GRUPO DE TRABALHO DE PROTECÇÃO DE DADOS DO ARTIGO 29.º

00062/10/PT
WP 173

Parecer 3/2010 sobre o princípio da responsabilidade

Adoptado em 13 de Julho de 2010

RESUMO

Os princípios e as obrigações da UE em matéria de protecção de dados encontram-se muitas vezes reflectidos de forma insuficiente nas medidas e práticas internas concretas. A menos que a protecção dos dados se torne parte das práticas e valores partilhados de determinada organização e a responsabilidade por essa protecção seja expressamente atribuída, a verdadeira conformidade correrá um risco considerável, sendo provável que continuem a ocorrer incidentes relacionados com a protecção de dados.

O quadro jurídico da UE necessita de instrumentos adicionais para promover a protecção de dados na prática. O presente parecer tem por objectivo aconselhar a Comissão sobre a melhor forma de alterar a Directiva Protecção de Dados nesse sentido. O presente parecer apresenta em particular uma proposta concreta de um princípio sobre a responsabilidade que exigirá das autoridades responsáveis pelo tratamento de dados a aplicação de medidas adequadas e eficazes que garantam o respeito dos princípios e obrigações estabelecidos pela Directiva e, quando solicitado, a sua demonstração às autoridades de controlo. A aplicação deste princípio deve contribuir para que a protecção de dados passe da «teoria à prática» e ajudar as autoridades de protecção de dados nas suas tarefas de controlo e execução.

O parecer contém sugestões para garantir que o princípio da responsabilidade proporcione segurança jurídica e permita a adaptabilidade (ou seja, a determinação das medidas concretas a aplicar em função do risco do tratamento e do tipo de dados tratados). Examina igualmente o impacto que o princípio pode ter noutros domínios, incluindo as transferências internacionais de dados, os requisitos de notificação, as sanções e, eventualmente, o desenvolvimento de programas ou selos de certificação.

O Grupo de Trabalho sobre a protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais

Instituído pela Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995,

Tendo em conta o artigo 29.º e o artigo 30.º, n.º 1, alínea a), e n.° 3 da referida directiva, bem como o artigo 15.º, n.º 3 da Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002,

Tendo em conta o seu regulamento interno,

Adoptou o seguinte parecer:

1. INTRODUÇÃO

1. A protecção de dados tem de passar da «teoria à prática». Os requisitos jurídicos têm de ser traduzidos em medidas reais de protecção dos dados. O quadro jurídico da UE em matéria de protecção de dados necessita de mecanismos adicionais para incentivar a protecção de dados na prática. Nas discussões sobre o futuro do quadro europeu e global de protecção de dados foram sugeridos mecanismos baseados na responsabilização como forma de incentivar as autoridades responsáveis pelo tratamento de dados a aplicar instrumentos práticos para uma protecção de dados efectiva.

2. No documento sobre o futuro da privacidade (WP168), de Dezembro de 2009, o Grupo de trabalho do artigo 29.º considerou que o actual quadro jurídico não tem conseguido assegurar a tradução dos requisitos da protecção de dados em mecanismos eficazes que proporcionem uma protecção efectiva. Para obviar a essa situação, o Grupo de trabalho do artigo 29.º propôs à Comissão que ponderasse a adopção de mecanismos baseados na responsabilização, com especial destaque para a possibilidade de incluir um princípio de «responsabilidade» na revisão da Directiva Protecção de Dados,[1] considerando que esse princípio iria reforçar o papel do responsável pelo tratamento de dados e aumentar a sua responsabilidade.

[1] «Para resolver este problema, conviria introduzir um princípio da responsabilidade no quadro jurídico geral, que obrigasse os responsáveis pelo tratamento de dados a tomar as medidas necessárias para garantir que o tratamento de dados pessoais respeita as obrigações e os princípios essenciais da actual directiva. Uma disposição neste sentido reforçaria a necessidade de aplicar políticas e mecanismos que tornassem efectivos as obrigações e os princípios essenciais da actual directiva. Serviria para reforçar a necessidade de tomar medidas efectivas que resultassem numa aplicação interna efectiva das obrigações e princípios significativos actualmente consagrados na directiva. Além do mais, o princípio da responsabilidade exigiria que os responsáveis pelo tratamento de dados implementassem os mecanismos internos necessários para demonstrar a conformidade perante partes interessadas externas, incluindo as autoridades nacionais responsáveis pelo tratamento de dados. A resultante necessidade de apresentar provas da adequação das medidas tomadas para garantir a conformidade irá, em grande medida, facilitar a execução das normas aplicáveis» (WP168, ponto 79. Para mais informações, ver também os pontos 74-78).

3. Em resumo, um princípio da responsabilidade juridicamente vinculativo exigiria expressamente dos responsáveis pelo tratamento de dados a aplicação de medidas adequadas e eficazes para pôr em prática as obrigações e princípios da directiva e proceder à sua demonstração quando solicitado. Na prática, tal deve traduzir-se em programas adaptáveis destinados à aplicação dos princípios existentes em matéria de protecção de dados (por vezes referidos como «programas de conformidade»). Requisitos adicionais específicos, destinados a pôr em prática garantias de protecção dos dados ou a assegurar a sua eficácia, poderiam ser criados em complemento do princípio. Um exemplo seria uma disposição que obrigasse à realização de uma avaliação do impacto sobre a privacidade resultante das operações de tratamento de dados de maior risco.

