COMISSÃO EUROPEIA

Bruxelas, 25.1.2012
COM(2012) 9 final

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

Proteção da privacidade num mundo interligado
Um quadro europeu de proteção de dados para o século XXI

(Texto relevante para efeitos do EEE)

[…]

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

Proteção da privacidade num mundo interligado
Um quadro europeu de proteção de dados para o século XXI

(Texto relevante para efeitos do EEE)

1. DESAFIOS ATUAIS EM MATÉRIA DE PROTEÇÃO DE DADOS

A rapidez da evolução tecnológica e da globalização transformou profundamente a forma como o volume crescente de dados pessoais são recolhidos, acedidos, utilizados e transferidos. Novas formas de partilha de informações através das redes sociais e da conservação distante de grandes quantidades de dados fazem agora parte da vida de muitos dos 250 milhões de internautas na Europa. Paralelamente, os dados pessoais tornaram-se um bem valioso para muitas empresas. A recolha, a compilação e a análise dos dados de potenciais clientes representam frequentemente um aspeto importante das suas atividades económicas[1].

Neste novo contexto digital, **as pessoas singulares têm o direito de exercer um controlo efetivo sobre os seus dados pessoais**. Na Europa, a proteção de dados é um direito fundamental consagrado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, bem como no artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE), e que deve ser protegido em conformidade.

A falta de confiança faz com que os consumidores hesitem em fazer compras em linha ou aceitem novos serviços. Por conseguinte, é essencial assegurar igualmente um elevado nível de proteção dos dados para reforçar a confiança nos serviços em linha e concretizar todo o potencial da economia digital, incentivando desta forma o **crescimento económico** e a **competitividade das empresas da UE**.

São necessárias regras modernas e coerentes, aplicáveis em toda a União, para permitir que os dados circulem livremente entre os Estados-Membros. As empresas necessitam de regras claras e uniformes que garantam segurança jurídica e minimizem os encargos administrativos. Isto é essencial para que o mercado único funcione eficazmente e para **fomentar o crescimento económico, criar novos empregos e estimular a inovação**[2]. A modernização das regras da UE em matéria de proteção de dados, que reforce a dimensão do seu mercado interno, permitirá

---

[1] O mercado da análise de grandes conjuntos de dados está a ter um crescimento mundial anual de 40%: http://www.mckinsey.com/mgi/publications/big_data/.

[2] Ver também as conclusões do Conselho Europeu, de 23 de outubro de 2011, que salientaram o «papel fundamental» do mercado único «no crescimento e no emprego», bem como a necessidade de concretizar o Mercado Único Digital até 2015.

assegurar um elevado nível de proteção de dados às pessoas singulares e promover a segurança jurídica, a clareza e a coerência, tendo, por conseguinte, um papel central no Plano de Ação da Comissão Europeia de aplicação do Programa de Estocolmo[3], na Agenda Digital para a Europa[4] e, em termos mais globais, contribuir para a estratégia de crescimento da União intitulada Europa 2020[5].

A Diretiva da UE de 1995[6], o principal instrumento legislativo em matéria de proteção de dados pessoais na Europa, constituiu um marco na história da proteção de dados. Os seus objetivos, que consistem em assegurar o funcionamento do mercado único e a proteção efetiva dos direitos e das liberdades fundamentais das pessoas singulares, mantêm-se válidos. Todavia, essa diretiva foi adotada há 17 anos, quando a Internet estava apenas no seu início. Atualmente, neste novo contexto digital estimulante, as regras em vigor não asseguram o grau de harmonização que se exige nem a eficácia necessária para garantir o direito à proteção dos dados pessoais. Por esta razão, a Comissão Europeia propõe agora uma reforma de fundo do quadro legislativo da UE em matéria de proteção de dados.

Além disso, o Tratado de Lisboa introduziu, no artigo 16.º do TFUE, uma nova base jurídica tendo em vista uma abordagem moderna e global sobre a proteção de dados e a livre circulação de dados pessoais, que cobre igualmente o domínio da cooperação policial e judiciária em matéria penal[7]. Esta abordagem encontra-se refletida nas Comunicações da Comissão Europeia relativas ao Programa de Estocolmo e ao Plano de Ação de aplicação do Programa de Estocolmo[8], que insistem na necessidade de a União «dotar-se de um regime completo de proteção dos dados pessoais que abranja o conjunto das competências da União» e «assegurar que o direito fundamental à proteção de dados é aplicado de forma sistemática».

