



17/PT

WP 247

**Parecer 1/2017 sobre
a proposta de regulamento relativo à privacidade e às comunicações eletrónicas
(2002/58/CE)**

Adotado em 4 de abril de 2017

Este grupo de trabalho foi criado pelo artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições são descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

O secretariado é assegurado pela Direção C (Direitos Fundamentais e Estado de Direito) da Direção-Geral da Justiça e dos Consumidores da Comissão Europeia, B-1049 Bruxelas, Bélgica, Gabinete n.º MO-59 05/035.

Sítio Web: http://ec.europa.eu/justice/data-protection/index_en.htm

O GRUPO DE TRABALHO SOBRE A PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS

Criado pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,

Tendo em conta os artigos 29.º e 30.º,

Tendo em conta o seu regulamento interno,

ADOTOU O SEGUINTE PARECER:

SÍNTESE

O grupo de trabalho congratula-se com a proposta da Comissão Europeia, de 10 de janeiro de 2017, respeitante a um regulamento relativo à privacidade e às comunicações eletrónicas. O grupo de trabalho acolhe com agrado **a escolha de um regulamento** como instrumento jurídico, que garante a uniformidade das regras em toda a UE e proporciona clareza às autoridades de controlo e organizações similares. Contribui igualmente para assegurar a coerência com o Regulamento Geral sobre a Proteção de Dados (RGPD). Essa coerência é ainda apoiada pela opção de tornar **a mesma autoridade responsável pelo controlo do cumprimento do GDPR** também responsável pela execução das regras relativas à privacidade e às comunicações eletrónicas.

Simultaneamente, a escolha (manutenção) de um **instrumento jurídico complementar** é positiva. A proteção da confidencialidade das comunicações e dos equipamentos terminais apresenta características específicas que não são abordadas pelo GDPR. Por conseguinte, são necessárias disposições complementares no que diz respeito a estes tipos de serviços, a fim de assegurar a proteção adequada do direito fundamental à privacidade e à confidencialidade das comunicações, incluindo a confidencialidade dos equipamentos terminais. A este respeito, o grupo de trabalho manifesta o seu vivo apoio à **posição de princípio**, adotada na proposta de regulamento, que consiste em prever **extensas proibições e limitar as exceções** e em **aplicar a noção de consentimento de forma criteriosa**.

O grupo de trabalho saúda o alargamento do âmbito de aplicação da proposta de regulamento, com vista a **incluir os fornecedores de conteúdos audiovisuais em linha (OTT)**, serviços que são funcionalmente equivalentes aos meios de comunicação mais tradicionais e podem, por conseguinte, ter um impacto semelhante na privacidade e no direito à confidencialidade das comunicações das pessoas na UE. É igualmente positivo que a proposta de regulamento contemple, de forma clara, os **conteúdos e metadados associados** e reconheça que **os metadados podem conter dados sensíveis**.

Não obstante, o grupo de trabalho regista ainda quatro **motivos de grande preocupação**. No que diz respeito ao **rastreio da localização dos equipamentos terminais, às condições em que a análise de conteúdos e metadados é autorizada e às predefinições dos equipamentos terminais e do software, bem como às barreiras de rastreio («tracking walls»)**, a proposta de regulamento deverá baixar o nível de proteção de que gozam ao abrigo do GDPR. No presente parecer, o grupo de trabalho apresenta sugestões específicas tendentes a assegurar que o regulamento relativo à privacidade e às comunicações eletrónicas garantirá um nível de proteção igual ou superior adequado ao carácter sensível dos dados das comunicações (tanto o conteúdo como os metadados).

No atinente ao **rastreio via Wi-Fi («WiFi-tracking»)** e consoante as circunstâncias e as finalidades da recolha de dados, esse rastreio ao abrigo do GDPR poderá estar subordinado ao consentimento ou só poderá ser efetuado se os dados pessoais recolhidos forem tornados anónimos. No último caso, as quatro condições seguintes terão de ser respeitadas: a finalidade da recolha de dados provenientes de equipamentos terminais restringe-se à mera contagem estatística, o rastreio é limitado no tempo e no espaço, na medida do estritamente necessário para o efeito, os dados serão imediatamente eliminados ou anonimizados e existem opções

eficazes de autoexclusão. A Comissão Europeia é convidada a promover uma norma técnica para que os dispositivos móveis assinalem automaticamente uma oposição contra tal rastreio.

No que respeita à **análise de conteúdos e metadados**, o ponto de partida deve consistir na proibição do tratamento de dados das comunicações sem o consentimento de todos os utilizadores finais (remetentes e destinatários). A fim de permitir aos fornecedores que prestem serviços expressamente solicitados pelo utilizador, como, por exemplo, a funcionalidade de pesquisa e indexação ou serviços de conversão de texto em voz, deverá existir uma exceção ao nível doméstico para o tratamento de conteúdos e metadados para fins estritamente pessoais do próprio utilizador.

No que diz respeito ao **consentimento para o rastreio**, o grupo de trabalho apela para uma proibição explícita das barreiras de rastreio, ou seja, as opções de «pegar ou largar» (opções inegociáveis) que obrigam os utilizadores a dar o seu consentimento para o rastreio se quiserem ter acesso ao serviço.

Por último, mas não menos importante, o grupo de trabalho recomenda que os equipamentos terminais e o *software* devam, **por defeito, oferecer definições de proteção da privacidade**, assim como oferecer opções claras aos utilizadores para confirmarem ou alterarem essas predefinições durante a instalação. As predefinições devem ser facilmente acessíveis durante a utilização. Os utilizadores devem poder dar o seu consentimento explícito através das predefinições do seu programa de navegação. As preferências de privacidade não devem limitar-se às interferências por terceiros ou aos testemunhos de conexão («cookies»). O grupo de trabalho recomenda vivamente que a adesão à norma «Não Rastrear» (NR) seja tornada obrigatória.

Ademais, o grupo de trabalho identificou outros aspetos problemáticos relativos, por exemplo, ao âmbito, à proteção dos equipamentos terminais e ao *marketing* direto. Por último, mas não menos importante, o grupo de trabalho identificou questões que carecem de esclarecimento, por forma a proteger melhor os utilizadores finais e a introduzir mais segurança jurídica para todas as partes interessadas envolvidas.

ÍNDICE

1. INTRODUÇÃO.....	6
2. ASPETOS POSITIVOS DA PROPOSTA DE REGULAMENTO.....	6
<i>Harmonização em toda a UE, alinhamento das coimas e execução exclusiva pelas autoridades responsáveis pela proteção dos dados (APD)</i>	<i>6</i>
<i>Alargamento do âmbito de aplicação quando comparado com a Diretiva relativa à privacidade e às comunicações eletrónicas</i>	<i>8</i>
<i>Aplicação orientada da noção de consentimento</i>	<i>10</i>
3. MOTIVOS DE GRANDE PREOCUPAÇÃO	11
<i>A proteção ao abrigo do GDPR é comprometida pela proposta de regulamento</i>	<i>11</i>
4. OUTROS MOTIVOS DE PREOCUPAÇÃO.....	18
<i>O âmbito de aplicação territorial e material tem de ser alargado</i>	<i>18</i>
<i>A proteção dos equipamentos terminais carece de reforço</i>	<i>19</i>
<i>Marketing direto</i>	<i>23</i>
<i>Calendário</i>	<i>26</i>
<i>Outras preocupações</i>	<i>26</i>
5. SUGESTÕES DE ESCLARECIMENTO PARA GARANTIR A SEGURANÇA JURÍDICA	30
<i>Esclarecimentos sobre o âmbito de aplicação.....</i>	<i>30</i>
<i>Esclarecimentos sobre a noção de consentimento e a sua aplicação</i>	<i>33</i>
<i>Esclarecimentos sobre a localização e outros metadados.....</i>	<i>34</i>
<i>Esclarecimentos sobre as comunicações não solicitadas</i>	<i>36</i>
<i>Esclarecimentos sobre a aplicação dos instrumentos em matéria de direitos fundamentais</i>	<i>37</i>
<i>Outros esclarecimentos</i>	<i>38</i>

1. INTRODUÇÃO

1. O grupo de trabalho do artigo 29.º (a seguir designado por «grupo de trabalho» ou «WP29») acolhe com agrado a proposta de regulamento da Comissão Europeia (CE) relativo à privacidade e às comunicações eletrónicas (a seguir designado por «proposta de regulamento» ou «regulamento relativo à privacidade e às comunicações eletrónicas») ¹, que visa substituir a Diretiva relativa à privacidade e às comunicações eletrónicas².
2. Muitos aspetos da proposta de regulamento são positivos, tendo a Comissão Europeia dado um passo importante com a adoção da proposta de regulamento. A proposta de regulamento pode, no entanto, ser aperfeiçoada, o que serviria não só para proteger melhor os utilizadores finais, mas também para introduzir mais segurança jurídica para todas as partes interessadas envolvidas.
3. O grupo de trabalho tem, assim, vários motivos de preocupação e recomendações, cujos esclarecimentos devem ser abordados pelo Parlamento Europeu e o Conselho no seu debate sobre a proposta de regulamento. O presente parecer examinará em primeiro lugar os aspetos positivos da proposta de regulamento e, em seguida, realçará as questões de preocupação e os pontos que carecem de esclarecimento.

2. ASPETOS POSITIVOS DA PROPOSTA DE REGULAMENTO

HARMONIZAÇÃO EM TODA A UE, ALINHAMENTO DAS COIMAS E EXECUÇÃO EXCLUSIVA PELAS AUTORIDADES RESPONSÁVEIS PELA PROTEÇÃO DOS DADOS (APD)

4. O grupo de trabalho acolhe com agrado **a escolha de um regulamento como instrumento jurídico**, o que garante a uniformidade das regras em toda a UE (com algumas exceções, que serão debatidas a seguir) e proporciona clareza às autoridades de controlo e organizações similares. Além disso, tendo em conta o papel essencial desempenhado pelo Regulamento Geral sobre a Proteção de Dados (GDPR)³ na proposta de regulamento, tal contribui para assegurar a coerência entre os dois instrumentos. Simultaneamente, **a escolha (manutenção) de um instrumento jurídico complementar** é positiva. A proteção da confidencialidade das

¹ Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas), 2017/0003 (COD), URL: [http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017PC0010R\(01\)&qid=1507199911678&from=PT](http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017PC0010R(01)&qid=1507199911678&from=PT)

² 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. 37-47, URL: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32002L0058>

³ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), JO L 119 de 4.5.2016, p. 1-88, URL: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>

comunicações e dos equipamentos terminais apresenta características específicas que não são abordadas pelo GDPR. Por conseguinte, são necessárias disposições complementares referentes a estes tipos de serviços, a fim de assegurar a proteção adequada deste direito fundamental. Neste contexto, o grupo de trabalho **apoia igualmente a abordagem baseada em princípios, escolhida na proposta de regulamento, de uma ampla proibição e estritas exceções**, bem como considera que a introdução de exceções indeterminadas em conformidade com o artigo 6.º do GDPR e, nomeadamente, o artigo 6.º, alínea f), do GDPR, deve ser evitada.

5. **A execução dessas regras pela mesma autoridade responsável pelo controlo do cumprimento do GDPR** permitirá reforçar a coerência entre os dois instrumentos. Dada a relação existente entre a proteção dos dados pessoais e a proteção da confidencialidade das comunicações e dos equipamentos terminais, convém que a execução das disposições da proposta de regulamento seja confiada à mesma autoridade de controlo competente pela execução do GDPR (considerando 38 e artigo 18.º da proposta de regulamento). Mais ainda, a jurisprudência do Tribunal de Justiça da União Europeia (TJUE)⁴ reitera que é essencial que a autoridade de controlo seja independente, tal como previsto no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia («Carta»). Na prática, no entanto, esta situação acarretaria uma carga de trabalho suplementar considerável para as APD, sem quaisquer garantias de cumprimento na eventualidade de não ser obtido um orçamento suplementar. As APD congratulam-se, por conseguinte, com o considerando 38 da proposta de regulamento, o qual sublinha que cada autoridade de controlo deve dispor dos recursos humanos e financeiros, instalações e infraestruturas suplementares necessários ao bom desempenho das funções previstas no novo regulamento. É de saudar ainda o facto de o artigo 18.º, n.º 2, constituir a base jurídica para a cooperação entre as autoridades de controlo da proposta de regulamento e as autoridades reguladoras nacionais (ARN) da proposta de Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas («CECE»)⁵.
6. Dada a estreita relação existente entre a proposta de regulamento e o GDPR, **o alinhamento das coimas ao abrigo da proposta de regulamento com o GDPR é igualmente bem-vindo**. As atividades abrangidas pelo âmbito de aplicação da proposta de regulamento são muito sensíveis, envolvendo, *nomeadamente*, as interferências com comunicações confidenciais e equipamentos terminais. O nível das coimas deve ser proporcional ao presente contexto sensível. Este contexto constitui também a razão pela qual a harmonização em toda a UE é importante, a fim de proporcionar o mesmo elevado nível de proteção em toda a região. O artigo 23.º da proposta de regulamento prevê a aplicação de coimas efetivas pela violação do

⁴ Ver, por exemplo, acórdão do TJUE de 6 de outubro de 2015, processo C-362/14 - *Schrems (porto seguro)*, n.º 41, e acórdão do TJUE de 21 de dezembro de 2016, processo C-203/15 - *Tele2 Sverige* e processo C-698/15 - *Watson e o.*, n.º 123.

⁵ Proposta de diretiva do Parlamento Europeu e do Conselho que estabelece o Código Europeu das Comunicações Eletrónicas (Reformulação), 2016/0288 (COD), 12.10.2016, URL: http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=comnat:COM_2016_0590_FIN

regulamento, semelhantes ao nível das coimas fixadas para a violação das regras constantes do GDPR, exceto em relação a determinados pontos (ver nota 38).

7. **A supressão das regras relativas à notificação de violações de dados específicos** da presente legislação é igualmente bem-vinda, no sentido de evitar sobreposições desnecessárias com os requisitos em matéria de violação de dados do GDPR.
8. **É de saudar ainda o facto de a tónica incidir agora na garantia de um nível de proteção igual para todos os utilizadores finais**, uma vez que a proposta de regulamento tornou supérfluo o conceito de distinção entre «assinantes» e outros utilizadores de serviços de comunicações eletrónicas.

