categorias de dados pessoais que podem servir de base para procurar os seus dados de contacto. As categorias de dados pessoais incluídas na lista e as categorias de dados pessoais com base nas quais os dados de contacto do utilizador final podem ser procurados não devem ser necessariamente as mesmas.

Or. en

Justificação

Os serviços de listas publicamente disponíveis baseiam-se atualmente num sistema funcional de autoexclusão. A presente proposta criaria um sistema de participação em que os prestadores seriam forçados a obter o consentimento de todos os utilizadores finais, criando

encargos desnecessários para os prestadores. Assegurar o direito de oposição do utilizador final deverá ser suficiente.

Alteração 161
Jan Philipp Albrecht

Proposta de regulamento
Considerando 31

Texto da Comissão	*Alteração*
(31) Se os utilizadores finais que são pessoas singulares consentirem que os seus dados sejam incluídos em tais listas, devem poder determinar, com base no consentimento, que categorias de dados pessoais devem figurar na lista (por exemplo, nome e apelido, endereço de correio eletrónico, endereço postal, nome de utilizador, número de telefone). Além disso, os fornecedores de listas acessíveis ao público devem informar os utilizadores finais da finalidade da lista e das suas funções de procura, antes de os incluir na mesma. Os utilizadores finais devem poder determinar, mediante consentimento, as categorias de dados pessoais que podem servir de base para procurar os seus dados de contacto. As categorias de dados pessoais incluídas na lista e as categorias de dados pessoais com base nas quais os dados de contacto do utilizador final podem ser procurados não devem ser necessariamente as mesmas.	(31) Se os utilizadores finais que são pessoas singulares consentirem que os seus dados sejam incluídos em tais listas, devem poder determinar, com base no consentimento, que categorias de dados pessoais devem figurar na lista (por exemplo, nome e apelido, endereço de correio eletrónico, endereço postal, nome de utilizador, número de telefone). Além disso, os fornecedores de listas acessíveis ao público ***ou os prestadores de serviços de comunicações eletrónicas*** devem informar os utilizadores finais da finalidade da lista e das suas funções de procura, antes de os incluir na mesma. Os utilizadores finais devem poder determinar, mediante consentimento, as categorias de dados pessoais que podem servir de base para procurar os seus dados de contacto. As categorias de dados pessoais incluídas na lista e as categorias de dados pessoais com base nas quais os dados de contacto do utilizador final podem ser procurados não devem ser necessariamente as mesmas.

Or. en

Alteração 162
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposta de regulamento
Considerando 32

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

Or. en

Alteração 163
Anna Maria Corazza Bildt, Eva Maydell

Proposta de regulamento
Considerando 32

Texto da Comissão	*Alteração*
(32) No presente regulamento, «marketing direto» refere-se a qualquer forma de publicidade através da qual uma pessoa singular ou coletiva envia diretamente comunicações comerciais diretas a um ou mais ***utilizadores finais*** identificados ou identificáveis através da utilização de serviços de comunicações eletrónicas. Para além da oferta de produtos e de serviços para fins comerciais, deve incluir igualmente as mensagens	(32) No presente regulamento, «marketing direto» refere-se a qualquer forma de publicidade através da qual uma pessoa singular ou coletiva envia diretamente comunicações comerciais diretas a um ou mais ***consumidores*** identificados ou identificáveis através da utilização de serviços de comunicações eletrónicas. Para além da oferta de produtos e de serviços para fins comerciais, deve incluir igualmente as mensagens

enviadas pelos partidos políticos que contactam pessoas singulares através de serviços de comunicações eletrónicas para promover os seus partidos. O mesmo deverá aplicar-se às mensagens enviadas por outras organizações sem fins lucrativos para apoiar os objetivos da organização.	enviadas pelos partidos políticos que contactam pessoas singulares através de serviços de comunicações eletrónicas para promover os seus partidos. O mesmo deverá aplicar-se às mensagens enviadas por outras organizações sem fins lucrativos para apoiar os objetivos da organização.

