COMISSÃO EUROPEIA

Bruxelas, 4.11.2010
COM(2010) 609 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

«Uma abordagem global da protecção de dados pessoais na União Europeia»

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

«Uma abordagem global da protecção de dados pessoais na União Europeia»

1. NOVOS DESAFIOS EM MATÉRIA DE PROTECÇÃO DE DADOS PESSOAIS

A Directiva da Protecção de Dados de 1995[1] constituiu um marco na história da protecção de dados pessoais na União Europeia. Nela se consagram duas das mais antigas e igualmente importantes ambições do processo de integração europeia: a protecção dos direitos e liberdades fundamentais das pessoas e, em especial, do direito fundamental à protecção de dados, por um lado, e a realização do mercado interno – neste caso, a livre circulação de dados pessoais –, por outro.

Quinze anos depois, este duplo objectivo é ainda válido e os princípios consagrados na directiva mantêm a sua validade. **Porém, a rapidez dos avanços tecnológicos e da globalização vieram alterar profundamente o mundo que nos rodeia e trazer novos desafios para a protecção dos dados pessoais.**

As tecnologias actuais permitem que as pessoas partilhem facilmente informações acerca dos seus comportamentos e preferências, tornando-as públicas e globalmente acessíveis numa escala sem precedentes. Os sítios de redes sociais, com centenas de milhões de membros em todo o mundo, são talvez o mais óbvio, mas não o único, exemplo deste fenómeno. A «computação em nuvem» – isto é, a utilização do computador com base na Internet, em que o *software*, os recursos partilhados e as informações se encontram em servidores remotos («na nuvem») – poderá colocar também desafios à protecção de dados, uma vez que poderá implicar que as pessoas percam o controlo sobre informações potencialmente sensíveis que lhes dizem respeito ao procederem ao armazenamento desses dados em programas que se encontram albergados no *hardware* de outrem. Um estudo recente confirmou que parece ser opinião comum – das autoridades de protecção de dados, associações empresariais e consumidores – que os riscos para a privacidade e a protecção de dados pessoais associados às actividades em linha estão a aumentar[2].

Ao mesmo tempo, **as formas de recolher dados pessoais tornaram-se progressivamente mais elaboradas e difíceis de detectar**. A utilização de ferramentas sofisticadas, por exemplo, permite que os operadores económicos seleccionem determinadas pessoas graças ao estudo do respectivo comportamento. E a utilização crescente de mecanismos que permitem a recolha automática de dados, como os bilhetes electrónicos de empresas transportadoras, a cobrança das portagens nas auto-estradas ou os dispositivos de localização geográfica, tornam mais fácil localizar as pessoas pelo simples facto de usarem um dispositivo móvel. As

---

[1] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24.10.1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

[2] Cf. *Study on the economic benefits of privacy enhancing technologies*, London Economics, Julho de 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), p. 14.

autoridades públicas utilizam também cada vez mais dados pessoais para várias finalidades, nomeadamente para localizar pessoas em caso de aparecimento de uma doença contagiosa, para prevenir e lutar mais eficazmente contra o terrorismo e a criminalidade, para gerir os regimes de segurança social ou para efeitos fiscais, no âmbito das suas aplicações de administração em linha, etc.

Tudo isto suscita inevitavelmente a questão de saber se a legislação de protecção de dados da UE tem ainda condições para enfrentar plena e eficazmente estes desafios.

Para analisar esta questão, a Comissão lançou uma revisão do quadro normativo vigente, promovendo uma conferência de alto nível em Maio de 2009, a que se seguiu uma consulta pública até ao final de 2009[3]. Foram também lançados vários estudos[4].

As conclusões confirmaram que os princípios nucleares da directiva se mantêm válidos e que deve ser preservado o seu carácter tecnologicamente neutro. No entanto, foram assinaladas várias questões problemáticas, que representam desafios específicos. Entre elas, incluem-se:

- *Equacionar o impacto das novas tecnologias*

As respostas enviadas no âmbito das consultas, tanto de pessoas singulares como de pessoas colectivas, confirmaram a necessidade de clarificar e especificar a aplicação dos princípios de protecção de dados às novas tecnologias, no intuito de garantir que os dados pessoais das pessoas singulares são efectivamente protegidos hoje em dia, qualquer que seja a tecnologia utilizada para o seu tratamento, e que os responsáveis pelo tratamento de dados estão plenamente conscientes das implicações das novas tecnologias para a protecção de dados. No sector das comunicações electrónicas, esta questão foi parcialmente tratada na Directiva 2002/58/CE (a «Directiva da Privacidade Electrónica»)[5], que pormenoriza e completa a Directiva da Protecção de Dados, que tem âmbito mais geral[6].

---

3 Ver as respostas à consulta pública da Comissão: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. Durante o ano de 2010 efectuaram-se consultas a interessados mais seleccionados. A Vice-Presidente Viviane Reding presidiu a uma reunião de alto nível com partes interessadas em 5 de Outubro de 2010, em Bruxelas. A Comissão consultou igualmente o Grupo de Trabalho do Artigo 29.º, que enviou um contributo circunstanciado à consulta de 2009 (WP 168) e adoptou um parecer específico, em Julho de 2010, sobre o conceito de responsabilização (WP 173).

4 Além do *Study on the economic benefits of privacy enhancing technologies* (cf. nota 2), ver também o *Comparative study on different approaches to new privacy challenges, nomeadamente no âmbito dos avanços tecnológicos*, Janeiro de 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). Está igualmente em curso um estudo sobre a avaliação de impacto do futuro quadro normativo da UE em matéria de protecção de dados pessoais.

5 Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 Julho 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (directiva relativa à privacidade e às comunicações electrónicas) (JO L 201 de 31.7.2002, p. 37).

6 A Directiva da Protecção de Dados (95/46/CE) estabelece as normas de protecção de dados a utilizar em todos os actos legislativos da UE, incluindo a Directiva da Privacidade Electrónica (2002/58/CE, alterada pela Directiva 2009/136/CE, JO L 337 de 18.12.2009, p. 11). A Directiva da Privacidade Electrónica é aplicável ao tratamento de dados pessoais ligado à prestação de serviços de comunicações electrónicas acessíveis ao público em redes públicas de comunicação. Esta directiva traduziu os princípios estabelecidos na Directiva da Protecção de Dados em normas específicas a aplicar no sector das comunicações electrónicas. A Directiva 95/46/CE aplica-se, entre outros, aos serviços de comunicação que não são públicos.

- *Reforçar a vertente de protecção de dados do mercado interno*

Umas das preocupações mais frequentes dos interessados, sobretudo das empresas multinacionais, é a frequente ausência de harmonização entre as legislações de protecção de dados dos Estados-Membros, apesar da existência de um quadro normativo comum da UE. Todos sublinharam a necessidade de aumentar a segurança jurídica, reduzir a sobrecarga administrativa e garantir a igualdade de condições para os operadores económicos e outros responsáveis pelo tratamento de dados.

- *Equacionar a globalização e melhorar as transferências de dados internacionais*

Vários interessados sublinharam que a crescente externalização do tratamento, muito frequentemente para fora da UE, suscita vários problemas relativos à lei aplicável ao tratamento e à atribuição de responsabilidades. Quanto às transferências de dados internacionais, muitas organizações consideram que os mecanismos actuais não são totalmente satisfatórios, pelo que devem ser revistos e racionalizados, de forma a tornar as transferências mais simples e menos pesadas.

