COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

DSATS
Pela Secretária-Geral
09/03/27

Teresa Xardoné
Adjunta da Secretária-Geral

N/Ref. 03.01
N/ Ofº 3704
de 27.03.2009

Exmª Senhora
Juíza Cons. Maria Adelina Sá Carvalho
II. Secretária-Geral da
Assembleia da República
Palácio de S. Bento
Lisboa

Á DAPLEN
09/03/30

A Directora de Serviços

Req. 65-X-ua-AE

Junto envio a resposta desta Comissão ao Requerimento do Sr. Deputado João Portugal sobre "*Protecção da Privacidade dos Cidadãos*".

Aproveito para exprimir a minha muita admiração e estima pessoal.

O Presidente

Luís Lingnau da Silveira

ASSEMBLEIA DA REPÚBLICA
304884
Gabinete da Secretária-Geral
09/03/27
Proc.º n.º 4

amm

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

N/Refª 03.01
N/Ofº nº 3405

Resposta ao requerimento do Deputado João Portugal

1. A protecção da privacidade dos internautas em pesquisas feitas através de motores de busca e outras ferramentas de Internet não pode resultar de acções isoladas em cada país, dada a natureza global do âmbito de tais meios de informação.

   A CNPD tem, assim, intervindo nesse sentido em instituições de nível europeu em que se encontra integrada.

   Trata-se, nomeadamente, do Grupo do Artigo 29, organismo consultivo da Comissão Europeia.

   Este organismo elaborou, recentemente, texto recomendatório sobre a matéria dos motores de busca (o qual contou com o voto positivo dos representantes da CNPD) – cuja cópia se junta, para melhor elucidação.

   O Grupo do Artigo 29 está, presentemente, a realizar audições com as empresas responsáveis pelos mais importantes motores de busca, com vista a levá-las a conduzir-se de acordo com as recomendações constantes daquele texto.

2. A legislação vigente – nomeadamente a Lei nº 67/98, de 26 de Outubro – não estabelece directamente prazos relativos à conservação dos dados pessoais recolhidos pelas entidades responsáveis por motores de busca.

   Atribui, assim, à CNPD a competência para a fixação desses prazos (artigo 23º, nº 1, al f).

   A CNPD acompanha a posição preconizada pelo Grupo do Artigo 29, que aponta o período de 6 meses como adequado ao balanceamento entre as exigências de protecção de dados e os interesses das empresas.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

As entidades responsáveis por motores de busca têm vindo a aproximar-se desta solução.

De todo o modo, na última audição realizada perante esse Grupo, realizada em 10 de Fevereiro de 2009, a Google, realçando embora ter procedido a uma redução do prazo que inicialmente utilizava, mostrou relutância em admitir um período inferior.

3. Como já mencionado, a CNPD entende que também no tocante à questão dos prazos de conservação dos dados pessoais em causa se deve adoptar uma solução pelo menos a nível europeu.

   É claro que, do ponto de vista da protecção de dados pessoais, a solução ideal seria a da destruição imediata dos dados pessoais do utilizador, uma vez cessada cada operação de busca.

   De todo o modo, a forma mais eficiente para conseguir a redução desses prazos – e a experiência tem-no demonstrado – é a da pressão colectiva, por parte das instituições europeias e do conjunto de autoridades de protecção de dados, tal como se tem vindo a proceder.

4. Constituem princípios gerais em matéria de protecção de dados, definidos nos instrumentos internacionais e comunitários aplicáveis (nomeadamente a Convenção 108 do Conselho da Europa e a Directiva 95/46/CE, do Parlamento Europeu e do Conselho), bem como na já mencionada Lei nº 67/98, os de que os responsáveis por quaisquer tratamentos de dados pessoais devem informar os titulares destes sobre as finalidades desses tratamentos, os seus eventuais destinatários e o modo de exercício dos direitos de acesso e, sendo caso disso, rectificação ou actualização.

   As entidades responsáveis pelos maiores motores de busca têm vindo a publicitar textos apelidados de "*Política de privacidade*" em que informam os interessados sobre os aspectos em questão.

   Menos segura é, porventura, a situação relativa às redes sociais, designadamente devido ao seu maior número, menor institucionalização e variável grau de responsabilidade acerca dos seus deveres sociais por parte de quem as gere.

   De todo o modo, a CNPD entende que todos os responsáveis por redes sociais devem prestar esse tipo de informações, face à lei em vigor.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

5. O princípio básico em matéria de protecção de dados é o de que estes só devem poder ser tratados com base em consentimento dos respectivos titulares.

   E esse consentimento deve ser revogável a todo o tempo.

   Não é, todavia, sempre fácil comprovar a verificação do consentimento, informado e livre, no que concerne à utilização de redes sociais.

   Isto vale, sobretudo, em relação aos menores, com respeito aos quais o consentimento terá, em regra, de ser prestado pelos respectivos representantes.

   Há redes sociais especialmente destinadas a menores, cujo consentimento deve poder ser directamente prestado, se eles já tiverem suficiente maturidade para tanto. Também a este propósito, porém, se suscitam problemas de comprovação difíceis de resolver.

   Por estar consciente deste problema, e de outros mais também suscitados pelas redes sociais em matéria de privacidade, a CNPD incluiu o tema das redes sociais no Projecto Dadus*, que vem realizando nas escolas com base em Protocolo celebrado com o Ministério da Educação.

   Junta-se o Tema 3 das Fichas de Apoio de professores, integrado nesse Programa, precisamente dedicado às redes sociais.

Lisboa, 26 de Março de 2009

O Presidente

Luís Lingnau da Silveira

Projecto que a CNPD teve a oportunidade de apresentar em Julho de 2008 à Comissão Parlamentar de Educação e que está disponível em *www.dadus.cnpd.pt

Anexo: Cópia de texto
amm

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS

00737/PT
WP 148

Parecer 1/2008 sobre questões de protecção dos dados ligadas aos motores de pesquisa

Adoptado em 4 de Abril de 2008

Este Grupo de Trabalho foi instituído pelo artigo 29.º da Directiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de protecção de dados e privacidade. As suas atribuições são descritas no artigo 30.º da Directiva 95/46/CE e no artigo 15.º da Directiva 2002/58/CE.

O secretariado é assegurado pela Direcção C (Justiça Civil, Direitos Fundamentais e Cidadania) da Comissão Europeia, Direcção-Geral da Justiça, da Liberdade e da Segurança , B-1049 Bruxelas, Bélgica, Gabinete n.º LX-46 06/80.

Sítio Web: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Índice

RESUMO

Os motores de pesquisa tornaram-se parte integrante da vida quotidiana das pessoas que usam a Internet e as tecnologias de pesquisa da informação. O Grupo de Trabalho do artigo 29.° reconhece a utilidade dos motores de pesquisa e a sua importância.

No presente parecer, o Grupo de Trabalho define um conjunto claro de responsabilidades dos fornecedores de motores de pesquisa na sua qualidade de responsáveis pelo tratamento dos dados tal como previsto na Directiva Protecção dos Dados (95/46/CE). Dado serem fornecedores de dados de conteúdo (ou seja, do índice dos resultados da pesquisa), aplica-se-lhes igualmente em situações específicas a legislação europeia em matéria de protecção dos dados, por exemplo se prestarem um serviço de armazenagem temporária ("caching") ou se se especializarem na criação de perfis de pessoas. O principal objectivo do presente parecer consiste em estabelecer um equilíbrio entre as necessidades comerciais legítimas dos fornecedores de motores de pesquisa e a protecção dos dados pessoais dos utilizadores da Internet.

O presente parecer aborda a definição de motores de pesquisa, os tipos de dados tratados na prestação de serviços de pesquisa, o enquadramento jurídico, os as finalidades/fundamentação do tratamento, a obrigação de informar as pessoas em causa e os direitos das pessoas em causa.

O presente parecer chega à conclusão fundamental de que a Directiva Protecção dos Dados se aplica de uma forma geral ao tratamento dos dados pessoais nos motores de pesquisa, mesmo que as suas sedes estejam situadas fora do EEE, e que incumbe aos motores de pesquisa nesta situação esclarecer o seu papel no EEE e o âmbito das suas responsabilidades ao abrigo da Directiva. A Directiva Conservação dos Dados (2006/24/CE) é claramente apontada como não aplicável aos fornecedores de motores de pesquisa.

O presente parecer conclui que os dados pessoais apenas devem ser tratados para fins legítimos. Os fornecedores de motores de pesquisa devem suprimir ou tornar anónimos de forma irreversível os dados pessoais que já não sirvam os objectivos especificados e legítimos da sua recolha e devem poder sempre justificar a conservação e a duração dos testemunhos de conexão ("cookies"). É necessário obter o consentimento dos utilizadores em todos os cruzamentos previstos de dados dos utilizadores e nos exercícios de enriquecimento de perfis de utilizadores. Os motores de pesquisa devem respeitar as opções de exclusão dos editores de sítios Web e os pedidos dos utilizadores de actualização/refrescamento da memória cache devem ser imediatamente satisfeitos. O Grupo de Trabalho recorda a obrigação de os motores de pesquisa informarem antecipada e claramente os utilizadores de todas as utilizações previstas dos respectivos dados e de prontamente respeitarem os direitos de acesso, verificação ou correcção dos seus dados pessoais em conformidade com o artigo 12.° da Directiva Protecção dos Dados (95/46/CE).

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

Tendo em conta o artigo 255.º 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 PRESENTE DOCUMENTO:

1. INTRODUÇÃO

Os fornecedores de motor de pesquisa da World Wide Web desempenham um papel crucial na sociedade da informação na sua qualidade de intermediários. O Grupo de Trabalho reconhece a necessidade e a utilidade dos motores de pesquisa e o seu contributo para o desenvolvimento da sociedade da informação.

No que respeita às autoridades independentes de protecção dos dados no EEE, na perspectiva de protecção dos dados, a cada vez maior importância dos motores de pesquisa reflecte-se no número crescente de queixas apresentadas por pessoas (pessoas em causa) sobre potenciais violações do seu direito à privacidade. Registou-se igualmente um aumento acentuado de pedidos dos responsáveis pelo tratamento dos dados e da imprensa sobre as implicações dos serviços de pesquisa da Web no que respeita à protecção dos dados pessoais.

As queixas das pessoas em causa e os pedidos dos responsáveis pelo tratamento dos dados e da imprensa reflectem os dois papéis diferentes desempenhados pelos fornecedores de motores de pesquisa no tocante aos dados pessoais.

Em primeiro lugar, na sua qualidade de prestadores de serviços aos utilizadores, os motores de pesquisa recolhem e tratam vastas quantidades de dados dos utilizadores, incluindo dados obtidos por meios técnicos, como os testemunhos de conexão. Os dados recolhidos vão desde o endereço IP dos utilizadores individuais a historiais do comportamento passado de pesquisa passando por dados fornecidos pelos próprios utilizadores quando subscrevem serviços personalizados. A recolha dos dados dos utilizadores levanta muitas questões. Após o caso da AOL, uma vasta audiência foi consciencializada para a sensibilidade das informações pessoais constantes dos registos de pesquisa[2]. O Grupo de Trabalho considera que os motores de pesquisa, na sua

---

1 Jornal Oficial n.º L 281 de 23/11/1995, p. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 No Verão de 2006, o prestador dos serviços publicou uma amostra de pesquisas e resultados de cerca de 650.000 utilizadores ao longo de um período de 3 meses. Apesar de a AOL ter substituído os nomes

qualidade de receptáculos de dados dos utilizadores, até ao momento, têm vindo a descrever de forma insuficiente aos utilizadores dos seus serviços o carácter e o objectivo das suas operações.

Em segundo lugar, na sua qualidade de fornecedores de conteúdo, os motores de pesquisa contribuem para tornar as publicações mais facilmente acessíveis a um público mundial. Alguns motores de pesquisa publicam novamente os dados no chamado "cache". Ao extraírem e agruparem informação das mais variadas origens e tipos sobre uma só pessoa, os motores de pesquisa podem criar uma nova imagem, que implica um risco muito mais elevado para a pessoa em causa do que se cada elemento de dados publicado na Internet permanecesse separado. As capacidades de representação e agregação dos motores de pesquisa podem afectar significativamente as pessoas na sua vida pessoal e social, nomeadamente se os dados pessoais constantes dos resultados da pesquisa forem incorrectos, incompletos ou excessivos.

O Grupo de Trabalho Internacional relativo à Protecção de Dados nas Telecomunicações[3] adoptou uma posição comum sobre a protecção da privacidade e os motores de pesquisa em 15 de Abril de 1998, que foi revista em 6-7 de Abril de 2006[4]. O Grupo de Trabalho manifestou então a sua preocupação em relação à perspectiva de os motores de pesquisa permitirem a criação de perfis de pessoas singulares. Esta posição comum descreveu a forma como algumas actividades dos motores de pesquisa podem constituir uma ameaça para a privacidade das pessoas e refere que qualquer tipo de informação pessoal publicada num sítio Web pode ser utilizada por terceiros para criar perfis.

Além disso, a 28.ª Conferência Internacional sobre protecção de dados e privacidade adoptou a resolução sobre a protecção da privacidade e os motores de pesquisa[5] em 2-3 de Novembro de 2006 em Londres. A resolução apela a que os fornecedores de motores de pesquisa respeitem regras de privacidade em consonância com a legislação nacional de muitos países, assim como com documentos políticos e tratados internacionais e alterem as suas práticas em conformidade. Aborda igualmente diversos motivos de preocupação ligados aos registos de servidor, a pesquisas combinadas e à sua armazenagem e à execução de perfis pormenorizados dos utilizadores.

2. DEFINIÇÃO DE MOTOR PESQUISA E DE MODELO DE NEGÓCIOS

Em linhas gerais, os motores de pesquisa são serviços que ajudam os seus utilizadores a encontrar informação na Web. Podem ser distinguidos de acordo com os vários tipos de dados que pretendem obter, incluindo imagens e/ou vídeos e/ou som ou outros tipos de formatos diferentes. Uma nova área de desenvolvimento é a respeitante aos motores de pesquisa que se destinam especificamente à elaboração de perfis de pessoas baseados em dados pessoais encontrados em qualquer local da Internet.