4. O presente parecer, que pretende ser uma continuidade das contribuições anteriores do Grupo de trabalho do artigo 29.º relativamente a este tema formuladas no seu parecer sobre o futuro da privacidade visando aconselhar a Comissão na revisão em curso da Directiva 95/46, está dividido em quatro secções. A primeira, aborda a necessidade dos responsáveis pelo tratamento de dados fortalecerem as suas metodologias práticas internas (políticas e procedimentos) de forma a garantir que todos os procedimentos são realizados em conformidade com as regras aplicáveis e a forma como os sistemas baseados na responsabilidade podem contribuir para esse objectivo. Em seguida, explora a possível arquitectura jurídica de um sistema baseado na responsabilidade, bem como os precedentes na protecção de dados e noutros domínios. A segunda secção apresenta uma proposta concreta de um princípio da responsabilidade e descreve os argumentos lógicos subjacentes aos vários aspectos da proposta. A terceira secção examina os diversos elementos associados a um sistema jurídico que integre um sistema geral de responsabilidade. Inclui uma discussão sobre a necessidade da proposta proporcionar segurança jurídica, sendo ao mesmo tempo formulada em termos suficientemente abrangentes para permitir a adaptabilidade (ou seja, a determinação das medidas concretas a aplicar em função do risco do tratamento e do tipo de dados tratados). Examina por fim temas afins, como a relação com as transferências para o estrangeiro, descreve as vantagens de um mecanismo baseado na responsabilidade para as autoridades de protecção de dados e examina o possível papel da certificação.

II. RESPONSABILIDADE: OBJECTIVOS, ARQUITECTURA JURÍDICA, PRECEDENTES E TERMINOLOGIA

II.1 A responsabilidade como factor impulsionador da aplicação efectiva dos princípios de protecção dos dados

5. Actualmente, os responsáveis pelo tratamento de dados têm uma necessidade e um interesse crescente em garantir que tomam medidas efectivas para assegurar uma verdadeira protecção dos dados. Tal deve-se a vários motivos, que se analisam de seguida.

6. Em primeiro lugar, estamos a assistir a um efeito designado por «dilúvio de dados», em que o volume de dados existentes, processados e depois transferidos não cessa de crescer. Tanto os desenvolvimentos tecnológicos, ou seja, a expansão

dos sistemas de informação e comunicação, como a capacidade acrescida dos indivíduos para utilizar e interagir com as tecnologias, favorecem este fenómeno. O risco de violação de dados pessoais aumenta à medida que um número cada vez maior de dados fica disponível e circula no mundo. Esse facto sublinha ainda mais a necessidade de que os responsáveis pelo tratamento de dados, tanto no sector público como no privado, implementem mecanismos internos reais e efectivos para salvaguardar a protecção dos dados pessoais.

7. Em segundo lugar, o volume crescente de informação pessoal é acompanhado por um aumento do seu valor em termos económicos, políticos e sociais. Em alguns sectores, especialmente no ambiente em linha, os dados pessoais tornaram-se a verdadeira moeda de troca para os conteúdos em linha. Simultaneamente, de um ponto de vista societal, há um crescente reconhecimento da protecção de dados enquanto valor social. Em resumo, com o aumento do valor da informação pessoal para os responsáveis pelo tratamento de dados de todos os sectores, os cidadãos, consumidores e sociedade em geral estão também cada vez mais conscientes do seu significado, o que, por sua vez, reforça a necessidade de aplicar medidas rigorosas para a protecção dessa informação.

8. Por último, depreende-se dos factos acima referidos que a violação de informação pessoal poderá ter efeitos negativos significativos para os responsáveis pelo tratamento de dados nos sectores público e privado. Potenciais falhas nas aplicações da administração em linha e da saúde em linha teriam consequências nefastas a nível económico e especialmente em termos de imagem. Portanto, minimizar os riscos, construir e manter uma boa reputação e garantir a confiança dos cidadãos e consumidores, está a tornar-se essencial para os responsáveis pelo tratamento de dados em todos os sectores.

9. Em resumo, estes factos revelam como é absolutamente fundamental que os responsáveis pelo tratamento de dados apliquem medidas de protecção de dados eficazes visando uma boa governação na matéria, e que simultaneamente minimizem os prováveis riscos jurídicos, económicos e em termos de imagem decorrentes de práticas de protecção deficientes. Como se exporá mais adiante, os mecanismos baseados na responsabilidade visam atingir esses objectivos.

II.2 Uma possível arquitectura jurídica global dos mecanismos baseados na responsabilidade

10. Neste contexto, importa debater, entre outras questões, de que forma o quadro jurídico poderia incentivar os responsáveis pelo tratamento de dados a tomarem medidas que, na prática, resultassem numa protecção real, ou seja, que configuração deve ter a arquitectura jurídica de um sistema baseado na responsabilidade.

11. Como observação preliminar à discussão dessa arquitectura, importa sublinhar que, à partida, os referidos sistemas, longe de alterarem ou afectarem os princípios fundamentais da protecção de dados, são concebidos para os pôr a funcionar com maior eficácia.

