I

(Resoluções, recomendações e pareceres)

RECOMENDAÇÕES

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

Recomendações da AEPD sobre as opções da União Europeia para a reforma da proteção de dados

(o texto integral está disponível em alemão, francês e inglês no sítio web *da AEPD em www.edps.europa.eu)*

(2015/C 301/01)

Em 24 de junho de 2015, as três principais instituições da União Europeia (UE) — o Parlamento Europeu, o Conselho e a Comissão Europeia — encetaram negociações no âmbito do processo de codecisão relativas à proposta de regulamento geral sobre a proteção de dados (RGPD), um procedimento conhecido como um «trílogo» informal ([1]). A base para o trílogo é constituída pela proposta da Comissão de janeiro de 2012, pela resolução legislativa do Parlamento Europeu de 12 de março de 2014 e pela orientação geral do Conselho adotada em 15 de junho de 2015 ([2]). As três instituições estão empenhadas em tratar o RGPD como parte do pacote de reforma mais alargada da proteção de dados, o qual inclui a proposta de diretiva relativa a atividades policiais e judiciais. O processo deverá ficar concluído no final de 2015 e provavelmente irá permitir a adoção formal de ambos os instrumentos no início de 2016, à qual se seguirá um período de transição de dois anos ([3]).

A Autoridade Europeia para a Proteção de Dados (AEPD) é uma instituição independente da UE. A Autoridade não participa no trílogo, mas, nos termos do artigo 41.º, n.º 2, do Regulamento n.º 45/2001, «No que se refere ao tratamento de dados pessoais, está encarregada de assegurar que os direitos e liberdades fundamentais das pessoas singulares, especialmente o direito à vida privada, sejam respeitados pelas instituições e órgãos comunitários», e é responsável «… por aconselhar as instituições e órgãos comunitários e as pessoas em causa sobre todas as questões relativas ao tratamento de dados pessoais». A Autoridade e a Autoridade-Adjunta foram nomeadas em dezembro de 2014, com a missão específica de serem mais construtivas e pró-ativas, e em março de 2015 publicaram uma estratégia quinquenal em que estabeleciam como tencionavam executar essa missão e prestar contas por essa execução ([4]).

O presente parecer constitui a primeira etapa da estratégia da AEPD. Com base em discussões com as instituições da UE, os Estados-Membros, a sociedade civil, os representantes do setor e outras partes interessadas, pretendemos com este nosso parecer ajudar os participantes no trílogo a chegar atempadamente a um consenso adequado. O parecer sobre o RGPD divide-se em duas partes:

— a visão da AEPD das regras de proteção de dados orientadas para o futuro, com exemplos ilustrativos das nossas recomendações; e

— um anexo («anexo do Parecer 3/2015: Quadro comparativo dos textos do RGPD com as recomendação da AEPD»), que contém um quadro de quatro colunas em que se compara, artigo a artigo, o texto do RGPD adotado, respetivamente, pela Comissão, pelo Parlamento e pelo Conselho, e a recomendação da AEPD.

O parecer é publicado no nosso sítio *web* e através de um aplicativo para dispositivos móveis. Será complementado no outono de 2015 com recomendações relativas não só aos considerandos do RGPD, mas também, assim que o Conselho tiver adotado a sua posição geral sobre a diretiva, à proteção de dados aplicável às atividades policiais e judiciais.

O parecer circunstanciado da AEPD sobre o pacote de reforma que a Comissão propôs em março de 2012 mantém a sua validade. No entanto, passados três anos, sentimos necessidade de atualizar o nosso parecer para termos um envolvimento mais direto nas posições dos colegisladores e oferecermos recomendações específicas ([5]). Tal como sucedeu com o parecer de 2012, também este está em sintonia com os pareceres e declarações do Grupo de Trabalho do artigo 29.º, incluindo o «anexo» intitulado «Core topics in the view of trilogue» (Temas centrais na perspetiva do trílogo) adotado em 17 de junho, para o qual a AEPD deu o seu contributo enquanto membro efetivo do referido Grupo de Trabalho ([6]).

Uma oportunidade rara: por que razão esta reforma é tão importante

A União Europeia encontra-se na reta final de uma maratona para reformar as suas regras sobre informações pessoais. O regulamento geral sobre a proteção de dados poderá vir a afetar, ao longo das próximas décadas, todas as pessoas da UE, todas as organizações da União que tratam dados pessoais, bem como as organizações fora da UE que tratam dados pessoais de cidadãos da UE ([7]). Chegou a hora de salvaguardar os direitos e liberdades fundamentais das pessoas na sociedade do futuro baseada nos dados.