Or. en

Alteração 164
Inese Vaidere

Proposta de regulamento
Considerando 32

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

Or. en

Alteração 165
Anna Maria Corazza Bildt, Eva Maydell

Proposta de regulamento

Considerando 33

Texto 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 lhe enviar comunicações eletrónicas comerciais para fins de marketing direto, a fim de proteger eficazmente os indivíduos contra a intrusão na sua vida privada***, assim como os interesses legítimos das pessoas coletivas***. A segurança jurídica e a necessidade de assegurar que as regras de proteção contra as comunicações eletrónicas não solicitadas permanecem orientadas para o futuro justificam a necessidade de definir um conjunto único de regras que não variam em função da tecnologia utilizada para enviar estas comunicações não solicitadas, garantindo ao mesmo tempo um nível equivalente de proteção para todos os cidadãos em toda a União. No entanto, é razoável permitir a utilização de contactos de correio eletrónico no contexto de uma relação existente entre o cliente e o fornecedor para a oferta de produtos ou serviços similares. Essa possibilidade deve aplicar-se apenas à mesma empresa que obteve as coordenadas eletrónicas de contacto em conformidade com o Regulamento (UE) n.º 2016/679.	(33) Há que prever salvaguardas para proteger os ***consumidores*** contra comunicações não solicitadas para fins de marketing direto, que invadem a vida privada dos ***consumidores***. 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 ***consumidor*** antes lhe enviar comunicações eletrónicas comerciais para fins de marketing direto, a fim de proteger eficazmente os indivíduos contra a intrusão na sua vida privada. 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) n.º 2016/679.

Or. en

Alteração 166
Jan Philipp Albrecht

Proposta de regulamento
Considerando 33

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

aplicar-se apenas à mesma empresa que obteve as coordenadas eletrónicas de contacto em conformidade com o Regulamento (UE) n.º 2016/679.

Essa possibilidade deve aplicar-se apenas à mesma empresa que obteve as coordenadas eletrónicas de contacto em conformidade com o Regulamento (UE) n.º 2016/679.

Or. en

Alteração 167
Eva Maydell, Pascal Arimont

Proposta de regulamento
Considerando 33

Texto 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 lhe enviar comunicações eletrónicas comerciais para fins de marketing direto, a fim de proteger eficazmente os indivíduos contra a intrusão na sua vida privada, assim como os interesses legítimos das pessoas coletivas. A segurança jurídica e a necessidade de assegurar que as regras de proteção contra as comunicações eletrónicas não solicitadas permanecem orientadas para o futuro justificam a necessidade de definir um conjunto único de regras que não variam em função da tecnologia utilizada para enviar estas comunicações não solicitadas, garantindo ao mesmo tempo	(33) Há que prever salvaguardas para proteger os utilizadores finais contra comunicações não solicitadas para fins de marketing direto, que invadem a vida privada dos utilizadores finais. O grau de invasão da privacidade e de incómodo é considerado relativamente semelhante, independentemente do amplo leque de tecnologias e meios utilizados para efetuar essas comunicações eletrónicas, quer utilizando sistemas de chamada e de comunicação automatizados, aplicações de mensagens instantâneas, mensagens de correio eletrónico, SMS, MMS, Bluetooth, etc. Por conseguinte, justifica-se exigir a obtenção do consentimento do utilizador final antes lhe enviar comunicações eletrónicas comerciais para fins de marketing direto, a fim de proteger eficazmente os indivíduos contra a intrusão na sua vida privada, assim como os interesses legítimos das pessoas coletivas. A segurança jurídica e a necessidade de assegurar que as regras de proteção contra as comunicações eletrónicas não solicitadas permanecem orientadas para o futuro justificam a necessidade de definir um conjunto único de regras que não variam em função da tecnologia utilizada para enviar estas comunicações não solicitadas, garantindo ao mesmo tempo

um nível equivalente de proteção para todos os cidadãos em toda a União. No entanto, é razoável permitir a utilização de contactos de correio eletrónico no contexto de uma relação existente entre o cliente e o fornecedor para a oferta de produtos ou serviços ***similares***. Essa possibilidade deve aplicar-se apenas à mesma empresa que obteve as coordenadas eletrónicas de contacto em conformidade com o Regulamento (UE) n.º 2016/679.	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. Essa possibilidade deve aplicar-se apenas à mesma empresa que obteve as coordenadas eletrónicas de contacto em conformidade com o Regulamento (UE) n.º 2016/679.
	Or. en

Alteração 168
Pascal Arimont

Proposta de regulamento
Considerando 33

Texto 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 lhe enviar comunicações eletrónicas comerciais para fins de marketing direto, a fim de proteger eficazmente os indivíduos contra a intrusão na sua vida privada, assim como os interesses legítimos das pessoas coletivas. A segurança jurídica e a necessidade de assegurar que as regras de proteção contra as comunicações eletrónicas não solicitadas permanecem orientadas para o	(33) Há que prever salvaguardas para proteger os utilizadores finais contra comunicações não solicitadas para fins de marketing direto, que invadem a vida privada dos utilizadores finais. O grau de invasão da privacidade e de incómodo é considerado relativamente semelhante, independentemente do amplo leque de tecnologias e meios utilizados para efetuar essas comunicações eletrónicas, quer utilizando sistemas de chamada e de comunicação automatizados, aplicações de mensagens instantâneas, mensagens de correio eletrónico, SMS, MMS, Bluetooth, etc. Por conseguinte, justifica-se exigir a obtenção do consentimento do utilizador final antes lhe enviar comunicações eletrónicas comerciais para fins de marketing direto, a fim de proteger eficazmente os indivíduos contra a intrusão na sua vida privada, assim como os interesses legítimos das pessoas coletivas. A segurança jurídica e a necessidade de assegurar que as regras de proteção contra as comunicações eletrónicas não solicitadas permanecem orientadas para o

