

PARECERES

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados sobre a Decisão 2011/141/UE da Comissão que altera a Decisão 2007/76/CE da Comissão relativa ao Sistema de Cooperação no domínio da Defesa do Consumidor («CPCS») e sobre a Recomendação 2011/136/UE da Comissão sobre orientações para a aplicação das regras de protecção de dados no CPCS

(2011/C 217/06)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 16.º,

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente os artigos 7.º e 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ⁽¹⁾,

Tendo em conta o pedido de parecer apresentado nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados ⁽²⁾,

ADOPTOU O SEGUINTE PARECER:

I. INTRODUÇÃO

1. Em 1 de Março de 2011, a Comissão Europeia adoptou uma decisão da Comissão que altera a Decisão 2007/76/CE da Comissão relativa ao CPCS (a seguir designada «segunda alteração do CPC») ⁽³⁾. Na mesma data, a Comissão adoptou também uma Recomendação sobre orientações para a aplicação das regras de protecção de dados no Sistema de Cooperação no domínio da Defesa do Consumidor (CPCS) (a seguir designada «orientações sobre a protecção de dados

⁽¹⁾ JO L 281 de 23.11.1995, p. 31.

⁽²⁾ JO L 8 de 12.1.2001, p. 1.

⁽³⁾ Decisão da Comissão, de 1 de Março de 2011, que altera a Decisão 2007/76/CE que aplica o Regulamento (CE) n.º 2006/2004 do Parlamento e do Conselho relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor no que respeita a assistência mútua (2011/141/UE) (JO L 59 de 4.3.2011, p. 63).

no sistema CPC») ⁽⁴⁾. Ambos os documentos foram enviados à AEPD para consulta, nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001.

2. O CPCS é um sistema informático concebido e gerido pela Comissão nos termos do Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor (a seguir designado «Regulamento CPC»). O CPCS facilita a cooperação entre as «autoridades competentes» dos Estados-Membros da UE e a Comissão nesse domínio, no que se refere às infracções a um conjunto pré-definido de directivas e regulamentos da UE. Para serem abrangidas pelo âmbito de aplicação do Regulamento CPC, as infracções devem ser de natureza transfronteiriça e prejudicar «os interesses colectivos dos consumidores».
3. Os utilizadores do CPCS trocam informações no quadro da sua cooperação, incluindo dados pessoais. Esses dados pessoais podem ser relativos aos directores ou aos trabalhadores de um vendedor ou fornecedor suspeito de ter cometido uma infracção, ao próprio vendedor ou fornecedor (caso se trate de um indivíduo), bem como a terceiros como os consumidores ou os autores da denúncia.
4. O sistema foi concebido para ser um instrumento de comunicação seguro entre as autoridades competentes, bem como uma base de dados. O CPCS é utilizado pelas autoridades competentes para requerer informações que ajudem na investigação de um caso ⁽⁵⁾ ou para pedir assistência na aplicação ⁽⁶⁾ («pedidos de assistência mútua»). Além disso, as autoridades competentes também podem enviar uma mensagem de advertência («alerta») para informar as outras autoridades competentes e a Comissão a respeito de uma infracção ou de uma suspeita de infracção ⁽⁷⁾. O CPCS

⁽⁴⁾ Recomendação da Comissão, de 1 de Março de 2011, sobre orientações para a aplicação das regras de protecção de dados no Sistema de Cooperação no domínio da Defesa do Consumidor (CPCS) (2011/136/UE) (JO L 57 de 2.3.2011, p. 44).

⁽⁵⁾ Ver artigo 6.º do Regulamento CPC sobre «intercâmbio de informações a pedido».

⁽⁶⁾ Ver artigo 8.º do Regulamento CPC sobre «pedido de medidas de aplicação».

⁽⁷⁾ Ver artigo 7.º do Regulamento CPC sobre «intercâmbio de informações sem pedido» (ou «alerta», para abreviar).

também inclui outras funcionalidades, com um sistema de notificação⁽⁸⁾ e um fórum de intercâmbio de dados não relacionados com processos.

5. No presente parecer, a AEPD aborda várias questões de protecção de dados relacionadas com o quadro normativo do CPCS, concentrando-se essencialmente na segunda alteração do CPC recentemente adoptada. Além disso, a AEPD faz um balanço dos progressos já realizados, destacando selectivamente algumas preocupações remanescentes e certas considerações para o futuro. Comenta ainda algumas disposições das orientações sobre a protecção de dados no sistema CPC.
6. Em paralelo com o presente parecer [adoptado nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001], a AEPD está também a formular um parecer de controlo prévio, na sua qualidade de autoridade de controlo (ao abrigo do artigo 27.º do mesmo regulamento) (a seguir designado «parecer de controlo prévio»). Esse parecer contém uma descrição mais pormenorizada do CPCS, bem como do tratamento de dados pessoais efectuado no seu âmbito, e a AEPD formula recomendações relativas a medidas específicas que devem ser tomadas a nível prático, técnico e organizativo para melhorar o cumprimento da legislação em matéria de protecção de dados no CPCS. Uma vez que as orientações sobre a protecção de dados no sistema CPC também estão estreitamente relacionadas com estas medidas específicas, o parecer de controlo prévio pronuncia-se igualmente sobre certas disposições dessas orientações.