---

dos utilizadores por um número, os jornalistas apuraram que estes resultados podem frequentemente conduzir a utilizadores individuais, não só devido às chamadas "pesquisas de vaidade" (pessoas que pesquisam informação sobre si próprias) mas também devido ao cruzamento de diversas pesquisas de um só utilizador.

3 O Grupo de Trabalho foi lançado por Comissários de Protecção de Dados de vários países a fim de melhorar a privacidade e a protecção dos dados nas telecomunicações e nos meios de comunicação.

4 http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_en.pdf

5 http://www.privacyconference2006.co.uk/index.asp?PageID=3

No contexto da Directiva Comércio Electrónico (2000/31/CE), os motores de pesquisa foram classificados como um tipo de serviço da sociedade da informação[6], ou seja, como ferramentas de localização de informação[7]. O Grupo de Trabalho está a utilizar esta categorização como ponto de partida.

No presente parecer, o Grupo de Trabalho centra-se nos fornecedores de motores de pesquisa que adoptam o modelo de negócios dominante dos motores de pesquisa, baseado na publicidade. Esta tónica diz respeito a todos os motores de pesquisa bem conhecidos e importantes, assim como a motores de pesquisa especializados, como os centrados nos perfis de pessoas e os metamotores de pesquisa que apresentam e eventualmente reagrupam os resultados de outros motores de pesquisa existentes. O presente parecer não aborda funções de pesquisa existentes em sítios Web para efeitos da pesquisa apenas do próprio domínio desses sítios.

A rentabilidade de tais motores de pesquisa depende geralmente da eficácia da publicidade que acompanha os resultados da pesquisa. As receitas são geradas na maior parte dos casos por um método de pagamento por clique ("pay per click"). Neste modelo, o motor de pesquisa cobra à empresa de publicidade sempre que um utilizador clique numa ligação patrocinada. Muita investigação sobre a exactidão dos resultados da pesquisa e os anúncios incide sobre o direito de contextualização. Para que o motor de pesquisa produza os resultados pretendidos e apresente correctamente os anúncios a fim de optimizar as receitas, os motores de pesquisa procuram obter uma visão tão vasta quanto possível das características e contexto de cada pesquisa específica.

3. QUE TIPO DE DADOS?

Os motores de pesquisa tratam uma série de dados[8]. A lista dos dados em causa consta do apêndice.

Ficheiros de registo

Os ficheiros de registo da utilização de serviços do motor de pesquisa por pessoas específicas são – partindo do princípio de que não são tornados anónimos - os dados pessoais mais importantes que são tratados pelos fornecedores de motores de pesquisa. Os dados que descrevem a utilização do serviço podem ser subdivididos em várias categorias: registos de pesquisa (conteúdo das interrogações, data e hora, fonte (endereço IP e testemunho de conexão ou "cookie"), preferências do utilizador e dados referentes ao computador do utilizador); dados sobre o conteúdo disponibilizado (ligações e anúncios na sequência de cada interrogação); e dados sobre a navegação subsequente do utilizador (cliques). Os motores de pesquisa podem igualmente tratar dados operacionais referentes a dados do utilizador, dados sobre utilizadores registados e dados de outros

---

6 Os motores de pesquisa da Internet são considerados na legislação europeia relativa aos serviços da sociedade da informação, definidos no artigo 2.° da Directiva 2000/31/CE. Este artigo remete para a Directiva 98/34/CE, que especifica o conceito de serviço da sociedade da informação.

7 Ver n.° 2 do artigo 21.°, conjugado com o Considerando 18 da Directiva sobre Comércio Electrónico (2000/31/EC).

8 Um dos meios utilizados pelo Grupo de Trabalho do artigo 29.° foi a elaboração de um questionário em matéria de políticas de privacidade. O questionário foi enviado a diversos motores de pesquisa dos Estados-Membros, assim como a diversos motores estabelecidos nos Estados Unidos. O presente parecer assenta em parte na análise das respostas a este questionário. O questionário encontra-se anexado ao presente parecer (ver Anexo 2).

serviços e fontes, como o correio electrónico, a pesquisa no computador local e a publicidade em sítios Web de terceiros.

Endereços IP

Um fornecedor de motores de pesquisa pode estabelecer uma ligação entre vários pedidos e sessões de pesquisa provenientes de um único endereço IP[9]. É, portanto, exequível acompanhar e correlacionar todas as pesquisas Web provenientes de um só endereço IP se tais pesquisas forem registadas. A identificação pode ser melhorada se o endereço IP for correlacionado com um testemunho de conexão distribuído pelo fornecedor do motor de pesquisa que atribua um identificador único a cada utilizador, uma vez que este testemunho não muda quando o endereço IP é alterado.

O endereço IP pode igualmente ser utilizado como informação de localização, embora actualmente seja frequentemente inexacto.

Testemunhos de conexão Web

Os testemunhos de conexão do utilizador são criados pelo motor de pesquisa e armazenados no computador do utilizador. O conteúdo dos testemunhos varia consoante os fornecedores de motores de pesquisa. Os testemunhos criados pelos motores de pesquisa contêm geralmente informação sobre o sistema operativo e o navegador do utilizador, assim como um número de identificação único de cada conta de utilizador. Possibilitam uma identificação mais exacta do utilizador do que o endereço IP. Assim, por exemplo, se o computador for partilhado por diversos utilizadores com contas distintas, cada utilizador terá o seu próprio testemunho que o identifica como sendo o utilizador do computador. Quando um computador tem um endereço IP dinâmico e variável, e os testemunhos não são apagados no final de uma sessão, tais testemunhos permitem seguir o percurso do utilizador entre endereços IP. Podem igualmente ser utilizados para correlacionar pesquisas provenientes de computadores móveis, como os computadores portáteis, uma vez que o utilizador tem o mesmo testemunho em locais diferentes. Por último, se diversos computadores partilharem uma ligação Internet (p. ex., utilização de uma caixa ou de um gestor de rotas com tradução de endereços de rede), o testemunho permite identificar utilizadores individuais em computadores diferentes.

Os motores de pesquisa utilizam os testemunhos (geralmente testemunhos persistentes) para melhorar a qualidade do seu serviço mediante a armazenagem das preferências do utilizador e o registo de tendências dos utilizadores, de que é exemplo a forma como as pessoas pesquisam. A maior parte dos navegadores é configurada por defeito para aceitar testemunhos, embora seja possível configurá-los para que recusem todos os testemunhos, apenas aceitem testemunhos de sessão ou indiquem que está a ser enviado um testemunho. No entanto, algumas características e serviços podem não funcionar correctamente se os testemunhos forem inactivados e a configuração das características avançadas de gestão dos testemunhos nem sempre é muito fácil.

Testemunhos Flash

Algumas empresas de motores de pesquisa instalam testemunhos Flash no computador do utilizador. Actualmente, os testemunhos Flash não podem ser apagados com facilidade, por exemplo por intermédio de ferramentas de apagamento existentes por defeito nos navegadores Web. Os testemunhos Flash foram utilizados, por exemplo, para

---

[9] Um número crescente de FSI atribui endereços IP fixos a utilizadores individuais.

reforçar os testemunhos Web normais, que podem ser facilmente apagados pelos utilizadores, ou para armazenar muita informação sobre as pesquisas do utilizador (como todas as interrogações da Web enviadas a um motor de pesquisa).

4. QUADRO JURÍDICO

4. 1. Responsáveis pelos dados dos utilizadores

4.1.1. Direito fundamental: o respeito da vida privada

A recolha e armazenagem extensivas do historial de pesquisa das pessoas sob forma directa ou indirectamente identificável remete para a protecção nos termos do artigo 8.° da Carta Europeia dos Direitos Fundamentais.

O historial de pesquisa de uma pessoa constitui uma indicação dos seus interesses, relações e intenções. Estes dados podem ser subsequentemente utilizados para fins comerciais e pedidos e operações de obtenção de informação e/ou mineração de dados por parte de autoridades de aplicação da lei ou de serviços de segurança nacionais.

De acordo com o Considerando 2 da Directiva 95/46/CE, "os sistemas de tratamento de dados estão ao serviço do Homem; ... devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos".

Os motores de pesquisa desempenham um papel crucial como primeiro ponto de contacto de acesso livre à informação existente na Internet. Este livre acesso à informação é essencial para a criação de opiniões pessoais no nosso regime democrático. Por conseguinte, o artigo 11.° da Carta Europeia dos Direitos Fundamentais é especialmente importante, uma vez que estabelece que "*Todas as pessoas têm direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras*".

4.1.2. Aplicabilidade da Directiva 95/46/CE (Directiva Protecção dos Dados)

Em documentos de trabalho anteriores, o Grupo de Trabalho do artigo 29.° apresentou esclarecimentos em relação às regras de protecção dos dados desencadeadas pelo registo de endereços IP e pelo recurso a testemunhos no contexto de serviços da sociedade da informação. O presente parecer apresenta orientações adicionais em relação à aplicação das definições de "dados pessoais" e de "responsável pelo tratamento" no que respeita aos fornecedores de motores de pesquisa. Os serviços de motores de pesquisa podem ser prestados na Internet a partir da UE/EEE, de um local fora do território dos Estados-Membros da UE/EEE, ou de múltiplos locais na UE/EEE e no estrangeiro. Por conseguinte, será igualmente analisado o disposto no artigo 4.° da Directiva Protecção

dos Dados, que aborda a aplicabilidade da legislação nacional relativa à protecção dos dados.

Dados pessoais: endereços IP e testemunhos de conexão

No seu parecer (WP 136) sobre o conceito de dados pessoais, o Grupo de Trabalho clarificou a definição de dados pessoais[10]. O historial de pesquisa de uma pessoa constitui uma forma de dados pessoais se a pessoa a que diz respeito for identificável. Embora os endereços IP não sejam na maior parte dos casos directamente identificáveis pelos motores de pesquisa, a identificação pode ser efectuada por terceiros. Os fornecedores de acesso à Internet dispõem de dados sobre endereços IP. As autoridades de aplicação de lei e de segurança nacional podem aceder a estes dados e, nalguns Estados-Membros, entidades privadas acederam igualmente por intermédio de litígios cíveis. Por conseguinte, na maior parte dos casos - incluindo os casos em que se verifica a atribuição dinâmica de endereços IP - estarão disponíveis os dados necessários para identificar o ou os utilizadores do endereço IP.

No seu WP 136, o Grupo de Trabalho notou que "*... a menos que o Fornecedor de Serviço esteja em posição de distinguir com certeza absoluta que os dados correspondem a utilizadores que não podem ser identificados, terá de tratar toda a informação IP como dados pessoais, por uma questão de precaução*". O mesmo se aplica aos operadores de motores de pesquisa.

Testemunhos de conexão

Se um testemunho contiver um identificador único do utilizador, esse identificador constitui claramente um dado pessoal. A utilização de testemunhos persistentes ou de meios análogos com um identificador único do utilizador permite acompanhar os utilizadores de um determinado computador mesmo que sejam utilizados endereços IP dinâmicos[11]. Os dados comportamentais que são gerados através da utilização destes meios permitem aprofundar ainda mais as características pessoais da pessoa em causa, o que está em consonância com a lógica fundamental do modelo de negócios dominante.

Responsável pelo tratamento

O fornecedor de um motor de pesquisa que trata dados dos utilizadores, como o endereço IP e/ou testemunhos persistentes com um identificador único, é abrangido pelo âmbito material da definição de responsável pelo tratamento, uma vez que ele determina de facto as finalidades e meios do tratamento. O carácter multinacional dos grandes fornecedores de motores de pesquisa - com sedes frequentemente situadas fora do EEE, serviços prestados no mundo inteiro, a participação de várias sucursais e eventualmente terceiros no tratamento dos dados pessoais – gerou um debate sobre se devem ser considerados responsáveis pelo tratamento dos dados pessoais.

---

10 WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp110_pt.pdf

11 WP 136: "Neste ponto, deverá notar-se que, enquanto a identificação a partir do nome é o caso mais comum na prática, um nome pode não ser necessário em todos os casos para identificar uma pessoa.. Isto poderá acontecer quando são utilizados outros "identificadores" para distinguir alguém. De facto, ficheiros informáticos que registam dados pessoais atribuem normalmente um identificador único às pessoas registadas para evitar confusão entre duas pessoas no mesmo ficheiro."

O Grupo de Trabalho gostaria de sublinhar a diferença entre as definições de legislação de protecção dos dados do EEE e a questão do direito aplicável numa dada situação. Um fornecedor de motores de pesquisa que trate dados pessoais, como registos com historiais de pesquisa que possibilitem a identificação das pessoas, é considerado o responsável pelo tratamento destes dados pessoais, independentemente da questão da jurisdição.

Artigo 4.° da Directiva Protecção dos Dados/legislação aplicável

O artigo 4.° da Directiva Protecção dos Dados aborda a questão da legislação aplicável. O Grupo de Trabalho apresentou orientações adicionais em relação ao disposto no artigo 4.° no seu "**Documento de trabalho sobre a determinação da aplicação internacional da legislação da UE em matéria de protecção de dados ao tratamento de dados pessoais na Internet efectuado por sites não-europeus**"[12]. Há duas justificações desta disposição. A primeira consiste em evitar lacunas e a evasão em relação ao sistema comunitário estabelecido de protecção dos dados. A segunda é evitar a possibilidade de a mesma operação de tratamento poder ser regida pela legislação de mais de um Estado-Membro da UE. Dado o carácter transnacional dos fluxos de dados induzidos pelos motores de pesquisa, o Grupo de Trabalho aborda especificamente ambas estas complicações.