Uma proteção de dados eficaz capacita a pessoa e estimula empresas e autoridades públicas responsáveis. A legislação neste domínio é complexa e técnica, exigindo aconselhamento especializado, em particular o das autoridades de proteção de dados independentes que compreendem os desafios que o seu cumprimento coloca. O RGPD poderá vir a ser um dos atos legislativos mais longos da União, pelo que agora a UE tem de procurar ser seletiva, focalizar-se nas disposições que são efetivamente necessárias e evitar os pormenores que de forma não intencional possam vir a interferir indevidamente com futuras tecnologias. Os textos de cada uma das instituições apregoam clareza e inteligibilidade no tratamento dos dados pessoais: por isso, o RGPD tem de pôr em prática aquilo que apregoa, sendo tão conciso e compreensível quanto possível.

Cabe ao Parlamento Europeu e ao Conselho, enquanto colegisladores, determinar o texto jurídico final, com a ajuda da Comissão, enquanto detentora da iniciativa legislativa e «guardiã dos tratados». A AEPD não participa nas negociações do «trílogo», mas é juridicamente competente para emitir o seu parecer, e fazê-lo de forma proativa, em conformidade com o mandato conferido à Autoridade e à Autoridade-Adjunta aquando da sua nomeação, e com a recente estratégia da AEPD. O presente parecer beneficia de uma década de experiência de controlo do cumprimento da proteção de dados e de aconselhamento político com vista a ajudar a orientar as instituições para um resultado que sirva os interesses da pessoa.

A legislação é a arte do possível. Cada uma das opções que se encontram em cima da mesa, sob a forma dos textos preferidos, respetivamente, pela Comissão, pelo Parlamento e pelo Conselho, contém muitas disposições valiosas mas pode ser melhorada. Embora consideremos que o resultado não será perfeito, tencionamos ajudar as instituições a alcançar o melhor resultado possível. Por essa razão, as nossas recomendações mantêm-se dentro dos limites dos três textos. Somos movidos por três preocupações constantes:

— melhores condições para os cidadãos;

— regras que funcionem na prática;

— regras que perdurem por uma geração.

O presente parecer é um exercício de transparência e responsabilização, dois princípios que constituem porventura a inovação mais notável do RGPD. O processo do trílogo nunca antes foi alvo de tanta atenção. As nossas recomendações são públicas e gostaríamos de instar todas as instituições da UE a aproveitarem esta iniciativa e a darem o exemplo, para que esta reforma legislativa seja o resultado de um processo transparente e não de um compromisso secreto.

A UE precisa de um novo acordo sobre proteção de dados, precisa de um novo capítulo. O resto do mundo está a acompanhar este processo com toda a atenção. A qualidade da nova legislação e a forma como esta interage com os sistemas e tendências jurídicos globais são de suma importância. Com o presente parecer, a AEPD manifesta a sua vontade e disponibilidade para ajudar a garantir que a União aproveita ao máximo esta oportunidade histórica.

1. Melhores condições para os cidadãos

As regras da União Europeia sempre procuraram facilitar os fluxos de dados, tanto dentro da UE como entre esta e os seus parceiros comerciais, mas com uma preocupação primordial de salvaguardar os direitos e liberdades da pessoa. A Internet permitiu um grau de conectividade, auto-expressão e alcance sem precedentes para trazer valor às empresas e aos consumidores. No entanto, a privacidade assume mais importância do que nunca para os cidadãos europeus. De acordo com o inquérito do Eurobarómetro sobre a proteção de dados realizado em junho de 2015 ([8]), mais de seis em cada dez cidadãos não confiam nas empresas que operam em linha e dois terços estão preocupados por não terem controlo total sobre as informações que fornecem em linha.

É necessário que o quadro reformado mantenha e, sempre que possível, aumente o nível das normas a favor da pessoa. O pacote de reforma da proteção de dados começou por ser proposto como um veículo para reforçar os direitos à privacidade em linha, assegurando uma melhor informação das pessoas sobre os seus direitos e um maior controlo sobre as suas informações ([9]). Representantes de organizações da sociedade civil escreveram à Comissão Europeia em abril de 2015 para instarem as instituições a manterem-se fiéis a estas intenções ([10]).