Com vista à preparação da reforma do quadro legislativo de proteção de dados da UE de forma transparente, a Comissão organizou, desde 2009, consultas públicas sobre esta questão[9] e encetou diálogos intensivos com as partes interessadas[10]. Em 4 de novembro de 2010, a Comissão publicou uma Comunicação relativa a uma abordagem global da proteção de dados pessoais na União Europeia[11], que apresentava os principais temas da reforma. Entre setembro e dezembro de 2011, a

---

3 COM (2010) 171 final.

4 COM (2010) 245 final.

5 COM (2010) 2020 final.

6 Diretiva 95/46/CE relativa à proteção 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

7 As regras específicas relativas ao tratamento de dados pelos Estados-Membros no domínio da Política Externa e de Segurança Comum são estabelecidas por uma decisão do Conselho com base no artigo 39.º do TUE.

8 Ver, respetivamente, COM (2009) 262 e COM (2010) 171.

9 Foram lançadas duas consultas públicas sobre a reforma da proteção de dados: a primeira, de julho a dezembro de 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) e, a segunda, de novembro de 2010 a janeiro de 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

10 Foram organizadas consultas específicas em 2010 com autoridades dos Estados-Membros e partes interessadas do setor privado. Em novembro de 2010, a Comissária da UE responsável pela Justiça, Viviane Reding, organizou uma mesa redonda subordinada à reforma da proteção de dados. Realizaram-se também sessões de trabalho e seminários adicionais sobre temas específicos (nomeadamente, notificações das violações de dados) no decurso de 2011.

11 COM (2010) 609.

Comissão participou num diálogo reforçado com as autoridades nacionais de proteção de dados da Europa, por um lado, e com a Autoridade Europeia para a Proteção de Dados, por outro, a fim de explorar as possibilidades de uma aplicação mais coerente das regras da UE relativas à proteção de dados no conjunto dos Estados-Membros[12].

Estes debates deixaram claro ser do interesse tanto dos cidadãos como das empresas que a Comissão Europeia procedesse a uma reforma substancial das regras da UE em matéria de proteção de dados. Depois de avaliar os impactos de diferentes opções estratégicas[13], a Comissão Europeia propõe presentemente **um quadro legislativo sólido e coerente, transversal a todas as políticas da União, que reforça os direitos das pessoas singulares, consolida a dimensão «mercado único» da proteção de dados e reduz a burocracia para as empresas**[14]. Na proposta da Comissão, o novo quadro legislativo é constituído por:

– um **regulamento** (que substitui a Diretiva 95/46/CE) que estabelece um quadro geral da UE em matéria de proteção de dados[15];

– e uma **diretiva** (que substitui a Decisão-Quadro 2008/977/JAI[16]) que enuncia as regras relativas à proteção de dados pessoais tratados para efeitos de **prevenção, investigação, deteção ou repressão de infrações penais e atividades judiciárias conexas.**

A presente comunicação apresenta os elementos principais da reforma do quadro legislativo da UE relativo à proteção de dados.

2. PERMITIR ÀS PESSOAS SINGULARES O CONTROLO DOS SEUS DADOS PESSOAIS

Ao abrigo da Diretiva 95/46/CE - atualmente o principal instrumento legislativo da União em matéria de proteção de dados - as modalidades segundo as quais as pessoas singulares podem exercer o seu direito à proteção dos dados não se encontram suficientemente harmonizadas entre os Estados-Membros. Do mesmo modo, as competências conferidas às autoridades nacionais responsáveis pela proteção de

---

12 Ver a carta da Comissária da UE responsável pela Justiça, Viviane Reding, de 19 de setembro de 2011, aos membros do Grupo de Trabalho do artigo 29.º, publicada em http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

13 Ver a avaliação de impacto SEC (2012) 72.

14 A reforma incluirá, numa fase posterior, alterações tendo em vista a harmonização dos instrumentos específicos e setoriais, por exemplo o Regulamento (CE) n.° 45/2011, JO L 8 de 12.1.2001, p. 1.

15 O regulamento citado prevê também um número limitado de adaptações técnicas à diretiva relativa à privacidade e às comunicações eletrónicas (Diretiva 2002/58/CE, com a última redação que lhe foi dada pela Diretiva 2009/136/CE, JO L 337 de 18.12.2009, p. 11), de modo a ter em conta a transformação da Diretiva 95/46/CE num regulamento. As consequências jurídicas substantivas que o novo regulamento e a nova diretiva implicarão para a diretiva relativa à privacidade serão revistas pela Comissão em data oportuna, tendo em conta o resultado das negociações sobre as atuais propostas com o Parlamento Europeu e o Conselho.