No caso de um prestador de serviços de motores de pesquisa estabelecido em um ou mais Estados-Membros e que neles presta todos os seus serviços, não há qualquer dúvida de que o tratamento dos dados pessoais que efectua é abrangido pelo âmbito da Directiva Protecção dos Dados. É importante sublinhar que, neste caso, as regras de protecção dos dados não se limitam às pessoas em causa no território nem à nacionalidade de um dos Estados-Membros.

Se o prestador de serviços de motor de pesquisa for um responsável pelo tratamento não sediado no EEE, há duas situações em que a legislação comunitária relativa à protecção dos dados ainda se aplica. Em primeiro lugar, se o fornecedor do motor de pesquisa dispuser de um estabelecimento num Estado-Membro, como previsto no n.° 1, alínea a), do artigo 4.°. Em segundo lugar, se o motor de pesquisa utilizar meios no território de um Estado-Membro, como previsto no n.° 1, alínea c), do artigo 4.°. Neste último caso, o motor de pesquisa, em conformidade com o disposto no n.° 2 do artigo 4.°, deve designar um representante no território desse Estado-Membro específico.

Estabelecimento no território de um Estado-Membro (EEE)

O n.° 1, alínea a), do artigo 4.° estabelece que a legislação de protecção de dados de um Estado-Membro deve ser aplicada se determinadas operações de tratamento de dados pessoais efectuadas pelo responsável pelo tratamento forem realizadas "no contexto das actividades de um estabelecimento" desse mesmo responsável no território de um Estado-Membro. O ponto de partida deve ser uma operação específica de tratamento de dados pessoais. No caso de um motor de pesquisa específico cuja sede esteja localizada fora do EEE, a é necessário determinar se o tratamento dos dados dos utilizadores envolve estabelecimentos situados no território de um Estado-Membro.

---

12 WP 56, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_pt.pdf

convites automáticos para "amigos", quer através da publicação de comentários automáticos, que remetem para *sites* de publicidade ou de pornografia. Os *spammers* criam falsos perfis para se poderem integrar na rede social e usufruir destas ferramentas para chegar a um número elevadíssimo de pessoas.

As redes sociais, devido à sua estrutura interligada, constituem locais privilegiados para ataques de vírus, que se propagam com uma rapidez espantosa, infectando milhões de perfis. Esta vulnerabilidade pode ter como consequências adicionais a exposição do perfil individual, a diversão para um ataque de *phishing*[1], o envio de conteúdos não solicitados por correio electrónico e por mensagens instantâneas.

.6. Fonte de informação para potenciais empregadores

Devido ao manancial de informação pessoal que as redes sociais proporcionam, regista-se uma tendência crescente de os gestores de recursos humanos realizarem pesquisas em redes sociais para o seu trabalho de selecção de candidatos a emprego, ou mesmo relativamente a empregados já ao serviço.
Com efeito, com vista a verificar ou completar informações sobre as candidaturas que recebem, as empresas recorrem aos dados pessoais disponíveis nos perfis de utilizadores das redes sociais, em muitos casos, correspondendo a informações publicadas há alguns anos, mas que permitem elaborar um perfil histórico e detalhado das pessoas, antes de as escolher.
Ora, o resultado de tais pesquisas pode vir a ter um efeito absolutamente perverso no futuro pessoal e profissional das pessoas, podendo prejudicá-las gravemente, por actos ou opções, aceitáveis e compreensíveis, praticados na fase da juventude, muitos anos atrás.

[1] ***Phishing*** – esquema fraudulento, realizado através de mensagens electrónicas, cujo remetente se apresenta com uma falsa identidade (de uma pessoa, empresa ou instituição existentes), com o objectivo de levar o destinatário a fornecer dados pessoais que serão usados posteriormente para roubo de identidade.

.7. Ameaças sociais

Pelas ferramentas e pelas funcionalidades que proporcionam, as redes sociais podem ser usadas de forma positiva ou potencialmente mal utilizadas. Neste último caso, as ameaças sociais que colocam podem ser dramáticas, em particular para os mais jovens.

As redes sociais são especialmente vulneráveis a situações de perseguição (*stalking*[2]) e de ameaça, dano ou ofensa (*cyberbyllying*[3]).
Dados estatísticos disponíveis indicam um crescimento do fenómeno do *cyberbullying*, a partir das redes sociais.

Na verdade, as redes sociais encorajam a publicação de dados pessoais, incluindo dados que podem revelar a localização e o horário de uma pessoa (morada, telefone de casa ou telemóvel, escola, horário das aulas) ou o seu padrão de utilização da Internet (perfis de mensagens instantâneas que podem indicar quando o utilizador está *online*).
Esta informação, fácil de obter, torna-se crucial para os perseguidores seguirem os seus alvos.
O impacto do *cyberstalking* na vítima é bem conhecido e pode variar entre a intimidação moderada e perda de privacidade e a ofensa física grave e danos psicológicos.

O comportamento de *cyberbullying* pode revestir-se de muitas formas, mas tem sempre consequências devastadoras para as suas vítimas [**ver Material de Apoio**].

---

[2] **Stalking** – perseguição que envolve um comportamento ameaçador, no qual o perpetrador procura repetidamente contacto com uma vítima através de proximidade física e/ou chamadas telefónicas, mas também através de meios electrónicos, como o correio electrónico (e-mail), mensagens instantâneas e mensagens nas redes sociais (cyberstalking).

[3] ***Cyberbullying*** – termo usado para descrever actos intencionais e repetidos de ameaça e ofensa, através da utilização de tecnologia, em particular dos telemóveis e da Internet.

.8. Utilização indevida dos dados do perfil pessoal por terceiros

Um dos maiores riscos das redes sociais relaciona-se com as ameaças à identidade da pessoa. A grande quantidade de dados pessoais disponível nos perfis de utilizador potencia o roubo de identidade através da apropriação de perfis por terceiros mal intencionados.

As redes sociais facilitam, pelas debilidades de segurança da sua própria infra-estrutura, os ataques de *phishing* personalizados - após recolha fácil de dados nos perfis pessoais e nos respectivos círculos de "amigos" - que visam a obtenção de *usernames* (nomes de utilizador) e *passwords* (palavras-passe), apropriando-se deste modo dos perfis.

Tal permite personificar o utilizador e agir em nome dele, o que significa roubar a sua identidade, podendo levar a cabo um conjunto de acções de consequências imprevisíveis: prejuízo da sua reputação, dano financeiro, envolvimento em actividades criminosas.

❑ Boas práticas para os utilizadores

Apesar dos muitos riscos enunciados, é possível minimizá-los substancialmente, desde que se adoptem as necessárias precauções e comportamentos correctos na utilização das redes sociais.

É fundamental que os jovens estejam bem conscientes dos riscos que correm. Isso já é meio caminho andado. A palavra-chave é não divulgar informação pessoal e respeitar escrupulosamente informação que detemos sobre outras pessoas.

Para tal, deixamos aqui um conjunto de boas práticas a observar quando se usa uma rede social.

FICHA DE APOIO # 3

.1. Utilização de pseudónimos

Deve pensar-se duas vezes antes de se usar o nome verdadeiro num perfil e, pelo menos, nunca dar o nome completo. É preferível utilizar um pseudónimo (discreto, que não chame muito a atenção sobre a pessoa) e, melhor ainda, usar esse pseudónimo só para efeitos desse perfil numa rede social. Usar diferentes pseudónimos em diferentes plataformas, pois dificulta a agregação de informação. Sabendo que todas as informações que disponibilizamos podem ser vistas e acedidas por terceiros e ficam nas malhas da Internet para sempre, o ideal é mesmo não revelarmos a nossa identidade verdadeira.

.2. Não disponibilizar informação pessoal

- É essencial ter extrema atenção aos dados pessoais que publicamos, seja no nosso perfil, seja depois em comentários ou mensagens. Se a essa informação estiver associado o nome verdadeiro, maior cuidado se deve ter quando se publicam muitos dados.

- Nunca dar a morada, o número de telefone, a data de nascimento, ou quaisquer outros dados que permitam a nossa localização. Não revelar a escola ou a turma e o horário das aulas (há escolas que têm os horários nos seus *websites*), o nome dos professores, ou outras informações que, sem grande esforço, permitem indirectamente enquadrarem-nos. Mesmo quando se pensa que se está anónimo, não é preciso ser um génio para combinar algumas pistas e descobrir quem somos ou onde estamos.

- É também preferível abrir uma conta de e-mail só para as comunicações no âmbito da rede social. Uma vez que para criar um perfil, é preciso fornecer um endereço de correio electrónico, então o melhor é ter uma caixa de correio à parte para não comprometer as nossas outras comunicações.

- Utilizar um nome de utilizador e uma palavra-passe diferente de qualquer outra só para aceder à rede social. Não esquecer as regras para fazer uma *password* forte e mais difícil de violar.

- Pensar bem antes de decidir pôr uma fotografia pessoal no perfil. Há sempre outras opções de imagem, até bem engraçadas, que não comprometem a identidade. Estar consciente que se perde o controlo da fotografia, pois qualquer pessoa pode copiá-la, editá-la (fazendo montagens nada agradáveis ou mesmo humilhantes) e publicá-la.

- Deve ter-se especial atenção à publicação de outros dados pessoais, que podem ser solicitados no formulário para a criação do perfil pessoal. Não é obrigatório preencher esses campos, e é até desejável que fiquem em branco: para quê partilhar com o mundo, por exemplo, a nossa religião, a nossa orientação sexual ou as nossas doenças.

- Também informações detalhadas sobre o quotidiano, pormenores da vida familiar ou segredos entre amigos, não devem ser partilhados *online*. Os verdadeiros amigos podem ouvir de viva voz as nossas alegrias e tristezas, medos e ansiedades, e não se corre o risco de desconhecidos ficarem a conhecer a nossa intimidade e abusarem dessa informação. E mesmo quando se usa pseudónimos, se se viver num meio pequeno, há sempre a possibilidade de se ser identificado.

- Relembrar que uma vez publicada informação na Internet, não é possível retirá-la. Mesmo apagando os dados do *site*, versões antigas já existem no computador de alguém.

.3. Respeitar a privacidade dos outros

Participar numa rede social deve ser um acto de responsabilidade. E mesmo quando uma pessoa está disposta a correr certos riscos pessoais, nunca deve pôr em perigo a privacidade de outros, sejam amigos, familiares ou simplesmente conhecidos.

Não se deve nunca revelar informação sobre outras pessoas, a reboque da nossa própria informação, a menos que essas pessoas consintam claramente nisso.

Isto é tanto mais importante quando se trata de publicar fotografias de grupo, às quais muitas vezes se associam os nomes (verdadeiros) ou outra informação que permite identificar e/ou localizar as pessoas.
Convém também ter presente que a publicação ilegal de imagens é crime, pelo que pode ser sancionada.

.4. Restringir as pessoas que podem ter acesso ao perfil

- Uma das regras mais importantes que se deve observar quando se cria um perfil numa rede social é restringir o leque de pessoas que pode ter acesso às nossas informações pessoais.

- Escolher, por isso, uma rede social que tenha opções que permitam ao utilizador controlar com quem partilha informação (grupo de amigos da escola, do clube, da equipa, da família, de outros grupos comunitários). Assim, é possível escolher exactamente a quem se dá acesso ao nosso perfil, evitando a difusão em massa dos nossos dados pessoais na Internet.

- Outro procedimento importante a adoptar é usar configurações que não permitam que o nosso perfil fique indexado aos motores de busca,

limitando em muito a possibilidade de encontrarem informação sobre nós, pela simples introdução de um nome ou de qualquer outra palavra-chave.

- Escolher criteriosamente quem se adiciona como amigo, abrindo a porta a tudo o que está relacionado com o nosso perfil. Os índices de popularidade pelo número de "amigos" virtuais que se tem são engodos para recolher informação pessoal.
  Do lado de lá, também pode estar alguém com identidade disfarçada, que diz ser uma pessoa, sendo afinal outra. E uma fotografia continua a não ser prova bastante.

- Não se deve reconhecer como amigo quem não se conhece verdadeiramente. Mesmo quando parece que aquela pessoa tem tudo a ver connosco e nos compreende, confidenciar-lhe aspectos privados da nossa vida é correr um risco muito elevado. Muitas vezes, as supostas afinidades que parecem estabelecer-se (os mesmos gostos musicais, cinematográficos ou de *hobbies*) não são mais do que investidas de estranhos mal intencionados.

.5. Ter atenção quando um "amigo" virtual quer um encontro

Se acontecer um desses "amigos" virtuais sugerir um encontro pessoal (o que pressupõe já saber aproximadamente em que localidade se vive ou pretender saber), **nunca** comparecer a esse encontro sozinho(a).
Antes de mais, deve informar-se os pais e conversar com eles sobre isso. Se decidir comparecer no encontro, ir sempre acompanhado(a), pelo menos por amigos em quem se confia. O encontro deve ser num local público, durante o dia, e deve sempre dizer-se a um adulto onde se vai e quando se espera regressar.

.6. Como agir em caso de ameaças

Se um jovem se sentir perseguido, humilhado, ofendido ou ameaçado por alguém ou por alguma coisa que se tenha passado *online*, enfim se estiver a ser vítima de *cyberbullying*:

- Reportar a situação a um adulto da sua confiança e insistir até que o adulto tome providências;
- Não abrir ou ler mensagens provenientes de *cyberbullies*, mas não as apagar, pois podem vir a ser necessárias para tomar medidas;
- Expor a situação à escola (professores, director de turma, conselho executivo) se o caso estiver relacionado com a escola;
- Nunca concordar encontrar-se com a pessoa que apenas conheceu *online*;
- Se for fisicamente ameaçado, pedir aos pais que informem a polícia.

Julho 2008

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Ministério da Educação

dgidc
Direcção-Geral de Inovação e de Desenvolvimento Curricular

Como o Grupo de Trabalho já referiu num seu documento de trabalho anterior[13], a existência de um "estabelecimento" implica o exercício efectivo e real de uma actividade através de disposições estáveis e tem de ser determinado em conformidade com a jurisprudência do Tribunal de Justiça das Comunidades Europeias. A forma jurídica do estabelecimento - um escritório, uma subsidiária com personalidade jurídica ou uma agência de terceiros - não é decisiva.