12. O aditamento de um princípio da responsabilidade à versão revista da Directiva seria uma forma de persuadir os responsáveis pelo tratamento de dados a aplicar essas medidas. A aplicação de medidas e procedimentos internos que aplicassem os princípios existentes de protecção de dados, garantindo a sua eficácia e a obrigação de o demonstrar caso as autoridades de protecção de dados o requeiram, seriam os efeitos previsíveis da adopção da medida. Como se descreve mais adiante, o tipo de procedimentos e mecanismos dependeria dos riscos representados pelo tratamento e natureza dos dados.

13. Poderia reflectir-se ainda sobre requisitos específicos, como a obrigação de realizar avaliações do impacto na privacidade em determinados casos ou a nomeação de profissionais em matéria de protecção de dados. Esses requisitos específicos podiam completar o princípio geral de responsabilidade.

14. O Grupo de trabalho do artigo 29.º reconhece que os responsáveis pelo tratamento de dados poderão querer aplicar políticas e procedimentos que não se encontram especificamente previstos na legislação em matéria de protecção de dados. Por exemplo, um responsável pelo tratamento de dados poderá querer comprometer-se a responder a pedidos de acesso dentro de prazos muito curtos, apesar de a lei permitir uma certa flexibilidade. Poderá ainda querer comprometer-se a responder a pedidos de acesso simultaneamente em linha e fora de linha, de forma a garantir a recepção rápida e eficaz da informação. Seria também possível imaginar situações em que o responsável pelo tratamento de dados deseja exceder os requisitos mínimos definidos no quadro jurídico geral. Por exemplo, um responsável pelo tratamento de dados poderá decidir nomear um profissional em matéria de protecção de dados apesar de não ser obrigatório pela lei em vigor. Um responsável pelo tratamento de dados poderá ainda querer contratar terceiros para executar auditorias a *todas* as suas operações de tratamento de dados, para avaliar a sua conformidade com o quadro jurídico em matéria de protecção de dados. O Grupo de trabalho do artigo 29.º elogia essas iniciativas e desejaria que o novo quadro jurídico em matéria de protecção de dados incentive os responsáveis pelo tratamento de dados a tomarem tais medidas.

15. Na sequência do acima exposto, a «arquitectura jurídica» dos mecanismos de responsabilidade devia prever dois níveis: o primeiro consistiria num requisito jurídico básico vinculativo para *todos* os responsáveis pelo tratamento de dados. O conteúdo do requisito incluiria dois elementos: a aplicação de medidas/procedimentos e a manutenção da necessidade de comprovação. Esse primeiro nível podia ser completado por requisitos específicos. Um segundo nível incluiria sistemas de responsabilidade voluntários, mais abrangentes que os requisitos jurídicos mínimos, a nível dos princípios de protecção de dados subjacentes (proporcionando garantias mais elevadas que as exigidas pela lei em vigor) e/ou da forma como implementam ou asseguram a eficácia das medidas (aplicação de requisitos que vão além do nível mínimo). Apesar de reconhecer a importância e os benefícios de tais sistemas, o presente parecer debruça-se principalmente sobre os requisitos do primeiro nível e, em especial, sobre o princípio geral de responsabilidade.

II.3 O princípio da responsabilidade em matéria de protecção de dados e noutros domínios, terminologia

Precedentes

16. O Grupo de trabalho do artigo 29.º nota que o princípio da responsabilidade não é propriamente novo. O seu reconhecimento explícito consta das linhas directrizes da Organização de Cooperação e Desenvolvimento Económico (OCDE) regulamentadoras da protecção da vida privada, adoptadas em 1980. O seu princípio da responsabilidade estabelece que os responsáveis pelo tratamento de dados devem prestar contas relativamente ao cumprimento das medidas que põem em prática os princípios [materiais] acima enunciados.

17. Recentemente, este princípio foi incluído de forma explícita nas normas internacionais de Madrid, elaboradas pela Conferência internacional de autoridades em matéria de protecção de dados e da vida privada[2]. O princípio da responsabilidade também está incorporado no recente projecto de norma ISO 29100, que estabelece um quadro jurídico para a privacidade e é igualmente um dos principais conceitos do quadro jurídico da APEC e das suas regras transfronteiras relativas à privacidade[3].

18. Numa perspectiva «regulamentar», o Grupo de trabalho do artigo 29.º recorda que os *Canadian Fair Information Principles*, incluídos na lei canadiana em matéria de dados pessoais e documentos electrónicos, fazem referência à responsabilidade. Entre outros, o primeiro princípio exige a elaboração e a implementação de políticas e práticas para o cumprimento dos dez princípios de informação justa, incluindo a aplicação de procedimentos para a protecção de informações pessoais e o estabelecimento de procedimentos para receber e dar resposta a dúvidas e reclamações.

19. O Grupo de trabalho do artigo 29.º observa ainda que as regras empresariais obrigatórias (Binding Corporate Rules - BCR), utilizadas no contexto das transferências internacionais de dados, reflectem o princípio da responsabilidade. Com efeito, as BCR são códigos de conduta, elaborados e respeitados por organizações multinacionais, que incluem medidas internas concebidas para pôr em prática os princípios da protecção de dados (como as auditorias, programas de formação, rede de profissionais em matéria de privacidade, gestão do sistema de reclamações). Uma vez revistas pelas autoridades nacionais encarregadas da protecção de dados, as BCR devem assegurar garantias adequadas para as transferências ou categorias de transferências de dados pessoais entre empresas

---

[2] A pessoa responsável deve: a) Adoptar todas as medidas necessárias ao cumprimento dos princípios e obrigações dispostos no presente documento e na legislação nacional aplicável, e b) possuir os mecanismos internos necessários para a demonstração desse cumprimento perante as pessoas em causa e perante as autoridades de controlo no exercício dos seus poderes, segundo o disposto na secção 23.

