ARTIGO 29.º - Grupo de Protecção de Dados Pessoais

01189/09/PT
WP 163

Parecer 5/2009 sobre as redes sociais em linha

Adoptado em 12 de Junho de 2009

Índice

Síntese

O presente parecer aborda a forma como o funcionamento dos sítios de redes sociais pode cumprir os requisitos da legislação comunitária no domínio da protecção de dados. Pretende-se, principalmente, dar orientações aos fornecedores de serviços de redes sociais (SRS) sobre as medidas que devem ser instituídas para assegurar o cumprimento da legislação comunitária.

O parecer observa que os fornecedores de SRS e, em muitos casos, os terceiros fornecedores de aplicações, são responsáveis pelo tratamento dos dados com obrigações correspondentes para com os utilizadores dos SRS. O parecer aborda o facto de haver um grande número de utilizadores que actuam numa esfera estritamente pessoal, contactando outras pessoas como parte da organização da sua vida pessoal, familiar ou doméstica. Nestes casos, o parecer considera que se aplica a «isenção doméstica» e que não se aplicam os regulamentos que abrangem a actividade dos responsáveis pelo tratamento dos dados. O parecer especifica igualmente as circunstâncias em que as actividades de um utilizador de um SRS não estão cobertas pela «isenção doméstica». A difusão e a utilização das informação disponíveis nos SRS para outros fins secundários e involuntários constituem uma preocupação fundamental para o Grupo de Trabalho do Artigo 29.º Em todo o parecer são defendidos valores pré-definidos de privacidade como ponto de partida ideal no que se refere a todos os serviços oferecidos. O acesso à informação contida nos perfis surge como um domínio-chave de preocupação. São igualmente abordadas questões como o tratamento de dados sensíveis e imagens, a publicidade e o marketing directo nos SRS, assim como as questões que se prendem com a conservação de dados.

As recomendações essenciais dizem respeito às obrigações dos fornecedores de SRS de cumprirem a Directiva Protecção dos Dados e de defenderem e reforçarem os direitos dos utilizadores. É da máxima importância que os fornecedores de SRS informem os utilizadores da sua identidade desde o início e apresentem todos os diferentes fins para os quais fazem o tratamento de dados pessoais. Os fornecedores de SRS devem ser particularmente cautelosos no que se refere ao tratamento dos dados pessoais de menores. O parecer recomenda que os utilizadores carreguem apenas imagens ou informações sobre outros indivíduos com o consentimento do indivíduo em questão e considera que os SRS têm igualmente um dever de advertir os utilizadores para o direito à privacidade dos outros utilizadores.

O GRUPO DE PROTECÇÃO DAS PESSOAS SINGULARES NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS

Instituído pela Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995[1],

Tendo em conta o artigo 29.º e o artigo 30.º, n.º 1, alínea a), e n.º 3, da referida directiva e o artigo 15.º, n.º 3, da Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002,

Tendo em conta o artigo 255.° do Tratado CE e o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de Maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão,

Tendo em conta o seu regulamento interno,

ADOPTOU O SEGUINTE PARECER:

1. Introdução

A evolução das comunidades Web e dos serviços disponíveis na Web, como os serviços de redes sociais («SRS») é um fenómeno relativamente recente, continuando o número de utilizadores destes sítios a multiplicar-se a uma taxa exponencial.

A informação pessoal que um utilizador afixa em linha, combinada com dados que descrevem as acções dos utilizadores e as interacções com outras pessoas, podem criar um perfil bastante completo dos interesses e actividades dessa pessoa. Os dados pessoais publicados nos sítios de redes sociais podem ser utilizados por terceiros para uma grande variedade de fins, inclusive com objectivos comerciais, e podem apresentar riscos graves, como o roubo de identidade, prejuízos financeiros, perda de oportunidades de negócios ou de emprego e danos físicos.

O Grupo de Trabalho Internacional relativo à Protecção de Dados nas Telecomunicações (Grupo de Berlim) adoptou o *Memorando de Roma*[2] em Março de 2008. O memorando analisa os riscos para a vida privada e para a segurança constituídos pelas redes sociais e apresenta orientações para reguladores, fornecedores e utilizadores. Recentemente, foi adoptada a Resolução sobre a Protecção da Privacidade nas Redes de Socialização[3] que também aborda os desafios lançados pelos SRS. O grupo de trabalho tem igualmente em conta o documento estratégico publicado pela Agência Europeia para a Segurança das Redes e da Informação (ENISA), em Outubro de 2007, intitulado «*Security Issues and Recommendations for Online Social Networks*»[4], destinado a reguladores e a fornecedores de redes sociais.