ALARGAMENTO DO ÂMBITO DE APLICAÇÃO QUANDO COMPARADO COM A DIRETIVA RELATIVA À PRIVACIDADE E ÀS COMUNICAÇÕES ELETRÓNICAS

9. O grupo de trabalho saúda **o alargamento do âmbito de aplicação da proposta de regulamento, com vista a incluir os fornecedores de conteúdos audiovisuais em linha (OTT)**, serviços que são funcionalmente equivalentes aos meios de comunicação mais tradicionais e, por conseguinte, têm um potencial de impacto semelhante sobre a privacidade e o direito à confidencialidade das comunicações dos cidadãos da UE. O grupo de trabalho acolhe com especial agrado o facto de que todas as categorias de OTT (OTT0, OTT1 e alguns OTT2)⁶ já se encontram abrangidas pelo âmbito de aplicação do regulamento, uma vez que este não só inclui os meios de comunicação tradicionais (OTT0), mas também os serviços funcionalmente equivalentes (OTT1), tal como referido no artigo 8.º, n.º 1, alínea c), da proposta de regulamento. Além disso, é também positivo que, a par das definições no âmbito do CECE, alguns OTT2 sejam abrangidos sempre que proporcionem comunicações interpessoais e interativas acessórias intrinsecamente ligadas ao seu serviço, tais como em jogos, aplicações de encontros ou sítios de opiniões (artigo 4.º, n.º 2, da proposta de regulamento). Do mesmo modo, é de saudar **o esclarecimento de que a proteção abrange igualmente a interação entre máquinas**. O considerando 12 torna claro que os dispositivos que comunicam entre si são abrangidos pelo âmbito da proteção conferida pela proposta de regulamento. Trata-se de uma medida desejável, atendendo a que essas comunicações contêm, muitas vezes, informações protegidas ao abrigo dos direitos à privacidade. Não obstante, a aplicabilidade poderá ser objeto de esclarecimento (ver nota 40h).
10. É igualmente positivo que **a proposta de regulamento contemple, de forma clara, conteúdos e metadados associados**. O considerando 14 evidencia que a definição de «dados de comunicações eletrónicas» constante do artigo 4.º, n.º 3, alínea a), pretende

⁶ Para mais explicações dos referidos termos, ver ORECE, *Report on OTT Services* (Relatório sobre serviços OTT), BoR (16) 35, 29 de janeiro de 2016, p. 15 e 16, URL:

http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services Ver também o comentário constante do relatório de que as categorias são concebidas como conceitos a utilizar no debate sobre a revisão e não constituem conceitos jurídicos.

ser suficientemente abrangente, por forma a incluir *todos* os conteúdos e metadados associados, independentemente, por exemplo, dos meios de envio de sinais. No entanto, o grupo de trabalho assinala na nota 39, como um motivo de preocupação, que a atual definição de «dados de comunicações eletrónicas» ainda é objeto de debate. Em consonância com este alargamento do âmbito de aplicação, o grupo de trabalho considera o **reconhecimento de que os metadados podem revelar dados sensíveis** (ver ponto 2.2 da exposição de motivos; considerando 2) uma adição fundamental. O grupo de trabalho congratula-se com o facto de a Comissão Europeia, ao fazê-lo, integrar as apreciações do Tribunal de Justiça constantes dos processos apenas *Digital Rights Ireland e Seitlinger e o.* e *Tele2 Sverige e Watson e o.* O WP29 aplaude igualmente o **reconhecimento de que a análise dos conteúdos constitui um tratamento de elevado risco**. O considerando 19 e o artigo 6.º, n.º 3, alínea b), estabelecem a presunção jurídica lógica de que a digitalização de conteúdos constitui, ao abrigo do artigo 35.º do GDPR, um tratamento de elevado risco e aparentemente, independentemente da existência de um risco residual elevado, requer sempre a consulta prévia da (principal) autoridade responsável pela proteção dos dados. Ao mesmo tempo, o grupo de trabalho manifesta preocupação com o âmbito da definição de «metadados» e o facto de a análise de metadados não estar sujeita ao mesmo requisito obrigatório de avaliação de impacto sobre a proteção de dados (ver notas 33 e 46).

11. É ainda de saudar o contínuo **reconhecimento da importância da anonimização**. Na Diretiva relativa à privacidade e às comunicações eletrónicas, as medidas de anonimização já desempenhavam um papel na garantia da compatibilidade (por exemplo, artigo 6.º, n.º 1, da Diretiva relativa à privacidade e às comunicações eletrónicas, que estabelece que os dados de tráfego devem ser eliminados ou tornados anónimos quando deixam de ser necessários para efeitos da transmissão da comunicação). No artigo 6, n.º 2, alínea c), e no artigo 6.º, n.º 3, alínea b), da proposta de regulamento, é permitida uma exceção à proibição do tratamento de metadados e conteúdos com base no consentimento, desde que a finalidade ou finalidades em causa «*não possam ser atingidas através do tratamento de informações tornadas anónimas*». A imposição de tais medidas de proteção da privacidade, a par do pedido de consentimento aos utilizadores, protege estes utilizadores de um tratamento injustificado. No entanto, o grupo de trabalho tem, ao mesmo tempo, um motivo de grande preocupação de que a adoção dessas técnicas de anonimização não seja exigida aquando do rastreio da localização dos utilizadores através dos seus equipamentos móveis (ver nota 17). Além disso, mesmo quando são aplicadas medidas de anonimização, os prestadores de serviços deverão sempre efetuar uma avaliação de impacto sobre a proteção de dados (AIPD) (ver notas 33 e 46), e, por conseguinte, o grupo de trabalho propõe uma obrigação adicional de tornar pública a forma como os dados são anonimizados e agregados (ver nota 42b).
12. Outro ponto positivo reside na **ampla formulação da proteção dos equipamentos terminais**. O considerando 20 e o artigo 8.º definem que as tecnologias utilizadas para aceder aos equipamentos terminais não são relevantes: quaisquer interferências com o equipamento terminal, incluindo a utilização das suas capacidades de tratamento, carecem do consentimento do utilizador final (com algumas exceções). A Comissão Europeia já confirmou, construtivamente, que a «impressão digital do

aparelho» é abrangida por esta disposição. Mais ainda, o grupo de trabalho regista com agrado que a inobservância por parte de um terceiro das preferências expressas nas **predefinições do programa de navegação** de uma pessoa **seja oponível**, tal como descrito no considerando 22. Esta possibilidade é útil para as situações em que um terceiro (por exemplo, uma rede de publicidade) não respeite essas predefinições. No entanto, esta possibilidade deveria igualmente ser consagrada numa disposição pertinente da proposta de regulamento.

13. Por último, é de saudar a constante **inclusão das pessoas coletivas no âmbito de aplicação da proposta de regulamento** (ver ponto 2.2 da exposição de motivos; considerandos 3, 33 e 42; artigos 1.º, 15.º e 16.º, n.º 5). Tal já se encontrava assegurado pela Diretiva relativa à privacidade e às comunicações eletrónicas, mas, como as autoridades responsáveis pela proteção dos dados serão incumbidas da execução das novas regras, convém especificamente salientar esse facto. Esta situação permite às autoridades responsáveis pela proteção dos dados tomar medidas nos casos em que as pessoas coletivas são vítimas de uma infração, por exemplo quando as empresas recebem *spam* ou as suas comunicações são sub-repticiamente controladas. Não obstante, o grupo de trabalho regista igualmente, como motivos de preocupação, que a aplicação da noção de consentimento às pessoas coletivas não está bem definida (ver nota 41a) e que também não é claro o que se entende por «os interesses legítimos» das pessoas coletivas em caso de *marketing* direto (ver nota 43c).

APLICAÇÃO ORIENTADA DA NOÇÃO DE CONSENTIMENTO

14. O grupo de trabalho congratula-se com outra categoria de melhorias relacionada com a aplicação e a interpretação da noção de consentimento. Primeiro, é de saudar a **clarificação de que o acesso à Internet e a telefonia (móvel) são serviços essenciais e que os prestadores desses serviços não podem «obrigar» os seus clientes a dar o seu consentimento para quaisquer operações de tratamento de dados desnecessárias para a prestação do serviço essencial em si**. No considerando 18, é de referir, em especial, que os serviços de acesso à Internet de banda larga básica e de comunicações de voz devem ser considerados serviços essenciais, o que significa que, dada a dependência das pessoas em aceder a esses serviços, o consentimento para o tratamento dos dados das suas comunicações para essas finalidades adicionais (por exemplo, tratamento para fins de publicidade ou de *marketing*) não pode ser válido. Ao mesmo tempo, o grupo de trabalho receia que esta clarificação seja demasiado limitada. Os serviços de determinados fornecedores OTT também podem ser considerados serviços essenciais, devendo, por conseguinte, o regulamento relativo à privacidade e às comunicações eletrónicas proibir especificamente as opções de «pegar ou largar» noutras circunstâncias (ver nota 20).
15. Adicionalmente, é positiva a harmonização **do requisito de consentimento aplicável à inclusão dos dados pessoais das pessoas singulares em listas**. Ao abrigo do artigo 15.º da proposta de regulamento, o tratamento de dados em listas acessíveis ao público só é permitido com o consentimento das pessoas singulares e com a possibilidade de oposição no caso das pessoas coletivas. Este aspeto é aprofundado

no considerando 31, que regista que este consentimento deve ser específico no que respeita às categorias de dados pessoais específicos que devem figurar na lista. No entanto, o grupo de trabalho assinala, como uma preocupação, que a proposta de regulamento poderia ser mais clara, no sentido de que será necessário o consentimento específico em separado para a pesquisa e a pesquisa inversa (ver nota 37).

16. **A nova exceção específica para a interferência não intrusiva com os equipamentos terminais** é também apreciada. O WP29 considera útil que a proposta de regulamento clarifique que a proibição não é aplicável à medição do tráfego de um sítio Web [ao abrigo da estrita exceção de que essa medição seja efetuada pelo prestador do serviço da sociedade de informação solicitado pelo utilizador final (ver artigo 8.º, n.º 1, alínea d), da proposta de regulamento)]. Para mais informações, ver considerando 21. Contudo, o grupo de trabalho sugere a utilização de uma definição mais neutra do ponto de vista tecnológico e a clarificação da aplicabilidade desta exceção (ver nota 25).

3. MOTIVOS DE GRANDE PREOCUPAÇÃO

A PROTEÇÃO AO ABRIGO DO GDPR É COMPROMETIDA PELA PROPOSTA DE REGULAMENTO

Tal como mencionado anteriormente, existe uma série de melhorias fundamentais na proposta de regulamento. No entanto, existem também motivos que suscitem preocupações, com diferentes graus de gravidade. Na presente secção, o grupo de trabalho aborda as quatro questões sobre as quais **exprime a sua profunda preocupação**. Trata-se de disposições que **comprometem o nível de proteção conferido pelo GDPR**:

17. As obrigações previstas no regulamento para o rastreio de localização dos equipamentos terminais devem cumprir os requisitos do GDPR. O artigo 8.º, n.º 2, alínea b), da proposta de regulamento apenas exige a afixação de um aviso e a aplicação de medidas de segurança para a recolha das informações emitidas pelo equipamento terminal. O artigo 8.º, n.º 2, alínea b), assinala ainda que a pessoa responsável por essa recolha deve indicar qualquer medida que o utilizador final dos equipamentos terminais possa tomar para reduzir ou fazer cessar a recolha de dados. Desta forma, o artigo 8.º, n.º 2, alínea b), suscita a impressão de que as organizações podem recolher informações emitidas pelos equipamentos terminais para rastrear os movimentos físicos das pessoas [tais como rastreio via *Wi-Fi* («WiFi-tracking») ou rastreio via *Bluetooth* («Bluetooth-tracking»)] sem o consentimento da pessoa em causa. A parte que recolhe estes dados poderá aparentemente dar cumprimento ao acima exposto mediante um aviso informando os utilizadores para desligar os seus dispositivos se não quiserem ser rastreados. Uma abordagem desta natureza seria contrária a um dos objetivos fundamentais da política das telecomunicações da Comissão Europeia de fornecimento de conectividade à Internet móvel de elevado débito com fortes garantias de proteção da privacidade a um preço reduzido a todos os europeus e a nível transfronteiriço.

Ademais, a proposta de regulamento não impõe quaisquer limitações claras no que se refere ao âmbito da recolha de dados ou às atividades de tratamento posteriores. Neste contexto, é de salientar que estes endereços MAC constituem dados pessoais, mesmo após terem sido tomadas medidas de segurança, como a técnica de controlo da integridade dos dados («hashing»). Ao não impor outros requisitos ou limitações, o nível de proteção desses dados pessoais ao abrigo da proposta de regulamento é significativamente inferior àquele ao abrigo do GDPR, segundo o qual esse rastreio deverá ser efetuado de forma leal, lícita e transparente. O considerando 25 inutilmente assinala ainda que algumas das funcionalidades de rastreio via *Wi-Fi* não acarretam riscos de privacidade elevados, ao passo que outras sim, como, por exemplo, o rastreio das pessoas ao longo do tempo. Embora o grupo de trabalho valorize o reconhecimento de que esta última funcionalidade acarreta riscos de privacidade elevados, de nada serve decidir já, antecipadamente, que determinadas outras funcionalidades não acarretam esse risco, sem que se proceda a uma nova avaliação das circunstâncias e da proporcionalidade do tratamento. A realização da referida avaliação deve atender às seguintes condições relativas ao rastreio via *Wi-Fi* não anonimizado.

Consoante as circunstâncias e as finalidades da recolha de dados, o rastreio ao abrigo do GDPR poderá estar subordinado à obtenção de consentimento ou poderá apenas ser efetuado se os dados pessoais recolhidos forem tornados anónimos. Esta anonimização é, de preferência, realizada imediatamente após a recolha. Caso a anonimização imediata não seja possível, tendo em conta os fins a que os dados recolhidos se destinam, esses dados só podem ser tratados durante um período em que não estejam anonimizados nas seguintes condições: i) a finalidade da recolha de dados deve restringir-se à simples contagem estatística (ver exemplos abaixo), ii) o rastreio é limitado no tempo e no espaço, na medida do estritamente necessário para a referida finalidade, iii) os dados são apagados ou tornados anónimos imediatamente a seguir e iv) deve existir uma possibilidade eficaz de autoexclusão. Em quaisquer circunstâncias, os responsáveis pelo tratamento devem, evidentemente, respeitar a exigência de prestação de informações apropriadas.

O grupo de trabalho receia que uma potencial oferta de uma autoexclusão individual por cada organização que recolhe estes dados acarretaria encargos inaceitáveis para os cidadãos, tendo em conta o aumento da implantação dessas tecnologias de rastreio pelas organizações quer do setor público quer do setor privado. Por conseguinte, o grupo de trabalho apela ao legislador da União para que promova o desenvolvimento de normas técnicas para os dispositivos sinalizarem automaticamente uma oposição contra esse rastreio, bem como para garantir que a adesão a um sinal desse tipo tem força executória.