16 Decisão-Quadro 2008/977/JAI, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, JO L 350 de 30.12.2008, p. 60. Este pacote de reforma legislativa sobre a proteção de dados inclui um relatório sobre a execução da decisão-quadro pelos Estados-Membros.

dados também não estão suficientemente harmonizadas para garantir a aplicação coerente e efetiva das regras na matéria. Isto significa que o exercício desses direitos é mais difícil em determinados Estados-Membros do que noutros, especialmente num ambiente em linha.

As referidas dificuldades prendem-se também com o elevado volume de dados recolhido diariamente e o facto de os utilizadores não estarem plenamente cientes de que os seus dados são recolhidos. Embora muitos europeus considerem que a divulgação de dados pessoais faz cada vez mais parte da vida moderna[17], 72% dos internautas na Europa ainda ficam apreensivos quando lhes são solicitados demasiados dados pessoais em linha[18]. Sentem que deixam de controlar os seus próprios dados. Não são devidamente informados quanto ao tratamento que é feito das suas informações pessoais, bem como sobre a identidade do destinatário e a finalidade da transmissão. Frequentemente ignoram as modalidades de exercício dos seus direitos num ambiente em linha.

«Direito a ser esquecido»

Um estudante europeu, membro de uma rede social em linha, decide solicitar o acesso a todos os dados pessoais que o referido serviço detém sobre si. Ao fazê-lo, apercebe-se que a rede social recolhe muitos mais dados do que pensava e que alguns dados pessoais que julgou terem sido apagados ainda estavam conservados.

A reforma das regras da UE em matéria de proteção de dados garantirá que esta situação não se volte a reproduzir no futuro, ao introduzir:

- uma condição explícita que obriga as redes sociais em linha (e todos os outros responsáveis pelo tratamento de dados) a limitarem ao mínimo o volume de dados pessoais dos utilizadores que recolhem e tratam;

- uma condição de configuração por defeito dos sistemas para assegurar que os dados não serão tornados públicos;

- uma obrigação explícita de que os responsáveis pelo tratamento de dados apaguem os dados pessoais de uma pessoa quando esta o solicitar expressamente e se não existir qualquer outra razão legítima para os conservar.

Neste caso específico, o fornecedor da rede social seria obrigado a apagar imediata e totalmente os dados do estudante.

Tal como destacado na Agenda Digital para a Europa, as preocupações com a privacidade são uma das razões mais frequentes para as pessoas não comprarem bens e serviços em linha. Dada a contribuição do setor das tecnologias da informação e comunicações (TIC) para o aumento global da produtividade na Europa, 20% devido diretamente ao setor TIC e 30% aos investimentos realizados nas TIC[19], a confiança nestes serviços é fulcral para estimular o crescimento da economia da UE e a competitividade da sua indústria.

---

17 Ver Eurobarómetro Especial 359 – *Attitudes on Data Protection and Electronic Identity in the European Union*, junho de 2011, p. 23.

18 Ibidem , p. 54.

19 Ver a Agenda Digital para a Europa citada, p. 4.

Notificação das violações de dados

Piratas informáticos atacaram um serviço de jogos em linha direcionado para utilizadores da UE. Essa violação afetou as bases de dados que continham dados pessoais (incluindo nomes, moradas e, provavelmente, dados de cartões de crédito) de dezenas de milhões de utilizadores de todo o mundo. A empresa em causa esperou uma semana antes de notificar os utilizadores afetados.

A reforma das regras da UE em matéria de proteção de dados garantirá que esta situação não se volte a reproduzir no futuro. As novas regras irão obrigar as empresas:

- a reforçar as suas medidas de segurança para prevenir e evitar as violações de dados;

- a notificar rapidamente eventuais violações de dados tanto à autoridade nacional de proteção de dados - se possível, no prazo de 24 horas a contar da deteção da violação - como às pessoas afetadas.

O objetivo dos novos instrumentos legislativos propostos pela Comissão consiste em reforçar os direitos, proporcionar às pessoas singulares meios eficazes e práticos para assegurar que estão plenamente informadas quanto ao que sucede aos seus dados pessoais e permitir-lhes o exercício dos seus direitos de forma mais efetiva.

De modo a reforçar o direito das pessoas singulares à proteção de dados, a Comissão propõe novas regras para:

Melhorar a capacidade de controlo das pessoas singulares sobre os seus dados, designadamente:

- assegurando que, quando o seu **consentimento** é exigido, este deve ser **dado de forma expressa**, **ou seja, deve ter por base uma declaração ou um ato inequívoco da pessoa em causa,** e que deve ser dado de forma livre;

- dotando os internautas de um **direito** efetivo **a serem esquecidos** no ambiente em linha: o direito de os seus dados serem apagados caso retirem o seu consentimento, se não existirem outros motivos legítimos de conservação dos dados;

- garantindo-lhes um **acesso fácil aos seus próprios dados** e o **direito de portabilidade dos dados**: o direito de obter do responsável pelo tratamento uma cópia dos dados conservados e a liberdade de os transferir de um prestador de serviços para outro sem entraves;

- reforçando o **direito à informação** para que as pessoas entendam perfeitamente como são tratados os seus dados, em especial quando as atividades de tratamento digam respeito a **crianças**.