---

1 JO L 281 de 23.11.1995, p. 31, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

3 Adoptado na 30.ª Conferência Internacional dos Comissários para a Protecção dos Dados e da Vida Privada, realizada em Estrasburgo, em 17.10.2008, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf

4 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

2. Definição de um «serviço de redes sociais (SRS)» e modelo empresarial

Os SRS podem ser definidos, em sentido lato, como plataformas de comunicação em linha que permitem a indivíduos aderirem a redes de utilizadores com interesses semelhantes ou criarem redes deste tipo. Na acepção jurídica, as redes sociais são serviços da sociedade da informação, conforme definidos no artigo 1.º, ponto 2, da Directiva 98/34/CE, com a redacção que lhe foi dada pela Directiva 98/48/CE. Os SRS partilham de certas características:

- os utilizadores são convidados a fornecer dados pessoais para efeitos da geração de uma descrição de si próprios ou «perfil»;

- os SRS disponibilizam igualmente ferramentas que permitem aos utilizadores afixar o seu próprio material (conteúdos gerados pelo utilizador, como fotografias ou crónicas, música ou vídeos ou ainda ligações a outros sítios[5]);

- as «redes sociais» são activadas através de ferramentas que fornecem uma lista de contactos para cada utilizador e com os quais os utilizadores podem interagir.

Os SRS geram grande parte das suas receitas através de publicidade que é apresentada em conjunto com as páginas Web criadas e visitadas pelos utilizadores. Os utilizadores que afixam grandes quantidades de informação sobre os seus interesses nos respectivos perfis proporcionam um mercado seleccionado para os anunciantes que pretendam colocar anúncios orientados com base nessa informação.

É, pois, importante que os SRS funcionem de uma maneira que respeite os direitos e liberdades dos utilizadores, os quais têm uma expectativa legítima de que os dados pessoais que divulgam sejam processados de acordo com a legislação europeia e nacional de protecção dos dados e da vida privada.

3. Âmbito de aplicação da Directiva Protecção dos Dados

As disposições da Directiva Protecção dos Dados aplicam-se aos fornecedores de SRS na maioria dos casos, mesmo que as suas sedes se situem fora do EEE. O Grupo de Trabalho do Artigo 29.º remete para o seu parecer anterior relativo aos motores de pesquisa, para mais orientações respeitantes às questões do estabelecimento e da utilização de equipamento como determinantes para a aplicabilidade da Directiva Protecção dos Dados e das normas subsequentemente suscitadas pelo tratamento de endereços IP e pela utilização de testemunhos (*cookies*)[6].

3.1 Quem é o responsável pelo tratamento dos dados?

Fornecedores de SRS

Os fornecedores de SRS são responsáveis pelo tratamento dos dados ao abrigo da Directiva Protecção dos Dados. Fornecem os meios para o tratamento dos dados dos utilizadores e prestam todos os serviços «básicos» relacionados com a gestão dos utilizadores (por exemplo, registo e eliminação de contas). Os fornecedores de SRS determinam igualmente a utilização que pode ser feita dos dados dos utilizadores para fins de publicidade e de marketing - incluindo a publicidade feita por terceiros.

---

5 Nestes casos, em que os SRS prestam serviços de comunicações electrónicas, aplicam-se igualmente as disposições da Directiva Privacidade Electrónica (Directiva 2002/58/CE).

6 WP 148, «Parecer 1/2008 sobre questões de protecção dos dados ligadas aos motores de pesquisa».

Fornecedores de aplicações

Os fornecedores de aplicações podem também ser responsáveis pelo tratamento dos dados, se desenvolverem aplicações que funcionem em conjunto com as dos SRS e se os utilizadores decidirem usar essa aplicação.