II. QUADRO NORMATIVO DO CPCS

7. A AEPD verifica com satisfação que o CPCS tem uma sólida base jurídica, nomeadamente um regulamento adoptado pelo Conselho e o Parlamento. Além disso, a AEPD constata com agrado que a base jurídica foi complementada, ao longo do tempo, a fim de fornecer indicações mais pormenorizadas e abordar as preocupações em matéria de protecção de dados. A AEPD manifesta especial satisfação por a Decisão 2007/76/CE da Comissão, de 22 de Dezembro de 2006, que aplica o Regulamento CPC (a seguir designada «decisão de aplicação do CPC») ter sido adoptada e posteriormente alterada em 17 de Março de 2008 e, mais recentemente, em 1 de Março de 2011, através da segunda alteração do CPC. O facto de a Comissão ter adoptado as orientações sobre a protecção de dados no sistema CPC, especificamente centradas nas questões de protecção de dados, também é motivo de satisfação.
8. Embora a AEPD lamente não ter sido consultada na altura em que o Regulamento CPC e a Decisão de aplicação do CPC foram inicialmente adoptados, está satisfeita por a Comissão a ter consultado aquando da adopção de cada uma das duas alterações à Decisão de aplicação do CPC, bem como em relação às orientações sobre a protecção de

dados no sistema CPC. É igualmente com agrado que a AEPD constata que a Comissão também consultou previamente o Grupo de Trabalho de Protecção de Dados do Artigo 29.º (a seguir designado por «GT29»), que emitiu, em 21 de Setembro de 2007, o seu Parecer n.º 6/2007 (WP 139). Por último, a AEPD congratula-se com o facto de nos considerandos das orientações sobre a protecção de dados no sistema CPC se fazer referência a essas consultas.

9. A AEPD constata que i) a Comissão analisou atentamente as recomendações formuladas pela AEPD em anteriores trocas informais de pontos de vista, bem como as que foram expressas pelo GT29 no Parecer n.º 6/2007, e que ii) muitas dessas recomendações foram seguidas no desenvolvimento subsequente do quadro legislativo relativo ao CPCS e/ou a nível prático, técnico e organizativo. As suas observações no presente parecer, bem como no seu parecer de controlo prévio, devem ser apreciadas neste contexto positivo.

III. QUESTÕES DE PROTECÇÃO DE DADOS RELATIVAS À SEGUNDA ALTERAÇÃO DO CPC

3.1. Conservação de dados pessoais no CPCS

3.1.1. Introdução

10. Como observação preliminar, a AEPD faz notar que a questão do encerramento de casos e dos períodos de conservação não foi abordada de forma adequada e exaustiva no Regulamento CPC⁽⁹⁾.
11. Na verdade, o Regulamento CPC só estabelece duas regras específicas em relação à eliminação dos dados e nada dispõe a respeito do encerramento de casos⁽¹⁰⁾. Em primeiro lugar, determina que, se um alerta «carece comprovadamente de fundamento», a autoridade competente o deve retirar e a Comissão deve remover sem demora a informação da base de dados. Em segundo lugar, exige que, sempre que uma autoridade competente notifique, nos termos do artigo 8.º, n.º 6, do Regulamento CPC, que cessou uma infracção, os dados armazenados devem ser suprimidos cinco anos após a notificação.
12. O Regulamento CPC não determina a finalidade do período de conservação de cinco anos, nem fornece quaisquer outras especificações sobre a forma e o momento em que se deve avaliar se um alerta «carece de fundamento». Além disso, o Regulamento CPC também não indica por quanto tempo as informações devem permanecer na base de dados em casos não abrangidos pelas duas regras específicas acima mencionadas (por exemplo, o Regulamento não especifica por quanto tempo os pedidos de assistência mútua

⁽⁸⁾ Ver artigos 7.º, n.º 2, e 8.º, n.º 6, do Regulamento CPC.

⁽⁹⁾ Ver também o Parecer n.º 6/2007 do Grupo de Trabalho do Artigo 29.º (mencionado na Parte II *supra*).

⁽¹⁰⁾ Ver artigo 10.º, n.º 2, do Regulamento CPC.

são conservados na base de dados, caso não tenham conduzido a medidas de aplicação da lei capazes de fazer cessar a infracção).

13. A AEPD verifica com agrado que a Decisão de aplicação do CPC, alterada, e as orientações sobre a protecção de dados no sistema CPC procuram prestar esclarecimentos adicionais. Contudo, a AEPD continua preocupada com vários aspectos das regras relativas ao encerramento de casos e à conservação de dados no CPCS, como é mais adiante examinado nas secções 3.1.2 a 3.1.4.
14. A AEPD recomenda que se abordem estas preocupações na próxima revisão do quadro normativo do CPCS, através de uma nova alteração da Decisão de aplicação do CPC ou, preferencialmente, através de uma alteração do próprio Regulamento CPC.
15. Até essa acção legislativa ser possível, a AEPD recomenda que as preocupações relativas aos períodos de conservação sejam resolvidas a nível prático, técnico e organizativo, bem como claramente apresentadas no documento «Rede de Cooperação no domínio da Defesa do Consumidor: regras de funcionamento», mencionado na Secção 3.1.2, *infra*.