A título exemplificativo, o consentimento ao abrigo do GDPR será provavelmente necessário no caso de um responsável pelo tratamento de dados recolher e gravar os endereços MAC (de *Wi-Fi* ou *Bluetooth*) indiretamente identificáveis dos dispositivos, e calcular a localização do utilizador, com o fito de rastrear a localização do utilizador ao longo do tempo, por exemplo, em vários estabelecimentos. Esta situação é particularmente evidente quando esse rastreio é realizado em locais públicos, onde os utilizadores têm uma expectativa legítima de

não serem identificados ou rastreados, ainda que os endereços MAC dos transeuntes sejam recolhidos. Esse consentimento poderá ser obtido, por exemplo, com a ajuda de uma aplicação móvel, que convida os utilizadores a permitirem o rastreio da sua localização em zonas específicas em troca de ofertas comerciais, ou mediante a oferta de pontos de registo dentro de locais específicos ou através de um módulo de consentimento em zonas de Internet sem fios.

Apenas num número limitado de circunstâncias, os responsáveis pelo tratamento de dados poderão ser autorizados a tratar as informações emitidas pelo equipamento terminal para efeitos de rastreio dos seus movimentos físicos sem o consentimento da pessoa em causa. Por exemplo, essa situação pode ocorrer no caso da contagem da quantidade de clientes dentro de um local específico ou aquando da recolha de dados emitidos em ambos os lados de um ponto de controlo de segurança para indicar o tempo de espera. No entanto, em ambos os exemplos, os dados têm de ser apagados ou anonimizados logo que os fins estatísticos possam ser cumpridos, o que significa que os endereços MAC dos dispositivos dos visitantes dentro de um local específico, como, por exemplo, um estabelecimento, devem ser imediatamente anonimizados após a recolha, sem qualquer armazenamento permanente dos endereços MAC, e de forma que a reidentificabilidade fique tecnicamente excluída. No caso do cálculo do tempo de espera, os endereços MAC têm de ser apagados ou anonimizados logo que deixem de ser relevantes para o referido cálculo (por exemplo, porque o visitante chegou ao outro lado do controlo de segurança ou porque abandonou a fila de espera).

Além disso, o responsável pelo tratamento de dados tem de cumprir os requisitos da minimização dos dados (por exemplo, não efetuar o rastreio permanente sempre que o objetivo se limite ao horário de funcionamento da loja e/ou à amostragem por intervalos). Os responsáveis pelo tratamento de dados devem igualmente tomar outras medidas de atenuação destinadas a garantir a inexistência de impacto ou um impacto reduzido nos direitos à privacidade dos utilizadores, por exemplo para proteger a privacidade das pessoas que vivem junto a um ponto de recolha.

A escolha de uma mera obrigação de afixação de avisos constante do artigo 8.º, n.º 2, da proposta de regulamento é ainda mais notável dada a conclusão constante do considerando 20 de que as informações relacionadas com o dispositivo do utilizador final podem igualmente ser recolhidas à distância para efeitos de identificação e rastreio, e que esse tratamento, de acordo com a proposta de regulamento, pode constituir uma grave intrusão na privacidade desses utilizadores finais. Ademais, a referida obrigação não excede a obrigação de facultar informações já prevista nos artigos 13.º e 14.º do GDPR. A grave intrusão na privacidade gerada pelo rastreio é ainda agravada pelo potencial acesso de terceiros aos dados recolhidos, tal como a possibilidade de as autoridades de aplicação da lei identificarem os utilizadores finais com base no(s) endereço(s) MAC armazenado(s) e difundido(s) pelos seus dispositivos móveis.

18. As condições de autorização da análise dos conteúdos e metadados devem ser elaboradas.

No artigo 6.º da proposta de regulamento, são atribuídos diferentes níveis de proteção aos metadados e aos conteúdos. O WP29 não apoia esta distinção: ambas as categorias de dados são altamente sensíveis. Por conseguinte, deve ser atribuído o mesmo nível elevado de proteção tanto aos metadados como aos conteúdos. Deste modo, o ponto de partida deve consistir na proibição do tratamento de metadados e conteúdos sem o consentimento de todos os utilizadores finais (ou seja, remetentes e destinatários).

No entanto, consoante a finalidade, determinado tipo de tratamento pode ser autorizado sem consentimento caso seja estritamente necessário para as seguintes finalidades:

- Os fornecedores podem tratar dados de comunicações eletrónicas para os efeitos referidos no artigo 6.º, n.º 1, alíneas a) e b), e no artigo 6.º, n.º 2, alíneas a) e b), da proposta de regulamento⁷.
- Importa esclarecer que determinadas técnicas de deteção/filtragem de *spam* e de mitigação de *botnets* poderão também ser consideradas estritamente necessárias para detetar ou impedir a utilização abusiva de serviços de comunicações eletrónicas (artigo 6.º, n.º 2, alínea b)). No que concerne à filtragem de *spam*, devem ser oferecidas, sempre que tal seja tecnicamente possível, amplas opções de autoexclusão aos utilizadores finais que recebem *spam*.
- Convém esclarecer que a análise dos dados de comunicações eletrónicas para efeitos de atendimento ao cliente pode igualmente ser abrangida pela exceção «se tal for necessário para proceder à faturação» (ver artigo 6, n.º 2, alínea b)). Os metadados em causa podem ser conservados até ao final do período durante o qual uma fatura pode ser contestada judicialmente ou exigido o seu pagamento em conformidade com o direito nacional. Os dados relevantes (tais como os URL) só podem ser conservados a pedido do utilizador final e, nesse caso, apenas por um período estritamente necessário para a resolução de um litígio relativo a uma fatura (o que significa que o artigo 7.º, n.º 3, deve, por conseguinte, ser alterado).
- Assim, deverá ser possível tratar os dados das comunicações eletrónicas para efeitos da prestação de serviços explicitamente solicitados pelo utilizador final, tais como a funcionalidade de pesquisa ou indexação por palavras-chave, os assistentes virtuais, os motores de conversão de texto em voz e os serviços de tradução. Para o efeito, é necessária a introdução de uma isenção aplicável à análise de tais dados para utilização puramente individual

⁷ No que se refere à necessidade de cumprir as obrigações em matéria de qualidade do serviço, tal como previsto no artigo 6.º, n.º 2, alínea a), da proposta de regulamento, os fornecedores devem ter em conta as condições descritas no Regulamento (UE) 2015/2120, nomeadamente o artigo 3.º e os considerandos 10 e 13 a 15. Com base nesta disposição, poder-se-á solicitar aos fornecedores o tratamento de dados de comunicações com vista à deteção e filtragem de programas maliciosos e programas espíões, podendo estes ser autorizados a comprimir os dados.

(familiar), bem como para uma utilização relacionada com trabalhos individuais⁸. Esta situação será, assim, viável sem o consentimento de todos os utilizadores finais, mas só poderá ocorrer com o consentimento do utilizador final que solicita o serviço. Esse consentimento específico também impedirá o fornecedor de utilizar esses dados para finalidades diferentes.

Isto significa que a análise dos conteúdos e/ou metadados para todos as outras finalidades, tais como as análises, a definição de perfis, a publicidade comportamental ou outras finalidades em benefício (comercial) do fornecedor, carece do consentimento de todos os utilizadores finais cujos dados serão objeto de tratamento. Quanto a essas situações, a proposta de regulamento deve esclarecer que o simples ato de enviar uma mensagem de correio eletrónico ou outro tipo de comunicação de carácter pessoal a partir de outro serviço a um utilizador final que deu pessoalmente o seu consentimento para o tratamento dos seus conteúdos e metadados (por exemplo, por ocasião da assinatura de um serviço de correio eletrónico) não constitui um consentimento válido do remetente.

Por último, convém esclarecer que o tratamento de dados de pessoas envolvidas que não sejam os utilizadores finais (por exemplo, uma fotografia ou uma descrição de um terceiro numa troca entre duas pessoas) também tem de cumprir todas as disposições pertinentes do GDPR.

19. **Os equipamentos terminais e o *software* devem, por defeito, desincentivar, prevenir e proibir interferências ilícitas com os mesmos e fornecer informações sobre as opções.** Apesar de a proposta de regulamento obrigar os fornecedores de *software* que permite comunicações eletrónicas a «oferecer a possibilidade» de impedir uma forma limitada de interferência com o equipamento terminal e, aquando da instalação, obrigar os fornecedores de *software* a exigir que o utilizador final dê o seu consentimento relativamente a uma predefinição (artigo 10.º, n.ºs 1 e 2), essas opções não equivalem à *privacidade por defeito*. Além disso, a «possibilidade» de impedir determinadas interferências já existe atualmente e, até à data, não redundou na resolução suficiente do problema do rastreio injustificado. É precisamente por essa razão que, ao abrigo do GDPR, foi feita uma opção política refletida no sentido de introduzir os princípios da proteção de dados e privacidade desde a conceção e por defeito (artigo 25.º do GDPR). A proposta de regulamento põe em causa estes princípios no que diz respeito aos dados das comunicações e do dispositivo. Entretanto, a Diretiva Equipamentos de Rádio 2014/53/UE («DER»)⁹ (mencionada no considerando 10) apenas prevê uma obrigação de segurança muito limitada, exigindo que os equipamentos de rádio incluam «salvaguardas que assegurem a proteção dos dados pessoais e da privacidade do utilizador e do assinante» (artigo 3.º, n.º 3, alínea

⁸ Embora o considerando 13 da proposta de regulamento exclua expressamente as redes de empresas do âmbito de aplicação do regulamento, esta nova exceção atinente à utilização individual deve igualmente abordar a utilização dos serviços em nuvem pelos trabalhadores para utilização profissional, como as pesquisas no seu correio eletrónico.

⁹ Diretiva Equipamentos de Rádio 2014/53/UE.

e)), o que não pode substituir as predefinições de privacidade específica ao abrigo da proposta de regulamento. Neste contexto, importa ainda ressaltar o facto de o inquérito Eurobarómetro sobre privacidade e comunicações eletrónicas, publicado em dezembro de 2016, salientar que «[q]uase sete em cada dez pessoas (69 %) concordam totalmente que as predefinições do seu programa de navegação devam parar a partilha das suas informações»¹⁰. O grupo de trabalho manifesta uma preocupação distinta com as predefinições do programa de navegação e a definição de «terceiros». Ver nota 24. Mais ainda, não se deve esquecer que esta disposição não só se refere aos programas de navegação utilizados em computadores, mas também abrange outros tipos de *software* que permite a comunicação (incluindo sistemas operativos, aplicações móveis e interfaces de *software* para dispositivos conectados à Internet das Coisas). Em resumo, os equipamentos terminais e o *software* devem, *por defeito*, oferecer definições de proteção da privacidade e orientar os utilizadores através do menu de configuração para se desviarem dessas predefinições aquando da instalação. O referido menu de configuração deve ser sempre facilmente acessível durante a utilização. Para esse efeito, o grupo de trabalho exorta o legislador da União a clarificar o âmbito do artigo 10.º.

20. **O regulamento relativo à privacidade e às comunicações eletrónicas deve explicitamente proibir as barreiras de rastreio**, ou seja, a prática segundo a qual o acesso a um sítio Web ou serviço é recusado, a não ser que os interessados concordem em ser rastreados em outros sítios Web ou serviços. Tal como já foi assinalado em anteriores pareceres do grupo de trabalho sobre a Diretiva relativa à privacidade e às comunicações eletrónicas¹¹, estas abordagens de «pegar ou largar» são raramente legítimas¹². Sempre que a utilização das capacidades de tratamento e de armazenamento dos equipamentos terminais e a recolha de informações provenientes dos equipamentos terminais dos utilizadores finais permitam o rastreio das atividades dos utilizadores ao longo do tempo ou em vários serviços (por exemplo, diferentes sítios Web ou aplicações móveis), essas atividades de tratamento podem constituir uma grave intrusão na privacidade desses utilizadores. Dada a importância primordial da Internet para viabilizar o direito fundamental de liberdade de expressão, incluindo o direito de acesso à informação, a capacidade dos indivíduos para aceder aos conteúdos em linha não deve estar dependente da aceitação do rastreio das atividades nos dispositivos e sítios Web/aplicações móveis. O futuro regulamento relativo à privacidade e às comunicações eletrónicas deve, por conseguinte, especificar que o acesso aos conteúdos, por exemplo, em sítios Web e aplicações móveis não pode ser subordinado à aceitação dessas atividades de tratamento intrusivas, independentemente da tecnologia de rastreio aplicada, como, por exemplo, os testemunhos de conexão, a recolha da impressão digital do aparelho, a injeção de identificadores únicos ou outras técnicas de controlo. A necessidade desta proibição é

¹⁰ Ver *Flash Eurobarometer 443, Report e-Privacy* (Eurobarómetro Flash 443, Relatório sobre privacidade e comunicações eletrónicas) (publicado em dezembro de 2016), p. 5.

¹¹ Ver, por exemplo, *WP 240 (ePrivacy review)* [WP 240 (Revisão da Diretiva relativa à privacidade e às comunicações eletrónicas)], p. 16; WP 208 (isenção de consentimento), p. 5.

¹² A presente posição não prejudica o artigo 7.º, n.º 4, do GDPR, o que poderá também impedir as opções de «pegar ou largar» em outros casos em que tal se revele adequado.

reforçada pelo recente inquérito Eurobarómetro sobre privacidade e comunicações eletrónicas, que refere que «[q]uase dois terços dos inquiridos consideram inaceitável que as suas atividades em linha sejam controladas em troca de acesso ilimitado a um determinado sítio Web (64 %)».