Utilizadores

Na maioria dos casos, os utilizadores são considerados como pessoas em causa. A directiva não impõe os deveres de um responsável pelo tratamento dos dados a um indivíduo que faça o tratamento de dados pessoais «*no exercício de actividades exclusivamente pessoais ou domésticas*» - a chamada «isenção doméstica». Em alguns casos, é possível que as actividades de um utilizador de um SRS não estejam cobertas pela isenção doméstica, podendo considerar-se que o utilizador assumiu algumas das responsabilidades de um responsável pelo tratamento dos dados. São apresentados, em seguida, alguns exemplos dessas situações:

3.1.1. Finalidade e natureza

Uma tendência crescente dos SRS é a «*passagem da "Web 2.0 para divertimento" para a Web 2.0 para produtividade e serviços*»[7], em que as actividades de alguns utilizadores das SRS podem ir além de uma actividade meramente pessoal ou doméstica, por exemplo, quando o SRS é utilizado como plataforma de colaboração para uma associação ou empresa. Se um utilizador de um SRS agir em nome de uma empresa ou associação ou se utilizar o SRS principalmente como plataforma para atingir objectivos comerciais, políticos ou caritativos, a excepção não se aplica. Neste caso, o utilizador assume as plenas responsabilidades de um responsável pelo tratamento dos dados que está a divulgar dados pessoais a outro responsável pelo tratamento dos dados (SRS) e a terceiros (outros utilizadores do SRS ou até, potencialmente, outros responsáveis pelo tratamento dos dados com acesso aos dados). Nestas circunstâncias, o utilizador necessita do consentimento das pessoas em causa ou de outra base legítima facultada pela Directiva Protecção dos Dados.

Tipicamente, o acesso aos dados (dados do perfil, mensagens, crónicas, etc.) fornecidos por um utilizador está limitado aos contactos seleccionados pelo próprio utilizador. Em alguns casos, porém, os utilizadores podem adquirir um grande número de contactos terceiros, alguns dos quais poderão não conhecer de facto. Um número elevado de contactos pode ser uma indicação de que a excepção doméstica não se aplica e, por conseguinte, que o utilizador seria considerado um responsável pelo tratamento dos dados.

3.1.2. Acesso à informação do perfil

Os SRS devem garantir a existência de valores pré-definidos respeitadores da privacidade e gratuitos, que restrinjam o acesso aos contactos seleccionados pelo próprio utilizador.

Quando o acesso à informação do perfil se alarga para além dos contactos seleccionados pelo próprio utilizador, como, por exemplo, se o acesso a um perfil for dado a todos os membros do SRS[8] ou se os dados forem indexáveis por motores de pesquisa, o acesso ultrapassa a esfera pessoal ou doméstica. Da mesma maneira, se um utilizador tomar uma decisão informada de alargar o acesso além dos «amigos» seleccionados pelo próprio, entram em vigor as responsabilidades de responsável pelo tratamento dos dados. Efectivamente, o mesmo regime jurídico aplicar-se-á então, tal como quando qualquer pessoa utiliza outras plataformas tecnológicas para publicar dados pessoais na Web[9]. Em vários Estados-Membros, a falta de restrições ao acesso (ou seja, o carácter público) significa que a Directiva Protecção dos Dados se aplica em termos de utilizador da Internet que adquire as responsabilidades de responsável pelo tratamento dos dados[10].

Não deve esquecer-se que, mesmo que não se aplique a isenção doméstica, o utilizador do SRS pode beneficiar de outras isenções, como a isenção para fins jornalísticos e para

---

7 «*Internet of the future: Europe must be a key player*» discurso de Viviane Reding, Comissária Europeia para a Sociedade da Informação e Meios de Comunicação, na reunião da iniciativa sobre o futuro da Internet do Conselho de Lisboa, Bruxelas, 2 de Fevereiro de 2009.

8 Ou quando se pode afirmar que não está a ser feita uma selecção de facto na aceitação de contactos, ou seja, o utilizador aceita «contactos» independentemente da relação com esses utilizadores.

9 Como acontece com as plataformas de publicação, que não são SRS, ou com o software em sítio próprio (*self-hosted*).

10 No seu acórdão Satamedia, o TJE decidiu em contrário no n.º 44: «*Daí decorre que esta segunda excepção deve ser interpretada no sentido de que tem apenas por objecto as actividades que se inserem no quadro da vida privada ou familiar dos particulares (v. acórdão Lindqvist, já referido, n.º 47). Manifestamente, não é esse o caso das actividades da Markkinapörssi e da Satamedia, cujo objecto é dar a conhecer os dados recolhidos a um número indefinido de pessoas.*»

expressão artística ou literária. Nesses casos, é necessário um equilíbrio entre a liberdade de expressão e o direito ao respeito pela vida privada.