3.1.2. Encerramento dos casos em tempo útil

16. A segunda alteração do CPC não estabelece uma data-limite obrigatória para o encerramento dos casos que envolvam um pedido de assistência mútua (pedido de informação ou pedido de aplicação da lei).
17. No parecer de controlo prévio, a AEPD toma nota de várias medidas pragmáticas que a Comissão está a tomar para que os casos pendentes possam ser encerrados em tempo útil.
18. No presente parecer, a AEPD recomenda que se estabeleçam prazos máximos para os pedidos de informação e os pedidos de aplicação da lei. Esses prazos devem ser especificados no quadro legislativo, aquando da sua próxima revisão. Os prazos estabelecidos devem estar ligados ao tipo de caso bem como à actividade propriamente dita. Simultaneamente, as regras também devem proporcionar às autoridades competentes a flexibilidade necessária para prolongarem os casos por motivos razoáveis, a fim de que estes não sejam encerrados prematuramente, mesmo que um caso complexo demore mais a encerrar do que a média.
19. Para este efeito, a AEPD recomenda que se utilize como ponto de partida o documento intitulado «Rede de Cooperação no domínio da Defesa do Consumidor: regras de funcionamento», que o Comité CPC aprovou em 6 de Dezembro de 2010. No ponto 2.7 das regras de funciona-

mento, intitulado «*fases e prazos num caso CPC*», analisam os casos típicos e indicam que os pedidos de informação devem ser tratados, em média, num período de um a três meses. O tratamento dos pedidos de aplicação da lei, segundo as regras de funcionamento, deve ser exequível num período de seis a nove meses, em média (excepto no caso das injunções, ou num processo de recurso contra uma decisão administrativa, em que será mais realista prever um ano ou mais).

3.1.3. Alertas

20. A segunda alteração do CPC introduziu um novo parágrafo no ponto 2.2.2 do anexo da Decisão de aplicação do CPC exigindo que os alertas «com fundamento» sejam removidos da base de dados cinco anos depois de serem emitidos (quanto aos alertas «sem fundamento», as disposições existentes já exigiam que fossem eliminados assim que se constate que «o alerta é infundado»).
21. Para contextualizar esta nova disposição, a AEPD salienta que uma das suas principais preocupações é garantir que os dados pessoais não permanecem na base de dados do CPCS por mais tempo do que o necessário. Trata-se de uma questão sensível, em especial no que diz respeito aos alertas (que têm mais destinatários do que as trocas de informações bilaterais) e, entre os alertas, sobretudo aos que se referem a suspeitas de infracção. Na prática, a falta de um prazo claro para a manutenção do alerta em aberto levaria a que alguns alertas pudessem continuar pendentes por um período excessivamente longo (enquanto não se provar claramente que são infundados). Essas acções baseadas em suspeitas não confirmadas implicariam riscos significativos para o direito fundamental à protecção dos dados, bem como para outros direitos fundamentais, como a presunção de inocência.
22. Neste contexto, a AEPD constata com satisfação que foi estabelecido um prazo de conservação para os alertas. Considera, todavia, que a Comissão não forneceu uma justificação adequada para mostrar que um período de conservação de cinco anos seria proporcionado. A AEPD recomenda que a Comissão realize uma avaliação da proporcionalidade e reexamine a duração do período de conservação relativo aos alertas. Em princípio, todos os alertas notificados devem ser eliminados da base de dados muito mais cedo, a não ser que um alerta de infracção ou suspeita de infracção tenha conduzido a um pedido de assistência mútua e as medidas transfronteiriças de investigação ou de aplicação da lei ainda estejam em curso. O período de conservação deve ser suficientemente longo para permitir que cada autoridade que receba a mensagem decida se deseja tomar outras medidas de investigação ou de aplicação da lei, e se deseja ou não enviar um pedido de assistência mútua através do CPCS; contudo, deverá ser suficientemente curto para minimizar os riscos de os alertas poderem ser indevidamente utilizados para estabelecer listas negras ou fazer prospecção de dados.