- *Conseguir um quadro institucional mais firme para a aplicação efectiva das normas de protecção de dados*

É consensual entre os interessados que o papel das autoridades de protecção de dados deve ser reforçado, de modo a poderem garantir uma melhor aplicação das normas de protecção de dados. Algumas organizações pediram também maior transparência dos trabalhos do Grupo de Trabalho do Artigo 29.º (*ver ponto 2.5.*) e uma clarificação dos seus poderes e funções.

- *Aumentar a coerência do quadro normativo que rege a protecção de dados*

Na consulta pública, todos os interessados referiram a necessidade de aprovar um instrumento global, aplicável às operações de tratamento de dados em todos os sectores e políticas da União, que assegure uma abordagem integrada e também uma protecção contínua, coerente e efectiva[7].

Os desafios atrás referidos **exigem que a UE desenvolva uma abordagem global e coerente** que garanta que **o direito fundamental das pessoas singulares à protecção dos dados é plenamente respeitado na UE e fora dela.** O Tratado de Lisboa veio dar à UE meios adicionais para o conseguir: a Carta dos Direitos Fundamentais – cujo artigo 8.º reconhece um direito autónomo à protecção de dados – tornou-se vinculativa e foi introduzida[8] uma nova base legal, que permite a elaboração de legislação abrangente e coerente da União em matéria de protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. A nova base legal permite, em especial, que a UE disponha de um único instrumento para regular a protecção de dados, incluindo no domínio da cooperação policial e judiciária em matéria penal. A política externa e de segurança comum é apenas parcialmente abrangida pelo artigo 16.º do TFUE, visto que as normas específicas que

[7] Em observações separadas enviadas depois de terminada a consulta pública, a Europol e a Eurojust solicitaram, porém, que fossem tidas em conta as especificidades do seu trabalho no que se refere à coordenação da aplicação da lei e à prevenção da criminalidade.

[8] Cf. artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE).

regulam o tratamento de dados pelos Estados-Membros devem ser estabelecidas por uma decisão do Conselho com diversas bases legais[9].

Recorrendo a estas novas possibilidades legais, a Comissão dará grande prioridade ao respeito pelo direito fundamental à protecção de dados na União e em todas as suas políticas, reforçando em simultâneo a vertente do mercado interno e facilitando o livre fluxo de dados pessoais. Neste contexto, outros direitos fundamentais consagrados na Carta e outros objectivos dos Tratados também devem ser tidos plenamente em conta para proteger o direito fundamental à protecção de dados pessoais.

A presente comunicação destina-se a definir a abordagem seguida pela Comissão para modernizar o quadro normativo da UE em matéria de protecção de dados, tendo particularmente em conta os desafios resultantes da globalização e das novas tecnologias, de modo a continuar a garantir um elevado nível de protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais em todos os domínios de actividade da União. Desta forma a UE poderá continuar a ter um papel motor na promoção de níveis elevados de protecção de dados a nível mundial.

2. OBJECTIVOS PRINCIPAIS DA ABORDAGEM GLOBAL DA PROTECÇÃO DE DADOS

2.1. Reforçar os direitos das pessoas

2.1.1. Garantir a protecção adequada das pessoas em todas as circunstâncias

O objectivo dos instrumentos da UE em vigor no domínio da protecção de dados é **proteger os direitos fundamentais das pessoas singulares, em especial o direito à protecção de dados pessoais**, em conformidade com a Carta dos Direitos Fundamentais da União Europeia[10].

O conceito de «dados pessoais» é um dos conceitos essenciais da protecção das pessoas singulares previstos nos instrumentos da UE de protecção de dados actualmente em vigor e desencadeia a aplicação das obrigações que incumbem aos responsáveis pelo tratamento dos dados e aos subcontratantes[11]. A definição de «dados pessoais» engloba todas as informações relativas a uma pessoa identificada ou identificável, tanto directa como indirectamente. Para determinar se uma pessoa é identificável, importa considerar o «conjunto dos meios susceptíveis de serem razoavelmente utilizados, quer pelo responsável pelo tratamento dos dados quer por qualquer outra pessoa, para identificar a referida pessoa»[12]. Esta abordagem deliberada escolhida pelo legislador tem a vantagem de ser flexível, permitindo a sua aplicação a várias situações e desenvolvimentos que afectam os direitos fundamentais, incluindo os que não eram previsíveis no momento de adopção da directiva. No entanto, uma das consequências desta abordagem vasta e flexível é que há muitos casos em que nem

---

9 Cf. artigo 16.º, n.º 2, último parágrafo, do TFUE e artigo 39.º do Tratado da União Europeia.

10 Cf. os processos do Tribunal de Justiça da União Europeia C-101/01, *Bodil Lindqvist*, Col. [2003] I-1297, 96, 97, e C-275/06, *Productores de Música de España (Primusicae)/Telefónica de España SAU*, Col. [2008] I-271. Cf. também a jurisprudência do Tribunal Europeu dos Direitos do Homem, nomeadamente os processos: *S. e Marper/Reino Unido*, 4.12. 2008 (Pedidos n.os 30562/04 e 30566/04) e *Rotaru/Roménia*, 4.5. 2000; n.º 28341/95, § 55, TEDH 2000-V.

11 Cf. as definições de «responsável pelo tratamento» e de «subcontratante» do artigo 2.º, alíneas d) e e), da Directiva 95/46/CE.

12 Cf. considerando 26 da Directiva 95/46/CE.

sempre é claro, ao aplicar a directiva, qual a via a seguir, seja o direito à protecção de dados das pessoas, seja o cumprimento das obrigações previstas na directiva pelos responsáveis pelo tratamento de dados[13].

Há situações que implicam o tratamento de informações específicas, que poderão exigir medidas de protecção no âmbito do direito da União. Estas medidas já existem em algumas situações. A título de exemplo, a gravação de informações em equipamentos terminais (telemóveis, por exemplo) só é permitida se a pessoa tiver dado o seu consentimento. Esta questão poderá ter de ser regulada a nível da UE no que se refere, por exemplo, a dados codificados, a dados de localização geográfica, a tecnologias de prospecção de dados que permitem a combinação de dados de diversas fontes, ou nos casos em que a confidencialidade e integridade devem ser garantida em sistemas de tecnologias da informação[14].

Sendo assim, todas as questões atrás referidas devem ser objecto de análise cuidada.

A Comissão irá ponderar qual a **melhor forma de garantir a aplicação coerente das normas de protecção de dados, tendo em consideração o impacto das novas tecnologias nos direitos e liberdades das pessoas, e de alcançar o objectivo de garantir a livre circulação de pessoas no mercado interno**.

2.1.2. Aumentar a transparência para as pessoas em causa

A transparência é uma condição fundamental para que as pessoas possam exercer o controlo sobre os seus próprios dados e para garantir a protecção efectiva dos dados pessoais. Deste modo, é essencial que as pessoas **sejam informadas correcta e claramente, de forma transparente**, pelos responsáveis pelo tratamento de dados acerca de quem é que procede à recolha e tratamento dos dados, para que fins, durante quanto tempo e de quais são os direitos que lhes assistem se quiserem ter acesso, rectificar ou apagar esses dados. As disposições aplicáveis em matéria de informações a dar às pessoas em causa[15] não são suficientes.