3.1.3 Tratamento de dados pertencentes a terceiros pelos utilizadores

A aplicação da isenção doméstica é igualmente restringida pela necessidade de garantir os direitos de terceiros, especialmente no que se refere a dados sensíveis. Além disso, deve salientar-se que, mesmo que se aplique a isenção doméstica, um utilizador pode ser responsável ao abrigo das disposições gerais nacionais de direito civil ou penal em questão (por exemplo, difamação, responsabilidade delituosa por violação de personalidade ou responsabilidade penal).

3.2 Segurança e valores pré-definidos de privacidade

Dar segurança ao tratamento da informação é um elemento fundamental de confiança nos SRS. Os responsáveis pelo tratamento dos dados devem adoptar as medidas técnicas e organizacionais adequadas, «tanto aquando da concepção do sistema de tratamento como da realização do próprio tratamento», a fim de manter a segurança e impedir qualquer tratamento não autorizado, tendo em conta os riscos que o tratamento apresenta e a natureza dos dados[11].

Um elemento importante dos valores de privacidade é o acesso aos dados pessoais publicados num perfil. Se não houver restrições a esse acesso, terceiros podem associar todos os tipos de informações pessoais relativas aos utilizadores, tanto na qualidade de membros do SRS, como através de motores de pesquisa. Contudo, apenas uma minoria de utilizadores registados num serviço procederá a alterações dos valores pré-definidos. O SRS deve, pois, facultar valores pré-definidos de privacidade que dêem aos utilizadores a liberdade de consentir especificamente o acesso ao conteúdo do seu perfil para além dos contactos por si seleccionados, a fim de reduzir o risco de tratamento ilegal por terceiros. Os perfis de acesso restrito não devem ser passíveis de ser encontrados por motores de pesquisa internos, incluindo a possibilidade de pesquisa por parâmetros como a idade ou o local. As decisões no sentido de aumentar o acesso podem não estar implícitas[12], por exemplo, com uma «opção de recusa» (*opt-out*) proporcionada pelo responsável do SRS.

3.3 Informações a apresentar pelo SRS

Os fornecedores de SRS devem informar os utilizadores da sua identidade e das finalidades com que tratam os dados pessoais, em conformidade com as disposições do artigo 10.º da Directiva Protecção dos Dados, incluindo, a título de exemplo:

- a utilização dos dados para fins de marketing directo;
- a eventual partilha dos dados com categorias específicas de terceiros;
- um panorama dos perfis: a sua criação e as principais fontes de dados;
- a utilização de dados sensíveis.

O grupo de trabalho recomenda que:

---

11 Artigo 17.º e considerando 46 da Directiva Protecção dos Dados.

12 O relatório e as orientações em matéria de privacidade nos serviços de rede sociais (*Report and Guidance on Privacy in Social Network Services* - «Memorando de Roma») indicam riscos como a «noção enganadora de comunidade», p. 2 e «facultar mais informações do que se pensa», p. 3. Uma empresa de segurança informática adverte um SRS importante sobre o acesso pré-definido aos membros da mesma área geográfica: http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html.

- os fornecedores de SRS façam advertências adequadas aos utilizadores sobre os riscos em termos de privacidade para si próprios e para outros, quando carregam informação no SRS;

- os utilizadores de SRS sejam também relembrados de que carregar informações sobre outros indivíduos pode invadir a sua privacidade e violar os seus direitos de protecção dos dados;

- os utilizadores de SRS sejam advertidos pelo SRS de que, se desejarem carregar imagens ou informações sobre outros indivíduos, devem fazê-lo com o consentimento do indivíduo em questão[13].

3.4 Dados sensíveis

Consideram-se sensíveis os dados que revelam a origem étnica, as opiniões políticas, crenças religiosas ou filosóficas, a filiação sindical ou dados relativos à saúde ou à vida sexual. Os dados pessoais sensíveis só podem ser publicados na Internet com o consentimento explícito da pessoa em causa ou se a própria pessoa tornar esses dados manifestamente públicos[14].

Em alguns Estados-Membros da UE, as imagens das pessoas em causa são consideradas uma categoria especial de dados pessoais, uma vez que podem ser utilizadas para distinguir as origens étnicas ou para inferir crenças religiosas ou dados sobre a saúde. De uma maneira geral, o grupo de trabalho não considera que as imagens presentes na Internet sejam dados sensíveis[15], a menos que sejam claramente utilizadas para revelar dados sensíveis sobre os indivíduos.