[3] Para além do acima referido, o Centre for Information Policy Leadership está envolvido numa iniciativa destinada a examinar os efeitos do princípio da responsabilidade no que diz respeito à protecção de dados e da privacidade. Consultar: www.informationpolicycentre.com

que integram o mesmo grupo empresarial e que estão vinculadas por essas regras por força do artigo 25.º e do artigo 26.º, n.º 2, da Directiva 95/46.

20. Fora do domínio da protecção de dados, existem alguns exemplos do princípio da responsabilidade, como um programa que especifica as políticas e os procedimentos dos responsáveis pelo tratamento de dados tendo em vista garantir o cumprimento de leis e regulamentos. Os regulamentos dos serviços financeiros, por exemplo, estipulam a obrigatoriedade de programas de conformidade. Noutros casos, embora não sendo obrigatórios, são incentivados os programas de conformidade, por exemplo no domínio da legislação em matéria de concorrência. No Canadá, a Autoridade da concorrência desenvolveu políticas detalhadas relativas aos programas de conformidade das empresas. Para as empresas, a decisão de aplicar um programa é voluntária. No entanto, a Autoridade canadiana da concorrência sublinha os benefícios da conformidade enquanto ferramenta de diminuição do risco, destacando ainda os benefícios económicos, jurídicos e em termos de imagem[4].

Terminologia

21. Em inglês utiliza-se o termo «accountability» (responsabilidade), que tem origem no mundo anglo-saxónico, onde o seu uso é comum e onde existe um consenso generalizado sobre o seu significado – apesar de ser complexo defini-lo na prática. Em termos gerais, porém, a ênfase recai na forma como a responsabilidade é assumida e na forma como torná-la verificável. Em inglês, «responsability» e «accountability» são as duas faces da mesma moeda, sendo ambas elementos essenciais de uma boa governação. Apenas quando se demonstra que a responsabilidade funciona efectivamente na prática, será possível assegurar uma confiança suficiente.

22. Na maioria das outras línguas europeias, devido principalmente a diferenças nos sistemas jurídicos, a tradução do termo «accountability» não é fácil, pelo que existe um risco significativo de interpretações divergentes e, consequentemente, de falta de harmonização. Foram sugeridas outras expressões e palavras em inglês para captar o sentido de «accountability», nomeadamente «reinforced responsibility» (responsabilidade reforçada), «assurance» (garantia), «reliability» (fiabilidade), «trustworthiness» (carácter do que é digno de confiança) e, em francês, a «obligation de rendre des comptes», etc. Pode também sugerir-se que a «accountability» remete para a «aplicação dos princípios de protecção dos dados».

23. Para efeitos do presente documento, centramo-nos portanto nas medidas que deviam ser tomadas ou previstas para garantir a conformidade no domínio da protecção de dados. As referências à «responsabilidade» devem portanto ser entendidas no sentido utilizado neste parecer, sem prejuízo de se encontrar outra expressão que reflicta de forma mais precisa o conceito aqui descrito. Por essa razão, o documento não se centra em termos, preferindo centrar-se de forma mais pragmática nas medidas que necessitam de ser tomadas e não no conceito em si.

---

4 www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

III. RUMO A UMA PROPOSTA DE DISPOSIÇÃO GERAL EM MATÉRIA DE RESPONSABILIDADE

III.1 Uma disposição geral visando reafirmar e reforçar a responsabilidade dos responsáveis pelo tratamento

24. O Grupo de trabalho do artigo 29.º examinou novamente a possibilidade de introduzir soluções baseadas na responsabilidade no novo e abrangente quadro jurídico em matéria de protecção de dados, à luz das considerações tecidas na secção I.

25. Essa reflexão confirmou a sua opinião, já expressa no parecer sobre o futuro da privacidade, de que um quadro legislativo novo e abrangente devia incluir um princípio geral de responsabilidade. Essa disposição teria por objectivo reafirmar e reforçar a responsabilidade dos que efectuam o tratamento de dados pessoais, sem prejuízo de eventuais medidas concretas de responsabilidade que completariam este princípio.

26. Essa disposição nova inscrever-se-ia na mesma linha de determinadas disposições já existentes no actual quadro legislativo. Podemos remeter em particular para o artigo 6.º da Directiva 95/46/CE, que refere os princípios relativos à qualidade dos dados no n.º 1, e menciona no n.º 2, que «incumbe ao responsável pelo tratamento assegurar a observância do disposto no n.º 1». Enquadra-se também no artigo 17.º, n.º 1, que exige dos responsáveis pelo tratamento de dados a aplicação de medidas de natureza técnica e organizacional. Com efeito, uma disposição geral de responsabilidade reforçaria a necessidade de respeitar os requisitos de segurança do artigo 17.º por parte dos responsáveis pelo tratamento de dados, para além dos requisitos exigidos nas restantes disposições.