21. Em resumo, no atinente aos quatro pontos acima referidos, **a proposta de regulamento deve cumprir a sua promessa de assegurar um nível de proteção igual ou superior ao do GDPR**. Efetivamente, o considerando 5 refere que a proposta de regulamento não baixa o nível de proteção de que beneficiam as pessoas ao abrigo do GDPR. No entanto, conforme a redação atual da proposta de regulamento, esta afirmação é incorreta, designadamente no tocante ao rastreio dos dispositivos (nota 17), ao princípio em falta da privacidade por defeito (nota 19) e ao consentimento (nota 18). Este aspeto é particularmente importante, uma vez que é referido, no mesmo considerando, que a proposta de regulamento constitui uma «*lex specialis* no que respeita ao GDPR e pormenoriza-o e completa-o no que diz respeito aos dados de comunicações eletrónicas que sejam considerados dados pessoais». O grupo de trabalho sugere que, no mínimo, o texto do regulamento relativo à privacidade e às comunicações eletrónicas especifique que:

- i) as proibições ao abrigo do regulamento relativo à privacidade e às comunicações eletrónicas prevalecem sobre as autorizações ao abrigo do GDPR (por exemplo, a proibição de interferência ao abrigo do artigo 5.º do regulamento relativo à privacidade e às comunicações eletrónicas tem precedência sobre os direitos dos prestadores de serviços de comunicações eletrónicas de proceder ao tratamento posterior de dados pessoais ao abrigo do artigo 5.º, n.º 1, alínea b), e do artigo 6.º, n.º 4, do GDPR);
- ii) nos casos em que o tratamento é autorizado ao abrigo de qualquer exceção (incluindo o consentimento) às proibições previstas no regulamento relativo à privacidade e às comunicações eletrónicas, esse tratamento, caso se trate de dados pessoais, terá ainda de cumprir todas as disposições pertinentes do GDPR;
- iii) nos casos em que o tratamento é autorizado ao abrigo de qualquer exceção às proibições previstas no regulamento relativo à privacidade e às comunicações eletrónicas, é proibido qualquer outro tratamento realizado com base nas disposições do GDPR, nomeadamente o tratamento para outros fins baseado no artigo 6.º, n.º 4, do GDPR. Tal não obstará a que os responsáveis pelo tratamento peçam consentimento adicional para novas operações de tratamento, nem impedirá os legisladores de prever exceções adicionais, limitadas e específicas no regulamento relativo à privacidade e às comunicações eletrónicas, por exemplo a fim de permitir o tratamento para fins de investigação científica ou para fins estatísticos ao abrigo do artigo 89.º do GDPR ou para a defesa de «interesses vitais» das pessoas nos termos do artigo 6.º, alínea d), do GDPR.

Ademais, o regulamento relativo à privacidade e às comunicações eletrónicas deve ser interpretado por forma a garantir que oferece, pelo menos, um nível de proteção igual ou, se for caso disso, superior ao do GDPR.

4. OUTROS MOTIVOS DE PREOCUPAÇÃO

Além dos motivos acima mencionados, o grupo de trabalho do artigo 29.º **manifesta a sua preocupação** com o que se segue.

O ÂMBITO DE APLICAÇÃO TERRITORIAL E MATERIAL TEM DE SER ALARGADO

22. **O termo «metadados» é definido de forma bastante restrita.** No artigo 4.º, alínea c), o termo é agora definido como «os dados tratados numa rede de comunicações eletrónicas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas» (o sublinhado foi aditado). A utilização do termo «rede» parece sugerir que apenas os dados gerados no decurso da prestação de serviços na camada «mais baixa» da rede são passíveis de ser considerados «metadados», o que pode significar que os dados gerados no decurso da prestação de um serviço OTT serão excluídos deste âmbito de aplicação. Esta situação afigura-se indesejável e, provavelmente, também não foi a pretendida, dada a intenção de alargar o âmbito de aplicação da proposta de regulamento aos prestadores de serviços OTT. A fim de resolver esta questão, a definição de «metadados das comunicações eletrónicas» deve ser alterada por forma a incluir todos os dados tratados para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas.

23. Mais ainda, é também motivo de preocupação o facto de **o âmbito de aplicação territorial da proposta de regulamento no tocante às organizações sem um estabelecimento situado no território da UE só abordar os prestadores de serviços de comunicações eletrónicas.** Nos termos da proposta de regulamento, o prestador de um serviço de comunicações eletrónicas que não esteja estabelecido na UE deve designar, por escrito, um representante na União (artigo 3.º, n.º 2). No considerando 9 é igualmente referido que o regulamento deve aplicar-se ao tratamento de dados efetuado pelos prestadores de serviços de comunicações eletrónicas, independentemente do local de realização do tratamento. O grupo de trabalho congratula-se com este esclarecimento. No entanto, uma vez que a formulação se restringe aos prestadores de serviços de comunicações eletrónicas, desconhece-se em que medida este âmbito de aplicação territorial é aplicável a outros tipos de partes [por exemplo, as partes que interferem ou recolhem informações transmitidas pelos equipamentos terminais dos utilizadores finais (ver artigo 3, n.º 1, alínea c), e artigo 8.º da proposta de regulamento)]. Por conseguinte, o grupo de trabalho propõe a alteração do artigo 3.º, n.ºs 2 e 5, com vista a incluir os fornecedores de listas acessíveis ao público, os fornecedores de *software* que permite comunicações eletrónicas e as pessoas que enviam comunicações comerciais diretas ou recolhem (outras) informações relacionadas com equipamentos terminais dos utilizadores finais ou neles armazenadas, sempre que as suas atividades sejam orientadas para os utilizadores na UE (ver considerando 8 da proposta de regulamento)¹³.

¹³ Ver artigo 3.º, n.º 2, do GDPR: «O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados

Outra categoria de preocupações prende-se com a insuficiente proteção dos equipamentos terminais na proposta de regulamento.

24. Primeiro, **a proposta de regulamento sugere incorretamente que o consentimento válido pode ser dado através de predefinições do programa de navegação não específicas.** O grupo de trabalho reconhece a consideração de que os utilizadores finais são, atualmente, cada vez mais convidados a dar o seu consentimento (considerando 22). As predefinições do programa de navegação (e de outro *software* comparável) têm um papel a desempenhar na resolução deste problema. No entanto, uma vez que as definições gerais do programa de navegação não se destinam a ser aplicáveis à aplicação de uma tecnologia de rastreio num caso individual, não são, assim, adequadas para dar o consentimento ao abrigo do artigo 7.º e considerando 32 do GDPR (dado que o consentimento não é suficientemente informado e específico). O utilizador final deve poder dar o seu consentimento separadamente por sítio Web ou aplicação móvel para o rastreio para diferentes fins (tais como, a partilha de meios de comunicação social ou publicidade). Um responsável pelo tratamento de dados de vários sítios Web ou aplicações móveis pode ainda solicitar o consentimento para todos os restantes sítios Web ou aplicações móveis sob o seu controlo, desde que esse pedido de consentimento seja apresentado separadamente.
- Além disso, o responsável pelo tratamento tem de cumprir todas as demais obrigações relacionadas com o consentimento, nomeadamente a obrigação de facultar aos utilizadores informações adequadas. Tanto no caso dos programas de navegação como no caso dos responsáveis pelo tratamento de dados, isto significa que seria inválido se apenas oferecessem a opção de «aceitar todos os testemunhos de conexão», uma vez que esta opção não permitiria aos utilizadores dar o seu consentimento granular necessário. No entanto, deverá ser viabilizada a possibilidade de os programas de navegação permitirem aos utilizadores efetuar uma escolha informada e consciente para aceitar todos os testemunhos de conexão, evitando, assim, quaisquer futuros pedidos de consentimento específico dos sítios Web que visitam.
- O grupo de trabalho recomenda vivamente que o regulamento relativo à privacidade e às comunicações eletrónicas imponha a obrigação de os programas de navegação terem implementados mecanismos técnicos como a norma «Não Rastrear», a fim de garantir aos utilizadores uma escolha e um controlo verdadeiros sobre as interferências com os seus dispositivos¹⁴.

procederem a um pagamento; b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.» Esta obrigação pode igualmente abranger exceções em conformidade com as orientações enunciadas no artigo 27.º, n.º 2, do GDPR.

¹⁴ Ver URL: <https://www.w3.org/TR/tracking-compliance/>. O n.º 7 esclarece o modelo de exceção e a distinção entre as exceções à escala da Internet e à escala do sítio Web. O n.º 6 contém as informações de leitura ótica que os responsáveis pelo tratamento de dados podem fornecer em termos do requisito de informação para a obtenção de consentimento.

Mais importante ainda, o regulamento relativo à privacidade e às comunicações eletrónicas deve assegurar que tanto a escolha relativa ao armazenamento das informações no dispositivo como o sinal NR de um programa de navegação são aceites como uma indicação juridicamente vinculativa do consentimento ou da recusa por todos os responsáveis pelo tratamento de dados. Esta condição não obsta à emissão de novas orientações por parte do grupo de trabalho sobre o cumprimento da norma NR, nomeadamente o princípio da limitação da finalidade, quando a norma for concluída (conclusão prevista para o final de 2017).

Os tipos implícitos de «consentimento», como um clique no sítio Web ou o deslocamento na página, não podem sobrepor-se às escolhas inerentes ao armazenamento e ao sinal NR. Uma importante vantagem da utilização desta norma reside no facto de não estar limitada à tecnologia de rastreio dos testemunhos de conexão, mas também contemplar outros tipos de rastreio, como a recolha de impressões digitais.

Ao tornar juridicamente obrigatória a adesão a esta norma, resolver-se-á ainda outro problema com a atual utilização do termo «terceiros» no artigo 10.º. De um modo geral, uma página Web ou uma aplicação móvel contém muitos elementos, quer sejam provenientes do próprio sítio Web, quer sejam elementos externos. E o código externo poderá igualmente ser executado no contexto do sítio Web visitado, informando, ao mesmo tempo, um servidor de terceiros. Um testemunho persistente («tracking cookie») pode ser servido por uma primeira parte quando um utilizador visita, por exemplo, um sítio de uma rede social. Esse sítio de rede social pode também consistir num terceiro quando o utilizador em causa visita outro sítio que contém uma interação com o referido sítio de rede social. Em todos estes casos, independentemente de dizer respeito ao «acesso» ou ao «armazenamento» de informações no dispositivo do utilizador final, constitui uma interferência com o dispositivo, para a qual é necessário o consentimento (a menos que seja aplicável uma das exceções). Na norma NR, esta questão é abordada mediante a utilização das expressões «à escala do sítio Web» e «à escala da Internet». Por conseguinte, para aumentar a segurança jurídica de todas as partes interessadas, a referência a «terceiros» no regulamento relativo à privacidade e às comunicações eletrónicas deve ser reformulada, por forma a abranger todas as entidades com as quais um dispositivo interage (porque armazenam ou têm acesso a informações no dispositivo).

A fim de tornar a norma «Não Rastrear» compatível com o elevado nível de proteção da confidencialidade das comunicações e a proteção de dados concedidos ao abrigo da Carta, o regulamento relativo à privacidade e às comunicações eletrónicas deverá especificar que os pedidos de rastreio à escala da Internet, ao contrário do rastreio à escala do sítio Web, devem ser apresentados separadamente e os utilizadores devem ser livres de aceitar ou recusar esses pedidos. Além disso, para proteger os utilizadores de frequentes pedidos de consentimento, o regulamento relativo à privacidade e às comunicações eletrónicas deve assegurar que a recusa em aceitar o rastreio à escala da Internet da parte de uma organização específica (através da norma «Não Rastrear» ou através de uma lista negra em separado) impede essa organização de solicitar futuros pedidos de consentimento, durante, pelo menos, seis meses. Esta regra não impede a referida organização, quando diretamente visitada pelo utilizador (ou seja, enquanto primeira parte), de solicitar o consentimento no seu próprio sítio Web (ou seja, um pedido de consentimento à escala do sítio Web). Na prática, isto

significa, por exemplo, que um sítio de transferência vídeo em contínuo que serve testemunhos persistentes pode solicitar o consentimento sempre que o utilizador visite esse sítio, mas não pode solicitar um novo pedido de consentimento durante um período de seis meses quando esse utilizador tenha recusado dar o seu consentimento e visite outros sítios Web que contêm vídeos servidos a partir do sítio Web de transferência em contínuo.

25. Adicionalmente, **a exceção de «medição de audiência da Web» está formulada de forma imprecisa.** O artigo 8.º, n.º 1, alínea d), da proposta de regulamento prevê uma exceção aplicável à medição de audiência da Web. O primeiro motivo de preocupação reside na indefinição desta expressão, que pode ser confundida com a definição de perfis de utilizadores. Na definição cumpre clarificar que esta exceção não pode ser utilizada para quaisquer efeitos de definição de perfis. A exceção deve ser unicamente aplicável às análises de utilização necessárias para a análise do desempenho do serviço solicitado pelo utilizador, mas não às análises do utilizador (ou seja, a análise do comportamento dos utilizadores identificáveis de um sítio Web, de uma aplicação móvel ou de um dispositivo). Por conseguinte, a exceção não pode ser utilizada em circunstâncias em que os dados podem ser ligados aos dados de utilizadores identificáveis, tratados pelo prestador de serviços ou por outros responsáveis pelo tratamento de dados. Mais ainda, a sua descrição sugere uma aplicação muito específica da tecnologia. A expressão «medição de audiência da Web» deve, por isso, ser redefinida de forma tecnologicamente neutra, a fim de abarcar também as informações de utilização analítica similares, extraídas de aplicações móveis, computadores vestíveis e dispositivos da Internet das Coisas.

O grupo de trabalho sugere que se retire inspiração da exceção neerlandesa, a qual é aplicável caso seja estritamente necessária para obter informações sobre a qualidade técnica ou a eficácia da prestação de um serviço da sociedade de informação e caso tenha pouco ou nenhum impacto na privacidade do assinante ou do utilizador final em causa (ver artigo 11.7a, n.º 3, alínea b), da lei neerlandesa das telecomunicações). Esta exceção tem em conta o facto de que a maior parte dos dados recolhidos através de análises da Web ou das aplicações móveis continua a constituir dados pessoais, o que significa que o tratamento destes dados é igualmente objeto do GDPR. Isto implica, por exemplo, que as análises de utilização podem também ser efetuadas por um organismo externo, mas somente se:

- i) esse organismo atuar na qualidade de subcontratante;
- ii) for celebrado um acordo de subcontratação compatível com o GDPR;
- iii) a tecnologia de análise utilizada evitar a reidentificação, designadamente, entre outros aspetos, a anonimização dos endereços IP dos utilizadores;
- iv) o(s) testemunho(s) de conexão específico(s) ou outros dados utilizados para a análise puderem ser utilizados unicamente para esse sítio específico, aplicação móvel ou computador vestível e não puderem ser associados a outros dados identificáveis;
- v) os utilizadores tiverem o direito de autoexclusão (ver igualmente notas 17 e 50 do presente parecer).

Embora o consentimento não seja necessário se estas condições forem satisfeitas, ainda assim os responsáveis pelo tratamento de dados devem facultar informações

adequadas aos utilizadores, por exemplo através dos campos de representação do estado de rastreio na norma «Não Rastrear»¹⁵.