Melhorar os meios ao dispor das pessoas para exercerem os seus direitos, designadamente:

- reforçando a **independência e as competências das autoridades nacionais de proteção de dados** a fim de que estejam suficientemente equipadas para tratar de queixas de forma eficaz, em especial o poder de realizar investigações efetivas, de adotar decisões vinculativas e de impor sanções eficazes e dissuasivas;

- melhorando as **vias de recurso administrativo e judicial** em caso de **violação** dos direitos relativos à proteção de dados. Em particular, as associações habilitadas terão capacidade para intentar ações em tribunal em nome do interessado.

Reforçar a segurança dos dados, designadamente:

- incentivando a utilização de **tecnologias de reforço da proteção da privacidade** (ou seja, tecnologias que protegem a confidencialidade das informações minimizando a conservação de dados pessoais), de **configurações por defeito que respeitem a privacidade** e **regimes de certificação do respeito da privacidade;**

- introduzindo uma **obrigação geral**[20] que impõe aos responsáveis pelo tratamento de dados **notificarem sem atraso injustificado eventuais violações de dados** tanto as autoridades de proteção de dados (se possível, no prazo de 24 horas) como os interessados.

Melhorar a responsabilização das pessoas que efetuam o tratamento de dados, designadamente:

- exigindo aos responsáveis pelo tratamento de dados que designem um **delegado para a proteção de dados** nas empresas com mais de 250 assalariados e nas empresas que participam em operações de tratamento de dados que, pela sua natureza, âmbito de aplicação e finalidades, apresentam um risco específico para os direitos e as liberdades das pessoas singulares (*risky processing*);

- introduzindo o princípio da **proteção da privacidade desde a conceção** (*privacy by design*), de modo a assegurar que as garantias em matéria de proteção de dados são tomadas em consideração desde a fase de planeamento dos procedimentos e dos sistemas de tratamento;

- introduzindo a obrigação para as organizações envolvidas em tratamentos de risco de realizarem **avaliações de impacto sobre a proteção de dados**.

3. REGRAS DE PROTEÇÃO DE DADOS ADAPTADAS AO MERCADO ÚNICO DIGITAL

Não obstante o objetivo prosseguido pela diretiva em vigor de garantir um nível equivalente de proteção de dados no conjunto da UE, subsistem ainda divergências consideráveis entre as regras dos Estados-Membros. Consequentemente, os responsáveis pelo tratamento de dados podem ser obrigados a ter em conta 27 legislações e obrigações nacionais diferentes. Daqui resulta um **quadro jurídico fragmentado** que cria **insegurança jurídica** e uma proteção desigual das pessoas singulares. Este fator gera **custos e encargos administrativos desnecessários** para as empresas e constitui um desincentivo para as que operam no mercado único e pretendem expandir as suas atividades além-fronteiras.

[20] Atualmente tal obrigação só existe no setor das telecomunicações por força da diretiva relativa à privacidade e às comunicações eletrónicas.

Os recursos e as competências das autoridades nacionais de proteção de dados variam consideravelmente entre os Estados-Membros[21]. Em alguns casos, significa que são incapazes de desempenhar satisfatoriamente as suas funções de controlo da aplicação. A cooperação entre estas autoridades a nível europeu, através do grupo consultivo existente (conhecido por Grupo de Trabalho do artigo 29.º)[22], nem sempre conduz a uma aplicação coerente e, portanto, deve ser melhorada.

Aplicação coerente das regras em matéria de proteção de dados no conjunto da Europa

Uma empresa multinacional com vários estabelecimentos no território da UE desenvolveu um sistema de cartografia em linha na Europa que recolhe imagens de todos os edifícios, públicos e privados, e que também pode fotografar pessoas na via pública. Num Estado-Membro, a inclusão de fotografias não desfocadas de pessoas que ignoravam estar a ser fotografadas foi considerada ilícita, enquanto noutro, esta prática não representou qualquer infração à regulamentação em matéria de proteção de dados. Consequentemente, as autoridades nacionais de proteção de dados não tomaram medidas coerentes para remediar tal situação.