III.2 Rumo a uma proposta concreta de um princípio geral de responsabilidade

27. A nova disposição teria como objectivo incentivar a adopção de medidas práticas e concretas, traduzindo os princípios gerais de protecção de dados em políticas e procedimentos concretos, definidos a nível do responsável pelo tratamento, em conformidade com a legislação e regulamentos aplicáveis. O responsável pelo tratamento também devia assegurar a eficácia das medidas tomadas e poder demonstrar, quando solicitado, que as colocou em prática.

28. De forma esquemática, esta disposição geral centrar-se-ia em dois elementos principais:

    (i) a necessidade de o responsável pelo tratamento tomar medidas adequadas e eficazes para aplicar os princípios de protecção de dados;
    (ii) a necessidade de demonstrar, quando solicitado, que foram tomadas medidas adequadas e eficazes. Por conseguinte, o responsável pelo tratamento teria de apresentar comprovativos relativamente à execução do ponto (i) supra.

29. A obrigação devia abranger todos os responsáveis pelo tratamento e todas as situações.

30. O primeiro elemento da obrigação exigiria que os responsáveis pelo tratamento de dados implementassem medidas adequadas. Os tipos de medidas visadas não seriam especificados no texto da disposição geral, mas directrizes subsequentes, emitidas pelas autoridades nacionais encarregadas da protecção de dados, pelo Grupo de trabalho do artigo 29.º ou pela Comissão (através dos procedimentos de comitologia) poderiam definir, em certos casos, um conjunto mínimo de medidas específicas consideradas adequadas. Um exemplo dessas medidas seria a adopção, em determinados casos, de políticas e procedimentos internos necessários à aplicação dos princípios de protecção de dados, que reflectiriam a legislação e os regulamentos aplicáveis.

31. Esses procedimentos e medidas também podiam ser implementados de forma eficaz através da atribuição de responsabilidades e da formação dos colaboradores envolvidos nas operações de tratamento. Em particular, e em conformidade com o artigo 18.º da Directiva, os responsáveis pelo tratamento devem ser incentivados a designar encarregados da protecção dos dados pessoais. Em todo o caso, deve incentivar-se a atribuição de responsabilidades a diferentes níveis da organização, de forma a assegurar o cumprimento dessas responsabilidades.

32. No que diz respeito às transferências de dados pessoais para países terceiros, os responsáveis pelo tratamento de dados devem adoptar e aplicar medidas adequadas, de forma a cumprir o requisito de «garantias suficientes», exigido pelo artigo 26.º da Directiva, de que são exemplo as BCR.

33. Os responsáveis pelo tratamento deviam ainda assegurar a eficácia das medidas adoptadas para cumprir os princípios da protecção de dados. Em caso de operações de tratamentos de dados mais volumosas, mais complexas ou de maior risco, a eficácia das medidas adoptadas devia ser verificada regularmente. Existem diversas formas de avaliar a eficácia (ou ineficácia) das medidas: monitorização, auditorias internas e externas, etc.

34. Na sequência dos comentários acima apresentados, o Grupo de trabalho do artigo 29.º examinou a questão da formulação de uma disposição concreta que podia ser introduzida num quadro legislativo abrangente com a seguinte redacção:

«Artigo 10.° – Aplicação dos princípios da protecção de dados

1. O responsável pelo tratamento de dados deve aplicar medidas adequadas e eficazes para garantir o respeito dos princípios e obrigações da directiva.
2 A pedido da autoridade de controlo, o responsável pelo tratamento de dados deve demonstrar que respeitou o disposto no n.º 1.»

IV. EXAME DOS VÁRIOS ELEMENTOS ASSOCIADOS AO PRINCÍPIO GERAL DE RESPONSABILIDADE

IV.1 Reforço das obrigações existentes

35. O Grupo de trabalho do artigo 29.º observa que alguns responsáveis pelo tratamento de dados podem considerar o princípio geral de responsabilidade como

uma imposição de novas exigências jurídicas morosas, em especial no contexto da situação económica adversa que se vive actualmente na UE. Tal posição seria um erro.

36. O Grupo de trabalho do artigo 29.º deseja sublinhar que a maioria dos requisitos estabelecidos por esta nova disposição já existem, embora de forma menos explícita, na legislação actualmente em vigor. Por força do actual quadro jurídico, os responsáveis pelo tratamento de dados são obrigados a respeitar os princípios e obrigações consagrados na Directiva. Para lhes dar cumprimento, é necessário adoptar, e possivelmente verificar, procedimentos relacionados com a protecção de dados. Nesta perspectiva, uma disposição sobre a responsabilidade não representa uma grande novidade e, em grande medida, não impõe requisitos que não estivessem já implícitos na legislação existente. Em resumo, a nova disposição não se destina a sujeitar os responsáveis pelo tratamento de dados a novos princípios, mas a assegurar o respeito *de facto* dos princípios existentes.