Enquanto responsáveis pelo tratamento dos dados, os SRS não podem tratar quaisquer dados sensíveis sobre os seus membros ou não membros sem o seu consentimento explícito[16]. Se um SRS incluir no formulário do perfil dos utilizadores quaisquer perguntas relativas a dados sensíveis, deve deixar bem claro que a resposta a essas perguntas é inteiramente voluntária.

3.5 Tratamento de dados de não membros

Muitos SRS permitem aos utilizadores introduzir dados sobre outras pessoas, como acrescentar um nome a uma imagem, avaliar uma pessoa ou enumerar as «pessoas que conheci/quero conhecer» em eventos. Esta marcação com etiquetas (*tagging*) pode igualmente identificar não membros. Contudo, o tratamento desses dados sobre não membros pelo SRS só pode ser feito se for cumprido um dos critérios estabelecidos no artigo 7.º da Directiva Protecção dos Dados.

Além disso, a criação de perfis previamente elaborados de não membros através da agregação de dados que são independentemente fornecidos por utilizadores do SRS, incluindo dados

---

13 Tal poderia ser facilitado mediante a introdução de instrumentos de gestão de etiquetas (*tags*) nos sítios de redes sociais da Web, por exemplo, disponibilizando áreas de um perfil pessoal para indicar a presença do nome de um utilizador nas imagens ou vídeos com uma etiqueta, indicando que aguardam consentimento; ou definindo prazos para etiquetas que não tenham recebido o consentimento do indivíduo assinalado na etiqueta.

14 Os Estados-Membros podem estabelecer isenções desta regra; ver o artigo 8.º, n.º 2, alínea a), segundo período, e n.º 4, da Directiva Protecção dos Dados.

15 Todavia, com o desenvolvimento das tecnologias de reconhecimento facial, a publicação de imagens na Internet suscita preocupações de privacidade crescentes.

16 O consentimento tem de ser livre, informado e específico.

sobre relacionamentos inferidos a partir de livros de endereços carregados, carece de base jurídica[17].

Mesmo que o SRS dispusesse de meios para contactar o não utilizador e informá-lo da existência dos dados pessoais que se lhe referem, um possível convite por correio electrónico para aderir ao SRS, a fim de aceder a esses dados pessoais violaria a proibição estabelecida no artigo 13.º, n.º 4, da Directiva Privacidade Electrónica sobre o envio de mensagens electrónicas não solicitadas para fins de marketing directo.

3.6 Acesso de terceiros

3.6.1 Acesso através do SRS

Para além do serviço básico de SRS, a maioria dos SRS oferece aos utilizadores outras aplicações fornecidas por terceiros que as desenvolvem e que fazem também tratamento de dados pessoais.

Os SRS devem dispor dos meios para assegurar que as aplicações de terceiros cumprem as Directivas Protecção dos Dados e Privacidade Electrónica. Isso implica, em especial, que facultam informações claras e específicas aos utilizadores sobre o tratamento dos seus dados pessoais e que apenas têm acesso aos dados pessoais necessários. Por conseguinte, o SRS deve oferecer a terceiros criadores de software um acesso estratificado, para que estes possam optar por um modo de acesso que é intrinsecamente mais limitado. O SRS deve ainda assegurar que os utilizadores podem facilmente comunicar preocupações que tenham relativamente às aplicações.

3.6.2 Acesso de terceiros através dos utilizadores

Os SRS permitem, por vezes, que os utilizadores acedam aos seus dados noutras aplicações e os actualizem. Por exemplo, os utilizadores podem ter a faculdade de:

- ler e afixar mensagens na rede a partir do seu telemóvel;
- sincronizar os dados de contacto dos seus amigos no SRS com o livro de endereços que têm num computador de secretária;
- actualizar automaticamente no SRS a sua situação ou localização, a partir de outro sítio Web.

Os SRS publicam o modo como este software pode ser escrito sob a forma de uma «Interface de programa de aplicação» («API»). Essa interface permite a quaisquer terceiros escrever software para executar estas tarefas e aos utilizadores escolher livremente entre os diversos fornecedores terceiros[18]. Ao oferecer uma API que permite acesso aos dados dos contactos, os SRS devem:

- prever um nível de pormenor que permita ao utilizador escolher um nível de acesso para os terceiros que seja apenas suficiente para executar uma determinada função.