Contudo, é igualmente necessário que a operação de tratamento se desenrole "no contexto das actividades" do estabelecimento, o que significa que este deve igualmente desempenhar um papel relevante na operação específica de tratamento. É claramente o que sucede se:

- um estabelecimento for responsável por relações com os utilizadores do motor de pesquisa numa jurisdição específica;
- um fornecedor de motor de pesquisa estabelecer um escritório num Estado-Membro (EEE) que participa na venda dos anúncios orientados à população desse Estado;
- o estabelecimento de um fornecedor de motor de pesquisa cumprir as ordens do tribunal e/ou pedidos de aplicação da lei formulados pelas autoridades competentes de um Estado-Membro no que respeita aos dados dos utilizadores.

É o prestador do serviço de motor de pesquisa que é responsável por clarificar o grau de participação dos estabelecimentos no território dos Estados-Membros aquando do tratamento dos dados pessoais. Se um estabelecimento nacional estiver envolvido no tratamento de dados dos utilizadores, aplica-se o n.° 1, alínea a), do artigo 4.° da Directiva Protecção dos Dados.

Os fornecedores de motores de pesquisa não sediados no EEE devem informar os respectivos utilizadores sobre as condições em que devem observar a Directiva Protecção dos Dados, devido quer ao estabelecimento quer à utilização de meios.

Utilização de meios

Os motores de pesquisa que utilizem meios no território de um Estado-Membro (EEE) para o tratamento de dados pessoais são igualmente abrangidos pelo âmbito da legislação de protecção dos dados desse Estado-Membro. A legislação de protecção dos dados de um Estado-Membro aplica-se ainda se o responsável pelo tratamento [...] *recorrer, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade*.

No que respeita à prestação de serviços de motor de pesquisa fora da UE, os centros de dados situados no território de um Estado-Membro podem ser utilizados para a armazenagem e o tratamento remoto dos dados pessoais. Outros tipos de meios utilizados poderiam ser computadores pessoais, terminais e servidores. A utilização de testemunhos e de software análogo por um prestador de serviços em linha pode ser igualmente considerada uma utilização de meios no território do Estado-Membro, envolvendo assim a legislação de protecção dos dados desse Estado-Membro. Esta questão foi debatida no documento de trabalho acima referido (WP56), em que se refere que "*o PC do utilizador*

[13] WP 56, página 8, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_pt.pdf

pode considerar-se um meio na acepção do n.º 1, alínea c), do artigo 4.º da Directiva 95/46/CE. Está localizado no território de um Estado-Membro. O responsável pelo tratamento decidiu usar esse meio com a finalidade de tratar dados pessoais e, como se explicou já noutras partes deste documento, várias operações técnicas têm lugar sem o controlo da pessoa a quem os dados dizem respeito. O responsável pelo tratamento dos dados utiliza os meios do utilizador e esses meios não são usados apenas para trânsito no território da Comunidade".

Conclusão

O efeito combinado das alíneas a) e c) do n.º 1 do artigo 4.º da Directiva Protecção dos Dados é o de as suas disposições se aplicarem frequentemente ao tratamento dos dados pessoais por parte dos fornecedores de motores de pesquisa, mesmo que as suas sedes estejam localizadas fora do EEE.

A legislação nacional aplicável a um determinado caso requer uma análise mais aprofundada das suas circunstâncias. O Grupo de Trabalho aguarda que os fornecedores de motores de pesquisa contribuam para esta análise apresentando esclarecimentos adequados sobre o seu papel e actividades no EEE.

No caso dos fornecedores de motores de pesquisa multinacionais:

- os Estados-Membros em que o fornecedor do motor de pesquisa se encontra estabelecido aplicam ao tratamento a respectiva legislação nacional relativa à protecção dos dados, em conformidade com o n.º 1, alínea a), do artigo 4.º;
- se o fornecedor do motor de pesquisa não estiver estabelecido em nenhum Estado-Membro, os Estados-Membros aplicam ao tratamento a respectiva legislação nacional relativa à protecção dos dados, em conformidade com o n.º 1, alínea c), do artigo 4.º, se a empresa utilizar meios, automatizados ou não, no território desse Estado-Membro[14] para efeitos do tratamento de dados pessoais (por exemplo, a utilização de testemunhos).

Em determinados casos, um fornecedor de um motor de pesquisa multinacional deve observar múltiplas legislações de protecção dos dados devido às regras em relação à legislação aplicável e ao carácter transnacional do tratamento que faz dos dados pessoais:

- um Estado-Membro deve aplicar a respectiva legislação nacional a um motor de pesquisa estabelecido fora do EEE caso esse motor utilize meios;
- um Estado-Membro não pode aplicar a respectiva legislação nacional a um motor de pesquisa estabelecido noutra jurisdição do EEE, mesmo que o motor de pesquisa utilize meios. Em tais casos, é aplicável a legislação nacional do Estado-Membro em que o motor de pesquisa se encontra estabelecido.

---

[14] O Grupo de Trabalho atende aos critérios que se seguem para determinar a aplicabilidade do n.º 1, alínea c), do artigo 4.º no que se refere à utilização de testemunhos. O primeiro é a situação em que um prestador de serviços de motor de pesquisa dispõe de um estabelecimento num Estado-Membro a que não se aplica o n.º 1, alínea a), do artigo 4.º, devido a esse estabelecimento não ter impacto significativo no tratamento de dados (como pode suceder com um representante de imprensa). Outros critérios deste tipo são o desenvolvimento e/ou desenho de serviços de motor de pesquisa específicos do país, o conhecimento real pelo prestador de serviços em linha de que está a tratar de utilizadores existentes nesse país, assim como a vantagem de desfrutar de uma parte sólida do mercado dos utilizadores num Estado-Membro específico.

4.1.3 Aplicabilidade da Directiva 2002/58/CE (Directiva Privacidade Electrónica) e da Directiva 2006/24/CE (Directiva Conservação de Dados)

Os serviços de motores de pesquisa em sentido estrito não são de uma forma geral abrangidos pelo âmbito do novo quadro regulamentar das comunicações electrónicas em que se integra a Directiva Privacidade Electrónica. O artigo 2.º da Directiva-Quadro (2002/21/CE), que contém algumas definições gerais do quadro regulamentar, exclui explicitamente, na sua alínea c), os serviços que apresentam ou controlam editorialmente o conteúdo:

[Entende-se por] "Serviço de comunicações electrónicas", o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações electrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão, excluindo os serviços que prestem ou exerçam controlo editorial sobre conteúdos transmitidos através de redes e serviços de comunicações electrónicas; excluem-se igualmente os serviços da sociedade da informação, tal como definidos no artigo 1.o da Directiva 98/34/CE que não consistam total ou principalmente no envio de sinais através de redes de comunicações electrónicas;

Os motores de pesquisa não são, portanto, abrangidos pela definição de serviços de comunicações electrónicas.

Um fornecedor de motor de pesquisa pode, contudo, disponibilizar um serviço adicional abrangido pelo âmbito de um serviço de comunicações electrónicas, como um serviço de correio electrónico publicamente acessível que esteja sujeito à Directiva Privacidade Electrónica (2002/58/CE) e à Directiva Conservação de Dados (2006/24/CE).

O n.° 2 do artigo 5.° da Directiva Conservação de Dados estabelece especificamente que "nos termos da presente directiva, não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações". As interrogações em si seriam consideradas conteúdo e não dados de tráfego e a Directiva não obrigaria, portanto, à sua conservação.

Consequentemente, não se justifica qualquer referência à Directiva Conservação de Dados ligada ao armazenamento de registos de servidor gerados devido à disponibilização de um serviço de motor de pesquisa.

N.º 3 do artigo 5.° e artigo 13.° da Directiva Privacidade Electrónica

Determinadas disposições da Directiva Privacidade Electrónica, como o n.º 3 do artigo 5.° (testemunhos de conexão e programas de espionagem) e o artigo 13.° (comunicações não solicitadas) são disposições gerais aplicáveis não só aos serviços de comunicação electrónicas mas também a quaisquer outros serviços se estas técnicas forem utilizadas.

O n.° 3 do artigo 5.° da Directiva Privacidade Electrónica, que deve ser lido em conjugação com o Considerando 25 da Directiva Privacidade Electrónica, diz respeito à armazenagem de informação sobre o equipamento terminal dos utilizadores. O recurso a testemunhos persistentes com identificadores únicos permite o seguimento e a elaboração do perfil de utilização de um determinado computador mesmo que sejam utilizados

endereços IP dinâmicos. O n.° 3 do artigo 5.° e o Considerando 25 da Directiva Privacidade Electrónica estabelecem claramente que a armazenagem de tal informação no equipamento terminal dos utilizadores, ou seja, de testemunhos e meios semelhantes, a seguir denominados testemunhos), deve estar em conformidade com o disposto na Directiva Protecção dos Dados. O n.° 3 do artigo 5.° da Directiva Privacidade Electrónica clarifica, portanto, as obrigações em relação à utilização de testemunhos por parte de um serviço da sociedade da informação, decorrentes da Directiva Protecção dos Dados.

4.2 Fornecedores de conteúdo

Os motores de pesquisa tratam a informação, incluindo as informações pessoais, através do recurso ao varrimento, à análise e à indexação da World Wide Web e de outras fontes que tornam pesquisáveis e, por conseguinte, facilmente acessíveis por intermédio destes serviços. Alguns motores de pesquisa voltam a publicar os dados no chamado "cache".

4.2.1. Liberdade de expressão e direito à vida privada

O Grupo de Trabalho está consciente do papel especial que os motores de pesquisa desempenham no contexto da informação em linha. É necessário que o direito comunitário em matéria de protecção dos dados e a legislação dos vários Estados-Membros estabeleçam um equilíbrio entre, por um lado, a protecção do direito à vida privada e a protecção dos dados pessoais e, por outro, o fluxo livre de informação e o direito fundamental à liberdade de expressão.

O artigo 9.° da Directiva Protecção dos Dados destina-se a garantir este equilíbrio na legislação dos Estados-Membros, no contexto dos meios de comunicação. Além disso, o Tribunal de Justiça Europeu estabeleceu que as limitações da liberdade de expressão decorrentes da aplicação de princípios de protecção dos dados devem estar em conformidade com a legislação e respeitar o princípio da proporcionalidade[15].

4.2.2 Directiva Protecção dos Dados

A Directiva Protecção dos Dados não inclui uma referência específica ao tratamento dos dados pessoais por serviços da sociedade da informação que actuam na qualidade de intermediários na selecção. O critério decisivo da Directiva Protecção dos Dados (95/46/CE) no tocante à aplicabilidade das regras de protecção dos dados é a definição do responsável pelo tratamento, nomeadamente a questão de se saber se uma parte é ou não "individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais". A questão de se determinar se um intermediário deve ser considerado individualmente o responsável pelo tratamento ou o responsável pelo tratamento em conjunto com outrem no que se refere a determinados tratamentos de dados pessoais é distinta da questão de responsabilidade por tal tratamento[16].

---

[15] O Tribunal de Justiça Europeu analisou mais aprofundadamente a proporcionalidade do impacto das regras de protecção dos dados, designadamente na liberdade de expressão, no seu acórdão no processo Lindqvist/Suécia, pontos 88-90.

[16] Nalguns Estados-Membros, há isenções horizontais especiais ("portos seguros") em relação à responsabilidade dos motores de pesquisa ("ferramentas de localização de informação"). A Directiva

O princípio da proporcionalidade requer que, se um fornecedor de motor de pesquisa agir simplesmente na qualidade de intermediário, não deve ser considerado o principal responsável pelo tratamento no que se refere ao tratamento efectuado do conteúdo dos dados pessoais. Neste caso, os principais responsáveis pelo tratamento dos dados pessoais são os fornecedores de informação[17]. O controlo formal, jurídico e prático do motor de pesquisa sobre os dados pessoais em causa limita-se geralmente à possibilidade de suprimir os dados dos seus servidores. No que se refere à remoção dos dados pessoais dos seus índice e resultados da pesquisa, os motores de pesquisa têm controlo suficiente para poderem ser considerados responsáveis pelo tratamento nesses casos (individualmente ou em conjunto com outrem), embora o grau da obrigação de suprimir ou bloquear dados pessoais possa depender da legislação em matéria de responsabilidade civil e da regulamentação em matéria de responsabilidade de um dado Estado-Membro[18].

Os proprietários de sítios Web podem optar *a priori* por não participar no motor de pesquisa e no "cache" através da utilização do ficheiro robots.txt ou das balizas Noindex/NoArchive[19]. É essencial que os fornecedores de motores de pesquisa respeitem a vontade *a priori* de não inclusão manifestada pelos editores de sítios Web. Esta opção de não inclusão pode ser manifestada antes do primeiro varrimento do sítio Web ou já depois disso; neste último caso, as actualizações do motor de pesquisa deviam ser efectuadas o mais rapidamente possível.

Os motores de pesquisa nem sempre desempenham apenas um papel de intermediários. Por exemplo, alguns motores de pesquisa armazenam nos seus servidores partes integrais do conteúdo da Web - incluindo os dados pessoais dele constantes. Também não é claro até que ponto os motores de pesquisa estão a centrar-se activamente em informações pessoais que permitam a identificação pessoal no conteúdo que tratam. Varrer, analisar e indexar são tarefas que podem ser efectuadas automaticamente sem revelar a existência de informações pessoais que permitam a identificação. O formato dos tipos específicos de informações pessoais que permitam a identificação, que podem incluir números da segurança social, números de cartões de crédito, números de telefone e endereços

---

relativa ao comércio electrónico (2000/31/CE) não prevê portos seguros para os motores de pesquisa, mas nalguns Estados-Membros estas regras foram aplicadas. Ver "Primeiro relatório sobre a aplicação da Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços de sociedade da informação, em especial do comércio electrónico, no mercado interno" ("Directiva sobre comércio electrónico"), de 21.11.2003, COM/2003/0702 final, p. 13.