23. Nesta perspectiva, a AEPD recomenda que a Comissão reveja o quadro normativo para que os alertas sejam eliminados o mais tardar no prazo de seis meses após a sua introdução, a não ser que seja possível justificar outro período de conservação mais adequado.
24. Esta medida deverá contribuir para assegurar, em especial, que, nos casos em que a suspeita não foi confirmada (ou mesmo objecto de investigação posterior), as pessoas inocentes ligadas à suspeita não ficam incluídas numa «lista negra» ou «sob suspeita» por um período excessivamente longo, o que não estaria em conformidade com o artigo 6.º, alínea e), da Directiva 95/46/CE.
25. Esta limitação é igualmente necessária para garantir o princípio da qualidade dos dados [ver artigo 6.º, alínea d), da Directiva 95/46/CE], bem como outros princípios jurídicos importantes. Assim, não só as pessoas poderão ser mais adequadamente protegidas, como se permitirá também que os funcionários responsáveis pela aplicação da lei se concentrem mais eficazmente nos casos relevantes.
- 3.1.4. *Período de conservação para os pedidos de assistência mútua encerrados*
26. A segunda alteração do CPC aditou um novo parágrafo ao ponto 2.15 do anexo da Decisão de aplicação do CPC para exigir que «qualquer outra informação relativa a pedidos de assistência mútua nos termos do artigo 6.º do (Regulamento CPC) é removida da base de dados cinco anos após o encerramento do caso».
27. Lido em conjunto com o texto existente, o ponto 2.15 revisto exige a conservação, durante cinco anos após o encerramento do caso, de todas as informações trocadas ao abrigo do artigo 6.º, excepto:
- Se os dados inexactos tiverem sido eliminados,
 - Se a troca de informações não tiver gerado um alerta ou um pedido de aplicação da lei, ou
 - Se tiver sido determinado que não houve infracção na aceção do Regulamento CPC.
28. Na verdade, tal como se explica no parecer de controlo prévio, o tempo de conservação «normal» aplicado no CPCS após o encerramento de um caso (salvo excepções específicas) parece ser de cinco anos tanto para os pedidos de informação como para os pedidos de aplicação da lei.
29. O texto da Decisão de aplicação do CPC, alterada pela segunda alteração do CPC, não parece ser inteiramente coerente com o Regulamento CPC. Em especial, o artigo 10.º, n.º 2, do referido regulamento estabelece uma distinção entre, por um lado, as informações trocadas que levam a uma aplicação eficaz da lei (ou seja, os casos em que a infracção cessou em resultado das medidas adoptadas) e, por outro lado, as informações que não produzem esse efeito. Em relação às primeiras, prevê-se um período de conservação de cinco anos após o encerramento do caso. Relativamente às segundas, não são estabelecidas disposições específicas (excepto que os alertas infundados devem ser removidos e suprimidos).
30. Por outras palavras, o Regulamento CPC só exige um período de conservação de cinco anos após o encerramento de um caso se tiverem sido tomadas medidas de aplicação da lei e se estas tiverem feito cessar a infracção.
31. Embora a AEPD tenha dúvidas quanto à finalidade e à proporcionalidade da conservação de quaisquer dados durante cinco anos após o caso ter sido encerrado (ver as observações formuladas mais adiante na presente Secção 3.1.4), a distinção entre os casos que terminaram com uma aplicação eficaz da lei e os que não terminaram dessa forma tem alguma lógica do ponto de vista da protecção de dados. Em especial, a conservação, por um longo período, de dados relativos a simples suspeitas tem maior potencial para ser incorrecta e corre também o risco de violar outros princípios jurídicos importantes. Por conseguinte, pode afirmar-se, em termos gerais, que a conservação desses dados por um longo período é mais susceptível de suscitar problemas de protecção de dados do que a conservação de dados relativos a infracções concretas, que tenham sido devidamente comprovadas e conduzido à adopção de medidas de aplicação da lei.
32. Ao contrário do Regulamento CPC, afigura-se que a Decisão de aplicação do CPC, alterada, permite, pelo menos em alguns casos, que o período de conservação de cinco anos também seja aplicável a informações que não conduziram a medidas eficazes de aplicação da lei.
33. Por exemplo, nos termos da Decisão de aplicação do CPC, um pedido de informação que tenha suscitado um alerta mas não medidas de aplicação da lei parece permanecer no sistema durante cinco anos após o «encerramento do caso».

34. O Regulamento CPC e a Decisão de aplicação do CPC parecem seguir, assim, uma abordagem algo diferente. A Decisão de aplicação do CPC, embora reflecta, em alguma medida, as disposições do Regulamento CPC, também introduz outras regras importantes em relação à conservação. Ainda que a clarificação das regras seja, em si mesmo, positiva, a AEPD questiona a legalidade de se fixarem períodos de conservação mais longos, quando tal não era já exigido no Regulamento CPC. Seriam, assim, impostas restrições adicionais ao direito fundamental à protecção de dados, e isto na legislação de aplicação, contrariando o Regulamento CPC e a legislação aplicável em matéria de protecção de dados.

35. À luz destas considerações, a AEPD recomenda que a Comissão reveja o quadro normativo e reexamine se o período de conservação de cinco anos deve ser aplicável a outros casos para além daqueles em que houve uma aplicação eficaz da lei, como é indicado no Regulamento CPC.

36. A AEPD verifica ainda com satisfação que as orientações sobre a protecção de dados no sistema CPC pretendem especificar a finalidade da conservação após o encerramento dos casos, uma questão importante que não foi abordada nem pelo Regulamento CPC nem pela segunda alteração do CPC. As orientações sobre a protecção de dados no sistema CPC dispõem, designadamente, que «Durante o período de retenção, os funcionários responsáveis da autoridade competente a quem o caso foi entregue podem ser autorizados a consultar o ficheiro respectivo para investigar possíveis padrões de infracção e contribuir, assim, para reforçar a eficiência da aplicação da lei»⁽¹⁾.