37. com efeito, uma evolução legislativa semelhante ocorreu em 2009 quando a Directiva 2002/58 foi alterada[5]. Neste caso, a legislação impõe a aplicação de uma política em matéria de segurança, nomeadamente para obter «*a garantia da aplicação de uma política de segurança relativa ao tratamento dos dados pessoais*». Portanto, no que diz respeito às disposições da directiva em matéria de segurança, o legislador decidiu ser necessário introduzir um requisito explícito para elaborar e aplicar uma política de segurança. Além disso, o artigo 18.º da Directiva 95/46, referindo-se à designação de encarregados da protecção dos dados, assim como ao sistema das regras empresariais obrigatórias, acima mencionado, já oferece exemplos de medidas práticas que podem ser adoptadas pelos responsáveis pelo tratamento de dados.

38. Outra questão relacionada com a anterior é a consequência associada ao cumprimento (ou incumprimento) do princípio da responsabilidade. O Grupo de trabalho do artigo 29.º sublinha que o cumprimento do princípio da responsabilidade não significa necessariamente que um responsável pelo tratamento de dados esteja em conformidade com os princípios fundamentais enunciados na Directiva, ou seja, esse princípio não oferece uma presunção jurídica de conformidade, nem substitui nenhum desses princípios. Um responsável pelo tratamento de dados pode ter implementado e verificado as medidas em vigor e ainda assim estar a cometer uma irregularidade. Por conseguinte, a adopção de medidas para cumprir os princípios não deve isentar os responsáveis pelo tratamento de dados de medidas coercivas promovidas pelas autoridades de protecção de dados. Na prática, os responsáveis pelo tratamento de dados do sector público ou privado que adoptaram medidas através de programas de conformidade sólidos, têm maior probabilidade de estar em conformidade com a legislação. Com efeito, por terem posto em prática medidas eficazes destinadas ao cumprimento dos princípios fundamentais da protecção de dados, há uma

[5] Directiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor.

menor probabilidade de estarem a violar a lei. Portanto, ao avaliar sanções relacionadas com violações da protecção de dados, as autoridades de protecção de dados poderiam ter em conta a aplicação (ou a falta dela) de medidas e a sua verificação.

IV.2 Medidas adequadas tendo em vista a aplicação das disposições da Directiva

39. Uma disposição relativa à responsabilidade exigiria que os responsáveis pelo tratamento de dados definissem e aplicassem as medidas necessárias para assegurar a conformidade com os princípios e obrigações da Directiva e verificassem a sua eficácia periodicamente.

40. O princípio geral da responsabilidade proposto evita propositadamente especificar que tipo de medidas devem ser implementadas, o que suscita duas questões fundamentais interligadas: *(i)* que medidas comuns permitiriam aplicar o princípio da responsabilidade? *(ii)* como proporcionar e adaptar as medidas a circunstâncias específicas?

As medidas: ilustração

41. O Grupo de trabalho do artigo 29.º considera que as medidas comuns em matéria de responsabilidade podem incluir a seguinte lista, que não se pretende exaustiva:

- Estabelecimento de procedimentos internos *antes* da criação de novas operações de tratamento de dados pessoais (revisão interna, avaliação, etc.);[6]
- Adopção de políticas de protecção de dados formais e vinculativas a ter em conta e a aplicar às novas operações de tratamento de dados (por ex. conformidade com a qualidade dos dados, avisos, princípios de segurança, acesso, etc.), que devem ser disponibilizadas às pessoas em causa;
- Descrição dos procedimentos de forma a assegurar a adequada identificação de todas as operações de tratamento de dados e gestão de um inventário dessas operações;
- Designação de um encarregado da protecção de dados e outras pessoas com responsabilidade pela protecção de dados;
- Disponibilização de uma protecção de dados adequada, e de formação adequada nesta matéria aos colaboradores. Deve abranger as pessoas que tratam (ou são responsáveis pelo) tratamento de dados pessoais (como os directores de recursos humanos), mas também gestores de TI, criadores e directores de unidades operacionais. Devem ser atribuídos recursos suficientes para a gestão da protecção da privacidade, etc.;
- Criação de procedimentos para gerir os pedidos de acesso, de correcção e de supressão, que devem ser transparentes para as pessoas em causa;
- Estabelecimento de um mecanismo interno de gestão de reclamações;
- Elaboração de procedimentos internos para uma gestão e transmissão eficazes das violações da segurança;
- Realização de avaliações de impacto sobre a privacidade em circunstâncias específicas;

---

[6] As operações de tratamento de dados existentes necessitariam de um período de transição para serem adaptadas à legislação.

- Aplicação e controlo de procedimentos de verificação destinados a assegurar que as medidas existam não só no papel, mas que também são implementadas e funcionam na prática (auditorias internas ou externas, etc.).

42. Poderia prever-se também uma abordagem complementar ao princípio geral de responsabilidade. Nessa hipóteses, o quadro legislativo incluiria não só um princípio geral da responsabilidade, mas também uma lista de medidas indicativas que poderiam ser incentivadas a nível nacional[7]. Essa disposição podia incluir uma lista indicativa e não exaustiva de medidas que os responsáveis pelo tratamento de dados poderiam utilizar como «caixa de ferramentas». Orientaria os responsáveis pelo tratamento de dados sobre o que poderia constituir, dependendo do caso, as medidas adequadas a tomar. Essa lista acompanharia obviamente apenas a obrigação legal geral de adoptar medidas adequadas.