Os princípios vigentes estabelecidos na Carta, que faz parte do direito primário da UE, devem ser aplicados de forma coerente, dinâmica e inovadora, de modo a produzirem efeitos práticos para o cidadão. É necessário que a reforma seja abrangente, e daí o compromisso com um pacote, mas a probabilidade de o tratamento de dados ser objeto de instrumentos jurídicos distintos exige que haja clareza quanto ao seu âmbito de aplicação exato e quanto ao modo como funcionam em conjunto, sem quaisquer lacunas que comprometam as garantias ([11]).

Para a AEPD, o ponto de partida é a dignidade da pessoa, que transcende questões de mero cumprimento da lei ([12]). As nossas recomendações baseiam-se numa apreciação de cada artigo do RGPD, individual e cumulativa, para determinar se o mesmo irá reforçar a posição da pessoa em comparação com o regime atual. O ponto de referência é constituído pelos princípios que estão no cerne da proteção de dados, ou seja, o artigo 8.º da Carta dos Direitos Fundamentais ([13]).

1.1. *Definições: sejamos claros quanto ao que se entende por informações pessoais*

Uma pessoa deve ser capaz de exercer mais eficazmente os seus direitos em relação a quaisquer informações suscetíveis de a identificar ou distinguir, mesmo que se considere tratar-se de informações «sob pseudónimo» («pseudonimizadas») ([14]).

1.2. *Todo o tratamento de dados deve ser simultaneamente lícito e justificado*

— As exigências de que todo o tratamento de dados seja limitado a fins específicos e tenha uma base jurídica são cumulativas, não alternativas. Recomendamos que se evite qualquer fusão destes princípios e o seu consequente enfraquecimento. Em vez disso, a UE deve preservar, simplificar e operacionalizar a ideia estabelecida de que os dados pessoais devem ser utilizados unicamente de forma compatível com as finalidades para que foram inicialmente recolhidos ([15]).

— O consentimento pode constituir uma base jurídica para o tratamento, mas precisamos de impedir o recurso a caixas de validação (*tick boxes*) coerciva que não oferecem à pessoa uma opção válida e em que não há qualquer necessidade de processamento dos dados. Recomendamos que se permita que as pessoas deem o seu consentimento alargado ou restrito, para efeitos de investigação clínica, por exemplo, e que o mesmo seja respeitado e possa ser retirado ([16]).

— A AEPD apoia soluções sólidas e inovadoras para as transferências internacionais de dados pessoais, que facilitem o intercâmbio de dados e respeitem os princípios da proteção e do controlo dos dados. Desaconselhamos vivamente que se permitam as transferências com base em interesses legítimos do responsável pelo tratamento de dados por causa de uma proteção insuficiente da pessoa, e consideramos que a UE não deve possibilitar o acesso direto de autoridades de países terceiros a dados localizados no seu território. Qualquer pedido de transferência emitido por autoridades de um país terceiro só deve ser aceite se respeitar as normas estabelecidas em tratados de assistência jurídica mútua, acordos internacionais ou outros canais legais de cooperação internacional ([17]).

1.3. *Controlo mais independente e mais assertivo*

— As autoridades de proteção de dados da UE devem estar preparadas para exercer as suas funções a partir do momento em que o RGPD entrar em vigor, e o Comité Europeu para a Proteção de Dados deve estar totalmente operacional assim que o regulamento se tornar aplicável ([18]).

— As autoridades deverão estar aptas a receber e investigar queixas e reclamações apresentadas por titulares dos dados ou por organismos, organizações e associações.

— A aplicação dos direitos individuais requer um sistema eficaz de responsabilidade e indemnização pelos danos causados pelo tratamento ilícito de dados. Atendendo aos obstáculos óbvios que impedem a obtenção de reparação na prática, uma pessoa deve poder fazer-se representar por organismos, organizações e associações em processos judiciais ([19]).

2. **Regras que funcionem na prática**

Não se deve confundir garantias com formalidades. O excesso de pormenores ou as tentativas de microgestão de processos empresariais correm o risco de se tornar obsoletas no futuro. Neste aspeto, podemos aprender alguma coisa com o manual da concorrência da UE, onde um corpo relativamente limitado de legislação secundária é rigorosamente aplicado e estimula uma cultura de responsabilização e consciência entre empresas ([20]).

Cada um dos três textos exige maior clareza e simplicidade aos responsáveis pelo tratamento de dados pessoais ([21]). De igual modo, as obrigações técnicas devem também ser concisas e de fácil compreensão para que os responsáveis pelo tratamento dos dados possam aplicá-las de maneira apropriada ([22]).