37. No entanto, embora esta clarificação seja louvável, sem outras justificações da necessidade desse acesso, a AEPD não está persuadida que de esta finalidade seja proporcional e suficiente para justificar o período de conservação de cinco anos. Por conseguinte, recomenda que a Comissão:

— Esclareça melhor a finalidade do período de cinco anos para a conservação dos dados;

— Avalie se um período de conservação mais curto permitiria atingir os mesmos objectivos; e

⁽¹⁾ Ver Secção 8 das Orientações, «Orientação adicional; Por que está a retenção de dados fixada em cinco anos?» As orientações sobre a protecção de dados no sistema CPC acrescentam ainda que «O objectivo de um período de retenção é facilitar a cooperação entre as autoridades públicas responsáveis pela aplicação das leis em matéria de defesa do consumidor no âmbito do tratamento das infracções intracomunitárias e contribuir para o bom funcionamento do mercado interno, para a qualidade e coerência de aplicação dessas leis, supervisionar a defesa dos interesses económicos dos consumidores e contribuir para aumentar o nível e a coerência dessa aplicação».

— Analise se é necessário conservar todas as informações actualmente previstas ou se um subconjunto dessas informações seria suficiente (ou seja, deve analisar-se se seria suficiente conservar apenas as notificações a que o artigo 8.º, n.º 6, se refere e também importa avaliar especificamente se a conservação dos nomes de directores ou de anexos que possam conter dados pessoais adicionais é necessária, bem como estabelecer uma distinção entre os dados relativos a suspeitas de infracção e os referentes a infracções «comprovadas»).

3.2. O acesso da Comissão aos dados contidos no CPCS

38. A AEPD verifica com agrado que (através da introdução do novo ponto 4.3 no anexo da Decisão de aplicação do CPC) a segunda alteração do CPC clarifica o acesso da Comissão aos dados contidos no CPCS e que esse acesso está clara e especificamente limitado ao que é exigido pelo Regulamento CPC. A AEPD constata com particular satisfação que a Comissão não tem acesso às comunicações confidenciais entre as autoridades competentes dos Estados-Membros, como é o caso dos pedidos de assistência mútua.

39. Esta clarificação e esta limitação são particularmente importantes, uma vez que a falta de clareza poderia conduzir a uma situação em que a Comissão teria a possibilidade de aceder a informações, incluindo dados pessoais, que são exclusivamente destinados às autoridades competentes dos Estados-Membros.

40. Tal como é indicado na Secção 5 das orientações sobre a protecção de dados no sistema CPC, «o objectivo do acesso da Comissão é acompanhar a aplicação do Regulamento CPC, bem como a legislação em matéria de defesa do consumidor referida no anexo do Regulamento CPC, e compilar informação estatística relacionada com o desempenho desses deveres».

41. Isto não significa que a Comissão deva ter acesso a todos e quaisquer dados trocados entre os Estados-Membros no âmbito do CPCS.

42. Na verdade, a AEPD salienta que o acesso a bases de dados como a do CPCS está abrangido pela definição de tratamento de dados pessoais. Nos termos do artigo 5.º, alínea a), do Regulamento (CE) n.º 45/2001, que é relevante para os direitos de acesso da Comissão no âmbito do CPCS, as instituições só podem tratar dados pessoais se isso for necessário ao exercício de funções de interesse público, acrescentando-se ainda que o tratamento se baseia nos Tratados ou no seu direito derivado.

43. A AEPD entende destes requisitos — que decorrem directamente do direito à protecção de dados consagrado no artigo 8.º da Convenção Europeia dos Direitos do Homem e nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia — que a Comissão só pode ter acesso aos sistemas de informação dos Estados-Membros se este estiver previsto em disposições jurídicas específicas, fundamentadas numa base jurídica totalmente adequada (normalmente no processo legislativo ordinário). A segurança jurídica e a transparência são os dois valores subjacentes que explicam por que razão o facto de o acesso da Comissão ter uma base jurídica específica e segura constitui uma garantia particularmente importante de que os direitos fundamentais das pessoas em matéria de protecção de dados serão respeitados.

44. Nem a competência geral de controlo da Comissão como «guardião do Tratado», nem a obrigação dos Estados-Membros de garantirem uma cooperação leal são suficientemente precisos para que a Comissão possa ter acesso a bases de dados que contenham dados pessoais. A cooperação leal implica que os Estados-Membros devem fornecer informações à Comissão — em determinadas condições — quando solicitados a fazê-lo ou quando são obrigados a fornecer informações ao abrigo de uma regra específica. Contudo, não implica que a Comissão tenha acesso às suas bases de dados.

45. Neste contexto, a AEPD salienta igualmente que o Regulamento CPC exclui a possibilidade de a Comissão ter acesso às informações contidas nos pedidos de assistência mútua e de aplicação da lei. O artigo 6.º e o artigo 8.º do Regulamento CPC apenas designam a autoridade requerida, e não a Comissão, como destinatária desses dados.