Proporcionalidade das medidas

43. A lista acima referida ilustra as medidas que os responsáveis pelo tratamento de dados podiam aplicar para respeitar a primeira parte do princípio da responsabilidade (*o responsável deve tomar as medidas adequadas e eficazes para garantir o respeito dos princípios e obrigações enunciados na directiva*).

---

[7] Por exemplo, as normas internacionais adoptadas em Madrid pelas autoridades de protecção de dados contêm, no seu artigo 22.º, uma disposição relativa a medidas pró-activas, com o seguinte teor: *Os Estados devem incentivar, através da sua legislação nacional, a aplicação, por parte das pessoas envolvidas numa qualquer etapa do tratamento, de medidas de promoção de uma maior conformidade com a legislação aplicável referente à protecção da privacidade no que diz respeito ao tratamento de dados pessoais. Tais medidas incluem, entre outras:*

a) A aplicação de procedimentos para prevenir e detectar violações, que podem ter por base modelos normalizados de governação e/ou gestão da segurança da informação.

b) A nomeação de um ou mais encarregados de protecção de dados, com qualificações, recursos e poderes apropriados ao exercício adequado das suas funções de controlo.

c) A aplicação periódica de programas de educação, formação e sensibilização entre os membros da organização, com o intuito de compreender melhor a legislação aplicável à protecção da privacidade no que diz respeito ao tratamento de dados pessoais, assim como aos procedimentos estabelecidos pela organização com esse fim.

d) A realização periódica de auditorias transparentes, por um organismo qualificado e de preferência independente, para verificar a conformidade com a legislação aplicável relativa à protecção da privacidade no que diz respeito ao tratamento de dados pessoais, assim como com os procedimentos estabelecidos pela organização com esse fim.

e) A adaptação de sistemas e/ou tecnologias da informação no tratamento de dados pessoais à legislação relativa à protecção da privacidade no que diz respeito ao processamento de dados pessoais, especialmente no momento de decidir sobre as suas especificações técnicas e o seu desenvolvimento e aplicação.

f) A aplicação de avaliações do impacto sobre a privacidade antes da aplicação de novos sistemas e/ou tecnologias de informação no tratamento de dados pessoais, assim como antes de aplicar qualquer método novo de tratamento de dados pessoais ou modificações substanciais em tratamentos existentes.

g) A adopção de códigos de conduta cuja observância seja vinculativa e inclua elementos que permitam avaliar a eficácia no que diz respeito à conformidade e ao nível de protecção dos dados pessoais e que estabeleçam medidas eficazes em caso de não conformidade.

h) A aplicação de um plano de resposta que estabeleça directrizes de actuação no caso de se verificar uma violação da legislação aplicável em matéria de protecção da privacidade no que diz respeito ao tratamento de dados pessoais, incluindo pelo menos a obrigação de determinar a causa e extensão da violação, de descrever os seus efeitos prejudiciais e de tomar as medidas adequadas para evitar que se reproduzam no futuro.»

44. Algumas dessas medidas são elementos-chave que terão de ser implementadas na maioria das operações de tratamento de dados. A concepção de políticas e procedimentos internos para aplicação dos princípios (procedimentos para gerir pedidos de acesso, reclamações) podem constituir exemplos de medidas adequadas ao tratamento de alguns dados. A adequação das medidas terá de ser decidida caso a caso. Incumbe aos responsáveis pelo tratamento de dados tomar essas decisões, tendo por base as directrizes emitidas pelas autoridades nacionais de protecção de dados e pelo Grupo de trabalho do artigo 29.º, quando tal seja possível (ver infra).

45. Do exposto decorre que a única opção para determinar os tipos de medidas a aplicar são as soluções «sob medida». Com efeito, as medidas específicas a aplicar devem ser determinadas em função dos factos e das circunstâncias de cada caso particular, com especial atenção para o risco associado ao tratamento e aos tipos de dados. Uma abordagem única obrigaria os responsáveis pelo tratamento de dados a adoptar estruturas inadequadas e, por fim, acabaria por falhar.

46. Nesta abordagem, os responsáveis têm a possibilidade de adaptar as medidas às características concretas do responsável pelo tratamento de dados e das operações de tratamento de dados em questão. Nesse contexto, o Grupo de trabalho do artigo 29.º relembra os critérios utilizados no artigo 17.º da actual directiva[8] para determinar o tipo de medidas de segurança a aplicar, nomeadamente os riscos apresentados pelo tratamento e a natureza dos dados. Esses dois factores poderiam ser utilizados de forma análoga para determinar os tipos gerais de medidas a aplicar. Mais concretamente, aspectos como a dimensão das operações de tratamento de dados, a finalidade do tratamento e o número de transferências de dados previstas podem determinar o nível do risco. O tipo de dados, incluindo o seu carácter sensível ou não, também deve ser tido em conta. Uma reflexão sobre a necessidade de impor determinadas obrigações ao técnico que trata os dados ou aos criadores e/ou produtores de TIC (tecnologias da informação e da comunicação) poderia também ser desenvolvida à luz deste princípio da responsabilidade.