A reforma das regras da UE em matéria de proteção de dados irá assegurar que esta situação não se volte a reproduzir no futuro, uma vez que:

- os requisitos e as garantias em matéria de proteção de dados serão harmonizados entre os Estados-Membros através de um regulamento da UE diretamente aplicável no conjunto da União;

- apenas a autoridade de proteção de dados do Estado-Membro onde a empresa tem o seu estabelecimento principal será competente para decidir se a empresa está a agir no respeito da legislação;

- uma coordenação rápida e eficaz entre as autoridades nacionais de proteção de dados, dado que o serviço está direcionado para as pessoas em vários Estados-Membros, ajudará a garantir que as novas regras de proteção de dados da UE serão aplicadas e executadas de forma coerente no conjunto dos Estados-Membros.

As autoridades nacionais devem ser reforçadas e é necessário fortalecer a cooperação para assegurar uma execução coerente e, portanto, uma aplicação uniforme das regras no conjunto da UE.

Um quadro legislativo sólido, claro e uniforme a nível da UE contribuirá para desenvolver o potencial do mercado único digital e estimular o crescimento económico, a inovação e a criação de empregos. A adoção de um regulamento eliminará a fragmentação dos regimes jurídicos entre os 27 Estados-Membros, bem como os entraves à entrada no mercado, um fator especialmente importante para as micro, pequenas e médias empresas.

Graças às novas regras, as empresas da UE estarão igualmente em vantagem num contexto de concorrência global. Por força do quadro regulamentar reformado, as empresas poderão oferecer aos seus clientes garantias de que informações pessoais

---

21 Para mais detalhes sobre este assunto, consultar a avaliação de impacto que acompanha as propostas legislativas, SEC (2012) 72.

22 O Grupo de Trabalho do artigo 29.º foi criado em 1996 (por força do artigo 29.º da Diretiva 95/46/CE), tem natureza consultiva e é composto por representantes das autoridades nacionais de controlo em matéria de proteção de dados, da Autoridade Europeia para a Proteção de Dados (AEPD) e da Comissão. Para mais informações sobre as suas atividades, consultar http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

valiosas serão tratadas com o necessário cuidado e zelo. A confiança num regime regulamentar coerente da UE constituirá um elemento essencial para os prestadores de serviços e um incentivo para os investidores que procurem as melhores condições para a colocação dos seus serviços.

A fim de reforçar a **dimensão «mercado único» da proteção de dados**, a Comissão propõe:

- estabelecer, a nível da UE, regras em matéria de proteção de dados através de um **regulamento diretamente aplicável em todos os Estados-Membros**[23] que irá acabar com a aplicação cumulativa e simultânea de diferentes legislações nacionais de proteção de dados. Tal representará uma **poupança** líquida **para as empresas de cerca de 2,3 mil milhões de EUR por ano só em termos de encargos administrativos**;

- **simplificar o quadro regulamentar, reduzindo consideravelmente a burocracia** e eliminando as **formalidades**, designadamente as obrigações gerais de notificação (dando origem a uma poupança líquida de 130 milhões de EUR por ano só em termos de encargos administrativos). Dada a sua importância para a competitividade da economia europeia, é dada especial atenção às necessidades das micro, pequenas e médias empresas;

- **continuar a reforçar a independência e as competências das autoridades nacionais de proteção de dados,** a fim de lhes permitir conduzir investigações, adotar decisões vinculativas e impor sanções eficazes e dissuasivas, bem como obrigar os Estados-Membros a conceder-lhes os **recursos necessários** para esse efeito**;**

- **instituir um sistema de «balcão único» para a proteção de dados na UE:** os responsáveis pelo tratamento de dados na UE terão apenas **uma única autoridade de proteção de dados** como interlocutor, ou seja, a autoridade do Estado-Membro onde está situado o estabelecimento principal da empresa;

- criar condições para uma **cooperação rápida e eficaz entre as** autoridades de proteção de dados, incluindo a obrigação de cada autoridade conduzir investigações e inspeções a pedido de outra, e de reconhecer mutuamente as respetivas decisões;

- **instituir um mecanismo de controlo da coerência** a nível da UE para assegurar que as decisões de uma autoridade de proteção de dados com impacto mais amplo a nível europeu tenham plenamente em conta os pareceres emitidos pelas outras autoridades interessadas e sejam plenamente conformes com o direito da UE;

- conferir maior destaque ao Grupo de Trabalho do artigo 29.º, passando este a ser um **comité europeu para a proteção de dados independente,** a fim de melhorar o seu contributo para a aplicação coerente da legislação em matéria de proteção de dados e fornecer uma base sólida de cooperação entre as autoridades de proteção de dados, incluindo a Autoridade Europeia para a Proteção de Dados, bem como

[23] É proposta uma diretiva para definir as regras aplicáveis no domínio da cooperação policial e judiciária em matéria penal (consultar o ponto 4 infra), o que irá permitir uma maior flexibilidade aos Estados-Membros neste domínio específico.

reforçar as sinergias e a eficácia, prevendo que o secretariado do referido comité europeu de proteção de dados seja assegurado pela Autoridade Europeia para a Proteção de Dados.