Os procedimentos existentes não são sagrados: as nossas recomendações visam identificar formas de desburocratizar, minimizando as disposições relacionadas com documentação e formalidades irrelevantes. Recomendamos que se legisle apenas quando for verdadeiramente necessário. Assim, cria-se espaço de manobra quer para as empresas, quer para as autoridades públicas ou para as autoridades de proteção de dados: um espaço que deve ser preenchido pela responsabilização e pela orientação das autoridades de proteção de dados. Em geral, com as nossas recomendações, o texto do RGPD ficaria cerca de 30 % mais curto do que o tamanho médio dos textos das três instituições ([23]).

2.1. *Garantias eficazes, não procedimentos*

— A documentação deve ser um meio, não um fim, para garantir o cumprimento; a reforma deve concentrar-se nos resultados. Recomendamos uma abordagem escalonável que reduza as obrigações em matéria de documentação impostas aos responsáveis pelo tratamento dos dados a uma política única sobre a forma como irão cumprir o regulamento tendo em conta os riscos, com o cumprimento comprovado de forma transparente, quer se trate de transferências, de contratos com subcontratantes ou de notificações de violações de dados ([24]).

— Com base em critérios de avaliação de riscos explícitos e tendo em conta a experiência que adquirimos no controlo das instituições da UE, recomendamos que se exija a notificação de violações de dados à autoridade de controlo e a realização de avaliações do impacto da proteção de dados apenas quando estejam em risco os direitos e liberdades dos titulares dos dados ([25]).

— As iniciativas do setor, seja através de regras vinculativas para empresas, seja através de selos de privacidade, devem ser ativamente incentivadas ([26]).

2.2. *Um melhor equilíbrio entre interesse público e proteção de dados pessoais*

— As regras de proteção de dados não devem impedir investigações históricas, estatísticas e científicas que sejam verdadeiramente de interesse público. Os responsáveis devem tomar as medidas necessárias para impedir a utilização de informações pessoais contra o interesse da pessoa, tendo especialmente em atenção as regras que regulam as informações sensíveis relacionadas, por exemplo, com a saúde ([27]).

— Investigadores e arquivistas devem poder armazenar dados durante todo o tempo necessário, sem prejuízo destas garantias ([28]).

2.3. *Autoridades de controlo confiáveis e capacitantes*

— Recomendamos que se autorize as autoridades de controlo a emitir orientações destinadas aos responsáveis pelo tratamento de dados e a elaborar os seus próprios regulamentos internos no espírito de uma aplicação simplificada e mais fácil do RGPD por uma única autoridade de controlo (o «Balcão Único») próximo do cidadão («proximidade») ([29]).

— As autoridades devem estar aptas a estabelecer sanções corretivas e administrativas eficazes, proporcionais e dissuasoras com base em todas as circunstâncias relevantes ([30]).

3. **Regras que perdurem por uma geração**

O pilar principal em que assenta o quadro atual, a Diretiva 95/46/CE, tem servido de modelo para nova legislação sobre tratamento de dados na UE e em todo o mundo, e serviu inclusivamente de base para a formulação do artigo 8.º da Carta dos Direitos Fundamentais, que consagra o direito à proteção dos dados pessoais. Esta reforma irá moldar o tratamento de dados para uma geração que não tem memória do que é viver sem a Internet. Importa, por isso, que a UE compreenda perfeitamente as implicações deste ato para as pessoas e a sua sustentabilidade face à evolução tecnológica.

Tem-se assistido nos últimos anos a um aumento exponencial da geração, recolha, análise e intercâmbio de informações pessoais, resultante de inovações tecnológicas como a internet das coisas, a computação em nuvem, os megadados e os dados abertos, cuja exploração a UE considera essencial para a sua competitividade ([31]). A julgar pela longevidade da Diretiva 95/46/CE, é razoável esperar um quadro temporal semelhante antes da próxima grande revisão das regras de proteção de dados, que provavelmente não ocorrerá antes de finais da década de 2030. Muito antes dessa data, é expectável uma convergência das tecnologias baseadas em dados com a inteligência artificial, o processamento de linguagem natural e os sistemas biométricos, dotando as aplicações com capacidade de aprendizagem-máquina para inteligência avançada.