As condições de base para que exista transparência são o **fácil acesso e compreensão das informações, que devem ser redigidas numa linguagem clara e simples**. Estas condições são particularmente importantes num ambiente em linha, no qual muitas vezes os avisos de privacidade são pouco claros, de difícil acesso, pouco transparentes[16] e nem sempre em conformidade com as normas em vigor. A publicidade comportamental em linha pode ser considerada um desses casos, em que tanto a proliferação de operadores envolvidos no fornecimento deste tipo de publicidade como a complexidade tecnológica desta prática tornam difícil que as pessoas se apercebam da recolha de dados pessoais, por quem e para que fins.

---

13 Ver, por exemplo, o caso dos endereços IP analisado no Parecer 4/2007 do Grupo de Trabalho do Artigo 29.º, no que se refere ao conceito de dados pessoais (WP 136).

14 Cf., por exemplo, o acórdão do Tribunal Constitucional Federal da Alemanha (*Bundesverfassungsgericht*) de 27 de Fevereiro de 2008, 1 BvR 370/07.

15 Cf. artigos 10.º e 11.º da Directiva 95/46/CE.

16 Um inquérito Eurobarómetro efectuado em 2009 revelou que cerca de metade dos inquiridos considerava os avisos de privacidade dos sítios Web «muito» ou «relativamente» pouco claros (cf. Flash Eurobarómetro n.º 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

Neste contexto, os **menores** carecem de protecção especial, visto que podem estar menos cientes dos riscos, consequências, garantias e direitos relacionados com o tratamento de dados pessoais[17].

A Comissão irá ponderar:

- a introdução de um **princípio geral de tratamento transparente** de dados pessoais no quadro normativo;

- a introdução de **obrigações específicas** dos responsáveis pelo tratamento dos dados relativas ao tipo de informações a fornecer e às **modalidades** do seu fornecimento, incluindo no que diz respeito aos **menores**;

- elaboração de um ou mais **formulários-tipo da UE («avisos de privacidade»)** a utilizar pelos responsáveis pelo tratamento dos dados.

É igualmente importante que as pessoas sejam informadas sempre que os respectivos dados forem, por acidente ou de forma ilícita, destruídos, perdidos, alterados, vistos ou divulgados a pessoas não autorizadas. A recente revisão da Directiva da Privacidade Electrónica introduziu uma **notificação obrigatória em caso de violação de dados pessoais** que só cobre, porém, o sector das telecomunicações. Visto que o risco de violação de dados pessoais existe também noutros sectores (nomeadamente no sector financeiro), a Comissão irá analisar as possibilidades de extensão da obrigação de notificar as violações de dados pessoais a outros sectores, em conformidade com a declaração da Comissão a propósito da notificação de violações de dados feita no Parlamento Europeu em 2009, no contexto da reforma do quadro normativo das comunicações electrónicas[18]. Esta análise não prejudica o disposto na Directiva da Privacidade Electrónica, que deve ser transposta para o direito interno até 25 de Maio de 2011[19]. É necessário garantir uma abordagem coerente desta questão.

A Comissão irá:

- analisar as modalidades de introdução no quadro normativo geral de uma **notificação geral das violações de dados pessoais**, incluindo os destinatários dessas notificações e os critérios que determinam a obrigação de notificar.

---

17 Cf. o estudo qualitativo *Safer Internet for Children* relativo a crianças de 9-10 e 12-14 anos, que mostra que as crianças tendem a subestimar os riscos ligados à utilização da Internet e a minimizar as consequências dos seus comportamentos de risco (disponível em: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

18 «A Comissão toma nota da vontade do Parlamento Europeu de não limitar a notificação obrigatória das violações de dados pessoais ao sector das comunicações electrónicas, alargando o seu âmbito a entidades como os fornecedores de serviços da sociedade da informação (...). Consequentemente, a Comissão irá iniciar de imediato os necessários trabalhos preparatórios, nomeadamente a consulta das partes interessadas, com vista à apresentação, se for caso disso, de propostas neste domínio até final de 2011» – este documento pode ser consultado em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//PT. Cf. também o considerando 59 da Directiva 2009/136/CE, que altera a Directiva da Privacidade Electrónica (2002/58/CE): «Este interesse generalizado por parte dos utilizadores em serem notificados não se limita, claramente, ao sector das comunicações electrónicas, pelo que a comunicação obrigatória e explícita das exigências aplicáveis a todos os sectores deverá ser introduzida a nível comunitário com carácter prioritário.»

19 Cf. artigo 4.º da Directiva 2009/136/CE.

2.1.3. Aumentar o controlo sobre os próprios dados

Há duas condições prévias importantes para garantir que as pessoas gozem de um nível elevado de protecção de dados, a saber, **a limitação da actuação do responsável pelo tratamento dos dados às finalidades a atingir (princípio da minimização dos dados)** e a manutenção de um **controlo efectivo das pessoas sobre os dados que lhes dizem respeito**. O artigo 8.º, n.º 2, da Carta dispõe que «todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação». As pessoas devem poder sempre aceder, rectificar, apagar ou bloquear os respectivos dados, a menos que haja motivos legítimos, previstos na lei, para o impedir. Estes direitos já são previstos no quadro normativo em vigor. Contudo, a forma do seu exercício não está harmonizada, pelo que em alguns Estados-Membros o exercício desses direitos é actualmente mais fácil do que noutros. Além disso, esta situação tornou-se especialmente sensível no ambiente em linha, no qual os dados são muitas vezes obtidos sem que a pessoa em causa seja informada e/ou tenha dado consentimento para isso.

O exemplo das redes sociais em linha assume aqui especial relevância, uma vez que representa um desafio considerável ao controlo efectivo das pessoas sobre os dados que lhes dizem respeito. A Comissão recebeu várias perguntas de pessoas que nem sempre conseguiram obter dados pessoais junto de prestadores de serviços em linha, tais como as suas fotografias, e que se viram, assim, impedidas de exercer o direito de acesso, rectificação e supressão.

Por conseguinte, estes direitos devem tornar-se mais explícitos, mais claros e eventualmente ser reforçados.

Assim, a Comissão irá analisar formas de:

- reforçar o **princípio da minimização dos dados**;

- **melhorar as condições** para o **exercício** efectivo **dos direitos de acesso, rectificação, supressão ou bloqueamento de dados** (introduzindo, por exemplo, prazos de resposta aos pedidos das pessoas, autorizando o exercício de direitos através de meios electrónicos ou estabelecendo o princípio de que esse direito de acesso deve ser garantido de forma gratuita);

- clarificar o chamado **«direito a ser esquecido»**, isto é, o direito de as pessoas impedirem a continuação do tratamento dos respectivos dados e de os mesmo serem apagados quando deixarem de ser necessários para fins legítimos. É o caso, por exemplo, do tratamento baseado no consentimento da pessoa, se essa pessoa retirar o consentimento ou quando o período de armazenamento tiver acabado;

- complementar os direitos das pessoas em causa, garantindo a «**portabilidade dos dados**», isto é, prever de forma explícita o direito de retirar os respectivos dados (por exemplo, fotografias ou uma lista de amigos) de uma aplicação ou serviço e transferi-los para outro, na medida das possibilidades técnicas, sem que os responsáveis pelo tratamento o possam impedir.