3.3. Categorias específicas de dados no CPCS

46. A AEPD está satisfeita por a segunda alteração do CPC ter introduzido, no ponto 4.4 do anexo da Decisão de aplicação do CPC, uma disposição relativa ao tratamento de categorias específicas de dados no CPCS. Considera particularmente positivo que a disposição limite esse tratamento aos casos em que o cumprimento das obrigações previstas pelo Regulamento CPC seja «de outra forma impossível» e que o tratamento desses dados esteja sujeito à condição suplementar de ser «permitido ao abrigo da Directiva 95/46/CE».

IV. PRIVACIDADE DESDE A CONCEPÇÃO E RESPONSABILIZAÇÃO

47. Depois de analisar, na Parte III, as questões específicas suscitadas pela segunda alteração do CPC, nas Partes IV a VI, a AEPD deseja chamar a atenção da Comissão para outros aspectos que devem ser considerados no desenvolvimento futuro do quadro normativo do CPCS.

4.1. Privacidade desde a concepção

48. Há algum tempo que a AEPD vem incentivando a Comissão e outras instituições da UE a adoptarem medidas tecnológicas e organizativas que integrem a protecção e a segurança dos dados como elemento fundamental da concepção e execução dos seus sistemas de informação («privacidade desde a concepção») ⁽¹²⁾.

49. Embora se congratule e reconheça que foram tomadas algumas medidas nesse sentido, a AEPD recomenda que a Comissão faça uma avaliação exaustiva das garantias em matéria de privacidade desde a concepção que podem ser incorporadas na arquitectura do sistema CPCS. Entres outras, devem ponderar-se e implementar-se as seguintes, na medida do necessário:

— Soluções de privacidade desde a concepção para orientar os utilizadores do sistema na adopção de decisões «adequadas» em matéria de protecção de dados (ver Secção 3.2 do Parecer de Controlo Prévio);

— Medidas para facilitar o encerramento e a eliminação atempados dos casos (*idem*, Secção 3.3);

— Procedimentos para facilitar os direitos de informação e de acesso das pessoas em causa (*idem*, Secção 3.5);

— Procedimentos claros em relação a qualquer alteração directamente realizada a nível da base de dados, ao acesso ao registo, às razões da acção e à aprovação a um nível adequado (*idem*, Secção 3.6); e

— Armazenamento «cifrado» das informações na base de dados, para que os operadores de TI não lhes possam aceder (pelo menos a alguns dados, como os anexos confidenciais) (*idem*, Secção 3.6).

4.2. Responsabilização

50. A AEPD recomenda ainda, em conformidade com o princípio da «responsabilização» ⁽¹³⁾, a criação de um quadro claro neste domínio, que garanta o cumprimento da legislação relativa à protecção de dados e forneça elementos que o comprovem, nomeadamente:

⁽¹²⁾ Ver Secção 7 do Parecer da AEPD sobre a 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», emitido em 14 de Janeiro de 2011 (http://www.AEPD.europa.eu/AEPDWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

⁽¹³⁾ *Idem*.

- Adopção e actualização, na medida do necessário, de uma política de protecção de dados aprovada ao mais alto nível de gestão na DG SANCO. Esta política de protecção de dados também deve incluir um plano de segurança (ver Secção 3.6 do Parecer de Controlo Prévio) ⁽¹⁴⁾.
- Realização de auditorias periódicas para avaliar a adequação continuada e a conformidade com a política de protecção de dados (incluindo auditorias do plano de segurança, *idem*, Secção 3.6).
- Divulgação (pelo menos parcial) dos resultados dessas auditorias para tranquilizar as partes interessadas quanto ao cumprimento das regras de protecção de dados; e
- Notificação dos casos de violação dos dados e outros incidentes de segurança ao responsável pela protecção de dados (RPD) da Comissão e às pessoas em causa (bem como a outras partes interessadas e autoridades, se for caso disso) ⁽¹⁵⁾.

V. TRANSFERÊNCIA DE DADOS PESSOAIS PARA FORA DAS FRONTEIRAS DA UNIÃO EUROPEIA

5.1. Acordos bilaterais

51. O artigo 14.º, n.º 2, do Regulamento CPC dispõe que as informações comunicadas no seu âmbito também podem ser comunicadas a uma autoridade de um país terceiro, no quadro de um acordo bilateral de assistência celebrado com esse país, desde que i) a autoridade competente que inicialmente comunicou as informações tenha dado o seu acordo e que ii) a transferência esteja de acordo com a legislação da UE aplicável em matéria de protecção de dados.
52. Os artigos 25.º e 26.º da Directiva 95/46/CE sujeitam as transferências para países terceiros a certas condições adicionais, destinadas a assegurar que os dados serão adequadamente protegidos no estrangeiro. Além disso, também prevêm várias excepções. A aplicação e a interpretação dessas disposições da Directiva 95/46/CE podem diferir de um Estado-Membro para outro.
53. À luz do que precede, a AEPD pode aceitar as garantias contidas no Regulamento CPC, nomeadamente, que qualquer transferência para um país terceiro está sujeita i) ao acordo da autoridade competente que inicialmente comunicou as informações e ii) à legislação aplicável da UE em matéria de protecção de dados.