17 Os utilizadores do serviço de motor de pesquisa podem, a título estrito, ser considerados responsáveis pelo tratamento, embora o seu papel esteja habitualmente fora do âmbito da directiva enquanto "actividades exclusivamente pessoais" (ver o n.° 2, segundo travessão, do artigo 3.°).

18 Nalguns Estados-Membros da UE, as autoridades de protecção dos dados regulamentaram especificamente a responsabilidade que os fornecedores de motores de pesquisa têm de suprimir dados de conteúdo do índice de pesquisa, baseada no direito de oposição consagrado no artigo 14.° da Directiva Protecção dos Dados (95/46/CE) e na Directiva Comércio Electrónico (2000/31/CE). De acordo com essa legislação nacional, os motores de pesquisa são obrigados a observar uma política de informação e de supressão análoga à dos fornecedores de acolhimento ("hosting providers") Web para não porem em causa a sua responsabilidade.

19 Pode tratar-se de mais do que uma solução facultativa. Os editores de dados pessoais devem ponderar se a sua base jurídica de publicação abrange a indexação desta informação pelos motores de pesquisa e criar as respectivas salvaguardas necessárias, incluindo, nomeadamente, a utilização do ficheiro robots.txt e/ou das balizas Noindex/NoArchive.

electrónicos, torna estes dados facilmente detectáveis. Existe igualmente tecnologia mais sofisticada e cada vez mais utilizada pelos fornecedores de motores de pesquisa, como a tecnologia de reconhecimento facial no contexto do tratamento de imagens e da pesquisa de imagens.

Por conseguinte, os fornecedores de motores de pesquisa podem executar operações de valor acrescentado ligadas às características ou tipos de dados pessoais na informação que tratam. Em tais casos, ao abrigo da legislação de protecção dos dados, o fornecedor de motor de pesquisa é inteiramente responsável pelo conteúdo resultante, ligado ao tratamento dos dados pessoais. Está sujeito a essa mesma responsabilidade um motor de pesquisa que venda anúncios desencadeados por dados pessoais, como o nome de uma pessoa.

Funcionalidade de "cache"

A funcionalidade de "cache" é uma outra maneira de um fornecedor de motor de pesquisa pode exercer um papel mais vasto do que o de intermediário exclusivo. O período de conservação do conteúdo num "cache" devia limitar-se ao tempo necessário para solucionar o problema do não acesso temporário ao próprio sítio Web.

A superação do período de "cache" de dados pessoais contidos nos sítios Web indexados para além desta necessidade de atender à disponibilidade técnica deve ser considerada uma nova publicação independente. O Grupo de Trabalho considera o fornecedor de tal funcionalidade de "cache" responsável pelo cumprimento da legislação de protecção dos dados na sua qualidade de responsável pelo tratamento dos dados pessoais constantes das publicações colocadas em "cache". Em situações em que a publicação original seja alterada, por exemplo para suprimir dados pessoais incorrectos, o responsável pelo tratamento do "cache" devia satisfazer imediatamente os pedidos de actualização da cópia colocada em "cache" ou de bloqueio temporário dessa mesma cópia até que o sítio Web tenha sido revisitado pelo motor de pesquisa.

5. LEGALIDADE DO TRATAMENTO

Em conformidade com o artigo 6.° da Directiva Protecção dos Dados, os dados pessoais devem ser objecto de um tratamento leal e lícito; ser recolhidos para finalidades determinadas, explícitas e legítimas, e não ser posteriormente tratados de forma incompatível com essas finalidades. Além disso, devem ser adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente. Para que o tratamento de dados pessoais seja lícito, é necessário que observe um ou mais dos seis fundamentos de tratamento legítimo estabelecidos no artigo 7.° dessa mesma directiva.

5.1. Finalidades/fundamentos referidos pelos fornecedores de motores de pesquisa

De uma forma geral, os fornecedores de motores de pesquisa apontaram as seguintes finalidades e fundamentos para utilizar e armazenar dados pessoais na sua qualidade de responsáveis pelo tratamento dos dados dos utilizadores.

Melhoria do serviço
Muitos responsáveis pelo tratamento recorrem a registos de servidor para melhorar os seus serviços e a qualidade dos seus serviços de pesquisa. Em seu entender, a análise de registos de servidor constitui uma ferramenta importante para a melhoria da qualidade das pesquisas, dos resultados e dos anúncios, assim como para a criação de serviços novos e ainda não definidos.

Securização do sistema
Afirma-se que os registos de servidor contribuem para a segurança dos serviços de motor de pesquisa. Alguns fornecedores de motores de pesquisa declararam que a conservação de registos pode ajudar a proteger o sistema de ataques que comprometam a segurança. Necessitam de uma amostra suficiente do historial de registo de dados do servidor para detectar padrões e analisar ameaças de segurança.

Prevenção da fraude
Afirma-se que os registos do servidor contribuem para proteger os sistemas e utilizadores dos motores de pesquisa em relação à fraude e a abusos. Muitos fornecedores de motores de pesquisa utilizam um mecanismo de "pagamento por clique" no que respeita aos anúncios visionados. A desvantagem desta situação consiste no facto de ela pode conduzir a que uma empresa seja objecto de cobrança injusta se um atacante utilizar programas automáticos para clicar de forma sistemática nos anúncios. Os fornecedores de motores de pesquisa prestam atenção a esta situação e procuram assegurar que este tipo de comportamento seja detectado e erradicado.

Os requisitos contabilísticos são citados como finalidades no que respeita a serviços como cliques em ligações patrocinadas, em que há uma obrigação contratual e contabilística de conservação dos dados, pelo menos até que as facturas sejam pagas e que tenha expirado o prazo para litígios jurídicos.

Publicidade personalizada
Os fornecedores de motores de pesquisa estão interessados na publicidade personalizada a fim de aumentarem as suas receitas. As práticas actuais envolvem nomeadamente o atendimento ao historial das interrogações passadas, a categorização dos utilizadores e critérios geográficos. Por conseguinte, pode ser visualizado um anúncio personalizado com base no comportamento do utilizador e no seu endereço IP.

Alguns motores de pesquisa recolhem estatísticas para determinar que categorias de utilizadores acedem à informação em linha e em que altura do ano. Estes dados podem ser utilizados para melhorar o serviço, orientar os anúncios e até para fins comerciais, para determinar o custo para uma empresa que pretenda anunciar os seus produtos.

Aplicação da lei
Alguns fornecedores declaram que os registos são uma ferramenta importante para as autoridades de aplicação da lei investigarem e submeterem aos tribunais crimes graves, como a exploração infantil.

5.2. Análise das finalidades e fundamentos por parte do Grupo de Trabalho

Em termos gerais, os fornecedores de motores de pesquisa não apresentaram uma análise integral das finalidades determinadas, explícitas e legítimas em que assenta o tratamento dos dados pessoais. Em primeiro lugar, algumas finalidades, como a "melhoria do serviço" ou a "oferta de publicidade personalizada", são definidas de forma demasiado ampla para que possam constituir um quadro adequado para avaliar a legitimidade da finalidade. Em segundo lugar, uma vez que muitos fornecedores de motores de pesquisa mencionam muitas finalidades diferentes do tratamento, não é claro até que ponto os dados são mais uma vez tratados para uma outra finalidade que seja incompatível com a finalidade inicial da sua recolha.

A recolha e tratamento dos dados pessoais podem basear-se em um ou mais fundamentos legítimos. Há três fundamentos que os fornecedores de motores de pesquisa podem invocar para finalidades diferentes.

- Consentimento - alínea a) do artigo 7.° da Directiva Protecção dos Dados

A maior parte dos fornecedores de motores de pesquisa possibilita o acesso não registado e registado ao serviço. No segundo caso, por exemplo se um utilizador criar uma conta específica de utilizador, o consentimento[20] pode ser utilizado como motivo legítimo de tratamento de certas categorias muito específicas de dados pessoais para finalidades legítimas bem especificadas, incluindo a conservação de dados durante um lapso de tempo limitado. O consentimento não pode ser invocado no que respeita a utilizadores anónimos do serviço e aos dados pessoais recolhidos de utilizadores que não optaram voluntariamente por se autenticar. Estes dados não podem ser tratados nem armazenados para nenhuma outra finalidade que não seja o tratamento de um pedido específico com uma lista de resultados de pesquisa.

- Necessidade para a execução de um contrato - alínea b) do artigo 7.° da Directiva Protecção dos Dados

O tratamento pode ser igualmente necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa. Esta base jurídica pode ser invocada pelos motores de pesquisa para recolher dados pessoais que um utilizador forneça voluntariamente para assinar um determinado serviço, como uma conta de utilizador. Esta base pode igualmente ser invocada, tal como sucede com o consentimento, para tratar determinadas categorias bem específicas de dados pessoais para finalidades legítimas bem especificados de utilizadores autenticados.

---

[20] Alínea h) do artigo 2.° da Directiva Protecção dos Dados "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento"

Muitas empresas Internet referem igualmente que o utilizador estabelece uma relação contratual de facto ao utilizar serviços oferecidos no seu sítio Web, como um formulário de pesquisa. No entanto, este pressuposto geral não observa a limitação estrita da necessidade estabelecida na directiva[21].

- Necessidade para prosseguir interesses legítimos do responsável pelo tratamento - alínea f) do artigo 7.° da Directiva Protecção dos Dados

Nos termos da alínea f) do artigo 7.° da Directiva, o tratamento pode ser necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que esses interesses não prevaleçam sobre os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n.° 1 do artigo 1°.

Melhoria do serviço

Vários fornecedores de motores de pesquisa armazenam o conteúdo das interrogações dos utilizadores nos respectivos registos de servidor. Esta informação constitui uma ferramenta importante para fornecedores de pesquisas, permitindo-lhes melhorar os seus serviços mediante a análise do tipo de interrogações efectuadas, saber a forma como são aprofundadas essas pesquisas e quais os resultados da pesquisa que decidem aproveitar. Contudo, o Grupo de Trabalho do artigo 29.° considera desnecessário que as interrogações sejam associadas a pessoas identificadas para que possam ser utilizadas na melhoria dos serviços de pesquisa.

Para correlacionar as acções de um utilizador individual (e apurar assim, por exemplo, se as sugestões feitas pelo motor de pesquisa são úteis), apenas é necessário distinguir as acções de um utilizador das de um outro no decurso de uma interrogação; não é necessário poder identificar esses utilizadores. A título de exemplo, um motor de pesquisa pode pretender saber se o utilizador X pesquisou "deposito de madeira" e em seguida optou por clicar na variante ortográfica "depósito de madeira", mas não necessita de saber quem é o utilizador X. A melhoria do serviço não pode, portanto, ser considerada um motivo legítimo de armazenamento de dados que não tenham sido tornados anónimos.

Segurança do sistema

Os motores de pesquisa podem considerar a necessidade de manter a segurança do seu sistema como sendo um interesse legítimo e um fundamento adequado para tratar dados pessoais. Contudo, todos os dados pessoais armazenados para efeitos de segurança devem estar sujeitos a uma limitação estrita de finalidade. Por conseguinte, os dados armazenados para fins de segurança não podem ser utilizados para aperfeiçoar, por exemplo, um serviço. Os fornecedores de motores de pesquisa alegam que é necessário armazenar os registos de servidor durante um período razoável (o número de meses varia consoante os motores de pesquisa) a fim de poderem detectar modelos de comportamento dos utilizadores e de identificarem e impedirem assim ataques de recusa de serviço e outras ameaças de segurança. Todos esses fornecedores devem poder justificar de forma exaustiva o período de conservação que adoptam com essa finalidade, que dependerá da necessidade de tratar estes dados.

---

[21] Alínea b) do artigo 7.° da directiva. "...necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa".

Prevenção da fraude

Os motores de pesquisa podem igualmente ter um interesse legítimo na detecção e prevenção da fraude, como a "fraude de cliques", mas, a exemplo do que sucede com as finalidades de segurança, a quantidade de dados pessoais armazenados e tratados, assim como o período de tempo durante o qual os dados pessoais são conservados com esta finalidade, dependerá do facto de os dados serem efectivamente necessários para a detecção e prevenção de fraudes.

Contabilidade

Os requisitos contabilísticos não podem justificar o registo sistemático de dados de motores de pesquisa normais em que o utilizador não clique numa ligação patrocinada. O Grupo de Trabalho -com base na informação constante das respostas ao questionário pelos fornecedores de motores de pesquisa - tem igualmente sérias dúvidas de que dados pessoais dos utilizadores de motores de pesquisa sejam realmente essenciais para fins contabilísticos. Para uma avaliação conclusiva, seria necessária uma investigação mais aprofundada. Em todo o caso, o Grupo de Trabalho convida os fornecedores de motores de pesquisa a desenvolver mecanismos contabilísticos que protejam melhor a privacidade, por exemplo através da utilização de dados tornados anónimos.

Publicidade personalizada

Os fornecedores de motores de pesquisa que pretendam apresentar publicidade personalizada para aumentar as suas receitas podem invocar como fundamento para o tratamento legítimo de alguns dos dados pessoais as alíneas a) (consentimento) e b) (execução de um contrato) do artigo 7.° da Directiva, embora seja difícil apontar uma finalidade legítima desta prática no que respeita aos utilizadores que não criaram uma assinatura própria com base na informação específica sobre a finalidade do tratamento. O Grupo de Trabalho prefere claramente os dados tornados anónimos.

Aplicação da lei e pedidos jurídicos

As autoridades de aplicação da lei podem por vezes solicitar aos motores de pesquisa dados dos utilizadores a fim de detectar ou evitar a criminalidade. Entidades privadas podem igualmente tentar obter uma decisão judicial que requeira que um fornecedor de motor de pesquisa ceda dados sobre os utilizadores. Quando tais pedidos observam uma tramitação judicial válida e conduzem a decisões judiciais igualmente válidas, naturalmente que os fornecedores de motores de pesquisa as devem cumprir e fornecer a informação necessária. No entanto, tal cumprimento não deve ser confundido com uma obrigação ou justificação jurídica para armazenar tais dados unicamente para esta finalidade.