futuro justificam a necessidade de definir um conjunto único de regras que não variam em função da tecnologia utilizada para enviar estas comunicações não solicitadas, garantindo ao mesmo tempo um nível equivalente de proteção para todos os cidadãos em toda a União. No entanto, é razoável permitir a utilização de contactos de correio eletrónico no contexto de uma relação existente entre o cliente e o fornecedor para a oferta de produtos ou serviços ***similares***. Essa possibilidade deve aplicar-se apenas à mesma empresa que obteve as coordenadas eletrónicas de contacto em conformidade com o Regulamento (UE) n.º 2016/679.	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. Essa possibilidade deve aplicar-se apenas à mesma empresa que obteve as coordenadas eletrónicas de contacto em conformidade com o Regulamento (UE) n.º 2016/679.
	Or. de

Alteração 169
Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 34

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

comunicação, ou por conta de quem a comunicação é transmitida, e fornecer as informações necessárias para que os destinatários exerçam o seu direito de se oporem à receção de novas mensagens comerciais escritas e/ou orais.	comunicação, ou por conta de quem a comunicação é transmitida, e fornecer as informações necessárias para que os destinatários exerçam o seu direito de se oporem à receção de novas mensagens comerciais escritas e/ou orais.

Or. en

Alteração 170
Anna Maria Corazza Bildt

Proposta de regulamento
Considerando 35

Texto da Comissão	*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 ou apresentar um código específico que indique que se trata de uma chamada promocional.	(35) A fim de facilitar a retirada do consentimento, as pessoas singulares 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 ***consumidores*** para retirarem o seu consentimento. As pessoas singulares 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.

Or. en

Alteração 171
Pascal Arimont

Proposta de regulamento
Considerando 35

Texto da Comissão	*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 ***ou*** apresentar um código específico que indique que se trata de uma chamada promocional.	(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.

Or. de

Alteração 172
Inese Vaidere

Proposta de regulamento
Considerando 36

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

Or. en

Alteração 173

Kaja Kallas, Dita Charanzová

Proposta de regulamento
Considerando 37

Texto da Comissão	*Alteração*
(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) n.º 2016/***679***.	(37) Os ***fornecedores*** de serviços ***são obrigados*** a ***prestar serviços seguros e*** a ***notificar casos*** de ***violação da*** segurança***, em conformidade com o Regulamento (UE) n.º 2016/679***, ***[Diretiva do Parlamento Europeu*** e ***do Conselho que institui o Código Europeu das Comunicações Eletrónicas]*** e a ***Diretiva*** (UE) n.º 2016/***1148***.

Or. en

Alteração 174
Jan Philipp Albrecht

Proposta de regulamento
Considerando 37

Texto da Comissão	*Alteração*
(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	(37) Os prestadores de serviços que disponibilizam serviços de comunicações eletrónicas devem ***tratar os dados das comunicações eletrónicas de forma a impedir o tratamento não autorizado, nomeadamente o acesso, a divulgação ou a alteração não autorizados. Devem***

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) n.º 2016/679.

garantir que esse acesso, divulgação ou alteração não autorizados possam ser verificados e assegurar igualmente que esses dados de comunicações eletrónicas sejam protegidos através de software topo de gama e de tecnologias de encriptação. Os ***prestadores de serviços devem informar igualmente os*** utilizadores finais das medidas que podem tomar para proteger ***o seu anonimato e*** 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) n.º 2016/679.

Or. en

Alteração 175
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Marc Tarabella, Josef Weidenholzer

Proposta de regulamento
Considerando 39

Texto da Comissão	*Alteração*
(39) Cada autoridade de controlo deverá ser competente no território do seu Estado-Membro para exercer os poderes e para desempenhar as funções estabelecidas no presente regulamento. A fim de assegurar o controlo e a aplicação coerente do presente regulamento em toda a União, as autoridades de controlo devem ter as mesmas atribuições e poderes efetivos em	(39) Cada autoridade de controlo deverá ser competente no território do seu Estado-Membro para exercer os poderes e para desempenhar as funções estabelecidas no presente regulamento. A fim de assegurar o controlo e a aplicação coerente do presente regulamento em toda a União, as autoridades de controlo devem ter as mesmas atribuições e poderes efetivos em

cada Estado-Membro, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal ao abrigo do direito do Estado-Membro, para levar as infrações ao presente regulamento ao conhecimento das autoridades judiciais e para intentar processos judiciais. Os Estados-Membros e as suas autoridades de controlo são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas na aplicação do presente regulamento.	cada Estado-Membro, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal ao abrigo do direito do Estado-Membro, para levar as infrações ao presente regulamento ao conhecimento das autoridades judiciais e para intentar processos judiciais. Os Estados-Membros e as suas autoridades de controlo são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas na aplicação do presente regulamento. ***As autoridades de controlo devem cooperar com as autoridades competentes noutros domínios de aplicação, conforme adequado.***