⁽¹⁴⁾ A Comissão também deve ponderar, na medida do necessário, a realização de uma avaliação, pelo menos, parcial da protecção de dados e da privacidade, centrada na finalidade, na duração e nas modalidades do período de conservação e, eventualmente, debater outras questões pendentes que ainda não foram tratadas de forma aprofundada.

⁽¹⁵⁾ Ver Secção 6.3 do Parecer da AEPD de 14 de Janeiro de 2011 acima referido.

54. A AEPD também constata com agrado que as orientações sobre a protecção de dados no sistema CPC recomendam que qualquer acordo de assistência bilateral com um país terceiro — salvo se se considerar que o referido país garante um nível de protecção adequado — deve prever salvaguardas de protecção de dados adequadas e — se necessário — ser notificado às autoridades de supervisão relevantes em matéria de protecção de dados.
55. Contudo, as disposições do Regulamento CPC não são as ideais. A sua aplicação é complexa: uma autoridade competente que tenha de decidir sobre a transferência de informações para um país terceiro necessitará de ter em conta não só o acordo bilateral do seu próprio país com o país terceiro, a sua própria legislação nacional em matéria de protecção de dados e a sua própria avaliação da adequação da transferência de dados para o país terceiro em causa, com base nessa legislação, mas também se as outras autoridades competentes que contribuíram para o conteúdo do ficheiro (e podem ser várias) deram ou não o seu acordo, com base nas suas próprias legislações em matéria de protecção de dados.

56. Do ponto de vista da protecção de dados, esta complexidade gera incertezas quanto aos direitos da pessoa em causa e, sobretudo, quanto à transferência ou não dos seus dados para o estrangeiro e às condições em que é efectuada. As pessoas em causa também não estão a beneficiar, na medida do possível, de uma legislação europeia sólida e harmonizada neste domínio. Além disso, do ponto de vista das autoridades competentes, esta complexidade também é susceptível de entravar a cooperação entre as autoridades competentes e constitui uma sobrecarga administrativa.
57. A AEPD incentiva, assim, a celebração de acordos a nível da UE que prevejam garantias adequadas em matéria de protecção de dados e que, simultaneamente, ajudem a evitar a aplicação de critérios heterogéneos e o consequente aumento da carga administrativa para as autoridades competentes.

5.2. Acordos a nível da UE

58. Para além da possibilidade prevista no artigo 14.º em relação à cooperação bilateral, o artigo 18.º do Regulamento CPC sobre os acordos internacionais também dispõe que a «Comunidade colaborará com países terceiros e com as organizações internacionais competentes» e que «as disposições em matéria de cooperação, incluindo a criação de disposições de assistência mútua, podem ser objecto de acordos entre a Comunidade e os países terceiros interessados».

59. Pelas razões apresentadas na Secção 5.1, a AEPD apoia a Comissão na sua iniciativa de negociar e celebrar acordos a nível da UE, com garantias adequadas de protecção de dados, harmonizadas a nível da União, para substituir os acordos bilateral existentes.
60. O seu apoio à celebração desses acordos a nível da União Europeia está, todavia, sujeito à condição de a Comissão e os legisladores da UE se comprometerem a assegurar o mais elevado nível de protecção no intercâmbio de dados pessoais com os países terceiros. As implicações dos acordos de cooperação internacional com países terceiros devem ser cuidadosamente analisadas do ponto de vista da protecção de dados, devem estabelecer-se regras claras para esse intercâmbios e devem fornecer-se garantias adequadas em matéria de protecção de dados, com base numa consulta à AEPD e, se for caso disso, às autoridades nacionais de protecção de dados.
61. Embora o artigo 18.º do Regulamento CPC não aborde especificamente a questão do acesso directo ao CPCS pelas autoridades de países terceiros, este pode ser tecnicamente possível. A AEPD não deseja desencorajar a inclusão no CPCS de novas funcionalidades destinadas a permitir um acesso estritamente limitado e selectivo por parte das autoridades competentes de países terceiros, através de um mecanismo especificamente concebido (canal e interface de comunicação). Essa evolução poderia aumentar, efectivamente, a eficiência da cooperação.
62. Todavia, esse acesso directo tem os seus riscos e, por esse motivo, as suas implicações em matéria de protecção de dados, bem como as disposições e salvaguardas técnicas e organizativas necessárias, devem ser especificamente abordadas. Qualquer dessas funcionalidades técnicas deve ser incorporada em conformidade com os princípios de «privacidade desde a concepção», e a segurança também deve constituir uma clara prioridade. Por último, a AEPD deve ser consultada, bem como, se necessário, as autoridades nacionais de protecção de dados.