O novo regulamento da UE garantirá uma proteção firme do direito fundamental à proteção de dados no conjunto da União Europeia e fortalecerá o funcionamento do mercado único. Paralelamente, tendo em conta o facto de que, como sublinhado pelo Tribunal de Justiça da UE[24], o direito à proteção dos dados pessoais não é absoluto, devendo ser considerado em relação à sua função na sociedade[25] e ser equilibrado com outros direitos fundamentais em conformidade com o princípio da proporcionalidade[26], o regulamento incluirá disposições expressas que garantirão o respeito de outros direitos fundamentais, como a liberdade de expressão e de informação, o direito de defesa, bem como o direito de sigilo profissional (por exemplo para as profissões jurídicas), sem prejudicar o estatuto das igrejas definido pela legislação dos Estados-Membros.

4. A UTILIZAÇÃO DE DADOS NA COOPERAÇÃO POLICIAL E DE JUSTIÇA PENAL

A entrada em vigor do Tratado de Lisboa e, nomeadamente, a introdução de uma nova base jurídica (artigo 16.º do TFUE) permitem à União instaurar um quadro global em matéria de proteção de dados que garante um elevado nível de proteção dos dados das pessoas singulares, respeitando simultaneamente a natureza específica da cooperação policial e judiciária em matéria penal. Em especial, possibilita a adoção do quadro revisto da UE em matéria de proteção de dados para abranger tanto o tratamento transfronteiriço como nacional dos dados pessoais. Tal atenuaria as diferenças entre as legislações nacionais, muito provavelmente em benefício da proteção geral dos dados pessoais. Permitiria igualmente um intercâmbio de informações mais fácil entre as autoridades policiais e judiciárias dos Estados-Membros, melhorando desta forma a cooperação a nível da luta contra a criminalidade grave na Europa. Atualmente, o tratamento de dados pelas autoridades policiais e judiciárias em matéria penal é regido principalmente pela Decisão-Quadro 2008/977/JAI, que é anterior à entrada em vigor do Tratado de Lisboa. A Comissão não tem competência para fazer aplicar as suas disposições dado tratar-se de uma decisão-quadro, facto que tem contribuído para a sua execução irregular. Além disso, o âmbito de aplicação dessa decisão-quadro restringe-se a atividades de tratamento com dimensão transfronteiriça[27]. Tal significa que o tratamento de dados pessoais

---

24 Tribunal de Justiça da UE, acórdão de 9.11.2010 nos processos apensos C-92/09 e C-93/09, Volker e Markus Schecke e Eifert (Coletânea 2010), ainda não publicado oficialmente.

25 Em consonância com o artigo 52.°, n.° 1, da Carta, podem ser impostas restrições ao exercício do direito à proteção de dados desde que sejam previstas por lei e respeitem o conteúdo essencial desse direito e liberdade; na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.

26 Tribunal de Justiça da UE, acórdão de 6.11.2003 no processo C-101/01, Lindqvist (Coletânea 2003, p. I-12971, n.^{os} 82-90; acórdão de 16.12.2008 no processo C-73/07, Satamedia (Coletânea 2008, p. I-9831, n.^{os} 50-62).

27 Mais precisamente, a decisão-quadro aplica-se aos dados pessoais que são ou foram transmitidos ou disponibilizados entre Estados-Membros ou trocados entre Estados-Membros e instituições ou organismos da UE (ver artigo 1.º, n.º 2).

que não tenham sido objeto de intercâmbio não está atualmente coberto pelas regras da UE que regulam este tipo de tratamento e que protegem o direito fundamental à proteção de dados. Este facto cria, em alguns casos, dificuldades práticas às autoridades policiais e outras autoridades, que nem sempre conseguem distinguir facilmente entre o tratamento de dados meramente nacional e o tratamento transfronteiriço, ou prever se dados «nacionais» podem ser objeto de um intercâmbio transfronteiriço ulterior[28].

O novo quadro reformado da UE relativo à proteção de dados visa, portanto, garantir um nível coerente e elevado de proteção, a fim de **reforçar a confiança mútua entre as autoridades policiais e judiciárias dos diferentes Estados-Membros, contribuindo assim para a livre circulação de dados e uma cooperação efetiva entre as referidas autoridades**.