Além disso, a detenção pelos fornecedores de motores de pesquisa de elevadas quantidades de dados pessoais pode incentivar as autoridades de aplicação da lei ou outras a exercer os seus direitos mais frequente e intensamente, o que poderia por seu turno conduzir a uma diminuição da confiança dos consumidores.

5.3. Algumas questões a resolver pela indústria

Períodos de conservação

Se o tratamento efectuado pelo fornecedor de motor de pesquisa estiver sujeito à legislação nacional, deve satisfazer quer as normas de privacidade quer os períodos de conservação previstos na legislação desse Estado-Membro específico.

Se forem armazenados dados pessoais, o período de conservação não deve nunca exceder o necessário para a finalidade específica do tratamento. Por conseguinte, após o final de uma sessão de pesquisa, os dados pessoais podiam ser apagados, devendo, portanto, a armazenagem contínua ser adequadamente justificada. Contudo, algumas empresas de motores de pesquisa parecem conservar os dados por um período indeterminado, o que é proibido. Para cada finalidade devia ser definido um período de conservação limitado. Além disso, o conjunto de dados pessoais a conservar não deve ser excessivo em relação a cada finalidade.

Na prática, os principais motores de pesquisa conservam dados sobre os utilizadores num formato que os identifica pessoalmente durante até mais de um ano (a duração específica é variável). O Grupo de Trabalho acolhe com agrado as reduções recentes dos períodos de conservação dos dados pessoais pelos principais fornecedores de motores de pesquisa. No entanto, o facto de as principais empresas deste ramo terem podido reduzir os respectivos períodos de conservação sugere que os prazos precedentes eram mais longos do que o necessário.

Dadas as explicações iniciais apresentadas pelos fornecedores de motores de pesquisa sobre as possíveis finalidades da recolha de dados pessoais, o Grupo de Trabalho considera que se não justifica um período de conservação superior a 6 meses[22].

Contudo, a conservação dos dados pessoais e o período de conservação correspondente devem ser sempre justificados (com argumentos concretos e relevantes) e reduzidos ao mínimo, para melhorar a transparência, assegurar o tratamento leal e garantir a proporcionalidade em relação à finalidade que justifica tal conservação.

Para esse efeito, o Grupo de Trabalho convida os fornecedores de motores de pesquisa a aplicar o princípio da "privacidade desde a concepção", que contribuirá igualmente para encurtar ainda mais o período de conservação. Além disso, o Grupo de Trabalho considera que um período de retenção reduzido aumentará a confiança dos utilizadores no serviço e constituirá assim uma vantagem concorrencial significativa.

Se os fornecedores de motores de pesquisa conservarem dados pessoais durante mais do que 6 meses, terão de comprovar de forma clara que tal facto é estritamente necessário para o serviço.

Os fornecedores de motores de pesquisa devem sempre informar os utilizadores sobre as políticas de conservação aplicáveis relativamente a todos os tipos de dados dos utilizadores que tratam.

---

22 A legislação nacional pode requerer um apagamento mais precoce dos dados pessoais.

Tratamento posterior para finalidades diferentes

Depende do fornecedor do motor de pesquisa a medida e a forma como os dados dos utilizadores são analisados e a criação ou não de perfis (pormenorizados) dos utilizadores. O Grupo de Trabalho está consciente da possibilidade de este tipo de tratamento subsequente dos dados dos utilizadores estar ligado a um domínio fundamental da inovação da tecnologia dos motores de pesquisa e poder ter importantes implicações em termos de concorrência. A divulgação plena da utilização e análise subsequente dos dados dos utilizadores poderia igualmente aumentar a vulnerabilidade aos abusos dos serviços de motores de pesquisa. Contudo, este tipo de alegações não pode constituir uma desculpa para o não cumprimento da legislação aplicável de protecção dos dados dos Estados-Membros. Além disso, os fornecedores de motores de pesquisa não podem alegar que a finalidade da recolha de dados pessoais é o desenvolvimento de novos serviços cuja natureza ainda não foi especificada. A lealdade requer que as pessoas tenham conhecimento do grau de comprometimento da sua vida privada se os respectivos dados forem obtidos, o que não é possível a menos que as finalidades sejam definidas de forma mais precisa.

Testemunhos de conexão

Os testemunhos persistentes que contêm um identificador único do utilizador são dados pessoais e estão, portanto, sujeitos à legislação aplicável em matéria de protecção dos dados. A responsabilidade pelo seu tratamento não pode ser limitada à responsabilidade de o utilizador adoptar ou não determinadas precauções na configuração do seu navegador. O fornecedor do motor de pesquisa decide se é armazenado um testemunho, que testemunho é armazenado e para que finalidades é utilizado. Por último, as datas de expiração dos testemunhos fixadas por alguns fornecedores de motores de pesquisa afiguram-se excessivas. Por exemplo, diversas empresas criam testemunhos que expiram após muitos anos. Se for utilizado um testemunho, há que definir uma duração adequada que proporcione simultaneamente uma melhoria da navegação e uma duração limitada do testemunho. Nomeadamente devido à configuração por defeito dos navegadores, é muito importante que os utilizadores sejam plenamente informados sobre a utilização e os efeitos dos testemunhos. Esta informação deve ser mais visível do que a resultante da sua simples inclusão na política de privacidade de um motor de pesquisa, que pode não ser imediatamente aparente.

Anonimização

Se não houver motivos legítimos de tratamento, ou de utilização para além de determinadas finalidades bem especificadas, os fornecedores de motores de pesquisa devem apagar os dados pessoais. Em vez de as apagarem, os motores de pesquisa podem igualmente tornar os dados anónimos, mas tal anonimização deve ser completamente irreversível para que a Directiva Protecção dos Dados já não seja aplicável.

Mesmo que os endereços IP e os testemunhos sejam substituídos por um identificador único, a correlação das interrogações armazenadas pode permitir a identificação de pessoas. Por este motivo, se se optar pela anonimização em vez do apagamento, os métodos utilizados devem ser cuidadosamente ponderados e plenamente executados. Tal facto poderá implicar a supressão de partes do historial de pesquisa para evitar a possível identificação indirecta do utilizador que executou essas pesquisas.

A anonimização de dados deve excluir qualquer espécie de possibilidade de identificação de pessoas, designadamente através da articulação da informação tornada anónima detida pela empresa do motor de pesquisa com a informação detida por uma outra parte interessada (por exemplo, um fornecedor de serviços Internet). Actualmente, alguns fornecedores de motores de pesquisa truncam os endereços IPv4 removendo o seu octeto final, conservando assim de facto informação sobre o FSI ou a subrede do utilizador, mas não identificando directamente a pessoa. A actividade em causa poderá portanto provir de um de 254 endereços IP, o que pode não bastar para garantir a anonimização.

Por último, a anonimização ou o apagamento do registo devem igualmente ser aplicados retroactivamente e incluir todos os registos pertinentes do motor de pesquisa a nível mundial.

Correlação de dados entre serviços

Muitos fornecedores de motores de pesquisa proporcionam aos utilizadores a opção de personalizar a utilização dos seus serviços através de uma conta pessoal. Além da pesquisa, facultam serviços como o correio electrónico e/ou outras ferramentas de comunicação, como serviços de mensagens ou de discussão em linha, e ferramentas de estabelecimento de redes sociais, como blogs ou comunidades sociais. Embora a gama de serviços personalizados possa variar, uma característica comum é o modelo de negócios subjacente e o desenvolvimento contínuo de novos serviços personalizados.

A correlação do comportamento do cliente nos vários serviços personalizados de um fornecedor de motor de pesquisa e por vezes em diversas plataformas[23] é facilitada tecnicamente pelo recurso a uma conta pessoal central, embora possa ser igualmente alcançada por outros meios, através de testemunhos ou de outras características distintivas, como endereços IP individuais. Por exemplo, quando um motor de pesquisa oferece igualmente um serviço como a "pesquisa no computador local", o motor de pesquisa adquire informação sobre os documentos (e eventualmente o seu conteúdo) que um utilizador cria ou visualiza. Graças a estes dados, as pesquisas podem ser adaptadas para obter um resultado mais preciso.

O Grupo de Trabalho considera que a correlação de dados pessoais entre serviços e plataformas no que respeita a utilizadores autenticados apenas pode ser legitimamente efectuada com consentimento, após informação adequada dos utilizadores.

O registo num fornecedor de motor de pesquisa para beneficiar de um serviço de pesquisa mais personalizado deve ser voluntário. Os fornecedores de motores de pesquisa não podem sugerir que a utilização do seu serviço requer uma conta personalizada graças à reorientação automática de utilizadores não identificados para um formulário de entrada numa conta personalizada, uma vez que não é necessária e, portanto, se não justifica legitimamente a recolha de tais dados pessoais, excepto em caso de consentimento informado do utilizador.

A correlação pode igualmente ser efectuada no que respeita aos utilizadores não autenticados, com base no endereço IP ou num testemunho identificador único que pode ser reconhecido por todos os serviços oferecidos por um fornecedor de motor de pesquisa, o que envolve geralmente um processo automático, sem que o utilizador tenha

---

[23] Por exemplo no caso de Microsoft, entre o motor de pesquisa da World Wide Web e a consola de jogos ligada à Internet (Xbox).

conhecimento da mesma. A vigilância discreta do comportamento das pessoas e seguramente que do seu comportamento privado, como a visita de sítios Web, não está em conformidade com os princípios do tratamento leal e legítimo consagrados na Directiva Protecção dos Dados. Os fornecedores de motores de pesquisa devem clarificar muito bem o grau de correlação de dados entre serviços e actuar apenas numa base de consentimento.

Por último, alguns fornecedores de motores de pesquisa admitem explicitamente na respectiva política de privacidade o enriquecimento dos dados apresentados pelos utilizadores com os dados de terceiros e outras empresas que podem, por exemplo, juntar informação geográfica a gamas de endereços IP ou de sítios Web com anúncios vendidos pelo fornecedor do motor de pesquisa[24]. Este tipo de correlação poderá ser ilegal se as pessoas em causa não forem informadas desse facto na altura da recolha dos seus dados pessoais e se não lhes for concedida uma forma de acesso fácil aos seus perfis pessoais, assim como o direito de corrigirem ou suprimirem certos elementos incorrectos ou supérfluos. Se o tratamento em questão não fosse necessário para a prestação do serviço (de pesquisa), seria necessário o consentimento livre e informado do utilizador para que o tratamento fosse lícito.

6. OBRIGAÇÃO DE INFORMAR A PESSOA EM CAUSA

A maior parte dos utilizadores da Internet não tem conhecimento das elevadas quantidades de dados que são tratados sobre o seu comportamento de pesquisa, nem sobre as finalidades para que estão a ser utilizados. Se não tiverem conhecimento deste tratamento, não podem tomar decisões informadas sobre ele.

A obrigação de informar as pessoas sobre o tratamento dos seus dados é um dos princípios fundamentais da Directiva Protecção dos Dados. O artigo 10.° regulamenta a prestação desta informação em que os dados são obtidos directamente junto da pessoa em causa. Os responsáveis pelo tratamento dos dados são obrigados a fornecer à pessoa em causa as seguintes informações:

- a identidade do responsável pelo tratamento e, eventualmente, do seu representante;

---

24 Por exemplo a Microsoft, na sua Microsoft Online Privacy Notice Highlights (síntese noticiosa sobre a privacidade em linha da Microsoft), refere o seguinte: "Quando se regista em determinados serviços da Microsoft, ser-lhe-á pedida informação pessoal. A informação que recolhemos pode ser articulada com a informação obtida por outros serviços Microsoft e por outras empresas." URL: http://privacy.microsoft.com/. Sobre a partilha de dados com parceiros publicitários, a declaração integral sobre a privacidade da Microsoft afirma o seguinte: "Veiculamos igualmente anúncios e fornecemos ferramentas de análise de sítios Web para sítios e serviços não prestados pela Microsoft e podemos também recolher informação sobre a visualização de páginas nestes sítios de terceiros." URL: http://privacy.microsoft.com/en-us/fullnotice.aspx. Na sua política de privacidade, o Google afirma o seguinte: "Podemos articular a sua informação pessoal com a informação de outros serviços Google ou de terceiros para melhorar a experiência do utilizador, incluindo a personalização do conteúdo enviado para si próprio." URL: http://www.google.com/intl/en/privacy.html. Na sua política de privacidade, o Yahoo! afirma o seguinte: "O Yahoo! pode articular a informação que detém sobre a sua pessoa com informação que obtém através de parceiros de negócios ou de outras empresas." URL: http://info.yahoo.com/privacy/us/yahoo/details.html.

- as finalidades do tratamento a que os dados se destinam;

- outras informações, tais como:

  - os destinatários ou categorias de destinatários dos dados;

  - o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder;

  - a existência do direito de acesso aos dados que lhe digam respeito e do direito de os rectificar.

Na sua qualidade de responsáveis pelos dados do utilizador, os motores de pesquisa devem indicar de forma clara aos utilizadores qual a informação que é recolhida sobre eles e as finalidades a que se destina. Deve ser apresentada uma descrição básica da utilização da informação pessoal sempre que ela seja recolhida, mesmo que haja noutro lado uma descrição mais pormenorizada. Os utilizadores devem igualmente ser informados sobre o software, como testemunhos de conexão, que pode ser colocado no seu computador quando utilizam o sítio Web e sobre a forma como ele pode ser recusado ou apagado. O Grupo de Trabalho considera que esta informação é necessária no que respeita aos motores de pesquisa para garantir o tratamento leal.