2.1.4. Aumentar a sensibilização do público

A transparência é realmente essencial, mas é igualmente necessário aumentar a sensibilização do público em geral, especialmente dos mais novos, para os riscos relacionados com o tratamento de dados pessoais e para os direitos que lhes assistem. Um inquérito Eurobarómetro de 2008 mostrou que uma grande maioria de pessoas dos Estados-Membros

da UE considera que a sensibilização para a protecção de dados pessoais é baixa no respectivo país[20]. As actividades de sensibilização devem, assim, ser incentivadas e promovidas por uma vasta gama de agentes, isto é, autoridades dos Estados-Membros, em especial as autoridades responsáveis pela protecção de dados e entidades educativas, bem como os responsáveis pelo tratamento de dados e as associações da sociedade civil. Essas actividades devem incluir medidas não legislativas, como campanhas de sensibilização na imprensa escrita e electrónica e a inclusão de informações claras em sítios Web, explicitando com precisão quais os direitos das pessoas a que os dados se referem e as responsabilidades dos responsáveis pelo tratamento.

A Comissão irá ponderar:

- a possibilidade de **co-financiar actividades de sensibilização para a protecção de dados** com o orçamento da União;

- a necessidade e a oportunidade de incluir no quadro normativo uma **obrigação de organizar actividades de sensibilização** neste domínio.

2.1.5. Garantir o consentimento informado e livre

Sempre que se exige um consentimento informado, as normas em vigor estabelecem que o consentimento das pessoas para o tratamento dos respectivos dados pessoais deve ser uma «manifestação de vontade livre, específica e informada», pela qual a pessoa em causa aceita que alguns dados pessoais que lhe dizem respeito sejam objecto de tratamento[21]. No entanto, estas condições são actualmente interpretadas de formas diferentes nos vários Estados-Membros, que vão desde a exigência de consentimento escrito à aceitação do mero consentimento implícito.

Além disso, no ambiente em linha, dada a opacidade dos regimes de privacidade, é frequentemente mais difícil as pessoas estarem cientes dos respectivos direitos e darem um consentimento informado. A questão complica-se ainda mais pelo facto de, em alguns casos, nem sequer ser claro em que é que consiste o consentimento livre, específico e informado, como acontece na publicidade comportamental, em que a configuração do programa de navegação é considerada por alguns como um consentimento do utilizador para o tratamento de dados, mas por outros não.

Por conseguinte, devem ser esclarecidas as condições em que as pessoas devem dar o consentimento, de forma a garantir sempre um consentimento informado e que as pessoas estejam plenamente cientes do que estão a consentir e em que contexto de tratamento de dados, em conformidade com o artigo 8.º da Carta dos Direitos Fundamentais da UE. A clareza dos conceitos-chave pode igualmente favorecer o desenvolvimento de iniciativas de auto-regulação para conceber soluções práticas conformes com o direito da UE.

A Comissão irá analisar meios de **clarificar e reforçar as normas que regem o consentimento**.

[20] Cf. Flash Eurobarómetro n.º 225 – Protecção de Dados na União Europeia: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[21] Cf. artigo 2.º, alínea h), da Directiva 95/46/CE.

2.1.6. Proteger dados sensíveis

A regra geral actualmente em vigor já proíbe o tratamento de dados sensíveis, isto é, dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual, havendo um número limitado de excepções, com determinadas condições e garantias[22]. No entanto, devido aos desenvolvimentos tecnológicos e sociais, é necessário rever as normas em vigor aplicáveis aos dados sensíveis, ponderar a eventual junção de outras categorias de dados e clarificar ainda mais as condições para o tratamento destes dados. Trata-se, por exemplo, dos dados genéticos, que neste momento não são expressamente integrados na categoria dos dados sensíveis.

A Comissão irá ponderar:

- se outras categorias de dados devem ser considerados «**dados sensíveis**», por exemplo os dados **genéticos**;

- uma maior clarificação e **harmonização das condições** necessárias para o tratamento das diferentes categorias de dados sensíveis.

2.1.7. Tornar as soluções e as sanções mais eficazes

Para assegurar a aplicação das normas de protecção de dados, é essencial ter **disposições eficazes em matéria de recursos e sanções**. Muitos casos em que as pessoas são afectadas por uma violação das normas de protecção de dados afectam também um número considerável de outras pessoas em situações semelhantes.

Por conseguinte, a Comissão irá:

- ponderar a possibilidade de **ampliar os poderes para instaurar acções nos tribunais nacionais** às autoridades nacionais de protecção de dados e às associações da sociedade civil, bem como a **outras associações que representem os interesses das pessoas a que os dados se referem**;

- avaliar a necessidade de **reforçar as disposições sancionatórias em vigor**, nomeadamente através da inclusão explícita de sanções penais aplicáveis aos casos de violações graves das normas de protecção de dados, a fim de as tornar mais eficazes.

2.2. Aprofundar a vertente relativa ao mercado interno

2.2.1. Aumentar a segurança jurídica e assegurar a igualdade de condições para os responsáveis pelo tratamento dos dados

A protecção de dados na UE tem **uma forte vertente relativa ao mercado interno**, que se traduz na necessidade de assegurar o livre fluxo de dados pessoais entre Estados-Membros no mercado interno. Por conseguinte, a harmonização das legislações nacionais de protecção de dados resultante da directiva não se limita a uma harmonização mínima, mas é uma harmonização completa[23].

[22] Cf. artigo 8.º da Directiva 95/46/CE.

[23] Tribunal de Justiça da União Europeia, C-101/01, *Bodil Lindqvist*, Col. [2003], I-1297, 96, 97.

Em simultâneo, a directiva dá aos Estados-Membros margem de manobra em determinados domínios e autoriza-os a manter ou a introduzir regras específicas para situações especiais[24]. Esta margem de manobra, juntamente com o facto de a directiva ter sido por vezes incorrectamente transposta pelos Estados-Membros, deu origem a **divergências entre as legislações nacionais de aplicação da directiva, o que contraria um dos seus objectivos principais, a saber, garantir o livre fluxo de dados pessoais no mercado interno**. Essas divergências verificam-se em numerosos sectores e contextos, por exemplo no tratamento de dados pessoais para efeitos de emprego ou de saúde pública. A falta de harmonização é, na verdade, um dos problemas principais e recorrentes referidos pelas partes interessadas, especialmente os operadores económicos, visto que para eles representam custos adicionais e sobrecarga administrativa. Os responsáveis pelo tratamento de dados estabelecidos em vários Estados-Membros e que devem cumprir as condições e as práticas de cada um desses países são especialmente afectados por esta situação. Além disso, as divergências na transposição da directiva entre os Estados-Membros são fonte de insegurança jurídica não só para os responsáveis pelo tratamento de dados, mas também para as pessoas em causa, podendo assim distorcer o nível de protecção equivalente que a directiva visa alcançar.

A Comissão irá analisar os meios de conseguir **maior harmonização das normas de protecção de dados a nível da UE**.

2.2.2. Reduzir a carga administrativa

A igualdade de condições irá reduzir não só a necessidade de cumprir condições nacionais diferentes, mas também consideravelmente a sobrecarga administrativa dos responsáveis pelo tratamento. Outro elemento concreto para a redução da sobrecarga administrativa e dos custos dos responsáveis pelo tratamento seria a **revisão e simplificação do sistema de notificação actual**[25]. É consensual entre os responsáveis pelo tratamento que a actual obrigação geral de notificar todas as operações de tratamento de dados às autoridades de protecção de dados é uma obrigação bastante pesada que não traz, por si só, qualquer valor acrescentado à protecção dos dados pessoais. Além disso, este é um dos casos em que a directiva deixa uma certa margem de manobra aos Estados-Membros, que podem decidir quais as eventuais isenções e simplificações e quais os procedimentos a seguir.