Para assegurar um elevado nível de proteção dos dados pessoais no domínio da cooperação policial e judiciária em matéria penal e para facilitar o intercâmbio de dados pessoais entre as autoridades policiais e judiciárias dos Estados-Membros, a Comissão propõe como parte do pacote de reformas da proteção de dados, uma diretiva, que irá:

- **aplicar os princípios gerais em matéria de proteção de dados** à cooperação policial e judiciária em matéria penal, respeitando a natureza específica destes domínios[29];

- prever **condições e critérios mínimos harmonizados relativos a eventuais limitações** às regras gerais. Estas medidas dizem respeito, em especial, aos direitos das pessoas singulares a serem informadas quando as autoridades policiais e judiciárias tratem ou consultam os seus dados. Essas limitações são necessárias para garantir a eficácia da prevenção, investigação, deteção ou repressão de infrações penais;

- estabelecer **regras específicas para ter em conta a natureza particular das atividades de aplicação da lei,** incluindo uma **distinção entre as diferentes categorias de titulares de dados** cujos direitos podem ser diferentes (designadamente, as testemunhas e os suspeitos).

5. A PROTEÇÃO DE DADOS NUM MUNDO GLOBALIZADO

Os direitos das pessoas singulares devem continuar a ser garantidos quando os dados pessoais são transferidos da UE para países terceiros, e sempre que esses dados digam respeito a pessoas que se encontram nos Estados-Membros, e tenham sido referenciadas, e os seus dados utilizados ou analisados por prestadores de serviços estabelecidos em países terceiros. Isto significa que as normas da UE em matéria de

[28] Tal foi confirmado por alguns Estados-Membros aquando da resposta ao questionário da Comissão em relação ao relatório sobre a execução da decisão-quadro [COM (2012) 12].

[29] Ver a Declaração n.º 21 sobre a proteção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial, anexada à Ata Final da Conferência Intergovernamental que adotou o Tratado de Lisboa.

proteção de dados devem ser aplicadas independentemente da localização geográfica da empresa ou do seu serviço de tratamento de dados.

No contexto de globalização atual, os dados pessoais são transferidos através de um número cada vez maior de fronteiras, virtuais e geográficas, sendo conservados em servidores instalados em vários países. Cada vez mais empresas oferecem serviços de computação em nuvem que permite aos seus clientes consultar e conservar dados em servidores distantes. Estes fatores impõem uma melhoria dos mecanismos de transferência de dados para os países terceiros. Tal pode incluir decisões sobre o nível adequado da proteção, ou seja, decisões que certifiquem a existência de normas «adequadas» de proteção de dados em países terceiros, bem como garantias apropriadas, tais como cláusulas contratuais normalizadas ou regras vinculativas para empresas[30], com o objetivo de garantir um elevado nível de proteção de dados nas operações de tratamento internacionais e facilitar os fluxos transfronteiriços de dados.

Regras vinculativas para empresas

Um grupo empresarial necessita de transferir regularmente dados pessoais de empresas suas filiais estabelecidas no território da UE para outras filiais situadas em países terceiros. O grupo empresarial gostaria de introduzir um conjunto de regras vinculativas para empresas (RVE) de forma a respeitar a legislação da UE e limitar simultaneamente as exigências administrativas aplicáveis a cada transferência. Na prática, as RVE garantem a aplicação de um conjunto único de regras a todo o grupo, em vez de ter de se recorrer a um contrato interno para cada transferência.

Graças às práticas atuais acordadas a nível do Grupo de Trabalho do artigo 29.º, o reconhecimento do caráter adequado das garantias previstas pelas RVE de uma empresa exige um controlo exaustivo efetuado por três autoridades de proteção de dados (uma «principal» e duas «revisoras»), mas pode receber também o parecer de outras autoridades. Além disso, a legislação de vários Estados-Membros exige autorizações nacionais adicionais para as transferências regidas pelas RVE, o que torna o processo de adoção destas regras muito complicado, oneroso, longo e complexo.

Na sequência da reforma da proteção de dados:

- este processo será mais simples e racionalizado;

- as RVE serão validadas apenas por uma autoridade de proteção de dados, com mecanismos para garantir a participação rápida de outras autoridades de proteção de dados relevantes;

- quando uma RVE for aprovada por uma autoridade, será válida no conjunto da UE, sem necessitar de qualquer autorização adicional a nível nacional.