Estas tecnologias estão a desafiar os princípios da proteção de dados. Uma reforma orientada para o futuro deve, portanto, ter a dignidade da pessoa como base e a ética como fundamento. Deve corrigir o desequilíbrio entre a inovação na proteção de dados pessoais e a sua exploração, tornando as garantias eficazes na nossa sociedade digitalizada.

3.1. *Práticas empresariais responsáveis e engenharia inovadora*

— A reforma deveria inverter a recente tendência para a deteção secreta e a tomada de decisões com base em perfis sem o conhecimento da pessoa em causa. O problema não está na publicidade direcionada nem na prática da definição de perfis, mas sim na falta de informação relevante acerca da lógica algorítmica que desenvolve esses perfis e afeta o titular dos dados ([32]). Recomendamos maior transparência por parte dos responsáveis pelo tratamento de dados.

— Apoiamos vivamente a introdução dos princípios da proteção de dados desde a conceção e por defeito como meio para lançar soluções impulsionadas pelo mercado na economia digital. Recomendamos uma formulação mais simples para exigir a integração dos direitos e interesses da pessoa no desenvolvimento de produtos e nas configurações padrão ([33]).

3.2. *Pessoas capacitadas*

A portabilidade dos dados é a porta de entrada no ambiente digital para o controlo do utilizador, e as pessoas estão agora a dar-se conta de que lhes falta esse controlo. Recomendamos que se permita uma transferência direta de dados de um responsável pelo tratamento para outro a pedido do titular dos dados e que se conceda aos titulares dos dados o direito de receber uma cópia dos dados que eles próprios podem transferir para outro responsável pelo tratamento ([34]).

3.3. *Regras válidas para o futuro*

Recomendamos que se evite uma linguagem e práticas suscetíveis de se tornarem obsoletas ou questionáveis ([35]).

4. **Questões pendentes**

A adoção de um pacote de reforma da proteção de dados da UE orientado para o futuro será um feito impressionante mas ainda assim incompleto.

Todas as instituições concordam que os princípios do RGPD devem aplicar-se de forma coerente às instituições da União Europeia. Nós temos defendido a segurança jurídica e a uniformidade do quadro jurídico, embora reconheçamos a singularidade do setor público da UE e a necessidade de evitar qualquer enfraquecimento do atual nível de obrigações (bem como a necessidade de prever a base jurídica e organizacional para a AEPD). A Comissão deveria, portanto, apresentar uma proposta coerente com o RGPD para a revisão do Regulamento n.º 45/2001, logo que possível após a conclusão das conversações sobre o RGPD, de modo que os dois textos possam tornar-se aplicáveis ao mesmo tempo ([36]).

Em segundo lugar, é evidente que a Diretiva 2002/58/CE (a Diretiva «Privacidade e comunicações eletrónicas») vai ter de ser alterada. Mas, acima de tudo, a UE precisa de um quadro claro para a confidencialidade das comunicações, um elemento indissociável do direito à privacidade, que regule todos os serviços que possibilitam as comunicações, e não apenas os fornecedores de comunicações eletrónicas à disposição do público. Para o efeito, deve ser adotado um regulamento juridicamente seguro e harmonizador que preveja pelo menos os mesmos níveis de proteção da Diretiva «Privacidade e comunicações eletrónicas» em condições equitativas.

O presente parecer recomenda, por conseguinte, que se apele a um compromisso com vista à adoção de propostas nestas duas áreas tão depressa quanto possível.

5. **Um momento decisivo para os direitos digitais dentro e fora da Europa**

Pela primeira vez numa geração, a UE dispõe de uma oportunidade para modernizar e harmonizar as regras relativas ao tratamento dos dados pessoais. A privacidade e a proteção dos dados não estão em concorrência com o crescimento económico e o comércio internacional, nem com serviços e produtos excelentes — elas fazem parte da proposta de qualidade e valor. Como reconhece o Conselho Europeu, a confiança é uma condição prévia necessária para produtos e serviços inovadores que dependem do tratamento de dados pessoais.

Em 1995, a UE foi pioneira na proteção de dados. Agora, mais de 100 países em todo o mundo dispõem de legislação em matéria de proteção de dados e menos de metade desses países são europeus ([37]). A UE continua, porém, a suscitar a atenção especial de países que estão a ponderar criar ou rever os seus quadros jurídicos. Numa altura em que a confiança das pessoas nas empresas e nos governos tem sido abalada por revelações de vigilância e violações de dados em larga escala, tal facto confere uma responsabilidade considerável aos legisladores da União cujas decisões este ano poderão vir a ter um impacto fora da Europa.