Or. en

Alteração 176
Inese Vaidere

Proposta de regulamento
Considerando 40

Texto da Comissão	*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	(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.

para garantir o cumprimento das obrigações constantes do presente regulamento e para prevenir ou atenuar as consequências da infração. ***As coimas aplicadas não devem conduzir a consequências irreversíveis para a empresa em caso de infração insignificante.*** 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.

Or. en

Alteração 177
Eva Maydell, Antanas Guoga, Roberta Metsola

Proposta de regulamento
Considerando 40

Texto da Comissão	*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	(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.

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. ***Devem ser evitadas sanções duplas resultantes de infrações ao presente regulamento e ao Regulamento (UE) n.º 2016/679.***

Or. en

Alteração 178
Kaja Kallas, Dita Charanzová

Proposta de regulamento
Considerando 41

Texto da Comissão	*Alteração*
(41) ***A fim de cumprir os objetivos do presente regulamento, nomeadamente proteger os direitos e liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais, e assegurar a livre circulação desses dados na União, o poder de adotar atos em conformidade com o artigo 290.º do Tratado sobre o Funcionamento da União Europeia deve ser delegado na Comissão para complementar o presente regulamento. Em especial, convém adotar atos delegados no que respeita à informação a apresentar, nomeadamente por meio de ícones normalizados, que ofereçam uma perspetiva geral inteligível e facilmente visível da recolha das informações emitidas pelo equipamento terminal, o seu objetivo, a pessoa responsável por ela e qualquer medida que o utilizador final dos equipamentos terminais pode tomar para minimizar a recolha de dados. São igualmente necessários atos delegados para especificar um código de identificação de chamadas de marketing direto, incluindo as efetuadas através de***	(41) Para assegurar condições uniformes de execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão nos casos previstos no presente regulamento. Essas competências devem ser exercidas em conformidade com o Regulamento (UE) n.º 182/2011.

sistemas de chamada e de comunicação automatizados. É particularmente importante que a Comissão proceda a consultas adequadas e que essas consultas sejam realizadas em conformidade com os princípios estabelecidos no Acordo Interinstitucional «Legislar Melhor», de 13 de abril de 2016[25]. Em especial, a fim de assegurar a igualdade de participação na preparação de atos delegados, o Parlamento Europeu e o Conselho devem receber todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os seus peritos devem ter sistematicamente acesso às reuniões dos grupos de peritos da Comissão incumbidos da elaboração dos atos delegados. Além disso, para assegurar condições uniformes de execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão nos casos previstos no presente regulamento. Essas competências devem ser exercidas em conformidade com o Regulamento (UE) n.º 182/2011.

_____

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

Or. en

Alteração 179
Jan Philipp Albrecht

Proposta de regulamento
Considerando 43

Texto da Comissão	*Alteração*
(43) A Diretiva 2002/58/CE ***deverá*** ser ***revogada***.	(43) A Diretiva 2002/58/CE ***e o Regulamento (UE) n.º 611/2013 da Comissão deverão*** ser ***revogados***.

Or. en

Justificação

O Regulamento (UE) n.º 611/2013 da Comissão que estabelece regras específicas sobre a notificação de violações de dados deverá ser revogado, uma vez que a sua base jurídica, a Diretiva 2002/58/CE, será revogada e o Código Europeu das Comunicações Eletrónicas será aplicável às notificações de violações.

Alteração 180
Roberta Metsola

Proposta de regulamento
Considerando 43-A (novo)

Texto da Comissão	*Alteração*
	(43-A) O bom funcionamento das futuras redes de infraestruturas inovadoras, como as redes de quinta geração (5G), depende de um número cada vez maior de dispositivos, muitas vezes com uma capacidade computacional limitada, que sejam capazes de tratar dados a velocidades sem precedentes. A privacidade do utilizador final em tal cenário continua a ser uma prioridade e deve, por conseguinte, ser concebida de forma a complementar os requisitos dessas infraestruturas e a permitir a livre circulação dos dados das comunicações eletrónicas, de modo a que as comunicações 5G funcionem como previsto e satisfaçam as necessidades dos utilizadores finais, dos operadores, dos segmentos verticais da indústria, das empresas e dos decisores políticos.

Or. en