Um sistema harmonizado e simplificado permitiria reduzir os custos e a sobrecarga administrativa, sobretudo das empresas multinacionais estabelecidas em vários Estados-Membros.

A Comissão irá explorar as diversas possibilidades de **simplificação e harmonização do actual sistema de notificação**, incluindo a eventual criação de um **formulário de registo uniforme para a UE**.

2.2.3. Clarificar as normas sobre a lei aplicável e a responsabilidade dos Estados-Membros

O primeiro relatório da Comissão sobre a implementação da Directiva da Protecção de Dados, apresentado em 2003[26], chamava já a atenção para o facto de as disposições relativas à lei

[24] *Ibidem*, 97. Ver também o considerando 9 da Directiva 95/46/CE.

[25] Cf. artigo 18.º da Directiva 95/46/CE.

[26] Relatório da Comissão – Primeiro relatório sobre a implementação da Directiva relativa à protecção de dados (95/46/CE) – COM(2003) 265.

aplicável[27] serem «deficientes em diversos casos, permitindo a manifestação do tipo de conflitos jurídicos que o artigo mencionado pretende evitar». A situação não melhorou desde então, pelo que nem sempre é claro para os responsáveis pelo tratamento e para as autoridades de supervisão qual é o país responsável e qual a lei aplicável, se estiverem envolvidos vários Estados-Membros. É o que acontece, em especial, quando um responsável pelo tratamento está sujeito a exigências diferentes de diversos Estados-Membros, quando uma empresa multinacional está estabelecida em mais de um Estado-Membro ou quando o responsável pelo tratamento não está estabelecido na UE, mas presta serviços a clientes da UE.

A complexidade também aumenta devido à globalização e aos avanços tecnológicos: são cada vez mais os responsáveis pelo tratamento de dados que operam em vários Estados-Membros e jurisdições, prestando serviços e assistência 24 horas por dia. A Internet torna muito mais fácil a prestação de serviços à distância por responsáveis pelo tratamento estabelecidos fora do Espaço Económico Europeu (EEE)[28], procedendo ao tratamento de dados pessoais em linha; e muitas vezes é difícil determinar a localização dos dados pessoais e do equipamento utilizado num determinado momento (por exemplo, em aplicações e serviços de «computação em nuvem»).

No entanto, a Comissão considera que o facto de o tratamento de dados pessoais ser feito por um responsável estabelecido num país terceiro não deve privar as pessoas da protecção a que têm direito por força da Carta dos Direitos Fundamentais e da legislação de protecção de dados da UE.

A Comissão irá ponderar como **rever e clarificar as disposições em vigor sobre a lei aplicável**, incluindo a actual determinação dos critérios, no intuito de aumentar a segurança jurídica, clarificar a responsabilidade dos Estados-Membros na aplicação das normas de protecção de dados e, por último, proporcionar o mesmo nível de protecção de todas pessoas da UE a que os dados dizem respeito, independentemente da localização geográfica do responsável pelo tratamento.

2.2.4. Aumentar a responsabilidade dos responsáveis pelo tratamento de dados

A simplificação administrativa **não deve conduzir a uma diminuição geral da responsabilidade dos responsáveis pelo tratamento de dados quanto à protecção efectiva dos dados**. Pelo contrário, a Comissão considera que as obrigações desses responsáveis devem ser mais bem definidas no âmbito do quadro normativo, incluindo os mecanismos de controlo interno e a cooperação com as autoridades nacionais de supervisão responsáveis pela protecção de dados. Além disso, deve ser assegurado que essa responsabilidade abrange igualmente os responsáveis pelo tratamento sujeitos ao sigilo profissional (por exemplo, advogados), bem como os casos cada vez mais frequentes de responsáveis pelo tratamento que confiam o tratamento de dados a outras entidades (por exemplo, subcontratantes).

Sendo assim, a Comissão irá ponderar os modos de **garantir que os responsáveis pelo tratamento de dados apliquem medidas e mecanismos adequados para assegurar o cumprimento das normas de protecção de dados**. Ao fazê-lo, terá em conta o debate actualmente em curso sobre a eventual introdução de um princípio de «accountability»[29]. Com isto não se pretende aumentar a sobrecarga administrativa dos responsáveis pelo tratamento dos dados, visto que as referidas medidas centrar-se-ão sobretudo no estabelecimento de

---

27 Cf. artigo 4.º da Directiva 95/46/CE.

28 O Espaço Económico Europeu inclui a Noruega, o Liechtenstein e a Islândia.

29 Cf., em especial, o parecer 3/2010 adoptado pelo Grupo de Trabalho do Artigo 29.º em 13 de Julho.

garantias e mecanismos que tornem mais eficaz o cumprimento das normas de protecção de dados, reduzindo e simplificando em simultâneo determinadas formalidades administrativas como as notificações (*cf. ponto 2.2.2*).

A promoção de tecnologias de protecção da privacidade (PET/*Privacy Enhancing Technologies*), já referida na Comunicação da Comissão de 2007 sobre esta matéria, bem como do princípio da «privacidade desde a concepção», pode ter um papel importante neste domínio, inclusivamente para garantir a segurança dos dados[30].

A Comissão irá analisar os seguintes elementos para aumentar a responsabilidade dos responsáveis pelo tratamento de dados:

– tornar obrigatória a nomeação de um **responsável pela protecção de dados** independente e harmonizar as normas relativas às suas funções e competências[31], tentando avaliar ao mesmo tempo qual será o limiar adequado para evitar uma sobrecarga administrativa desnecessária, especialmente para as pequenas e médias empresas;

– incluir no quadro normativo uma obrigação dos responsáveis pelo tratamento de dados de procederem a **uma avaliação de impacto em termos de protecção de dados** em casos específicos, por exemplo o tratamento de dados sensíveis, ou se o tipo de tratamento implicar riscos de outro tipo, em especial se recorrer a tecnologias, mecanismos ou procedimentos específicos, incluindo a criação de perfis ou a videovigilância;

– continuar a promover a utilização de tecnologias PET e as possibilidades de aplicação concreta do princípio da «**privacidade desde a concepção**».

2.2.5. Incentivar as iniciativas auto-reguladoras e explorar os regimes de certificação da UE

A Comissão continua a considerar que as **iniciativas auto-reguladoras** dos responsáveis pelo tratamento de dados podem **contribuir para uma melhor aplicação das normas de protecção de dados**. As actuais disposições sobre auto-regulação da directiva de protecção de dados, nomeadamente a possibilidade de elaborar códigos de conduta[32], foram raramente utilizadas até agora e as partes interessadas não as consideram satisfatórias.

Por outro lado, a Comissão irá ponderar a possibilidade de criar **regimes de certificação** da UE (**por exemplo, «rótulos de protecção da privacidade»)** para procedimentos, tecnologias, produtos e serviços que respeitem a privacidade[33]. Deste modo, não só as pessoas poderiam obter orientações enquanto utilizadores dessas tecnologias, mas seria também importante para a responsabilização dos responsáveis pelo tratamento de dados: a escolha de tecnologias,

---

30 Acerca das tecnologias PET, cf.: Comunicação da Comissão ao Parlamento Europeu e ao Conselho relativa à promoção da protecção de dados através de tecnologias de protecção da privacidade – COM(2007) 228. O princípio da «protecção desde a concepção» implica que a protecção da privacidade e dos dados esteja incorporada em todo o ciclo de vida das tecnologias, desde a fase inicial de projecto até à sua implantação, utilização e eliminação final. Este princípio é referido, entre outros, na Comunicação da Comissão com o título «Uma Agenda Digital para a Europa» – COM(2010) 245.