Para fazer face aos desafios da globalização, são necessários instrumentos e mecanismos flexíveis, particularmente para as empresas ativas a nível mundial, que garantam uma proteção sem falhas dos dados pessoais. A Comissão propõe as seguintes medidas:

30 Entende-se por «regras vinculativas para empresas», os códigos de boas práticas baseados em normas europeias de proteção de dados e aprovadas, pelo menos, por uma autoridade de proteção de dados, que as entidades elaboram voluntariamente e respeitam para garantir uma proteção adequada a categorias de transferências de dados pessoais entre as empresas de um mesmo grupo ligadas por essas regras. Essas regras não se encontram explicitamente previstas na Diretiva 95/46/CE, mas foram desenvolvidas na prática pelas autoridades de proteção de dados, com o apoio do Grupo de Trabalho do artigo 29.º.

- **regras claras** que definam os casos em que **o direito da União se aplica aos responsáveis pelo tratamento de dados estabelecidos em países terceiros**, nomeadamente especificando que sempre que bens e serviços sejam propostos às pessoas singulares na UE, ou sempre que o seu comportamento seja controlado, **são aplicáveis as regras da UE;**

- qualquer **decisão sobre o nível adequado** de proteção de dados adotada pela Comissão Europeia terá como base critérios explícitos e claros, incluindo no domínio da cooperação policial e da justiça penal;

- os fluxos lícitos de dados para países terceiros serão facilitados através do reforço e da simplificação das **regras relativas às transferências internacionais** de dados para países não abrangidos por uma decisão sobre o nível adequado de proteção, nomeadamente racionalizando e alargando a utilização de instrumentos, como as **regras vinculativas para empresas**, para que estas possam ser utilizadas pelos **responsáveis pelo tratamento de dados** e a nível de **grupos de empresas**, desta forma refletindo melhor o número crescente de empresas envolvidas nas atividades de tratamento de dados, especialmente no domínio da computação em nuvem;

- encetar um **diálogo** e, se for caso disso, **negociações**, com países terceiros, particularmente os parceiros estratégicos da UE e os países envolvidos na Política Europeia de Vizinhança, bem como organizações internacionais relevantes (por exemplo, o Conselho da Europa, a Organização de Cooperação e Desenvolvimento Económico, a Organização das Nações Unidas) para **promover, a nível mundial, a adoção de normas de elevado nível e interoperáveis em matéria de proteção de dados**.

6. CONCLUSÃO

A reforma da UE relativa à proteção de dados tem por objetivo estabelecer um **quadro moderno, sólido, coerente e global em matéria de proteção de dados para a União Europeia.** O direito fundamental das pessoas singulares à proteção de dados será reforçado. Serão respeitados outros direitos, como a liberdade de expressão e de informação, o direito das crianças, o direito de liberdade de empresa, o direito a um processo equitativo e ao sigilo profissional (por exemplo, para as profissões jurídicas), bem como o estatuto das igrejas tal como definido nas legislações dos Estados-Membros.

A reforma irá acima de tudo beneficiar as pessoas singulares, reforçando os seus direitos à proteção de dados e a sua confiança no ambiente digital. Além disso, a reforma irá simplificar substancialmente o quadro jurídico em que evoluem as empresas e o setor público. Prevê-se que tal possa estimular o desenvolvimento da economia digital no conjunto do mercado único da UE e além-fronteiras, em consonância com os objetivos da Estratégia Europa 2020 e da Agenda Digital para a Europa. Por último, a reforma irá reforçar a confiança entre as autoridades de aplicação da lei, a fim de facilitar o intercâmbio de dados entre elas e a cooperação na luta contra a criminalidade grave, garantindo simultaneamente às pessoas singulares um elevado nível de proteção.

A Comissão Europeia irá trabalhar em estreita colaboração com o Parlamento Europeu e o Conselho para garantir a obtenção de um acordo relativo ao novo quadro de proteção de dados da UE até final de 2012. Ao longo deste processo de adoção e para além dele, especialmente no contexto da execução e aplicação dos novos instrumentos jurídicos, a Comissão manterá **um diálogo estreito e transparente com todas as partes interessadas**, envolvendo representantes dos setores privado e público. Entre as partes interessadas encontram-se representantes das autoridades policiais e judiciárias, dos reguladores de comunicações eletrónicas, das organizações da sociedade civil, das autoridades de proteção de dados e do setor académico, bem como de agências especializadas da UE, designadamente a Eurojust, a Europol, a Agência dos Direitos Fundamentais e a Agência Europeia para a Segurança das Redes de Informação.

Num contexto de evolução constante das tecnologias da informação e dos comportamentos sociais, esse diálogo é da maior importância para congregar os contributos necessários tendo em vista assegurar um elevado nível de proteção dos dados das pessoas singulares, bem como o crescimento e a competitividade das empresas da União, a eficácia operacional do setor público (incluindo os serviços policiais e judiciários) e um nível reduzido de encargos administrativos.