No entender da AEPD, os textos do RGPD estão no bom caminho, mas há preocupações que subsistem, algumas muito sérias. Com o processo de codecisão existe sempre o risco de enfraquecimento de certas disposições, por causa de alguns negociadores bem-intencionados em busca do compromisso político. No entanto, com a reforma da proteção de dados, a situação é diferente, pois estamos a lidar com direitos fundamentais e o modo como estes serão garantidos durante toda uma geração.

Assim, o presente parecer procura ajudar as principais instituições da UE na resolução dos problemas. Não queremos apenas direitos reforçados para o titular de dados individual e maior responsabilização do responsável pelo tratamento dos dados; queremos facilitar a inovação com um quadro jurídico que seja neutro em relação à tecnologia mas positivo em relação aos benefícios que esta pode oferecer à sociedade.

Com as negociações na reta final, esperamos que as nossas recomendações ajudem a UE a ultrapassar a linha de chegada com uma reforma que continue a ser adequada ao fim a que se destina durante os próximos anos e as próximas décadas: um novo capítulo para a proteção de dados com uma perspetiva global, com a UE a dar o exemplo.

Feito em Bruxelas, em 27 de julho de 2015.

Giovanni BUTTARELLI

Autoridade Europeia para a Proteção de Dados

([1]) Declaração Comum do Parlamento Europeu, do Conselho e da Comissão sobre as regras práticas do processo de codecisão (artigo 251.º do Tratado CE) (2007/C 145/02), JO C 145 de 30.6.2007.

([2]) COM(2012)11 final; resolução legislativa do Parlamento Europeu, de 12 de março de 2014, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados) P7_TA(2014)0212; proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados) — Preparação da orientação geral, documento do Conselho 9565/15, 11 de junho de 2015.

([3]) O título por extenso é: proposta de diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e de repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, COM(2012)10 final; resolução legislativa do Parlamento Europeu, de 12 de março de 2014, sobre a proposta de diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e de repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, P7_TA(2014)0219. Relativamente ao calendário e âmbito do trílogo, consultar as conclusões do Conselho Europeu de 25 e 26 de junho de 2015, EUCO 22/15; o «roteiro» do trílogo foi anunciado numa conferência de imprensa conjunta Parlamento-Conselho-Comissão http://audiovisual.europarl.europa.eu/AssetDetail.aspx?id=690e8d8d-682d-4755-bfb6-a4c100eda4ed (último acesso em 20 de julho de 2015) mas não foi publicado oficialmente. O RGPD entrará em vigor 20 dias após a sua publicação no Jornal Oficial e deverá estar totalmente aplicável dois anos após a sua entrada em vigor (artigo 91.º).

([4]) Anúncio de vaga para a Autoridade Europeia para a Proteção de Dados COM/2014/10354 (2014/C 163 A/02), JO C 163 A/6 de 28.5.2014. Na sua estratégia para 2015-2019, a AEPD prometeu que iria procurar encontrar soluções exequíveis para evitar a burocracia, manter a flexibilidade face à inovação tecnológica e aos fluxos de dados transfronteiras e permitir que as pessoas exerçam mais eficazmente os seus direitos, tanto na Internet como fora dela; «Leading by example: The EDPS Strategy 2015-2019» (Dar o exemplo: a Estratégia da AEPD para 2015-2019), março de 2015.

([5]) Parecer da AEPD sobre o pacote de reforma da proteção de dados, 7 de março de 2015.

([6]) Ver anexo à Carta do Grupo de Trabalho do artigo 29.º endereçada à Comissária Věra Jourová, responsável pela Justiça, Consumidores e Igualdade de Género, 17 de junho de 2015.

([7]) É difícil resumir sucintamente o âmbito material e territorial do RGPD. Parece que as instituições concordam, pelo menos, que o âmbito de aplicação abarca as organizações estabelecidas na União Europeia que são responsáveis pelo tratamento de dados pessoais quer na UE quer fora dela, as organizações estabelecidas fora da União que tratam dados pessoais de cidadãos da UE durante a oferta de bens ou serviços a pessoas na UE ou durante o controlo do comportamento dessas pessoas (ver artigo 2.º sobre o âmbito de aplicação material e o artigo 3.º sobre o âmbito de aplicação territorial).