26. O regulamento relativo à privacidade e às comunicações eletrónicas **deve garantir exceções aos requisitos de consentimento redigidas de forma precisa e estrita**. A redação da exceção ao requisito de consentimento para a interferência com dispositivos enunciada no artigo 8.º, n.º 1, alínea c), é quase idêntica à atual redação constante do artigo 5.º, n.º 3, da Diretiva relativa à privacidade e às comunicações eletrónicas – «*que sejam estritamente necessários para fornecer um serviço no âmbito da sociedade de informação que tenha sido explicitamente solicitado pelo assinante ou pelo utilizador*» –, porém o essencial termo «estritamente» é omitido e sem qualquer explicação. Esta omissão constitui uma preocupação por dois motivos. Primeiro, o disposto na Diretiva relativa à privacidade e às comunicações eletrónicas já deu origem a um amplo debate sobre o seu âmbito de aplicação entre os organismos e autoridades de controlo, pelo que a supressão do termo «estritamente» garantirá ainda menos segurança jurídica. Esta omissão constitui ainda uma preocupação, porque o grupo de trabalho já apresentou orientações sobre a interpretação do termo «estritamente» neste contexto. O grupo de trabalho propôs a seguinte clarificação no Parecer sobre a isenção de consentimento para a utilização de testemunhos de conexão (WP 194):

*«O testemunho é [estritamente] necessário para fornecer uma funcionalidade específica ao utilizador (ou assinante): se estiver desativado, a funcionalidade não estará disponível; A funcionalidade foi expressamente solicitada pelo utilizador (ou assinante), como parte de um serviço da sociedade da informação.»*¹⁶

Além disso, o grupo de trabalho esclareceu que:

*«os testemunhos de terceiros normalmente não são "estritamente necessários" para o utilizador que visita um sítio Web, uma vez que estão geralmente associados a um serviço distinto daquele que foi "expressamente solicitado pelo utilizador"»*¹⁷.

O grupo de trabalho acrescentou que a utilização de módulos de extensão para partilha de conteúdos em redes sociais destinados a não utilizadores de uma plataforma ou sítio Web também não devem ser considerados estritamente necessários.

Além disso, embora o artigo 6.º, n.º 1, alínea b), da proposta de regulamento permita o tratamento de dados de comunicações eletrónicas se tal for «necessário» para fins de segurança, o considerando 49 do GDPR exige que esse tratamento seja estritamente necessário. A omissão do termo «estritamente» poderá não ter sido

¹⁵ Ver: *Tracking Preference Expression (DNT)* [Expressão de Preferência de Rastreio (NR)], projeto do editor de 7 de março de 2016.

¹⁶ Grupo de Trabalho sobre a Proteção de Dados do Artigo 29.º, WP 194, Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão, adotado em 7 de junho de 2012, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_pt.pdf

¹⁷ Ibid.

intencional, na medida em que o considerando 21 da proposta de regulamento refere que o consentimento para a interferência não deve ser solicitado nos casos que sejam «estritamente» necessários. Não obstante, a proposta de regulamento constitui uma oportunidade para esclarecer ainda que o critério da necessidade no contexto do presente regulamento deve ser objeto de uma interpretação restritiva no que diz respeito a todas as exceções. O grupo de trabalho sugere, por conseguinte, que, no que diz respeito a todas as exceções previstas nos artigos 6.º e 8.º, n.º 1, da proposta de regulamento, o termo «estritamente» deva ser aditado antes de «necessário/necessárias».

Por outro lado, o regulamento relativo à privacidade e às comunicações eletrónicas deve explicitamente permitir a interferência com os equipamentos para a instalação de atualizações de segurança. O envio de atualizações de segurança através da Internet é o método preferido para a instalação dessas atualizações na maior parte dos dispositivos dos utilizadores finais. A instalação de atualizações é considerada uma interferência com os equipamentos terminais. Há um interesse legítimo em garantir que a segurança destes dispositivos permanece atualizada. Em geral, um fornecedor de *patches* de segurança deve, por conseguinte, poder instalar as atualizações de segurança estritamente necessárias sem o consentimento do utilizador final. No entanto, o grupo de trabalho questiona-se sobre se esta interferência pode beneficiar da exceção da «sociedade de informação» à proibição de interferência (artigo 8.º, n.º 1, alínea c)). Importa esclarecer que a instalação de atualizações de segurança é permitida no âmbito desta exceção, mas só na medida em que i) as atualizações de segurança são discretamente empacotadas e não alteram de forma alguma a funcionalidade do *software* no equipamento (incluindo a interação com outro *software* ou as definições escolhidas pelo utilizador), ii) o utilizador final é informado com antecedência cada vez que uma atualização é instalada e iii) o utilizador final tem a possibilidade de desligar a instalação automática dessas atualizações.

MARKETING DIRETO

Outra categoria de preocupações prende-se com a insuficiente proteção contra o *marketing* direto.

27. Primeiro, um motivo de preocupação reside no facto de **o âmbito do marketing direto ser demasiado limitado**. No artigo 4.º, n.º 3, alínea f), da proposta de regulamento, as «comunicações comerciais diretas» são definidas como «qualquer forma de publicidade, oral ou escrita, enviada a um ou mais utilizadores finais identificados ou identificáveis de serviços de comunicações eletrónicas». A utilização do termo «enviada» implica a utilização de meios de comunicação tecnológicos que envolvem necessariamente o envio de uma comunicação, ao passo que a maior parte da publicidade na Internet (através de plataformas de comunicação social ou em sítios Web) não implica o «envio» de publicidade no sentido estrito. Esta apreciação é reforçada pelos exemplos veiculados na definição em apreço (SMS, correio eletrónico) e no considerando 33. Todos eles referem-se a formas bastante tradicionais de comunicações comerciais, e, mesmo assim, a utilização de sistemas de chamada bastante tradicionais não é, discutivelmente, abrangida pelo âmbito de

aplicação. O artigo e o considerando devem ser alterados com vista a incluir toda a publicidade *enviada, dirigida ou apresentada* a um ou mais utilizadores finais identificados ou identificáveis. Além disso, há que assegurar ainda que a publicidade comportamental (com base nos perfis de utilizadores finais) é igualmente considerada uma comunicação comercial direta dirigida a «um ou mais utilizadores finais identificados ou identificáveis» (uma vez que essa publicidade é direcionada para utilizadores específicos e identificáveis).

Ademais, de acordo com o âmbito de aplicação proposto das «comunicações comerciais diretas», a proteção conferida pelo artigo 16.º, n.º 1, limitar-se-ia às mensagens que contêm material publicitário, não protegendo as pessoas de outras mensagens enviadas, dirigidas ou apresentadas para fins comerciais (tais como as mensagens de geração de oportunidades potenciais que procuram obter o consentimento, a promoção de opiniões políticas ou preferências de votação, a promoção de organizações de beneficência ou outras organizações sem fins lucrativos ou da marca geral de uma organização). Mais ainda, as máquinas de fax continuam a ser utilizadas como um método de *marketing* direto, embora não sejam mencionadas na definição. Por conseguinte, o artigo 4.º, n.º 3, alínea f), deve contemplar qualquer forma de publicidade, angariação ou promoção, inclusivamente para as organizações sem fins lucrativos, e deve explicitamente incluir as máquinas de fax conjuntamente com o correio eletrónico e os SMS (ver também a sugestão de esclarecimento na nota 43, alínea a)). Por último, o considerando 32 estipula que o *marketing* direto inclui as mensagens enviadas pelos partidos políticos para promover os seus partidos. Esta disposição deve ser atualizada, por forma a integrar os políticos e os candidatos às eleições que promovem a sua candidatura.

28. Segundo, **a retirada do consentimento para o *marketing* direto não é gratuita, nem é tão fácil como dar o consentimento.** A opção de retirar o consentimento ao abrigo da proposta de regulamento carece de esclarecimento, para assegurar a coerência e melhorar a proteção dos destinatários. O artigo 16.º, n.º 6, da proposta de regulamento prevê atualmente que os destinatários de *marketing* direto devem ser informados acerca das «informações necessárias para que estes possam exercer o seu direito de retirar, de forma fácil, o seu consentimento em relação à receção de novas comunicações comerciais» (o sublinhado foi aditado). Este entendimento é corroborado pelo considerando 34. Contudo, decorre do considerando 70 do GDPR que os titulares de dados ao abrigo do GDPR devem não só ter o direito de se opor ao tratamento para efeitos de *marketing* direto de forma fácil, mas também têm o direito a o fazer «gratuitamente». Este termo («gratuita») é igualmente utilizado no artigo 16.º, n.º 2, da proposta de regulamento, mas apenas no que se refere à possibilidade de autoexclusão do *marketing* direto com base nos dados de contacto obtidos no contexto de uma venda.

O artigo 7.º, n.º 3, do GDPR prevê que o consentimento deve ser tão fácil de retirar quanto de dar e que as pessoas devem poder retirar o seu consentimento a qualquer momento. Além disso, no seu Parecer 4/2010 sobre a FEDMA (WP 174), o grupo de trabalho já tinha reconhecido a importância de oferecer «um método simples, eficaz,

gratuito, direto e acessível de cancelar a subscrição» de *marketing* direto¹⁸. Esta norma de retirada do consentimento deve ser incluída nas regras relativas ao *marketing* direto da proposta de regulamento. O mesmo se aplica ao requisito previsto no artigo 7.º, n.º 3, do GDPR de que o consentimento deve ser tão fácil de retirar quanto de dar a qualquer momento.

29. A este respeito, **a forma de retirar o consentimento ou a autoexclusão das chamadas de *marketing* direto deve ser objeto de esclarecimento.** Com base no artigo 16.º, n.º 4, da proposta de regulamento, os Estados-Membros podem optar por um regime de autoexclusão relativamente às chamadas vocais de *marketing* direto. O regulamento relativo à privacidade e às comunicações eletrónicas deve especificar as modalidades da retirada do consentimento e da autoexclusão relativamente às chamadas de *marketing*. O considerando 36 especifica que os Estados-Membros *devem, pois, poder* estabelecer e/ou manter sistemas nacionais de autoexclusão. Com base nesta disposição, os Estados-Membros podem, por conseguinte, até mesmo permitir uma situação em que um utilizador tenha de optar pela autoexclusão junto de fornecedores de comunicações individuais. Uma implementação desta natureza não consegue proteger os utilizadores contra os incómodos das comunicações injustificadas¹⁹ ou proporcionar um mecanismo compatível com o GDPR para a retirada do consentimento de forma fácil e em qualquer momento. Por conseguinte, o regulamento deve especificar que cada Estado-Membro *deve* criar um registo nacional «Do-Not-Call» (registo nacional de números a não ligar). Mais ainda, o regulamento deve precisar que os destinatários das chamadas vocais dispõem de duas opções para retirar o seu consentimento: relativamente às futuras chamadas de determinada empresa ou organização e a possibilidade de, durante estas chamadas, inscrever-se no registo nacional «Do-Not-Call».

30. Outro motivo de preocupação reside no facto de **a utilização de falsas identidades aquando do envio de comunicações comerciais diretas não ser explicitamente proibida.** Convém notar que no considerando 34 se declara que «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» são proibidas. No entanto, no artigo 16.º, n.º 6, apenas se afirma que os utilizadores finais devem ser informados acerca «da identidade da pessoa coletiva ou singular por conta da qual a comunicação é transmitida». Esta obrigação de informar os destinatários acerca da identidade deve ser complementada com uma proibição clara de utilizar falsos endereços de contacto ou endereços de contacto ocultos para fins de *marketing* direto.

¹⁸ Grupo de Trabalho sobre a Proteção de Dados do Artigo 29.º, WP 174, Parecer 4/2010 sobre o código de conduta europeu da FEDMA relativo ao uso de dados pessoais no *marketing* direto, adotado em 13 de julho de 2010, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_pt.pdf

¹⁹ Por exemplo, no Reino Unido, a operadora de telecomunicações BT registou 31 milhões de chamadas incomodativas durante uma semana. Ver: <http://www.bbc.com/news/business-38635921>

31. Este motivo está associado a outra preocupação: **a exigência do prefixo para as chamadas de *marketing* direto é apresentada como uma alternativa à exigência de identificação da linha de contacto.** Ao abrigo do artigo 16.º, n.º 3, as chamadas de *marketing* direto são permitidas se o autor da chamada ou i) apresentar a identificação de uma linha na qual a pessoa singular ou coletiva que efetua a chamada pode ser contactada (artigo 16.º, n.º 3, alínea a)) ou ii) apresentar um código ou prefixo de identificação específico que indique que se trata de uma chamada comercial (artigo 16.º, n.º 3, alínea b)). Embora o grupo de trabalho acolha com agrado a obrigação de utilizar um prefixo, prevista no artigo 16.º, n.º 3, alínea b), considera, no entanto, que esta exigência não aborda a mesma questão abordada pela exigência de identificação da linha de contacto, prevista no artigo 16.º, n.º 3, alínea a). Enquanto a exigência do prefixo tem por objetivo permitir aos destinatários identificar à partida uma chamada comercial (e aplicar medidas destinadas a bloquear essas chamadas), a exigência de identificação da linha de contacto pretende proporcionar aos destinatários (e às autoridades de controlo) os meios para identificar e contactar o instigador da chamada comercial. Esta questão assume particular relevância no caso das chamadas automáticas, nas quais se verifica um forte desequilíbrio entre as possibilidades do responsável pelo *marketing* de enviar chamadas incomodativas e as possibilidades do destinatário de evitar essas chamadas. As exigências não devem, por conseguinte, ser alternativas, mas devem ser complementares entre si.

CALENDÁRIO

32. O grupo de trabalho do artigo 29.º felicita a Comissão Europeia pelo reconhecimento da necessidade de a proposta de regulamento entrar em vigor juntamente com o GDPR em maio de 2018, a fim de evitar incoerências entre os dois atos legislativos. No entanto, continua a ser preocupante que este seja um calendário ambicioso, o qual requer igualmente que o projeto do CECE seja concluído. O WP29 solicita, por isso, que todas as partes interessadas no processo legislativo se comprometam com o prazo de maio de 2018.

OUTRAS PREOCUPAÇÕES

A presente secção aborda uma série de preocupações acrescidas.