---

[17] O considerando 38 da Directiva Protecção dos Dados especifica: «*Considerando que, para que o tratamento de dados seja leal, a pessoa em causa deve poder ter conhecimento da existência dos tratamentos e obter, no momento em que os dados lhe são pedidos, uma informação rigorosa e completa das circunstâncias dessa recolha.*» Para alguns SRS, a publicação de perfis de não membros tornou-se alegadamente uma forma importante de comercializar os seus «serviços».

[18] Embora «API» seja um termo técnico de sentido amplo, neste caso refere-se ao acesso em nome de um utilizador, ou seja, os utilizadores têm de facultar as suas credenciais de entrada ao software, para que este possa actuar em seu nome.

Ao aceder a dados pessoais através de API de terceiros, em nome de um utilizador, os serviços de terceiros não devem:

- tratar e armazenar os dados mais do que o tempo necessário para executar uma função específica;

- executar qualquer operação com os dados importados dos contactos do utilizador, além da utilização pessoal pelo utilizador que forneceu os dados.

3.7 Bases jurídicas para o marketing directo

O marketing directo constitui uma parte essencial do modelo de negócios dos SRS; os SRS podem usar modelos de comercialização diferentes. No entanto, o marketing que utiliza dados pessoais dos utilizadores deve cumprir as disposições aplicáveis da Directiva Protecção dos Dados e da Directiva Privacidade Electrónica[19].

O *marketing contextual* é adaptado ao conteúdo que é visualizado ou consultado pelo utilizador[20].

O *marketing segmentado* consiste na apresentação de anúncios a grupos-alvo de utilizadores[21]; um utilizador é colocado num grupo, de acordo com a informação que tiver comunicado directamente ao SRS[22].

Finalmente, o *marketing comportamental* selecciona os anúncios com base na observação e na análise da actividade dos utilizadores ao longo do tempo. Estas técnicas podem estar sujeitas a requisitos jurídicos diferentes, dependendo das bases jurídicas aplicáveis e das características das técnicas utilizadas. O grupo de trabalho recomenda que não se utilizem dados sensíveis em modelos de publicidade comportamental, excepto se estiverem cumpridos todos os requisitos jurídicos.

Seja qual for o modelo ou a combinação de modelos que se utilize, os anúncios podem ser directamente apresentados pelo SRS (o fornecedor de SRS actua, neste caso, como intermediário) ou por um anunciante terceiro. No primeiro caso, os dados pessoais dos utilizadores não necessitam de ser divulgados a terceiros. No segundo caso, porém, o anunciante terceiro pode tratar os dados pessoais sobre os utilizadores, por exemplo, se processar o endereço IP do utilizador e um testemunho (*cookie*) que foi colocado no computador do utilizador.

3.8 Conservação de dados

Os SRS ficam fora do âmbito da definição de serviços de comunicações electrónicas previstos no artigo 2.º, alínea c), da Directiva-Quadro (2002/21/CE). Os fornecedores de SRS podem proporcionar outros serviços que sejam abrangidos pelo âmbito de um serviço de comunicações electrónicas, como, por exemplo, um serviço de correio electrónico publicamente acessível. Esse serviço estará sujeito às disposições da Directiva Privacidade Electrónica e da Directiva Conservação de Dados.

---

[19] No futuro próximo, o Grupo de Trabalho pretende abordar os diferentes aspectos da publicidade em linha num documento distinto.

[20] Por exemplo, se a página que é apresentada mencionar a palavra «Paris», o anúncio pode dizer respeito a um restaurante nessa cidade.

[21] Sendo cada grupo definido por um conjunto de critérios.

[22] Por exemplo, quando se inscreveu nesse serviço.

Alguns SRS dão aos seus utilizadores a possibilidade de enviar convites a terceiros. A proibição de utilização de correio electrónico para fins de marketing directo não se aplica às comunicações pessoais. Para cumprir a excepção relativa às comunicações pessoais, um SRS deve satisfazer os seguintes critérios:

- não há incentivos quer para o remetente quer para o destinatário;
- o fornecedor não selecciona os destinatários da mensagem[23];
- a identidade do utilizador que envia a mensagem deve ser claramente mencionada;
- o utilizador que envia a mensagem deve conhecer todo o teor da mensagem que será enviada em seu nome.