A informação que foi fornecida pelos fornecedores de motores de pesquisa em resposta ao questionário do Grupo de Trabalho revela a existência de importantes diferenças. Alguns motores de pesquisa cumprem o estabelecido na directiva, através de ligações à sua política de privacidade quer a partir da página principal quer das páginas geradas numa pesquisa, assim como de informação sobre testemunhos. Noutros motores de pesquisa é muito difícil localizar a política de privacidade. Os utilizadores devem poder aceder facilmente a essa política antes de efectuarem qualquer pesquisa, incluindo a partir da página principal do motor de pesquisa.

O Grupo de Trabalho recomenda que a versão integral da política de privacidade seja tão completa e pormenorizada quanto possível e mencione igualmente os princípios fundamentais constantes da legislação de protecção dos dados.

O Grupo de Trabalho observa que muitas políticas de privacidade manifestam algumas lacunas no que se refere aos direitos de acesso ou apagamento das pessoas em causa previstos nos artigos 12.°, 13.° e 14.° da Directiva Protecção dos Dados. Estes direitos são um dos elementos fundamentais da protecção da vida privada das pessoas.

7. DIREITOS DAS PESSOAS EM CAUSA

Os motores de pesquisa devem respeitar os direitos de acesso e, se necessário, correcção ou apagamento das pessoas no que respeita às informações sobre elas. Estes direitos aplicam-se em primeiro lugar aos dados dos utilizadores autenticados armazenados pelos motores de pesquisa, designadamente aos perfis pessoais. Contudo, estes direitos aplicam-se igualmente aos utilizadores não registados, que devem dispor de meios para poderem provar a sua identidade ao fornecedor do motor de pesquisa, registando-se, por exemplo, para acesso aos dados futuros e/ou mediante uma declaração do respectivo fornecedor de acesso sobre a sua utilização no passado de um endereço IP específico relativamente ao qual é solicitado o acesso. Se se tratar de dados de conteúdo, os

fornecedores de motores de pesquisa não são geralmente considerados os principais responsáveis ao abrigo da legislação europeia de protecção dos dados.

Em 2000, no seu documento de trabalho "Privacidade na Internet"[25], o Grupo de Trabalho já indicou o seguinte: *"A personalização dos perfis deve estar sujeita ao consentimento prévio e informado das pessoas em causa. Deve ser-lhes facultado o direito de retirarem o seu consentimento, a qualquer momento e com efeito futuro. Deve ser facultada aos utilizadores, em qualquer momento, a possibilidade de acederem aos seus perfis para inspecção. Devem ter também o direito de corrigir e eliminar os dados conservados."*

No caso específico dos motores de pesquisa, os utilizadores devem ter o direito de aceder a quaisquer dados pessoais sobre eles armazenados em conformidade com o artigo 12.° da Directiva Protecção dos Dados (95/46/CE), incluindo às suas interrogações passadas, a dados colhidos de outras fontes e a dados que revelam o seu comportamento ou origem. O Grupo de Trabalho do artigo 29.° considera que é essencial que os fornecedores de motores de pesquisa facultem os meios necessários para o exercício destes direitos, por exemplo através de uma ferramenta Web que proporcione aos utilizadores registados o acesso directo em linha aos respectivos dados pessoais e lhes permita oporem-se a determinados tratamentos de dados.

Em segundo lugar, o direito de corrigir ou suprimir informações aplica-se igualmente a alguns dos dados específicos em "cache" detidos pelos fornecedores de motores de pesquisa, se estes dados já não corresponderem ao conteúdo real publicado na Web pelos responsáveis pelo tratamento do ou dos sítios Web que publicam esta informação[26]. Numa tal situação, após a recepção de um pedido de uma pessoa em causa, os fornecedores de motores de pesquisa devem actuar prontamente para remover ou corrigir a informação incompleta ou desactualizada. O "cache" pode ser actualizado através de uma nova visita instantânea e automática da publicação original. Os fornecedores de motores de pesquisa devem proporcionar aos utilizadores a possibilidade de solicitarem a remoção gratuita de tal conteúdo do respectivo "cache".

8. CONCLUSÕES

A Internet foi concebida como uma rede aberta e global que possibilita o intercâmbio de informação. Contudo, é necessário alcançar um equilíbrio entre o carácter aberto da Internet e a protecção dos dados pessoais dos seus utilizadores. Este equilíbrio pode ser alcançado se se distinguir entre os dois principais papéis dos fornecedores de motores de pesquisa. No seu primeiro papel, na qualidade de responsáveis pelo tratamento de dados dos utilizadores (como endereços IP que recolhem junto deles e o seu historial individual de pesquisa), devem considerados plenamente responsáveis ao abrigo da Directiva Protecção dos Dados. No seu segundo papel, na qualidade de fornecedores de dados de conteúdo (como os dados constante do índice), em geral não são considerados, ao abrigo da legislação europeia de protecção dos dados, os principais responsáveis pelos dados pessoais que tratam. Há excepções, como a disponibilidade de um "cache" a longo prazo e operações de valor acrescentado em dados pessoais (como motores de pesquisa

---

[25] WP 37, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37_pt.pdf

[26] O Grupo de Trabalho sugere que os editores de páginas Web desenvolvam meios para informar automaticamente os motores de pesquisa sobre qualquer pedido que recebam de supressão de dados pessoais.

destinados à elaboração de perfis de pessoas singulares). Ao prestar tais serviços, os motores de pesquisa devem considerados plenamente responsáveis ao abrigo da Directiva Protecção dos Dados e devem cumprir todas as disposições pertinentes.

O artigo 4.° da Directiva Protecção dos Dados estabelece que as suas disposições se aplicam aos responsáveis pelo tratamento que tenham um estabelecimento envolvido no tratamento de dados pessoais no território de pelo menos um Estado-Membro. As disposições da directiva podem igualmente aplicar-se a fornecedores de motores de pesquisa não estabelecidos no território comunitário, se utilizarem equipamento, automatizado ou não, situado no território de um Estado-Membro para tratar dados pessoais.

Com base nas considerações acima formuladas e atendendo ao actual *modus operandi* dos motores de pesquisa, é possível formular as seguintes conclusões:

Aplicabilidade das directivas comunitárias

1. **A Directiva Protecção dos Dados (95/46/CE) aplica-se de uma forma geral ao tratamento dos dados pessoais pelos motores de pesquisa, mesmo que as suas sedes se situem fora do EEE.**

2. **Os fornecedores de motores de pesquisa não sediados no EEE devem informar os respectivos utilizadores sobre as condições em que devem observar a Directiva Protecção dos Dados, devido quer ao estabelecimento quer à utilização de meios.**

3. **A Directiva Conservação de Dados (2006/24/CE) não se aplica aos motores de pesquisa da Internet.**

Obrigações dos fornecedores de motores de pesquisa

4. **Os motores de pesquisa apenas podem tratar dados pessoais para finalidades legítimas e a quantidade de dados tem de ser relevante e não excessiva em relação às várias finalidades a alcançar.**

5. **Os fornecedores de motores de pesquisa devem suprimir ou tornar anónimos (de forma irreversível e eficaz) os dados pessoais que já não sejam necessários para a finalidade para que foram recolhidos. O Grupo de Trabalho apela ao desenvolvimento de sistemas adequados de anonimização por parte dos fornecedores de motores de pesquisa.**

6. **Os períodos de conservação devem ser minimizados e proporcionais a cada finalidade indicada pelos fornecedores de motores de pesquisa. Dadas as explicações iniciais apresentadas por estes sobre as possíveis finalidades da recolha de dados pessoais, o Grupo de Trabalho considera que se não justifica um período de conservação superior a 6 meses. No entanto, a legislação nacional pode requerer um apagamento mais precoce dos dados pessoais. Se os fornecedores de motores de pesquisa conservarem dados pessoais durante mais do que 6 meses, terão de comprovar de forma clara que tal facto é estritamente necessário para o serviço. Em todo o caso, a**

informação sobre o período de conservação de dados adoptado pelos fornecedores de motores de pesquisa deve ser facilmente acessível a partir da sua página principal.

7. **Embora os fornecedores de motores de pesquisa recolham inevitavelmente alguns dados pessoais sobre os utilizadores dos seus serviços, como o seu endereço IP, que provém do tráfego HTTP normalizado, não é necessário recolher mais dados pessoais de utilizadores individuais a fim de poder executar o serviço que consiste na apresentação de resultados de pesquisa e de anúncios.**

8. **Se os fornecedores de motores de pesquisa utilizarem testemunhos de conexão, a sua duração não deve ser nunca superior à que se possa provar ser necessária. A exemplo do que sucede com os testemunhos de conexão Web, os testemunhos Flash apenas devem ser instalados se for prestada informação transparente sobre a finalidade da sua instalação e sobre como aceder, editar e apagar esta informação.**

9. **Os fornecedores de motores de pesquisa devem facultar aos utilizadores informações claras e inteligíveis sobre a sua identidade e localização e sobre os dados que pretendem recolher, armazenar ou transmitir, assim como sobre a finalidade para que são recolhidos[27].**

10. **O enriquecimento dos perfis dos utilizadores com dados não apresentados pelos próprios deve assentar no consentimento dos utilizadores.**

11. **Para os fornecedores de motores de pesquisa facultarem meios para conservar o historial de pesquisa individual, é necessário que obtenham o consentimento do utilizador.**

12. **Os motores de pesquisa devem respeitar as opções de exclusão dos editores de sítio Web que indiquem que o sítio Web não deve ser varrido e indexado, nem incluído nos "caches" dos motores de pesquisa.**

13. **Se os fornecedores de motores de pesquisa proporcionarem um "cache" em que dados pessoais sejam disponibilizados durante mais tempo do que a publicação original, devem respeitar o direito das pessoas em causa de remoção do "cache" de dados excessivos e inexactos.**

14. **Os fornecedores de motores de pesquisa que se especializam na criação de operações de valor acrescentado, como perfis de pessoas singulares (denominados "motores de pesquisa de pessoas") e software de reconhecimento facial em imagens, devem ter um fundamento legítimo para o tratamento, como o consentimento, e cumprir todos os outros requisitos da Directiva Protecção dos Dados, como a obrigação de garantir a qualidade dos dados e a lealdade do tratamento.**

---

[27] O Grupo de Trabalho recomenda um modelo estratificado para a política de privacidade tal como descrito no seu parecer sobre a prestação mais harmonizada da informação (WP 100, *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_pt.pdf*)

Direitos dos utilizadores

15. **Os utilizadores de serviços de motores de pesquisa têm direito de acesso, inspecção e, se necessário, correcção, em conformidade com o artigo 12.° da Directiva Protecção dos Dados (95/46/CE), de todos os seus dados pessoais, nomeadamente no que respeita aos respectivos perfis e historiais de pesquisa.**

16. **A correlação cruzada de dados provenientes de serviços diferentes pertencentes ao fornecedor do motor de pesquisa apenas pode ser efectuada mediante consentimento do utilizador desse serviço específico.**

Feito em Bruxelas, em 4 de Abril de 2008

Pelo Grupo de Trabalho
O Presidente
Alex TÜRK

ANEXO 1
EXEMPLOS DE DADOS TRATADOS POR MOTORES DE PESQUISA & TERMINOLOGIA

Registos de pesquisa	
Interrogação	A interrogação introduzida no serviço do motor de pesquisa, geralmente armazenada nos seus registos sob a forma do URL da página enviada na sequência da interrogação.
Endereço IP	O endereço de Protocolo Internet do computador do utilizador utilizado em cada uma das interrogações efectuadas.
Data e hora	A data e hora em que uma interrogação foi efectuada.
Testemunho de conexão ("cookie")	O ou os testemunhos de conexão (e/ou meios análogos) armazenados no computador do utilizador, incluindo todos os parâmetros do testemunho, como a data de início e de expiração. No servidor do motor de pesquisa, todos os dados referentes ao testemunho, como a seguinte informação: "testemunho/meio X foi inserido no computador com endereço IP y, na data e hora z".
Testemunho Flash	Também denominado "objecto partilhado local". Testemunho instalado através do recurso à tecnologia Flash. Actualmente, não pode ser simplesmente apagado intervindo na configuração do navegador, ao contrário dos testemunhos Web tradicionais.
URL de referência	O URL da página Web em que o pedido de pesquisa foi efectuado, possivelmente um URL de terceiros.
Preferências	Possíveis preferências específicas do utilizador na configuração avançada do serviço.
Navegador	Pormenores sobre o navegador, incluindo o tipo e versão.
Sistema operativo	Pormenores sobre o sistema operativo.
Língua	Configuração da língua do navegador do utilizador, que pode ser utilizada para presumir a preferência linguística do mesmo.
Conteúdo disponibilizado	
Ligações	As ligações que foram enviadas a um utilizador específico na sequência de uma interrogação numa determinada data e hora. Os resultados do motor de pesquisa são dinâmicos. Para poder avaliar os resultados em pormenor, o fornecedor do motor de pesquisa precisa de armazenar dados sobre as ligações específicas e a ordem segunda a qual são mostradas numa determinada data e hora em resposta a uma interrogação específica do utilizador.
Anúncios	Os anúncios que foram mostrados ao utilizador na sequência de uma interrogação específica do próprio.
Navegação pelo utilizador	Cliques efectuados pelo utilizador nos resultados concretos e nos anúncios da ou das páginas de resultados da pesquisa, incluindo a posição dos resultados específicos que foram utilizados (ex: em primeiro lugar, foi utilizada a ligação n.º 1 e depois o utilizador regressou à página de resultados e clicou na ligação n.º 8).
Dados operacionais	Tendo em conta o valor e a utilização operacionais de alguns dados acima descritos, por exemplo com vista à detecção de fraudes, à segurança/integridade do serviço, e à elaboração de perfis do utilizador, os motores de pesquisa assinalam e analisam estes dados de várias formas. Por exemplo, um endereço IP específico pode ser assinalado como fonte provável de pesquisas ou cliques que constituem "spam", um clique específico num anúncio pode ser assinalado como fraudulento e uma pesquisa pode ser assinalada como ligada a fontes de informação relativas a uma determinada matéria.
Dados sobre os utilizadores	Um fornecedor de um motor de pesquisa pode proporcionar o registo dos utilizadores com vista a serviços melhorados. O fornecedor habitualmente

registados	trata dados da conta do utilizador, como a identificação ("login") e senha do utilizador, um endereço electrónico e quaisquer outros dados pessoais apresentados pelo utilizador, como interesses, preferências, idade e sexo.
Dados de outros serviços/fontes	A maior parte dos fornecedores de motores de pesquisa proporciona outros serviços, como o correio electrónico, a pesquisa no computador local e publicidade relativa a sítios Web e serviços de terceiros. Estes serviços geram dados do utilizador, que podem ser correlacionados e utilizados para aumentar o conhecimento sobre os utilizadores do motor de pesquisa. Os dados e os eventuais perfis do utilizador podem ser igualmente enriquecidos com dados de outras fontes, como dados de localização geográfica de endereços IP e dados demográficos.