33. Primeiro, o WP29 manifesta preocupação com **a sugestão de que as medidas de conservação de dados não específicas são aceitáveis.** A exposição de motivos assinala que, ao abrigo da proposta de regulamento, os Estados-Membros continuam a ser livres de manter ou de criar quadros de conservação de dados nacionais que prevejam, nomeadamente, medidas de conservação específicas (ponto 1.3). Na sequência das deliberações dos processos apensos *Tele2 Sverige/Watson e o.*²⁰, é evidente que os quadros de conservação que prevejam qualquer outra coisa que não a

²⁰ ECLI:EU:C:2016:970, URL: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>

conservação específica não são permitidos ao abrigo da Carta (e, mesmo nesse caso, estão sujeitos a condições importantes como o controlo) e que o acesso generalizado aos metadados terá de ser considerado uma violação à essência do artigo 7.º, da mesma forma que o acesso generalizado ao conteúdo das comunicações eletrónicas assim o é (cf. TJUE, Schrems, e considerando 94). A redação desta frase sugere, assim, que os Estados-Membros dispõem de uma certa margem de manobra relativamente às medidas de conservação de dados, a qual não existe. A este respeito, **os metadados não beneficiam de um nível de proteção suficiente** na proposta de regulamento. Tal como referido na nota 10, o grupo de trabalho do artigo 29.º congratula-se com o reconhecimento de que os metadados podem revelar dados muito sensíveis. No entanto, os metadados enunciados na proposta de regulamento não beneficiam da proteção que decorre deste reconhecimento. Dado o carácter sensível dos metadados e, em especial, antes de uma análise nos termos do artigo 6.º, n.º 2, alínea c), deverá ser realizada uma avaliação de impacto sobre a proteção de dados (ver também nota 46).

34. Segundo, **a proposta de regulamento aumenta indesejavelmente as possibilidades de conservação de dados**. O artigo 11.º da proposta de regulamento faz referência ao artigo 23.º, n.º 1, alíneas a) a e), do GDPR ao descrever os efeitos para os quais os Estados-Membros podem restringir as obrigações e os direitos previstos nos artigos 5.º a 8.º do regulamento. O GDPR não prevê tais restrições no que respeita a determinadas categorias específicas de dados, em consonância com os elevados riscos para os titulares de dados. Embora o artigo 15.º da Diretiva relativa à privacidade e às comunicações eletrónicas preveja atualmente uma restrição semelhante, os efeitos são mais limitados. A nova proposta de regulamento possibilitará novas restrições para efeitos de «execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública» (artigo 23.º, n.º 1, alínea d), do GDPR) e de «[o]utros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social» (artigo 23.º, n.º 1, alínea e), do GDPR). Estes efeitos não são apenas elementos novos em relação à Diretiva relativa à privacidade e às comunicações eletrónicas, o último efeito enunciado no artigo 23.º, n.º 1, alínea d), e o efeito previsto no artigo 23.º, n.º 1, alínea e), são redigidos de forma extremamente genérica. Propõe-se, por conseguinte, que a referência ao artigo 23, n.º 1, alíneas a) a e), do GDPR seja suprimida e, em vez disso, sejam apenas mencionados os efeitos atualmente referidos no artigo 15.º da Diretiva relativa à privacidade e às comunicações eletrónicas.

35. **A obrigação de informar os utilizadores dos riscos de segurança tem um âmbito de aplicação minimalista**. O grupo de trabalho congratula-se com o facto de os prestadores de serviços deverem informar os utilizadores dos riscos de segurança e das medidas destinadas a dar resposta a esses riscos, como a encriptação (artigo 17.º e considerando 37). O título da disposição tem, no entanto, a seguinte redação: «Informações sobre os riscos de segurança detetados». O facto de o título fazer menção aos riscos detetados sugere que esta disposição só diz respeito às (potenciais) violações da segurança, embora a redação da disposição e do considerando apontem mais para a formação geral dos utilizadores finais. A título exemplificativo, se um

prestador de serviços detetar que o dispositivo de um utilizador está infetado com um programa malicioso e se tornou parte de um *botnet*, esta disposição parece impor uma obrigação direta ao prestador de informar o utilizador dos riscos daí resultantes. No entanto, o âmbito de aplicação da presente disposição é passível de ser esclarecido, não devendo limitar-se a este cenário específico. A disposição deve abranger, pelo menos, os riscos de segurança detetados em todos os equipamentos fornecidos ao utilizador final pelo fornecedor no âmbito da sua subscrição, como, por exemplo, roteadores e dispositivos móveis, e incluir formação sobre os riscos da alteração das definições que tenham sido estabelecidas para a proteção da privacidade, de acordo com o princípio da privacidade desde a conceção.

O grupo de trabalho preconiza que o âmbito de aplicação seja ampliado, por forma a incluir os fornecedores de *software* que permite comunicações eletrónicas (ver considerando 8) e, eventualmente, também uma nova categoria: os fornecedores de tecnologias essenciais para garantir a segurança das comunicações, que não são prestadores de serviços (por exemplo, os fornecedores de tecnologias de encriptação). No caso desta última ampliação, dever-se-á zelar por que esta obrigação não se sobreponha às obrigações de notificação da violação da segurança constantes de outros instrumentos como a Diretiva SRI²¹ e de outros instrumentos jurídicos em matéria de entidades que emitem certificados. Uma vez que esta última categoria de fornecedores de tecnologias não tem, geralmente, contacto direto com os utilizadores finais, convém ainda explicar de que forma podem cumprir esta obrigação de informação ao abrigo da presente disposição.

36. O grupo de trabalho acolhe favoravelmente as disposições dos artigos 2.º e 13.º, que se aplicarão aos serviços de comunicações interpessoais com base no número. No entanto, não é assim tão óbvio por que razão é que um **nível semelhante de proteção da privacidade não deverá também estar disponível para os serviços de chamadas OTT funcionalmente equivalentes.**
37. O grupo de trabalho manifesta igualmente a sua preocupação perante **a falta de clareza quanto ao granular consentimento para a pesquisa inversa em listas.** O artigo 15.º, n.º 2, da proposta de regulamento obriga os fornecedores a obterem o consentimento dos utilizadores finais antes de ativarem essas funções de pesquisa em relação aos seus dados (ver também considerando 31). O grupo de trabalho congratula-se com a harmonização do requisito de consentimento no atinente à inclusão em listas, mas lamenta a ausência de granularidade no que toca aos diferentes tipos de pesquisas. A atual Diretiva relativa à privacidade e às comunicações eletrónicas permite aos Estados-Membros exigirem a solicitação do consentimento em separado para a pesquisa inversa, com base no artigo 12.º, n.º 3. Este artigo estipula que *«[o]s Estados-Membros poderão exigir que o consentimento adicional dos assinantes seja solicitado para qualquer utilização de uma lista pública*

²¹ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, JO L 194 de 19.7.2016, p. 1-30, URL: <http://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1507563056463&uri=CELEX:32016L1148>

que não a busca de coordenadas das pessoas com base no nome e, se necessário, num mínimo de outros elementos de identificação». Com base nesta disposição, em muitos Estados-Membros é necessário um consentimento em separado para as funcionalidades de pesquisa inversa, tendo em conta os diferentes níveis de identificabilidade e, por conseguinte, o caráter invasivo das duas funcionalidades.

38. Em relação a um ponto mais formal, **o nível das coimas não se encontra harmonizado para todas as infrações ao regulamento.** Na proposta de regulamento, os Estados-Membros determinam o regime de sanções aplicáveis às infrações ao disposto no artigo 23.º, n.ºs 4 e 6, e no artigo 24.º da proposta de regulamento, pelo que é mais coerente estabelecer também o mesmo no próprio regulamento relativo à privacidade e às comunicações eletrónicas.

39. E por fim, **a proposta de regulamento assenta em definições que podem tornar-se «alvos móveis».** Relativamente a alguns dos seus conceitos fundamentais, a proposta de regulamento faz referência a um instrumento jurídico diferente, que está atualmente em fase de projeto: a proposta do CECE (ver, por exemplo, artigo 4.º, n.º 1, alínea b)). Dois importantes exemplos são a definição de «utilizador final», que atualmente inclui as pessoas singulares e coletivas, e as definições de «serviço de comunicações eletrónicas» e «serviço de comunicações interpessoais», que se refletem na proposta de regulamento, no artigo 4.º, n.º 1, alínea b), e, no caso da última definição, mais pormenorizadamente no artigo 4.º, n.º 2, por forma a incluir os tipos de serviços especificamente excluídos do CECE²². O presente parecer tem por base as definições tal como estão em vigor atualmente, no entanto é muito provável que a proposta do CECE e/ou seus conceitos fundamentais venham a sofrer alterações. Desde logo, tal situação terá implicações para o regulamento relativo à privacidade e às comunicações eletrónicas. Idealmente, todos os termos originários do CECE devem ser definidos de forma autónoma no regulamento relativo à privacidade e às comunicações eletrónicas; ou, no mínimo, a proposta de regulamento deve incluir um esclarecimento nos casos em que se verifique a existência de quaisquer termos cujas definições se afastam das contidas no CECE (por exemplo, a acima referida inclusão de «serviços acessórios» na definição de «serviço de comunicações interpessoais»). Não obstante, se tal não for possível, o grupo de trabalho gostaria de sugerir a todas as partes envolvidas no processo legislativo que assegurassem que tanto a proposta de regulamento como o CECE são debatidos e votados em simultâneo, a fim de permitir às partes interessadas avaliar corretamente o âmbito de aplicação e as implicações dos novos instrumentos.

²² Por exemplo, o artigo 4.º, n.º 2, da proposta de regulamento indica que um serviço de comunicações interpessoais «inclui os serviços de comunicação interpessoal e interativa que funcionam de modo acessório e que estejam intrinsecamente ligados a outro serviço», ao passo que o artigo 2.º, n.º 5, do CECE exclui especificamente esses serviços dessa definição. (O CECE inclui o «serviço de comunicações interpessoais» na categoria mais ampla do «serviço de comunicações eletrónicas» do artigo 2.º, ponto 4.)

5. SUGESTÕES DE ESCLARECIMENTO PARA GARANTIR A SEGURANÇA JURÍDICA

Além dos pontos anteriormente evocados, o grupo de trabalho deseja destacar algumas disposições da proposta de regulamento que beneficiariam de um esclarecimento. Esses esclarecimentos são considerados necessários para promover a segurança jurídica de todas as partes interessadas, de modo que haja um entendimento e uma aplicação uniformes do regulamento relativo à privacidade e às comunicações eletrónicas em toda a UE.

ESCLARECIMENTOS SOBRE O ÂMBITO DE APLICAÇÃO

40. No que se refere ao âmbito de aplicação da proposta de regulamento, o WP29 sugere os seguintes esclarecimentos:

- a. **O termo «utilizador final» deve abranger todos os utilizadores individuais.** O artigo 2.º, ponto 14, do CECE define «utilizador final» como o utilizador que não oferece redes de comunicações públicas, ou serviços de comunicações eletrónicas acessíveis ao público. Convém esclarecer que as pessoas que contribuem para as redes, por exemplo, redes em malha com os respetivos roteadores *Wi-Fi*, não estão excluídas do âmbito de proteção da proposta de regulamento;
- b. **Importa esclarecer que o âmbito de aplicação territorial é extensivo a todos os utilizadores finais na União.** O artigo 3.º, n.º 1, alínea a), prevê que a proposta de regulamento seja aplicável à prestação de serviços de comunicações eletrónicas a utilizadores finais «na União», enquanto o artigo 3.º, n.º 1, alínea c), estabelece que é aplicável à proteção das informações relativas ao equipamento terminal dos utilizadores finais «localizados na União» (o sublinhado foi aditado). Este aspeto difere nas diferentes traduções. A tradução alemã não estabelece esta distinção, ao passo que outras, como a francesa, a espanhola e a neerlandesa, o fazem. Decorre claramente do considerando 9 que o âmbito de aplicação territorial pretende ser alargado, independentemente do facto de os serviços serem prestados a partir de fora da União ou o tratamento ocorrer na União. Por conseguinte, propõe-se que o termo «localizados» seja suprimido do artigo 3.º, n.º 1, alínea c), a fim de sublinhar este âmbito de aplicação alargado;
- c. **A proposta de regulamento parece limitar-se apenas à proteção da confidencialidade das comunicações em trânsito e não quando armazenadas.** A atual abordagem da proposta de regulamento deve incidir na proteção da transmissão das comunicações. Ver, por exemplo, o considerando 15, segundo o qual a proibição da interceção de dados de comunicações deve ser aplicável durante o seu envio, ou seja, até à receção do conteúdo da comunicação pelo destinatário desejado. O âmbito desta proteção baseia-se num quadro conceptual de comunicações que está desatualizado. A maior parte dos dados das comunicações continua a ser conservada pelos prestadores de serviços, mesmo após a sua receção. Há que assegurar que a confidencialidade desses dados permanece protegida. Além disso, a comunicação entre os assinantes dos mesmos serviços baseados na

computação em nuvem (por exemplo, fornecedores de serviços de correio eletrónico) acarretará, frequentemente, apenas muito poucos envios: o envio de uma mensagem envolve sobretudo a sua reflexão na base de dados do fornecedor, em vez do envio efetivo de comunicações entre duas partes. O argumento de que esta situação já é abrangida pelo GDPR não é convincente: o objetivo global da proposta de regulamento consiste em proteger toda e qualquer comunicação confidencial, independentemente dos meios técnicos dessa comunicação. É possível que se trate de um mero erro de redação, atendendo ao facto de que a proibição prevista no artigo 5.º se refere ao «armazenamento» e «tratamento»;

- d. **Todos os pontos de acesso público à Internet sem fios devem ser abrangidos pelo âmbito de aplicação.** Dado que a utilização de pontos de acesso sem fios é uma prática comum, é absolutamente lógico que não subsistam quaisquer dúvidas quanto à questão de saber se a confidencialidade das comunicações transmitidas através desses pontos de acesso é protegida. No entanto, a tentativa de esclarecer esta situação no regulamento fracassa, uma vez que o âmbito só é alargado às redes disponibilizadas a um «grupo indefinido de utilizadores finais» (considerando 13). As expressões «grupo indefinido de utilizadores finais» e «grupo fechado de utilizadores finais» têm de ser definidas. Em especial, é necessário esclarecer que as redes sem fios seguras (ou seja, com uma palavra-passe) são igualmente abrangidas pelo âmbito de aplicação caso essa palavra-passe seja facultada a um grupo de utilizadores teoricamente indefinidos, cuja identidade não possa ser previamente determinada (por exemplo, os clientes de um café, os visitantes de um aeroporto). O princípio subjacente a este contexto reside, em consonância com o parecer prévio do WP29 sobre a revisão da Diretiva relativa à privacidade e às comunicações eletrónicas, no facto de que *«apenas os serviços que ocorrem numa situação oficial ou profissional unicamente para fins oficiais ou profissionais, ou a comunicação técnica entre organismos não públicos ou organismos públicos com o único objetivo de controlar os processos de trabalho ou de negócios, bem como a utilização de serviços para fins exclusivamente domésticos, podem ficar isentos do instrumento relativo à privacidade e às comunicações eletrónicas.»* (p. 8);
- e. **Os dados recolhidos no âmbito da oferta de serviços de radiodifusão digital devem ser abrangidos pela proposta de regulamento.** Em virtude do carácter sensível do comportamento de visualização, uma vez que revela os interesses pessoais e as características dos telespetadores, o regulamento relativo à privacidade e às comunicações eletrónicas deve especificar (eventualmente através de um considerando) que a exclusão dos serviços que oferecem «conteúdos transmitidos através de redes de comunicações eletrónicas» da definição de «serviço de comunicações eletrónicas» não significa que os prestadores de serviços que oferecem tanto serviços de comunicações eletrónicas como serviços de conteúdos não são abrangidos pelo âmbito de aplicação das disposições do regulamento relativo à privacidade e às comunicações eletrónicas, que visa os prestadores de serviços de comunicações eletrónicas. Esta questão assume particular relevância, porque a prestação de serviços que oferecem «conteúdos transmitidos através de redes de comunicações eletrónicas» está excluída da

definição de «serviço de comunicações eletrónicas» enunciada na proposta do CECE (artigo 2.º, n.º 4);