Alguns SRS conservam também os dados de identificação dos utilizadores que foram proibidos de usar o serviço, para garantir que não se inscrevam de novo. Nesse caso, estes utilizadores devem ser informados de que tal tratamento está a ser efectuado. Além disso, a única informação que pode ser conservada é a informação de identificação e não os motivos por que essas pessoas foram proibidas de utilizar o serviço. Essa informação não deve ser conservada durante mais de um ano.

Os dados pessoais comunicados por um utilizador quando se regista num SRS devem ser suprimidos logo que o utilizador ou o fornecedor do SRS decida suprimir a conta[24]. Do mesmo modo, a informação suprimida por um utilizador ao actualizar a sua conta não deve ser conservada. Os SRS devem notificar os utilizadores antes de tomarem estas medidas, com os meios que têm à sua disposição para informar os utilizadores sobre estes períodos de conservação. Por razões de segurança e jurídicas, em casos específicos, pode justificar-se o armazenamento de contas e de dados actualizados ou suprimidos durante um período definido, a fim de ajudar a impedir operações maliciosas resultantes de roubo de identidade e de outros crimes ou infracções.

Quando um utilizador não utiliza o serviço durante um período definido, o perfil deve ser definido como inactivo, ou seja, deixar de ser visível para outros utilizadores ou para o exterior e, após um período suplementar, os dados da conta abandonada devem ser suprimidos. Os SRS devem notificar os utilizadores antes de tomarem essas medidas, com os meios que têm à sua disposição.

3.9 Direitos dos utilizadores

Os SRS devem respeitar os direitos dos indivíduos afectados pelo tratamento, de acordo com as disposições apresentadas nos artigos 12.º e 14.º da Directiva Protecção dos Dados.

Os direitos de acesso e rectificação dos utilizadores não se limitam aos utilizadores do serviço, mas a qualquer pessoa singular cujos dados sejam tratados[25]. Os membros e não membros dos SRS devem dispor de um meio para exercer o seu direito de acesso, correcção e supressão. As páginas iniciais dos sítios SRS devem referir claramente a existência de um

---

[23] Ou seja, a prática de alguns SRS enviarem convites indiscriminadamente para todo o livro de endereços de um utilizador não é permitida.

[24] Nos termos do artigo 6.º, n.º 1, alínea e), da Directiva Protecção dos Dados, os dados devem ser «*conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente.*»

[25] O que aconteceria, por exemplo, se o endereço de correio electrónico dessa pessoa fosse utilizado pelo SRS para lhe enviar um convite.

«serviço de reclamações» criado pelo fornecedor de SRS para tratar de problemas e reclamações relacionados com a protecção dos dados e a privacidade dos membros e não membros.

O artigo 6.º, n.º 1, alínea c), da Directiva Protecção dos Dados exige que os dados sejam «*adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente*». Neste contexto, pode observar-se que os SRS poderão ter de registar alguns dados de identificação sobre os membros, mas não necessitam de publicar o nome verdadeiro dos membros na Internet. Consequentemente, os SRS devem considerar cuidadosamente se é justificável que obriguem os seus utilizadores a actuar com a sua identidade verdadeira e não com um pseudónimo. Há fortes argumentos a favor de se dar aos utilizadores a possibilidade de escolha a este respeito e, em pelo menos um Estado-Membro, trata-se de uma obrigação legal. Há argumentos particularmente fortes no caso dos SRS com grande número de membros.

O artigo 17.º da Directiva Protecção dos Dados exige que o responsável pelo tratamento dos dados aplique medidas de segurança técnicas e organizacionais adequadas para proteger os dados pessoais. Em especial, essas medidas de segurança incluem mecanismos de controlo e autenticação do acesso que podem ser aplicadas mesmo que se utilizem pseudónimos.

4. Crianças e menores

Uma grande percentagem de serviços SRS é utilizada por crianças/menores. O parecer WP 147 do grupo de trabalho[26] debruçou-se sobre a aplicação dos princípios de protecção dos dados na escola e no meio escolar. O parecer sublinhou a necessidade de ter em conta o interesse superior da criança, conforme estipulado também na Convenção das Nações Unidas sobre os Direitos da Criança. O grupo de trabalho deseja sublinhar a importância deste princípio também no contexto dos SRS.

Algumas iniciativas interessantes[27] foram realizadas pelas autoridades de protecção de dados em todo o mundo. A maioria destas iniciativas incide na sensibilização relativamente aos SRS e aos riscos possíveis. O grupo de trabalho incentiva a que se desenvolva investigação suplementar sobre a forma de abordar as dificuldades que se levantam à verificação da idade e à comprovação de consentimento esclarecido adequadas, a fim de lidar melhor com estes desafios.