31 A actual possibilidade de um responsável pelo tratamento de dados nomear um responsável pela protecção de dados a fim de garantir, de forma independente, a conformidade com as normas de protecção de dados nacionais e da UE e de prestar assistência às pessoas é já uma realidade em vários Estados-Membros (por exemplo, o *Beauftragter für den Datenschutz*, na Alemanha, e o *correspondant informatique et libertés*/CIL, em França).

32 Cf. artigo 27.º da Directiva 95/46/CE.

33 A este respeito, cf. também a comunicação sobre as tecnologias PET (v. nota 30).

produtos ou serviços certificados poderia contribuir para provar que os responsáveis cumpriram as respectivas obrigações (*ver ponto 2.2.4*). É certo que seria essencial **assegurar a fiabilidade dos rótulos de protecção da privacidade** e verificar como se poderiam adequar às obrigações legais e às normas técnicas internacionais.

A Comissão irá:

- analisar formas de **continuar a incentivar as iniciativas de auto-regulação**, incluindo a promoção activa de códigos de conduta;

- ponderar a possibilidade de criação de **regimes de certificação da UE** no domínio da privacidade e protecção de dados.

2.3. Rever as normas de protecção de dados no domínio da cooperação policial e judiciária em matéria penal

A Directiva da Protecção de Dados é aplicável a todas as actividades de tratamento de dados pessoais levadas a cabo nos Estados-Membros, tanto no sector público como no sector privado. Não se aplica, porém, ao tratamento de dados pessoais «no exercício de actividades não sujeitas à aplicação do direito comunitário», como as actividades realizadas nos domínios da cooperação policial e judiciária em matéria penal[34]. O Tratado de Lisboa suprimiu a anterior «estrutura em pilares» da UE e introduziu uma base jurídica abrangente para a protecção de dados pessoais nas políticas da União[35]. Tendo em conta esta evolução, e de acordo com a Carta dos Direitos Fundamentais da UE, as comunicações da Comissão sobre o Programa de Estocolmo e o Plano de Acção de Estocolmo[36] sublinharam a necessidade de um «regime global de protecção de dados» e de «reforço da posição da UE em matéria de protecção dos dados pessoais das pessoas singulares no contexto de todas as políticas da União, incluindo a aplicação da lei e a prevenção da criminalidade».

O instrumento da UE para a protecção de dados pessoais tratados no quadro da cooperação policial e judiciária em matéria penal é a **Decisão-Quadro 2008/977/JAI**[37]**.** Esta Decisão-Quadro constitui um passo em frente importante num domínio em que eram extremamente necessárias normas comuns de protecção de dados. No entanto, é necessário continuar a trabalhar nesse sentido.

A Decisão-Quadro aplica-se apenas ao intercâmbio transfronteiras de dados pessoais na UE e não às operações nacionais de tratamento nos Estados-Membros. Na prática, esta distinção é muito difícil de fazer e pode dificultar a transposição e aplicação efectivas da decisão-quadro[38].

---

34 Cf. artigo 3.º, n.º 2, primeiro travessão, da Directiva 95/46/CE.

35 Cf. artigo 16.º do TFUE.

36 Cf. COM(2009) 262 de 10.6.2009 e COM(2010) 171 de 20.4.2010.

37 Decisão-Quadro 2008/977/JAI do Conselho, de 27.11.2008, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60). A Decisão-Quadro prevê apenas uma harmonização mínima das normas de protecção de dados.

38 Esta distinção não existe nos instrumentos aplicáveis do Conselho da Europa, designadamente: Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, CETS n.º 108, no Protocolo Adicional a esta convenção, no que se refere às autoridades de supervisão e aos fluxos de dados transfronteiriços, ETS n.º 181 e a Recomendação n.º R (87) 15 do Comité de Ministros do Conselho da Europa destinada a regulamentar a utilização de dados de carácter pessoal no sector da polícia, aprovada em 17 de Setembro de 1987.

De igual modo, **a Decisão-Quadro prevê uma excepção demasiado ampla ao princípio da limitação da finalidade**. Outra das lacunas é a ausência de normas que determinem que devem ser distinguidas diferentes categorias de dados, de acordo com o seu grau de precisão e fiabilidade, que os dados baseados em factos devem ser distinguidos dos dados baseados em opiniões ou juízos pessoais[39] e que deve ser feita uma distinção entre diferentes categorias de pessoas a que os dados se referem (criminosos, suspeitos, vítimas, testemunhas, etc.), incluindo garantias específicas aplicáveis aos dados relativos a pessoas que não são suspeitas[40].

Além disso, **a decisão-quadro não substitui os vários diplomas legislativos aplicáveis a sectores específicos da cooperação policial e judiciária em matéria penal adoptados a nível da UE**[41], em especial os que regulam o funcionamento da Europol, da Eurojust, do Sistema de Informação Schengen (SIS) e do Sistema de Informações Aduaneiras (SIA)[42], que prevêem regimes especiais de protecção de dados e/ou que remetem habitualmente para os instrumentos de protecção de dados do Conselho da Europa. Relativamente às actividades realizadas no âmbito da cooperação policial e judiciária, todos os Estados-Membros subscreveram a Recomendação n.º R (87) 15 do Conselho da Europa, que define os princípios da Convenção 108 para o sector da polícia. Porém, não se trata de um instrumento vinculativo.

Esta situação pode afectar directamente as possibilidades de exercício dos direitos de protecção de dados das pessoas neste domínio (por exemplo, ter conhecimento de quais os dados pessoais tratados e objecto de troca, por quem e para que fins, e das formas de exercício dos respectivos direitos, nomeadamente o direito de aceder aos seus dados pessoais).

O objectivo de instituir um sistema global e coerente na UE e relativo a países terceiros implica a **necessidade de ponderar uma revisão das normas de protecção de dados actualmente em vigor aplicáveis à cooperação policial e judiciária em matéria penal**. A Comissão sublinha que o conceito de um sistema global de protecção de dados não exclui a existência de normas específicas de protecção de dados para o sector policial e judicial, incluídas no quadro geral, atendendo à sua natureza específica, tal como indicado na Declaração 21 anexada ao Tratado de Lisboa. Isso implica, por exemplo, a necessidade de ponderar até que ponto o exercício dos direitos de protecção de dados por uma pessoa é susceptível de comprometer a prevenção, investigação, detecção ou repressão de crimes ou a execução de sanções penais numa situação específica.

---

39 Que decorre do princípio 3.2 da Recomendação n.º R (87) 15.

40 Contrário ao princípio 2 da Recomendação n.º R (87) 15 e respectivos relatórios de avaliação.

41 Para uma visão geral destes instrumentos, cf. Comunicação da Comissão com o título «Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça» – COM(2010) 385.

42 Os instrumentos que garantem a supervisão da protecção de dados criaram autoridades de controlo comuns, que se vieram juntar aos poderes de supervisão geral da Autoridade Europeia para a Protecção de Dados (AEPD) sobre as instituições e os organismos da União, nos termos do Regulamento (CE) n.º 45/2001.