ANEXO 2

QUESTIONÁRIO ENVIADO AOS MOTORES DE PESQUISA SOBRE POLÍTICAS DE PRIVACIDADE

1. Armazenam dados sobre a utilização individual dos vossos serviços de pesquisa?

2. Que tipo de informação armazenam/arquivam no que respeita aos vossos serviços de pesquisa (como registos de servidor, palavras-chave, resultados de pesquisa, endereços IP, testemunhos de conexão, dados sobre cliques, imagens de sítios Web ("caches"), etc.) ?

3. Solicitam o consentimento do utilizador (consentimento informado) para armazenar os dados indicados na resposta à pergunta n.º 2 e, em caso afirmativo, como o solicitam? Se não o solicitam, com que base jurídica justificam a armazenagem destes dados?

4. Criam perfis de comportamento do utilizador baseados nos dados indicados na vossa resposta à pergunta n.º 2? Em caso afirmativo, para que finalidades? Que dados tratam? Sob que identificador (por exemplo, um endereço IP, um identificador do utilizador ou um testemunho de conexão identificador) armazenam os perfis ? Solicitam o consentimento do utilizador?

5. Se proporcionam outros serviços personalizados para além dos serviços de pesquisa, partilham dados recolhidos nos vossos serviços de pesquisa com esses outros serviços e/ou vice-versa? Em caso afirmativo, especificar que dados.

6. Durante quanto tempo armazenam os dados indicados na vossa resposta à pergunta n.º 2 e para que finalidades?

7. A que critérios atendem na determinação do período de armazenagem?

8. Quando armazenam dados durante um período predeterminado, o que fazem quando esse período expira e que procedimentos utilizam em relação a esta matéria?

9. Tornam os dados anónimos? Em caso afirmativo, como os tornam anónimos? A anonimização é irreversível? Que informação ainda contêm os dados tornados anónimos?

10. Os dados encontram-se acessíveis (por exemplo ao pessoal) ou são tratados sem intervenção humana?

11. Enviam dados a terceiros? Em que países? Queiram especificar em relação às categorias que se seguem que tipos de dados podem partilhar e em que países:

    - Anunciantes;

    - Parceiros de publicidade;

    - Autoridades de aplicação da lei (cumprimento das obrigações jurídicas de transmissão de dados, por exemplo em processos judiciais);

    - Outros – especificar.

12. Como informam os utilizadores sobre a recolha, o tratamento e a armazenagem de dados? Fornecem aos utilizadores informações exaustivas sobre, por exemplo, testemunhos de conexão, a elaboração de perfis e outras ferramentas de monitorização da actividade dos sítios Web? Em caso afirmativo, queiram anexar uma cópia da nota informativa, assim como uma descrição da sua localização.

13. Concedem aos utilizadores o direito de acesso e de rectificação dos dados ou de eles serem alterados, apagados ou bloqueados? É possível optar integralmente *a priori* pela inexistência de recolha ou armazenamento por forma a que não sejam recolhidos quaisquer dados individuais e não subsistam quaisquer indícios do utilizador específico qualquer que seja o sistema de armazenagem pertinente? Há custos associados ao exercício destes direitos?

14. Aplicam medidas de segurança na armazenagem de dados? Quais ?

15. Já notificaram uma autoridade nacional de protecção dos dados do EEE? Em caso afirmativo, queiram indicá-la. Caso contrário, queiram indicar os motivos da não notificação.

Ficha de Apoio# 3

AS REDES SOCIAIS NA INTERNET

O que são as redes sociais?

As redes sociais na Internet - conhecidas por *Social Networking Sites (SNSs)* ou *Online Social Networks* - baseiam-se na criação e alargamento de comunidades virtuais de pessoas que partilham interesses e actividades, permitindo que os seus utilizadores interajam entre si, de modo geralmente gratuito e informal, estabelecendo desse modo relações sociais, assentes na afinidade de gostos, ideias ou acções.
Os *sites* que disponibilizam estas redes sociais estão, actualmente, entre os mais visitados do mundo, tendo-se transformado num dos fenómenos tecnológicos mais notáveis do século XXI.

Estes serviços são particularmente populares entre os jovens, pois permite-lhes criar com muita facilidade páginas pessoais na Internet, onde disponibilizam o seu perfil pessoal, recheado de fotografias e vídeos. Por outro lado, proporcionam também meios de comunicação entre os membros da rede social, como *blogs* ou mensagens instantâneas.

Entre as mais conhecidas redes sociais encontram-se o Hi5 (muito utilizado em Portugal), MySpace, Facebook, Flickr, Friendster, Orkut, MSN Spaces e You Tube.

Além de beneficiarem da abolição do tempo e do espaço na publicação de informação e na comunicação em tempo real (que a introdução da Internet permitiu), as redes

sociais vieram esbater a linha entre os habituais fornecedores de serviços (autores) e os consumidores (leitores). No ambiente da rede social, cada um pode ser autor. E esse é precisamente um dos seus maiores atractivos.

Ao mesmo tempo, as redes sociais parecem ter alargado as fronteiras daquilo que as sociedades viam como o espaço da livre expressão da individualidade. Quantidades gigantescas de informação pessoal, especialmente fotografias e vídeos, tornaram-se pública e globalmente disponíveis de uma forma sem precedentes.

Um dos maiores desafios que se colocam à privacidade, neste contexto, é o facto de a maioria dos dados pessoais publicados numa rede social o serem por iniciativa do próprio utilizador e, nessa medida, contarem implicitamente com o seu consentimento.

De facto, as novas gerações, já nascidas na era digital, têm conceitos diferentes do que pode ser entendido como privado e público. Além disso, de uma maneira geral, os jovens estão mais dispostos a correr riscos relativamente à sua privacidade, parecendo sentir-se mais à vontade para publicar na Internet pormenores (íntimos) das suas vidas.

Contudo, essa visão deriva, muitas vezes, da ingenuidade, do natural desejo de transgressão e da falta de conhecimento dos riscos associados a essa disponibilização de informação pessoal sem limites. Embora as redes sociais ofereçam uma nova gama de oportunidades de comunicação e troca de informações e possam ser de grande utilidade até a nível educativo, a verdade é que a sua utilização comporta igualmente sérios riscos para a privacidade dos seus utilizadores e para a de outros que nem sequer são membros da rede social.

Riscos associados à utilização de redes sociais

O surgimento das redes sociais está apenas no começo. Embora seja possível identificar já alguns riscos relacionados com a utilização destes serviços, é muito provável que apenas estejamos a ver a ponta do icebergue. Novas aplicações e novos riscos continuarão a emergir, designadamente o uso dos dados pessoais contidos nos perfis dos utilizadores por empresas e por autoridades públicas.

.1. Informação pessoal que nunca desaparece

A noção de "esquecimento" não existe na Internet. Uma vez publicados, os dados permanecem lá para sempre, mesmo que as pessoas os apaguem do seu perfil. Poderá haver cópias feitas por terceiros, publicadas noutro sítio, e as quais não se controlam. Também a existência de comentários noutros perfis com *links* (ligações) para o nosso perfil, inviabilizam a eliminação bem sucedida da nossa conta numa rede social.

Além disso, os serviços de arquivo na Internet conservam toda a informação, apesar de esta poder estar aparentemente escondida. Com pouco esforço, esses dados podem sempre ser acedidos.

Por outro lado, quem fornece o serviço da rede social recusa-se, muitas vezes, a apagar o conteúdo dos perfis, sendo que essas empresas podem estar sediadas em países fora da União Europeia, onde não há legislação capaz de os obrigar a fazê-lo.

É, por isso, imprescindível ter bem presente que, a partir do momento em que se publica o nome, o telefone, a morada, as fotos da festa, as actividades, os desejos, os medos, o diário do que se fez, a religião, a orientação sexual, etc., se está a disponibilizar informação que muito dificilmente alguma vez deixará de estar acessível a outros. Não há caminho de regresso. Em 10, 20 ou 40 anos, ao fazer uma pesquisa sobre um nome (por exemplo), aparecerá toda a informação

que lhe está associada, incluindo o que se disse, o que se fez, o que se mostrou quando se tinha 13 ou 15 anos.

.2. A falsa noção de "comunidade" e de "amigos"

As redes sociais criam a ilusão de transpor para o ciberespaço exactamente as mesmas estruturas de comunicação do mundo real, isto é, que os laços que unem as pessoas na vida real são equivalentes no mundo virtual. Por isso, promovem a partilha de informação *online* do mesmo modo que o podemos fazer com os amigos cara-a-cara, através do desenvolvimento da ideia de relacionamento, confiança e intimidade.

Ora esta ideia é claramente falaciosa, na medida em que nestas "comunidades" a maioria dos "amigos" não se sabe quem são. Apenas alguém que afirma ter os mesmos interesses. Com efeito, no mundo da Internet, temos muita dificuldade em garantir que quem está do lado de lá é verdadeiramente quem diz ser. As redes sociais incentivam, inclusivamente, o adicionar de "amigos", pois o seu sucesso depende do maior número de utilizadores e respectiva rede de ligações que conseguir atrair. Facilmente se coleccionam centenas de amigos digitais, o que faz aumentar os índices pessoais de popularidade, que podem funcionar para os jovens como um bálsamo de auto-estima e satisfação, com particular relevância numa fase complexa da vida como é a adolescência.

Mas, na verdade, os jovens estão a partilhar informações sobre si, os seus amigos ou a sua vida familiar com um número incalculável de desconhecidos, não controlando de todo quem efectivamente acede a todo esse manancial de dados pessoais e o que faz com eles. Este engano deliberado, esta ilusão de intimidade na Internet, comporta riscos muito elevados, como iremos ver mais adiante.

.3. Disponibilização excessiva de dados pessoais (fotos)

Criar um perfil numa rede social é muito simples, não exigindo grande destreza técnica, pelo que está facilmente ao alcance de qualquer jovem que navegue na Internet. A idade mínima normalmente exigida pelos serviços de redes sociais para se tornar um utilizador da rede é de 13 anos. No entanto, como não existe qualquer controlo efectivo sobre a idade dos subscritores, qualquer criança pode abrir a sua conta numa rede social.

Basta ter um endereço de correio electrónico para criar uma conta numa rede social. A partir daí, basta preencher um formulário para criar um perfil. Nesse formulário, são feitas muitas perguntas (ver exemplos no Material de Apoio), às quais os jovens displicentemente respondem, sem equacionar sequer a quantidade de dados pessoais que estão a difundir na Internet. Em muitos casos, os jovens disponibilizam, logo à partida, o seu nome verdadeiro, a sua localização (morada, telefone, escola, turma, etc.) bem como um conjunto de outra informação de natureza pessoal sobre as suas opções, o seu percurso, a sua vida familiar, os seus gostos, etc.

Ao publicarem, adicionalmente, fotografias e vídeos, os jovens estão a disponibilizar muito mais informação pessoal do que poderiam pensar.
Actualmente e em franco desenvolvimento, há um conjunto de ferramentas tecnológicas que permitem uma análise massiva e sistemática de informação.

Por um lado, as fotografias poderão tornar-se em identificadores biométricos universais dentro de uma rede ou mesmo entre redes, constituindo uma fonte de dados adequada para correlacionar perfis transversalmente através do reconhecimento facial. O *software* de reconhecimento facial melhorou bastante nos últimos anos e os novos sistemas já permitem trabalhar uma grande variedade de condições de imagem.

Por outro lado, há uma tecnologia emergente (CBIR - *Content Based Image Retrieval*) que cria possibilidades acrescidas de localizar utilizadores a partir de características de identificação de um local (um prédio, um quadro numa sala, um jardim, etc.), podendo designadamente ser usada por agressores sexuais para localização das suas potenciais vítimas.

A publicação de fotografias de grupo põe igualmente em risco a privacidade de terceiros. A partir do momento em que se torne possível associar um nome real a uma foto, pode destruir-se, inadvertidamente, a protecção de outras pessoas, incluindo aquelas que usam pseudónimos ou que têm perfis anónimos, e que a partir desse momento ficarão expostas.

De igual modo, a possibilidade que as redes sociais oferecem de ligar as fotografias (*image tagging*) a nomes, perfis ou endereços de correio electrónico, coloca riscos adicionais para a privacidade.

.4. Cruzamento de informações

Os prestadores de serviços de redes sociais são tecnicamente capazes de registar cada acção, cada movimento que é feito no seu *site*. Deste modo, é possível também detectar as redes de contacto de cada utilizador, sabendo quem se relaciona com quem. Estes dados, associados à informação pessoal publicada em cada perfil individual, são extremamente apetecíveis para efeitos de marketing, em especial marketing dirigido a determinados públicos-alvo.
A necessidade crescente de financiar estes serviços e de apresentar lucros leva à recolha, processamento e utilização dos dados pessoais dos utilizadores para outros fins, designadamente a sua venda a empresas comerciais.

.5. *Spam e* vírus

As redes sociais tornaram-se ambientes de eleição para a propagação de *spam* (mensagens electrónicas não solicitadas para fins de marketing), quer através de