- f. **Os dados de comunicações são geralmente dados pessoais.** No considerando 4 é referido que os dados de comunicações podem incluir dados pessoais. No entanto, na sua maioria, os dados de comunicações são dados pessoais²³ e, uma grande parte, dados de carácter mais íntimo e sensível, pelo que este considerando deve ser alterado, por forma a indicar que estes dados são geralmente dados pessoais;
- g. **A comunicação confidencial inclui as mensagens em plataforma.** O considerando 1 especifica que o princípio da confidencialidade deve ser aplicável às «formas de comunicação atuais e futuras». Este considerando prossegue com uma lista de exemplos das referidas formas, designadamente as «mensagens pessoais nas redes sociais». O efeito pretendido é provavelmente a inclusão das mensagens privadas entre os utilizadores de uma rede social (por exemplo, Facebook ou Twitter) ou das mensagens publicadas numa cronologia que são acessíveis a um número limitado de pessoas, mas a redação do considerando não é suficientemente clara;
- h. **A forma como o regulamento relativo à privacidade e às comunicações eletrónicas se aplica à interação entre máquinas.** Tal como mencionado no n.º 9, o grupo de trabalho saúda o alargamento da proteção à interação entre máquinas. No entanto, este aspeto só é mencionado no considerando 12 e não num artigo correspondente. Esta proteção é desejável, uma vez que tais comunicações contêm frequentemente informações protegidas ao abrigo dos direitos à privacidade. Por outro lado, uma categoria restrita de pura comunicação máquina-máquina deve ficar isenta se não tiver qualquer impacto na privacidade ou na confidencialidade das comunicações, como, por exemplo, nos casos em que uma comunicação dessa natureza seja efetuada em execução de um protocolo de transmissão entre elementos da rede (por exemplo, servidores, comutadores) para se informarem mutuamente sobre o seu estado de atividade.

Um contexto específico em que a aplicação do regulamento relativo à privacidade e às comunicações eletrónicas carece de esclarecimento é o domínio dos sistemas de transporte inteligentes. Prevê-se que os veículos continuarão a transmitir, por feixes hertzianos, dados que contêm um identificador único. Sem a proteção adicional no regulamento relativo à privacidade e às comunicações eletrónicas no que toca às comunicações de dados, esta situação pode redundar no rastreio contínuo dos hábitos de condução, dos itinerários e da velocidade dos motoristas. O artigo 2.º, n.º 1, do CECE contém, no entanto, uma definição nova e alargada de redes de comunicações. Estas redes incluem os sistemas de transmissão que não dispõem de uma capacidade centralizada de administração e que permitem o

²³ Ver, por exemplo, acórdão do TJUE de 6 de novembro de 2003, processo C-101/01, n.º 24 (relativamente a um número de telefone), acórdão do TJUE de 19 de outubro de 2016, processo C-582/14 (*Breyer*), n.º 49 (no que respeita aos endereços IP dinâmicos), e acórdão do TJUE de 8 de abril de 2014, processos apensos C-293/12 e C-594/12 (*Digital Rights Ireland e Seitlinger e o.*), n.ºs 26 e 27 (tendo em conta o carácter sensível dos metadados).

envio de sinais por feixes hertzianos. O considerando 14 do regulamento relativo à privacidade e às comunicações eletrónicas especifica que esses dados são dados de comunicações eletrónicas. Com base no artigo 5.º da proposta de regulamento, qualquer tipo de interceção, controlo ou armazenamento desses dados das comunicações é proibido, a menos que seja aplicável uma das exceções. Ainda assim, há um interesse em tratar esses dados, permitindo que objetos como os dispositivos e veículos autónomos se alertem mutuamente sobre a sua proximidade ou outros riscos. A questão que, então, se coloca reside em saber qual é a exceção aplicável ao caso em apreço. O consentimento dos utilizadores finais não é uma exceção viável, uma vez que poderá ser necessário ter sempre a possibilidade de tratar esses dados. Os fornecedores devem, por conseguinte, estar em condições de invocar uma exceção específica que permita aos objetos, como os dispositivos e veículos autónomos, se alertarem mutuamente sobre a sua proximidade ou outros riscos.

ESCLARECIMENTOS SOBRE A NOÇÃO DE CONSENTIMENTO E A SUA APLICAÇÃO

41. No que se refere à noção de consentimento e à sua aplicação previstas na atual proposta de regulamento, o WP29 sugere os seguintes esclarecimentos:

- a. **A forma como a noção de consentimento deve ser aplicada no contexto das pessoas coletivas.** O considerando 3 especifica que o regulamento deve assegurar que as disposições do GDPR são igualmente aplicáveis aos utilizadores finais que sejam pessoas coletivas. Nos termos do considerando, tal inclui a definição de consentimento ao abrigo do GDPR (ver também considerando 18). Conforme referido na nota 13, o grupo de trabalho saúda a inclusão explícita das pessoas coletivas no âmbito de aplicação do regulamento. A aplicação prática deste princípio não é, contudo, clara. A definição de consentimento ao abrigo do GDPR prevê que o consentimento seja «informado», devendo a manifestação de vontade do titular dos dados ocorrer «mediante declaração ou ato positivo inequívoco» (artigo 4.º, n.º 11, do GDPR). Convém esclarecer quando é que uma pessoa coletiva pode, de facto, ser considerada «informada» e quando é que existe uma manifestação de vontade por parte de uma pessoa coletiva;
- b. Neste contexto, importa assinalar que o empregador não pode, na maioria dos casos, dar o seu consentimento em nome dos seus trabalhadores, porque, quando um empregador exigir o consentimento de um trabalhador e, dada a relação de poder desigual, a ausência de consentimento acarretar prejuízos relevantes reais ou potenciais, esse consentimento não será válido na medida em que não foi prestado de forma livre²⁴. No respeitante às **empresas que emitem dispositivos ou equipamentos para indivíduos, a proposta de regulamento não contém uma exceção (adequada) à proibição de**

²⁴ Ver Parecer 15/2011 sobre a definição de consentimento (WP 187), Parecer 8/2001 sobre o tratamento de dados pessoais no âmbito do emprego (WP 48) e o novo parecer sobre o tratamento de dados no trabalho (adotado simultaneamente com o presente parecer).

interferência. Um exemplo disso é o caso de um empregador pretender atualizar um telefone emitido pela empresa. Um segundo exemplo é o caso de um empregador oferecer aos trabalhadores «leasing» de automóveis e, para efeitos administrativos, permitir a um terceiro a recolha de dados de localização através da unidade de bordo de um automóvel. Em ambos os casos, o empregador tem interesse em interferir com estes dispositivos.

Esta interferência não pode ser considerada necessária para a prestação de um serviço da sociedade de informação (artigo 8.º, n.º 1, alínea c)) nem para uma medição de audiência da Web (artigo 8.º, n.º 1, alínea d)). Este problema pode ser resolvido através da criação de uma nova exceção, por forma a abranger os casos em que i) o empregador fornece determinados equipamentos no âmbito de uma relação laboral, ii) o trabalhador é o utilizador desse equipamento e iii) a interferência é estritamente necessária para o manuseamento do equipamento pelo trabalhador (o que implica a aplicação dos princípios da proporcionalidade e da subsidiariedade no que respeita à recolha de dados). O empregador só poderá interferir com o dispositivo do utilizador final se essas condições forem satisfeitas;

- c. **A melhoria dos controlos para impedir o reencaminhamento automático de chamadas.** O artigo 14.º prevê um controlo importante para os utilizadores finais impedirem o reencaminhamento automático de chamadas por terceiros. Esta proteção pode ainda ser melhorada através da solicitação do consentimento do utilizador final para dar início ao reencaminhamento da chamada em primeiro lugar.

ESCLARECIMENTOS SOBRE A LOCALIZAÇÃO E OUTROS METADADOS

- 42. No que respeita aos dados de localização e outros metadados, o grupo de trabalho propõe esclarecer o seguinte:

- a. O significado de **«dados de localização [que são] gerados fora do contexto de uma comunicação» constantes do considerando 17 deve ser esclarecido**. Não está bem claro se esses dados estão relacionados com os dados de localização recolhidos através de, por exemplo, aplicações móveis que utilizam os dados da funcionalidade GPS existente em dispositivos inteligentes e/ou geram dados de localização com base na proximidade de roteadores *Wi-Fi*, e/ou dados de localização recolhidos com assistentes de navegação instalados a bordo e/ou outras formas de geração de dados de localização. Esta falta de clareza cria incerteza jurídica quanto ao âmbito de aplicação da obrigação. Em qualquer caso, os dados de localização do equipamento terminal de uma pessoa singular são dados pessoais e, por conseguinte, o tratamento dos mesmos está sujeito às obrigações do GDPR;
- b. Cumpre esclarecer que **o tratamento mais legítimo de dados de localização e outros metadados não necessita de um identificador único**. O considerando 17 faz menção aos mapas térmicos («heatmaps») como um exemplo de utilizações comerciais dos metadados das comunicações eletrónicas por prestadores de serviços de comunicações eletrónicas. No entanto, para criar um mapa térmico básico, não são necessários quaisquer identificadores únicos, bastando a mera contagem estatística. Outro exemplo

mencionado no considerando é a utilização de – e a pressão sobre – infraestruturas que pode igualmente ser contabilizada por determinados pontos de medição, por exemplo através da criação de estatísticas agregadas sobre a utilização de torres de controlo do tráfego, a fim de fornecer uma indicação da pressão exercida num local em determinado momento, sem que para tal seja também necessário conhecer a identidade das pessoas conectadas.

Além disso, o considerando indica como exemplo a apresentação dos movimentos de tráfego em certas direções durante um determinado período de tempo, sempre que seja necessário um identificador único para estabelecer a ligação entre as posições das pessoas em certos intervalos de tempo. Com este exemplo, o considerando parece legitimar o tratamento posterior desses dados para apoiar a análise dos «megadados». A única condição prevista na proposta de regulamento para este tipo de tratamento consiste na obrigação de realizar uma avaliação de impacto sobre a proteção de dados sempre que o tratamento seja *suscetível de conduzir a um elevado risco para os direitos e liberdades das pessoas singulares*. Esta condição não é suficiente. Além disso, é contrária à obrigação prevista no artigo 6.º de que este tipo de tratamento só pode ser efetuado com o consentimento dos utilizadores e unicamente se os dados não puderem ser anonimizados, ou seja, sem quaisquer identificadores únicos. Muitas vezes, os utilizadores não podem recusar a recolha dos seus dados de geolocalização efetuada pelos prestadores de serviços de comunicações eletrónicas, sempre que essa recolha seja tecnicamente necessária para enviar a comunicação ao utilizador ou sempre que esse tratamento seja necessário para prestar o serviço (por exemplo, navegação) solicitado. Em pareceres anteriores, o grupo de trabalho concluiu que esses dados de localização provenientes de dispositivos inteligentes são dados pessoais de natureza sensível e que os benefícios da análise desses dados não prevalecem sobre os direitos dos utilizadores à proteção da confidencialidade dos metadados das suas comunicações, nem prevalecem sobre os seus direitos gerais à proteção de dados ao abrigo do GDPR. Por conseguinte, o considerando deve, no mínimo, especificar que os prestadores de serviços devem cumprir as obrigações decorrentes do artigo 25.º do GDPR em caso de tratamento posterior dos dados de localização ou outros metadados. Esta situação pressupõe, pelo menos, que tenham de ser tomadas as seguintes medidas:

- i) a utilização de pseudónimos temporários;
- ii) a supressão de qualquer tabela de pesquisa inversa entre esses pseudónimos e os dados de identificação originais;
- iii) a agregação a um nível em que os utilizadores individuais deixam de poder ser identificados através dos seus percursos específicos; e
- iv) a eliminação dos valores atípicos relativamente aos quais a identificação continuaria a ser possível (todas estas medidas têm de ser aplicadas em conjunto).

Por último, o regulamento relativo à privacidade e às comunicações eletrónicas deve obrigar as partes envolvidas no tratamento de dados de localização e outros metadados a tornarem públicos os seus métodos de

anonimização e agregação suplementar, sem prejuízo do sigilo protegido por lei, o que permitiria tanto às autoridades de controlo como ao público em geral verificar facilmente se o método escolhido é adequado.