A Comissão irá, nomeadamente:

- ponderar a **extensão da aplicação das normas gerais de protecção de dados ao domínio da cooperação policial e judiciária em matéria penal**, incluindo o tratamento de dados a nível nacional, prevendo em simultâneo, se for necessário, **limitações** harmonizadas de certos direitos individuais de protecção de dados, nomeadamente o direito de acesso, e do princípio da transparência;

- analisar a necessidade de introduzir **disposições específicas e harmonizadas** no novo quadro normativo geral da protecção de dados, incluindo designadamente o tratamento de **dados genéticos** para efeitos de direito penal ou a distinção de várias categorias de pessoas a que os dados se referem (testemunhas, suspeitos, etc.) no domínio da cooperação policial e judiciária em matéria penal;

- lançar, em 2011, uma **consulta** de todos os interessados acerca da melhor forma de **rever os actuais sistemas de supervisão no domínio da cooperação policial e judiciária**, a fim de garantir uma supervisão eficaz e coerente da protecção de dados em todas as instituições, órgãos e serviços da União;

- avaliar a necessidade de **harmonizar**, a longo prazo, as **normas específicas adoptadas a nível da UE para a cooperação policial e judiciária em matéria penal em determinados diplomas** com o novo quadro normativo geral da protecção de dados.

2.4. A dimensão mundial da protecção de dados

2.4.1. Clarificar e simplificar as normas aplicáveis às transferências internacionais de dados

Um dos meios para permitir a transferência de dados pessoais para fora da UE e do EEE é a designada **«avaliação da adequação»**. Neste momento, a adequação de um país terceiro – a saber, se esse país garante um nível de protecção que a UE considera adequado – pode ser determinada pela Comissão e pelos Estados-Membros.

Se a Comissão considerar que o nível é adequado, é possível transferir livremente dados pessoais dos 27 Estados-Membros e dos três países do EEE para esse país terceiro sem ser necessário prever garantias adicionais. No entanto, os requisitos a seguir para a Comissão proceder ao reconhecimento dessa adequação não são actualmente previstos de forma suficientemente detalhada na Directiva da Protecção de Dados. Além disso, a decisão-quadro não prevê a possibilidade de a Comissão tomar decisões neste sentido.

Em alguns Estados-Membros a adequação é avaliada, em primeiro lugar, pelo próprio responsável pelo tratamento que transfere os dados pessoais para um país terceiro, algumas vezes sob a supervisão subsequente da autoridade de protecção de dados. Esta situação pode dar origem a diferentes práticas de avaliação do nível de adequação dos países terceiros ou organizações internacionais e **é possível que o nível de protecção das pessoas a que os dados dizem respeito num determinado país terceiro seja apreciado de forma diferente consoante os Estados-Membros**. De igual modo, os diplomas actualmente em vigor não prevêem requisitos pormenorizados nem harmonizados para as transferências poderem ser consideradas lícitas, o que leva à existência de práticas diferentes nos Estados-Membros.

Além disso, no que se refere a transferências de dados para países terceiros que não asseguram um nível adequado de protecção, as actuais cláusulas-tipo da Comissão aplicáveis à transferência de dados pessoais por responsáveis pelo tratamento[43] e por subcontratantes[44] não foram redigidas para abranger também as situações não contratuais e não podem, por exemplo, ser utilizadas para as transferências entre administrações públicas.

Por outro lado, os acordos internacionais celebrados pela UE ou pelos seus Estados-Membros exigem com frequência a inclusão de princípios de protecção de dados e disposições específicas. Essa exigência pode dar origem a textos diversos, com normas e direitos incompatíveis, dando assim azo a interpretações divergentes, em detrimento das pessoas a que os dados dizem respeito. Por conseguinte, a Comissão anunciou que irá trabalhar nos elementos essenciais da protecção de dados pessoais dos acordos entre a União e países terceiros para efeitos de aplicação da lei[45].

Foram desenvolvidos outros modos como forma de auto-regulação, nomeadamente códigos internos das empresas, conhecidos como «normas vinculativas para as empresas» (*Binding Corporate Rules*)[46], que podem também ser um instrumento útil para a transferência lícita de dados pessoais entre empresas do mesmo grupo. No entanto, os interessados sugeriram que este mecanismo fosse aperfeiçoado e a sua aplicação facilitada.

Para regular as questões aqui identificadas é **necessário aperfeiçoar os actuais mecanismos que permitem as transferências internacionais de dados pessoais**, garantindo em simultâneo a protecção adequada dos dados pessoais durante a transferência e o tratamento fora da UE e do EEE.

---

43 Decisão 2001/497/CE da Comissão, de 15 de Junho de 2001, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Directiva 95/46/CE (JO L 181 de 4.7.2001, p. 19); Decisão 2002/16/CE da Comissão, de 27 Dezembro 2001, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Directiva 95/46/CE (JO L 6 de 10.1.2002, p. 52); Decisão 2004/915/CE da Comissão, de 27 de Dezembro de 2004, que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros (JO L 385 de 29.12.2004, p. 74).

44 Decisão da Comissão de 5 de Fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho (JO L 39 de 12.2.2010, p. 5).

45 Plano de Acção de Estocolmo, já referido (ver nota 36).

46 As «normas vinculativas para as empresas» são códigos internos de conduta baseados em normas europeias de protecção de dados, que as empresas multinacionais elaboram e cumprem de forma voluntária para garantir protecção adequada nas transferências ou categorias de transferências de dados pessoais entre empresas que fazem parte do mesmo grupo e que estão sujeitas a estes códigos. Ver:

http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

A Comissão tenciona analisar as formas de:

- **melhorar e racionalizar os procedimentos em vigor** para as transferências internacionais de dados, incluindo os instrumentos e as «normas para as empresas» de carácter vinculativo, a fim de garantir uma **abordagem mais uniforme e coerente da UE** face a países terceiros e a organizações internacionais;

- **clarificar o procedimento de adequação da Comissão** e definir melhor os **critérios e requisitos** para proceder à avaliação do nível de protecção de dados em países terceiros ou organizações internacionais;

- definir **os elementos fundamentais da protecção de dados na UE**, que poderiam ser utilizados em todos os tipos de acordos internacionais.

2.4.2. Promover princípios universais

O tratamento de dados é um fenómeno mundial e carece do desenvolvimento de princípios universais destinados a proteger as pessoas no que se refere ao tratamento de dados pessoais.

O quadro normativo da UE em matéria de protecção de dados serviu muitas vezes de **referência a países terceiros para regular a questão da protecção de dados**. Os seus efeitos, dentro e fora da União, foram extremamente importantes. Assim, a **União Europeia deverá continuar a ser a força motriz do desenvolvimento e da promoção de normas jurídicas e técnicas internacionais em matéria de protecção de dados**, com base noutros instrumentos da UE já existentes neste domínio. Este aspecto é especialmente importante no contexto da política de alargamento da UE.

No que se refere às normas técnicas internacionais elaboradas por organismos de normalização, a Comissão considera que a coerência entre o futuro quadro normativo e as referidas normas é muito importante, de forma que os responsáveis pelo tratamento possam aplicá-las de forma uniforme e fácil.