([8]) Outros resultados indicavam ainda que sete em cada dez inquiridos estavam preocupados com a possibilidade de as informações que forneciam serem utilizadas para fins diferentes daqueles para que tinham sido recolhidas, um em cada sete dizia que devia ser sempre exigida a sua aprovação explícita antes da recolha e tratamento dos seus dados, e dois terços consideravam importante conseguir transferir dados pessoais de um prestador de serviços antigo para um novo; Eurobarómetro especial 431 sobre proteção de dados, junho de 2015. Resultados comparáveis da Pew Research em 2014 revelaram que 91 % dos americanos sentem que perderam o controlo sobre o modo com as empresas recolhem e utilizam informações pessoais, 80 % dos utilizadores de redes sociais estão preocupados com o facto de terceiros, como anunciantes ou empresas, obterem os seus dados, e 64 % dizem que o governo deveria fazer mais para regulamentar os anunciantes; Pew Research Privacy Panel Survey, janeiro de 2014.

([9]) A Comissão propõe uma reforma abrangente das regras de proteção de dados com vista a aumentar o controlo dos utilizadores sobre os seus dados e reduzir os custos para as empresas.

([10]) Carta das ONG ao Presidente Juncker, 21 de abril de 2015 https://edri.org/files/DP_letter_Juncker_20150421.pdf e resposta do chefe do Gabinete do vice-presidente Timmermans, 17 de julho de 2015 https://edri.org/files/eudatap/Re_EC_EDRi-GDPR.pdf (acedido em 23 de julho de 2015). A AEPD reuniu-se com representantes de algumas destas ONG para discutir as suas preocupações em maio de 2015; COMUNICADO DE IMPRENSA EDPS/2015/04, 1.6.2015, Reforma da Proteção de Dados da UE: a AEPD reúne-se com grupos internacionais de defesa das liberdades civis; gravação integral das discussões disponível no sítio da AEPD (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Pressnews/Videos/GDPR_civil_soc).

([11]) Artigo 2.º, n.º 2, alínea e).

([12]) Artigo 1.º.

([13]) O artigo 8.º da Carta diz o seguinte (negrito nosso):

«1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um ***tratamento leal****, para* ***fins específicos*** *e* ***com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei****. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e* ***de obter a respetiva retificação****.*

3. O cumprimento destas regras fica sujeito a ***fiscalização por parte de uma autoridade independente****.»*

([14]) Artigo 10.º A menos que, e até que, haja uma definição clara e juridicamente vinculativa do termo «dados sob pseudónimo», por oposição a «dados pessoais», este tipo de dados deve continuar a estar abrangido pelas regras de proteção de dados.

([15]) Artigo 6.º, n.ºs 2 e 4. Dado que tem havido alguma incerteza quanto ao significado do termo «compatibilidade», recomendamos, na sequência do Parecer do Grupo de Trabalho do artigo 29.º sobre a limitação da finalidade, critérios gerais para avaliar se o tratamento é compatível (ver artigo 5.º, n.º 2).

([16]) Uma separação funcional eficaz é um meio de assegurar o tratamento lícito na ausência de consentimento, mas o interesse legítimo não deve ser interpretado de maneira excessiva. Um direito incondicional à autoexclusão pode também constituir uma alternativa apropriada em certas situações. Avaliar se o consentimento é dado livremente depende em parte *a)* da existência ou não de um desequilíbrio entre o titular dos dados e o responsável pelo tratamento dos mesmos e *b)* em casos de tratamento abrangidos pelo artigo 6.º, n.º 1, alínea b), do condicionamento ou não da execução de um contrato ou da prestação de um serviço à obtenção do consentimento ao tratamento de dados que não são necessários para essas finalidades (ver artigo 7.º, n.º 4). Isto reflete a disposição prevista no direito do consumidor da UE: de acordo com o artigo 3.º, n.º 1, da Diretiva 93/13/CEE de 5 de abril de 1993 relativa às cláusulas abusivas nos contratos celebrados com os consumidores, «Uma cláusula contratual que não tenha sido objeto de negociação individual é considerada abusiva quando, a despeito da exigência de boa-fé, der origem a um desequilíbrio significativo em detrimento do consumidor, entre os direitos e obrigações das partes decorrentes do contrato».

([17]) Estas regras incluem decisões de adequação para setores e territórios especificados, revisões periódicas das decisões de adequação e regras vinculativas para empresas (ver artigos 40.º a 45.º).

([18]) Artigo 73.º.