ESCLARECIMENTOS SOBRE AS COMUNICAÇÕES NÃO SOLICITADAS

43. O grupo de trabalho sugere que sejam esclarecidos os seguintes aspetos relativamente às comunicações não solicitadas:

- a. **A formulação da proibição das comunicações comerciais diretas sem consentimento.** O artigo 16.º, n.º 1, da proposta de regulamento assinala agora que os serviços de comunicações eletrónicas «podem» ser utilizados para o envio de comunicações comerciais diretas (com consentimento), mas não contém uma proibição explícita do envio (encaminhamento ou apresentação) de comunicações comerciais diretas sem consentimento. Esta abordagem contrasta com aquela contida nas demais disposições, em que primeiramente é formulada uma proibição e só depois é acompanhada de algumas exceções específicas. A atual formulação sugere uma abordagem mais flexível (o que provavelmente não é o que se pretende). O grupo de trabalho propõe uma formulação ligeiramente diferente do atual artigo 13.º, n.º 1, da Diretiva relativa à privacidade e às comunicações eletrónicas: «A utilização por parte de pessoas singulares ou coletivas de serviços de comunicações eletrónicas, nomeadamente chamadas vocais, sistemas de chamada e de comunicação automatizados, incluindo sistemas semiautomatizados que ligam a pessoa chamada a outra pessoa, faxes, correio eletrónico ou outra utilização de serviços de comunicações eletrónicas, para fins de apresentação de comunicações comerciais diretas aos utilizadores finais apenas poderá ser autorizada em relação aos utilizadores finais que tenham dado o seu consentimento prévio.»;
- b. **O âmbito de aplicação das disposições relativas às comunicações comerciais e chamadas para contactos existentes.** O artigo 16.º, n.º 2, prevê que, sempre que uma pessoa obtenha de um cliente existente coordenadas eletrónicas de contacto para correio eletrónico, pode utilizar essas coordenadas para futuros fins de *marketing* direto dos seus próprios produtos ou serviços, desde que ao cliente seja dada a clara possibilidade de se opor, de forma gratuita e fácil, na data da recolha e em cada mensagem. Esta disposição está atualmente limitada aos contactos comerciais obtidos «no contexto da venda de um produto ou serviço» e para futuros fins de *marketing* comercial dos seus próprios produtos ou serviços análogos. Dado que as disposições relativas ao *marketing* direto são igualmente aplicáveis às atividades promocionais não comerciais (por exemplo, de organizações de beneficência ou de partidos políticos), esta disposição deve ser alterada por forma a ser também aplicável às organizações não comerciais, no sentido de contactarem anteriores apoiantes aquando da promoção dos seus próprios objetivos ou ideais análogos, devendo o mesmo direito de oposição ser aplicável às chamadas de *marketing* direto. Mais ainda, deve ser fixado um prazo para a validade dos «contactos de clientes existentes» nas

comunicações eletrónicas para fins comerciais, de beneficência ou políticos, devendo esse prazo ser igualmente aplicável às chamadas de *marketing* direto. Se os Estados-Membros tiverem optado por um sistema de oposição contra as chamadas vocais de *marketing* direto, a existência de uma relação de «contacto de cliente existente» sobrepõe-se à inscrição num registo «Do-Not-Call». Nestas circunstâncias, os utilizadores finais não dispõem de qualquer possibilidade efetiva de impedir as chamadas incomodativas de empresas ou organizações com as quais já tiveram alguma vez contacto, mas não querem mais colaborar com as mesmas. Por conseguinte, como regra geral, o regulamento deve especificar um prazo de validade desta exceção de «cliente existente», por exemplo um ou dois anos, em relação às expectativas legítimas dos utilizadores finais em causa;

- c. **A aplicação das regras relativas ao *marketing* direto às pessoas coletivas.** O artigo 16, n.º 5, da proposta de regulamento prevê que os Estados-Membros devem assegurar que os interesses legítimos dos utilizadores finais que são pessoas coletivas são suficientemente protegidos em relação a comunicações não solicitadas. O artigo 13.º, n.º 5, da atual Diretiva relativa à privacidade e às comunicações eletrónicas descreve os interesses legítimos dos assinantes que não são pessoas singulares. Não se sabe ao certo quais são as implicações desta alteração ao nível da redação. Nos considerandos, convém esclarecer que esta alteração não reflete a intenção de prever um nível de proteção inferior. A este respeito, a proibição do *marketing* direto sem consentimento refere-se aos «utilizadores finais que sejam pessoas singulares que tenham dado o seu consentimento» (o sublinhado foi aditado). Dever-se-á esclarecer que tal abrange as pessoas singulares *que trabalham para* pessoas coletivas. Por outro lado, o consentimento não será necessário para abordar as pessoas coletivas através de coordenadas de contacto genéricas que tenham tornado públicas para esse fim (como «info@nomedaempresa.eu»);
- d. **A aplicação das regras relativas ao *marketing* direto às pessoas que agem na qualidade de representantes (políticos):** nos termos em que está redigido, o artigo 16.º pode impedir algumas comunicações enviadas aos representantes eleitos, indicando as preocupações ou interesses comerciais. Importa esclarecer que o regulamento não impede tais comunicações.

ESCLARECIMENTOS SOBRE A APLICAÇÃO DOS INSTRUMENTOS EM MATÉRIA DE DIREITOS FUNDAMENTAIS

44. **A aplicação do disposto na Carta e na CEDH à legislação nacional em matéria de conservação de dados** deve ser objeto de maior esclarecimento. O considerando 26 prevê que quaisquer medidas dos Estados-Membros destinadas a salvaguardar os interesses públicos, como as medidas de interceção legal, devem estar em conformidade com a Carta (além da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, CEDH). Trata-se de uma medida desejável, uma vez que é consentânea com o raciocínio desenvolvido nas deliberações dos processos apenas *Tele2 Sverige/Watson e o.* de que quaisquer

exceções nacionais às proteções do tratamento de dados consagradas na legislação da UE estão sujeitas às disposições da Carta (e as infrações cometidas através da legislação nacional podem, por conseguinte, ser submetidas ao Tribunal de Justiça da União Europeia). O artigo 11.º da proposta de regulamento limita-se, no entanto, a referir que as restrições do âmbito de aplicação dos artigos 5.º a 8.º da proposta de regulamento devem respeitar a essência dos direitos e liberdades fundamentais e constituir uma medida necessária e proporcionada. Aqui deve igualmente figurar uma referência explícita à Carta e à CEDH.

45. **A confidencialidade das comunicações é também protegida ao abrigo do artigo 8.º da CEDH.** O ponto 1.1 da exposição de motivos e o considerando 1 indicam que a proposta de regulamento aplica o artigo 7.º da Carta. O mesmo é reiterado no considerando 19. O direito fundamental à confidencialidade das comunicações, porém, não só é protegido nesta disposição, mas também nos termos do artigo 8.º da CEDH. A inclusão de uma referência explícita num artigo da proposta de regulamento reforçaria ainda que qualquer jurisprudência relevante do Tribunal Europeu dos Direitos do Homem seria igualmente tomada em consideração aquando da avaliação do regulamento (final). Esta referência já se encontra, aliás, incluída no considerando 20 (no que respeita aos equipamentos terminais) e no considerando 26 (no que respeita à interceção legal) e é ainda corroborada pelas considerações enunciadas no ponto 2.1 da exposição de motivos (sobre a relação entre a Carta e a CEDH no contexto das pessoas coletivas), mas não se encontra em nenhum dos artigos relevantes, como o artigo 11.º, n.º 1.

OUTROS ESCLARECIMENTOS

46. Importa esclarecer que **as obrigações decorrentes do GDPR, como, por exemplo, as respeitantes ao regime das violações de dados e às avaliações de impacto sobre a proteção de dados, continuam a ser aplicáveis** quando as partes tratam dados pessoais no contexto dos dados das comunicações eletrónicas. Tal como referido no considerando 5 que a proposta de regulamento constitui uma *lex specialis* no que respeita ao GDPR e que o tratamento de dados das comunicações eletrónicas deve apenas ser permitido em conformidade com a proposta de regulamento, poder-se-ia questionar se determinadas obrigações decorrentes do GDPR também se aplicam no contexto da proposta de regulamento. Tal é especialmente o caso quando a proposta de regulamento pode ser interpretada por forma a apresentar uma determinada obrigação, ao mesmo tempo que o GDPR abrange também esse aspeto. Entre os exemplos ilustrativos incluem-se os casos em que:
- (i) a proposta de regulamento obriga a uma determinada notificação dos riscos de segurança «detetados» (artigo 17.º) (ver também nota 35), porém o GDPR inclui um regime de notificação de violações de dados (artigos 33.º e 34.º);
 - (ii) a proposta de regulamento refere que a realização de uma avaliação de impacto sobre a proteção de dados e de uma consulta da autoridade de controlo em conformidade com o GDPR é obrigatória em determinadas circunstâncias (considerandos 17 e 19 e artigo 6.º, n.º 3, alínea b)), ao passo que o GDPR já determina quando é que uma avaliação de impacto sobre a

proteção de dados tem de ser realizada e quando é que é necessária uma consulta (artigos 35.º e 36.º); e

- (iii) não é especificado que, se se cumprir as condições necessárias de uma exceção à proibição de tratamento nos termos do artigo 5.º da proposta de regulamento, tem ainda de se cumprir todas as obrigações relevantes decorrentes do GDPR sempre que digam respeito ao tratamento de dados pessoais, sendo qualquer outro tratamento nos termos do GDPR proibido. Convém esclarecer que o teste de compatibilidade previsto no artigo 6.º, n.º 4, do GDPR não é, por conseguinte, aplicável;
- (iv) a proposta de regulamento relativo à privacidade e às comunicações eletrónicas não prevê procedimentos de certificação semelhantes aos enunciados nos artigos 42.º e 43.º do GDPR. Uma vez que o âmbito de aplicação do artigo 42.º do GDPR está, *stricto sensu*, limitado à criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade com o GDPR, importa ponderar se não deverá ser introduzida uma disposição comparável para permitir a certificação de operações de tratamento, normas, produtos ou serviços para a sua conformidade com o regulamento relativo à privacidade e às comunicações eletrónicas.

A fim de garantir que esta falta de clareza não é utilizada como argumento para baixar o nível de proteção ao abrigo da proposta de regulamento, há que esclarecer que, em todos estes casos, os responsáveis pelo tratamento têm igualmente de cumprir o disposto no GDPR.

- 47. Além disso, convém esclarecer que **o requisito de retirada do consentimento também é aplicável no contexto da interferência com os equipamentos terminais**. O artigo 8.º, n.º 1, alínea b), da proposta de regulamento prevê a possibilidade de interferir com os equipamentos terminais dos utilizadores finais com o seu consentimento. O artigo 9.º, n.º 3, estipula que os utilizadores finais tenham a possibilidade de retirar o seu consentimento em qualquer momento, mas esta obrigação só se aplica ao consentimento destinado à análise de metadados e conteúdos. Importa esclarecer que esta obrigação se estende à interferência com os equipamentos terminais.
- 48. A este respeito, dever-se-á esclarecer que **o aviso da possibilidade de retirar o consentimento é igualmente aplicável ao consentimento dado através das predefinições do programa de navegação**. O artigo 9.º, n.º 3, determina que os utilizadores finais sejam, a intervalos regulares de seis meses, recordados da possibilidade de retirar o seu consentimento em qualquer momento. Embora o grupo de trabalho considere que as definições gerais dos programas de navegação e de outro *software*, nomeadamente sistemas operativos, aplicações móveis e interfaces de *software* para dispositivos conectados à Internet das Coisas (ou seja, não com base em controlos granulares específicos), não podem ser uma medida válida para expressar o consentimento, uma vez que as definições gerais não são adequadas para dar o consentimento específico a cenários específicos (ver nota 24), as predefinições devem ser de fácil utilização (ver nota 19). Se este aspeto continuar a ser tratado na proposta de regulamento, as predefinições devem ser suficientemente pormenorizadas para controlar todo o tratamento de dados consentido pelo utilizador e abranger todas

as funcionalidades do equipamento que poderão levar ao tratamento de dados. Além disso, o utilizador final deve, pelo menos a intervalos regulares (seis meses), ser recordado da possibilidade de alterar essas predefinições.

49. É de saudar o facto de a proposta de regulamento impor que o *software* já colocado no mercado informe o utilizador final acerca das suas opções relativas às predefinições de privacidade (artigo 10.º). **No entanto, não está claro o modo como esta disposição pode ser eficazmente aplicada a produtos inicialmente existentes e a outros que deixaram de ser apoiados.** Ademais, devem ser fornecidos esclarecimentos adicionais quanto à forma como esta obrigação será aplicável ao *software* de código de fonte aberta, desenvolvido de uma forma aberta e descentralizada.
50. Convém esclarecer que **a oferta da possibilidade de bloquear testemunhos de conexão (de terceiros) nos termos do artigo 10.º da proposta de regulamento prevalece sobre a exceção de medição de audiência da Web** ao abrigo do artigo 8.º, n.º 1, alínea d). Ou, por outras palavras: mesmo que um sítio Web possa recorrer a análises para a medição de audiência da Web nos termos do artigo 8.º, n.º 1, alínea d), os utilizadores devem continuar a ter o direito de bloquear essas tecnologias de rastreio no seu programa de navegação.
51. **A definição de sistemas de chamada e de comunicação (semi)automatizados deve ser objeto de esclarecimento.** A definição desta expressão, constante do artigo 4.º, n.º 3, alínea h), da proposta de regulamento, contém uma referência à própria expressão na segunda parte da frase («incluindo chamadas efetuadas com recurso a sistemas de chamada e de comunicação automatizados que ligam a pessoa chamada a outra pessoa»). Por conseguinte, recomenda-se a supressão desta última parte da frase da definição e ainda a alteração da definição constante do artigo 4.º, n.º 3, alínea g), com vista a incluir as chamadas efetuadas com recurso a sistemas de comunicação semiautomatizados, como, por exemplo, os marcadores automáticos que ligam a pessoa chamada a outra pessoa.
52. As **informações que fazem «parte da subscrição de um serviço» devem ser objeto de esclarecimento.** O considerando 14 refere que 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». Não está claro o que se pretende com esta formulação.
53. **A aplicabilidade dos procedimentos de controlo da coerência e da cooperação** deve ser objeto de esclarecimento. O considerando 38 salienta que a proposta de regulamento assenta no procedimento de controlo da coerência previsto no GDPR. Além disso, o artigo 18.º, n.º 1, estipula que os capítulos VI e VII do GDPR são aplicáveis *mutatis mutandis*. O artigo 19.º sublinha ainda que o Comité Europeu para a Proteção de Dados («CEPD») exerce as funções previstas no artigo 70.º do GDPR. Embora a aplicação destas disposições seja relativamente clara, não se pode excluir que surjam questões de interpretação a propósito dos conceitos fundamentais dos procedimentos de controlo da coerência e da cooperação ao abrigo do GDPR. Por

exemplo, o procedimento da autoridade de controlo principal é aplicável aos casos em que se verifica a existência de «tratamento transfronteiriço» (artigo 56.º, n.º 1 do GDPR): não é, no entanto, claro o modo como esta disposição se aplica no caso da interferência com os equipamentos terminais ou da análise de conteúdos ou metadados ao abrigo da proposta de regulamento. Por conseguinte, é aconselhável esclarecer a aplicação destes conceitos fundamentais num considerando e sublinhar que quaisquer questões pendentes relativas à aplicabilidade desses capítulos do GDPR no contexto da proposta de regulamento serão resolvidas através da interpretação das disposições desses capítulos em consonância com a sua intenção. Além disso, é recomendável esclarecer que o artigo 70.º é aplicável *mutatis mutandis* ao CEPD no contexto da proposta de regulamento (atualmente em falta no considerando).

* * *