A Comissão irá:

- continuar a **promover a elaboração de normas jurídicas e técnicas para uma protecção de dados de elevado nível** em países terceiros e a nível internacional;

- defender o **princípio da reciprocidade da protecção nas actividades internacionais da União**, acima de tudo relativamente às pessoas cujos dados pessoais sejam exportados da UE para países terceiros;

- **reforçar, para este efeito, a cooperação com países terceiros e organizações internacionais**, como a OCDE, o Conselho da Europa, as Nações Unidas e outras organizações regionais;

- **seguir de perto a elaboração de normas técnicas internacionais pelos organismos de normalização** como o CEN e a ISO, para que estas sejam um complemento útil das normas jurídicas e para garantir a aplicação funcional e eficaz dos requisitos essenciais da protecção de dados.

2.5. Um quadro institucional mais forte para uma melhor aplicação das normas de protecção de dados

A transposição e aplicação dos princípios e regras de protecção de dados é um elemento fundamental para garantir o respeito pelos direitos das pessoas.

Neste contexto, **o papel das autoridades de protecção de dados é essencial** para a aplicação das normas nesta matéria. São guardiãs independentes dos direitos e liberdades fundamentais no tocante à protecção de dados pessoais, com os quais as pessoas contam para a protecção dos respectivos dados e a licitude das operações de tratamento. Por esta razão, a Comissão considera que o papel destas autoridades deve ser reforçado, sobretudo à luz da jurisprudência mais recente do Tribunal de Justiça da União Europeia acerca da independência das mesmas[47], recebendo os poderes e recursos necessários para exercer correctamente as suas funções, tanto a nível nacional como na cooperação entre si.

Por outro lado, a Comissão considera também que as **autoridades de protecção de dados devem reforçar a cooperação entre si e coordenar melhor as actividades que desenvolvem**, sobretudo quando confrontadas com questões que, pela sua natureza, tenham uma dimensão transfronteiriça. Estão especialmente nesta situação as empresas multinacionais que se encontram estabelecidas em vários Estados-Membros e desenvolvem actividades em todos eles, ou os casos em que se exija a supervisão coordenada com a Autoridade Europeia para a Protecção de Dados (AEPD)[48].

A este respeito, **o Grupo de Trabalho do Artigo 29.º pode ter um papel importante**[49], uma vez que já tem, além da sua função consultiva[50], a missão de contribuir para a aplicação uniforme das normas de protecção de dados da UE a nível nacional. No entanto, as autoridades de protecção de dados continuam a aplicar e interpretar de forma divergente as normas da UE, ainda que as ameaças à protecção de dados sejam comuns em toda a União, pelo que é necessário reforçar o papel deste grupo de trabalho para a coordenação das posições das autoridades de protecção, no intuito de garantir uma aplicação mais uniforme a nível nacional e, logo, um nível equivalente de protecção de dados.

---

47 Acórdão do TJ de 9.3.2010, *Comissão/Alemanha*, processo C-518/07.

48 É o caso dos sistemas de TI de grande escala, como o SIS [cf. artigo 46.º do Regulamento (CE) n.º 1987/2006, JO L 318 de 28.12.2006, p. 4] e o VIS [cf. artigo 43.º do Regulamento (CE) n.º 767/2008, JO L 218 de 13.8.2008, p. 60].

49 O Grupo de Trabalho do Artigo 29.º é um órgão consultivo composto por um representante dos Estados-Membros, das autoridades de protecção de dados, da Autoridade Europeia para a Protecção de Dados (AEPD) e da Comissão (sem direito de voto), assegurando esta última também o secretariado do grupo. Ver: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 O Grupo de Trabalho do Artigo 29.º tem o papel de aconselhar a Comissão acerca do nível de protecção na UE e em países terceiros e de quaisquer outras medidas relacionadas com o tratamento de dados pessoais.

A Comissão irá analisar:

- as formas de **reforçar, clarificar e harmonizar o estatuto e os poderes das autoridades de protecção de dados** no novo quadro normativo, incluindo a aplicação integral do conceito de «plena independência»[51];

- as formas de **melhorar a cooperação e a coordenação entre autoridades de protecção de dados;**

- a forma de garantir uma aplicação coerente das normas de protecção de dados da UE no mercado interno. Para este efeito, pode ser necessário **reforçar o papel das autoridades nacionais de protecção de dados, coordenar melhor o seu trabalho através do Grupo de Trabalho do Artigo 29.º (que deve tornar-se um órgão mais transparente) e/ou criar um mecanismo que garanta a coerência no mercado interno sob a autoridade da Comissão Europeia**.

3. CONCLUSÃO: CAMINHO A SEGUIR

Tal como a tecnologia, a forma como os nossos dados pessoais são utilizados e partilhados na nossa sociedade está constantemente a mudar. Para o legislador, o desafio consiste em estabelecer um quadro normativo que resista à passagem do tempo. No final do processo de reforma, as normas de protecção de dados devem continuar a garantir, durante várias gerações, um elevado nível de protecção e segurança jurídica aos particulares, às administrações públicas e às empresas. Independentemente da complexidade da situação ou do grau de sofisticação da tecnologia, as normas que as autoridades nacionais devem aplicar e que as empresas e os criadores de tecnologia devem cumprir têm de ser claras. Para as pessoas singulares é também importante que sejam claros os direitos que lhes assistem.

A **abordagem global da Comissão** para tratar esta questão e atingir os objectivos essenciais referidos na presente comunicação constituirá a base dos futuros debates com as restantes instituições europeias e outras partes interessadas, que se traduzirão em propostas e medidas concretas, de natureza legislativa e não legislativa. Para este efeito, a Comissão agradece o envio de observações acerca das questões suscitadas na presente comunicação

Com base nos contributos recebidos, e após uma avaliação de impacto, a Comissão irá apresentar **em 2011**, tendo em conta a Carta dos Direitos Fundamentais da UE, **propostas legislativas** de revisão do quadro normativo da protecção de dados, no intuito de reforçar a posição da UE em matéria de protecção dos dados pessoais das pessoas singulares no contexto de todas as políticas da União, incluindo a aplicação da lei e a prevenção da criminalidade, atendendo às especificidades destes últimos domínios. As medidas não legislativas, como as que promovem a auto-regulação e as que exploram a possibilidade de criar rótulos de protecção da privacidade da UE, serão propostas em paralelo.

Numa segunda fase, a Comissão irá **avaliar a necessidade de adaptar outros diplomas legais** ao novo quadro normativo geral de protecção de dados. Trata-se, em primeiro lugar, do Regulamento (CE) n.º 45/2001, cujas disposições terão de ser adaptadas a este novo quadro geral. O impacto noutros diplomas sectoriais deverá igualmente ser objecto de análise cuidada numa fase subsequente.

---

[51] Cf. acórdão do TJ de 9.3.2010, *Comissão/Alemanha*, processo C-518/07.

A Comissão continuará também a garantir o acompanhamento adequado da correcta aplicação do direito da UE neste domínio, **prosseguindo uma política de repressão das infracções** sempre que as normas de protecção de dados da UE não forem correctamente transpostas ou aplicadas. Na verdade, a actual revisão dos diplomas de protecção de dados não afasta a obrigação dos Estados-Membros de transpor e garantir a aplicação correcta da legislação em vigor em matéria de protecção de dados pessoais[52].

Um nível elevado e uniforme de protecção de dados na UE será a melhor forma de apoiar e promover em todo o mundo as normas de protecção de dados da UE.

[52] Incluindo também a Decisão-Quadro 2008/977/JAI do Conselho: os Estados-Membros devem tomar as medidas necessárias para cumprir o disposto nesta decisão-quadro antes de 27 de Novembro de 2010.