VI. «DIREITOS DE PROTECÇÃO DE DADOS DO CONSUMIDOR» E COOPERAÇÃO REFORÇADA DAS AUTORIDADES RESPONSÁVEIS PELA PROTECÇÃO DE DADOS, ATRAVÉS DO CPCS

63. Desde que as recomendações da AEPD (incluindo as do seu Parecer de Controlo Prévio) sejam seguidas, a AEPD está segura de que o CPCS poderá ser um instrumento eficaz e favorável à protecção de dados para a aplicação da lei a nível transfronteiras, contra a violação dos direitos dos consumidores no mercado interno.
64. Com o desenvolvimento do comércio electrónico e a crescente utilização das redes de comunicações electrónicas pelos consumidores de vários produtos e serviços, serão tratados cada vez mais dados pessoais referentes a essas

pessoas. É, pois, possível que os consumidores venham a enfrentar também um número crescente de infracções aos seus direitos de protecção de dados. Consequentemente, também é necessário que as autoridades responsáveis pela protecção de dados cooperem eficazmente para pôr termo a tais infracções.

65. Entre os casos mais comuns de violação dos «direitos de protecção de dados do consumidor» figuram as comunicações comerciais não solicitadas (*spam*), o roubo de identidade, a determinação ilegal de perfis, a publicidade comportamental ilícita e casos de violação dos dados (violações da segurança).
66. Uma vez que é provável que o número de casos de natureza transfronteiras aumente na sociedade da informação, a AEPD exorta a Comissão a ponderar a adopção de possíveis medidas legislativas para salvaguardar os «direitos de protecção de dados do consumidor» e a reforçar a cooperação transfronteiras entre as autoridades competentes: tanto as responsáveis pela protecção de dados como as autoridades de defesa do consumidor.
67. Em especial, e enquanto se consideram outras opções possíveis, deve ser cuidadosamente analisado se é conveniente permitir que as autoridades responsáveis pela protecção de dados acedam ao CPCS em função das suas necessidades, a fim de cooperarem entre si e com outras autoridades competentes que já tenham acesso ao sistema.
68. O acesso por parte das autoridades responsáveis pela protecção de dados deve estar claramente limitado ao estritamente necessário para o exercício das respectivas funções nos seus domínios de competência e ser conforme com as sinergias identificadas. Naturalmente, importa assegurar que o quadro para a participação dessas autoridades seja concebido de forma a ter devidamente em conta a sua independência.

VII. CONCLUSÕES

69. A AEPD verifica com agrado que o CPCS assenta numa base jurídica que também prevê garantias específicas em matéria de protecção de dados. Para solucionar eventuais preocupações remanescentes nessa matéria, a AEPD faz notar que as recomendações a seguir sintetizadas devem ser tomadas em consideração aquando da próxima revisão do quadro normativo do CPCS.
70. Entretanto, algumas medidas suplementares tomadas ao nível prático, técnico e organizativo (tal como é recomendado no Parecer de Controlo Prévio) podem fornecer uma solução parcial provisória para essas preocupações. Enquanto se aguardam as alterações legislativas, também podem ser introduzidas algumas alterações através das regras de funcionamento do CPCS.

71. No que respeita ao período de conservação, a AEPD recomenda que i) os pedidos de assistência mútua sejam encerrados em prazos especificamente fixados; ii) salvo se houver uma investigação ou uma acção de aplicação da lei em curso, os alertas devem ser removidos e suprimidos no prazo de seis meses a contar da sua emissão (salvo se for possível justificar outro período de conservação mais adequado); e iii) a Comissão deve clarificar e reexaminar a finalidade e a proporcionalidade de conservar todos os dados relativos a casos encerrados por mais cinco anos.
72. Além disso, a AEPD constata com agrado que a segunda alteração do CPC clarifica o acesso da Comissão aos dados contidos no CPCS. Em especial, a AEPD manifesta satisfação por a Comissão não ter acesso às comunicações confidenciais entre as autoridades competentes de Estados-Membros, como é o caso dos pedidos de assistência mútua.
73. Também apraz à AEPD que a segunda alteração do CPC tenha introduzido uma disposição relativa ao tratamento de categorias específicas de dados no CPCS.
74. Complementarmente, a AEPD recomenda que a Comissão reavalie as medidas técnicas e organizativas adicionais a tomar para garantir a incorporação da privacidade e da protecção de dados na arquitectura do sistema CPCS desde

a concepção («privacidade desde a concepção») e a existência de controlos adequados para assegurar o cumprimento da legislação em matéria de protecção de dados e fornecer elementos que o comprovem («responsabilização»).

75. Além disso, caso se celebre um acordo a nível da UE entre a União Europeia e um país terceiro para reger a cooperação em matéria de defesa dos consumidores, as respectivas implicações devem ser cuidadosamente ponderadas, o intercâmbio de dados deve ser sujeito a regras claras e devem adoptar-se salvaguardas adequadas de protecção dos dados.
76. Por último, a AEPD recomenda que a Comissão explore as eventuais sinergias que possam surgir se for permitido que as autoridades responsáveis pela protecção de dados se juntem à comunidade de utilizadores do CPCS para cooperarem na aplicação dos «direitos de protecção de dados do consumidor».

Feito em Bruxelas, em 5 de Maio de 2011.

Giovanni BUTTARELLI
*Autoridade Adjunta Europeia para a Protecção
de Dados*