([19]) Artigo 76.º Relativamente à dificuldade em obter reparação por violações das regras de proteção de dados, ver o relatório «Acesso a vias de recurso em matéria de proteção de dados nos Estados-Membros da União Europeia», publicado pela Agência dos Direitos Fundamentais da União Europeia em 2013.

([20]) As regras da UE colocam a ênfase na autoavaliação das empresas no que respeita ao cumprimento da proibição de acordos anticoncorrenciais prevista pelo artigo 101.º do TFUE, enquanto a detenção de uma posição dominante num mercado confere às empresas a «responsabilidade particular» de evitar qualquer ação suscetível de prejudicar uma concorrência efetiva (n.º 9 da Orientação da Comissão 2009/C 45/02); ver parecer preliminar da AEPD «Privacy and Competitiveness in the Age of Big Data» (Privacidade e Competitividade na Era dos Megadados) de 14 de março de 2014.

([21]) Os três textos referem-se a este aspeto de diferentes maneiras: «de modo e forma inteligíveis, utilizando uma linguagem clara e simples» (considerando 57, PE; artigo 19.º, COM e Conselho), «direitos claros e não ambíguos» (considerando 99, PE; artigo 10.º-A, PE), «prestação de informações claras e facilmente compreensíveis» (artigo 10.º-A, PE; artigo 11.º, PE), e informações que sejam «concisas, transparentes, claras e de fácil acesso» (considerando 25, PE, COM e Conselho; artigo 11.º, PE).

([22]) As disposições relativas a atos delegados têm sido eliminadas em larga medida das versões do Parlamento e do Conselho. Pensamos que a UE poderia ir mais longe e deixar estas matérias técnicas para as autoridades independentes especializadas.

([23]) As nossas recomendações produziriam um texto com cerca de 20 000 palavras; os textos das três instituições têm em média cerca de 28 000 palavras.

([24]) Artigo 22.º.

([25]) Artigos 31.º e 33.º.

([26]) Artigo 39.º.

([27]) Artigo 83.º Dado que o arquivamento e a investigação não constituem por si só uma base jurídica para o tratamento, recomendamos a eliminação do n.º 2 do artigo 6.º.

([28]) Artigo 83.º-A.

([29]) O Grupo de Trabalho do artigo 29.º delineou uma visão da governação, do mecanismo de controlo da coerência e do balcão único baseada em autoridades de proteção de dados (APD) independentes e formulada em três níveis:

— a APD individual que é sólida e está totalmente dotada de meios para lidar com casos dentro da sua esfera de competência;

— uma cooperação eficaz entre APD com uma liderança clara nos casos transfronteiriços;

— o Comité Europeu para a Proteção de Dados, que deve ser autónomo, dotado de personalidade jurídica própria e de meios suficientes, constituído por APD iguais que trabalham num espírito de solidariedade, com poder para tomar decisões vinculativas, e apoiado por um secretariado que serve o Comité por intermédio da presidência.

([30]) Recomendamos igualmente que se clarifique a competência das autoridades de controlo e a designação de uma autoridade para liderar nos casos de tratamento transnacional, preservando embora a capacidade das autoridades de controlo para tratar dos casos puramente locais. Recomendamos uma versão simplificada do mecanismo de controlo da coerência que seja mais clara quanto ao modo de identificar os casos em que as autoridades de controlo teriam de consultar o Comité Europeu para a Proteção de Dados e em que este teria de emitir uma decisão vinculativa a fim de assegurar a aplicação coerente do regulamento.

([31]) Comunicação da Comissão «Estratégia para o Mercado Único Digital na Europa» COM(2015) 192 final; Conclusões do Conselho Europeu de junho de 2015, EUCO 22/15; Conclusões do Conselho sobre a transformação digital da indústria europeia, 8993/15.

([32]) Artigo 14.º, alínea h).

([33]) Artigo 23.º.

([34]) Artigo 18.º Recomendamos ainda que, para ser eficaz, o direito à portabilidade dos dados deve ter um vasto âmbito de aplicação, e não se deve aplicar apenas às operações de tratamento que utilizam dados fornecidos pelo respetivo titular.

([35]) Recomendamos, por exemplo, que se omitam expressões como «em linha», «por escrito» e «a sociedade da informação».

([36]) Uma opção, que merece a nossa preferência, consistiria em fazer isso através de uma disposição do próprio RGPD.

([37]) Greenleaf, Graham, Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority (30 de janeiro de 2015); (2015) 133 Privacy Laws & Business International Report, fevereiro de 2015; UNSW Law Research Paper No. 2015-21.