Com base nestas considerações, o grupo de trabalho crê que seria adequada uma estratégia em várias vertentes para abordar a protecção dos dados das crianças no contexto dos SRS. Essa estratégia poderia basear-se em:

- iniciativas de sensibilização, que são fundamentais para garantir a participação activa das crianças (através da escola, a inclusão de noções básicas de tratamento de dados nos currículos educativos, a criação de instrumentos educativos pontuais, a colaboração dos organismos nacionais competentes);

- tratamento justo e legítimo no que se refere aos menores, como, por exemplo, não solicitar dados sensíveis nos formulários de inscrição, a ausência de marketing directo destinado especificamente a menores, o consentimento prévio dos pais antes de

[26] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf.

[27] Por exemplo, a iniciativa portuguesa «Dadus» http://dadus.cnpd.pt/ e o «*Chat Check Badge*» dinamarquês, http://www.fdim.dk/.

efectuar a inscrição e graus adequados de separação lógica entre as comunidades de crianças e de adultos;

- aplicação de tecnologias de protecção da privacidade (PET) - por exemplo, pré-definições de privacidade fáceis de utilizar, caixas de advertência instantâneas em etapas adequadas, software de verificação da idade);

- auto-regulação dos fornecedores, para incentivar a adopção de códigos de boas práticas que devem dispor de medidas eficazes de execução, também de natureza disciplinar;

- se necessário, medidas legislativas pontuais para desencorajar práticas desleais e/ou enganosas no contexto dos SRS.

5. Síntese de obrigações/direitos

Aplicabilidade das directivas comunitárias

1. A Directiva Protecção dos Dados aplica-se, de um modo geral, ao tratamento de dados pessoais pelos SRS, mesmo que as suas sedes se situem fora do EEE.

2. Os fornecedores de SRS são considerados responsáveis pelo tratamento dos dados na acepção da Directiva Protecção dos Dados.

3. Os fornecedores de aplicações podem ser considerados responsáveis pelo tratamento dos dados na acepção da Directiva Protecção dos Dados.

4. Os utilizadores são considerados pessoas em causa relativamente ao tratamento dos seus dados pelos SRS.

5. O tratamento de dados pessoais pelos utilizadores, na maioria dos casos, está abrangido pela isenção doméstica. Há casos em que as actividades de um utilizador não são abrangidas por esta isenção.

6. Os SRS encontram-se fora do âmbito da definição de serviço de comunicações electrónicas, pelo que a Directiva Conservação de Dados não se aplica aos SRS.

Obrigações dos SRS

7. Os SRS devem informar os utilizadores da sua identidade e facultar informações exaustivas e claras sobre os objectivos do tratamento que pretendem fazer dos dados pessoais e as diferentes formas desse tratamento.

8. Os SRS devem facultar valores pré-definidos de privacidade.

9. Os SRS devem dar informações e fazer advertências adequadas aos utilizadores sobre os riscos para a vida privada quando carregam dados para os SRS.

11. Os utilizadores devem ser informados pelos SRS de que as imagens ou informações sobre outros indivíduos devem apenas ser carregadas com o consentimento desses indivíduos.

12. A página inicial do SRS deve conter, no mínimo, uma ligação a um serviço de reclamações, que abranja questões de protecção dos dados, tanto para membros como para não membros.

13. A actividade de marketing deve cumprir as regras estabelecidas nas Directivas Protecção dos Dados e Privacidade Electrónica.

14. Os SRS devem fixar períodos máximos de conservação dos dados dos utilizadores inactivos. As contas abandonadas devem ser suprimidas.

15. No que se respeito aos menores, os SRS devem tomar as medidas adequadas para limitar os riscos.

<u>Direitos dos utilizadores</u>

16. Tanto os membros como os não membros dos SRS têm os direitos de pessoas em causa que forem aplicáveis, nos termos do disposto nos artigos 10.º-14.º da Directiva Protecção dos Dados.

17. Tanto os membros como os não membros devem ter acesso a um procedimento de tratamento das queixas que seja fácil de utilizar, criado pelo SRS.

18. Os utilizadores devem, em geral, ser autorizados a adoptar um pseudónimo.

Feito em Bruxelas, em 12 de Junho de 2009

Pelo Grupo de Trabalho
O Presidente
Alex TÜRK