47. A par da conformidade com estes critérios, em princípio as grandes organizações responsáveis pelo tratamento de dados deviam aplicar medidas rigorosas. Em alguns casos, os pequenos ou médios responsáveis pelo tratamento, por exemplo se efectuam operações arriscadas de tratamento de dados, como algumas operações de tratamento de dados de dossiês da saúde em linha, também podem ter de aplicar garantias rigorosas. Por exemplo, uma autarquia local (município), uma multinacional, uma pequena empresa (na Internet), uma organização centrada no tratamento de dados ou uma organização com um historial de infracções necessitam de medidas específicas próprias para assegurar uma governação credível e eficaz da informação. Consequentemente, nos casos simples e básicos, como o tratamento de dados pessoais relativos a recursos humanos para estabelecer um repertório de empresa, a «obrigação de demonstração», referida no n.º 2 da disposição relativa à responsabilidade, pode ser facilmente respeitada (por exemplo, através de notas de informação, da descrição de medidas básicas de

[8] «Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger».

segurança, etc.). Pelo contrário, em casos mais complexos, como por exemplo a utilização de dispositivos biométricos inovadores, o cumprimento da «obrigação de demonstração» pode exigir ainda mais requisitos. O responsável pelo tratamento dos dados pode ter de demonstrar por exemplo que realizou uma avaliação de impacto sobre a privacidade, que os colaboradores envolvidos no tratamento recebem formação e são informados regularmente, etc.

48. A transparência é um elemento integral de muitas medidas de responsabilidade. A transparência para com as pessoas em causa e o público em geral contribui para a responsabilização dos responsáveis pelo tratamento de dados. A publicação de políticas de privacidade na Internet, a transparência nos procedimentos internos de reclamação e a publicação de relatórios anuais, por exemplo, permitem atingir um nível de responsabilidade mais elevado.

Orientações e segurança jurídica

49. Embora a necessidade de uma solução evolutiva e, por conseguinte, de uma certa flexibilidade, promova o uso de linguagem aberta, o Grupo de trabalho do artigo 29.º tem consciência que uma disposição muito geral, com margem para a flexibilidade e a adaptabilidade, também pode gerar insegurança. Os responsáveis pelo tratamento podem considerar que a disposição não é suficientemente detalhada para conferir segurança jurídica. Poderão não saber ao certo o nível de pormenor que se espera dos procedimentos e políticas de privacidade, quando e como nomear um encarregado de protecção de dados, quando devem ser organizadas sessões de formação, etc. A insegurança também pode também estar relacionada com o tipo de verificação que se afigure necessária, interna ou externa. Os responsáveis pelo tratamento de dados podem ainda recear ser sujeitos a interpretações nacionais arbitrárias e divergentes sobre o âmbito e a natureza das suas obrigações.

50. O Grupo de trabalho do artigo 29.º compreende essas preocupações. No entanto, pelas razões acima enumeradas relativas à necessidade de prever uma certa flexibilidade e adaptabilidade, não pode ser a Directiva a fornecer a solução para garantir segurança jurídica. Como forma de garantir a necessária segurança jurídica, o Grupo de trabalho do artigo 29.º considera que orientações harmonizadoras publicadas pela Comissão (por exemplo através de medidas técnicas de execução) ou/e pelo Grupo de trabalho do artigo 29.º poderiam constituir ferramentas úteis para garantir maior segurança e eliminar potenciais divergências a nível da aplicação.[9] O Grupo de trabalho do artigo 29.º também poderia preparar orientações gerais com uma indicação dos elementos básicos necessários para um responsável pelo tratamento de dados padrão. Esse conjunto de elementos básicos poderia ser adaptado às necessidades específicas de cada responsável.

[9] Um exemplo deste tipo de orientação é a ferramenta de auto-avaliação PIPEDA, publicada pelo gabinete da Autoridade canadiana para a privacidade como forma de ajudar as organizações de média e grande dimensão a desenvolverem e aplicarem uma boa governação e gestão da privacidade. A ferramenta de auto-avaliação encontra-se disponível em: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf .

51. Também pode ser útil desenvolver um *modelo de programa de conformidade dos dados*, que podia ser utilizado por organizações de média e grande dimensão como elemento de base para a concepção dos seus programas específicos, à semelhança do que foi feito para as BCR, com base nas orientações desenvolvidas pelo Grupo de trabalho do artigo29.°[10]. Esses modelos devem ser criados após uma cuidadosa revisão das práticas actuais e modelos disponíveis e a consulta das respectivas partes interessadas. Este domínio necessitará de um sério investimento por parte de todas as partes interessadas.

Eficácia das medidas

52. A garantia de eficácia das medidas suscita as mesmas questões que foram discutidas relativamente às medidas aplicáveis. A forma de garantir a eficácia dependerá do tipo de tratamento de dados.

53. Os responsáveis pelo tratamento de dados podem avaliar a eficácia (ou ineficácia) das medidas de diferentes formas. Em tratamentos de dados de maior dimensão, mais complexos ou de maior risco, é frequente recorrer a auditorias internas e externas. A forma como as auditorias são conduzidas também pode variar, desde auditorias completas a auditorias negativas (que também podem assumir diversos formatos). Ao decidir como assegurar a eficácia das medidas, o Grupo de trabalho do artigo 29.º sugere a utilização dos mesmos critérios utilizados para escolher as medidas, que provêm do artigo 17.º da Directiva 95/46/CE, nomeadamente os riscos apresentados pelo tratamento de dados e a natureza dos dados. Por conseguinte, a forma como um responsável deve assegurar a eficácia das medidas irá depender da sensibilidade dos dados, do volume de dados processados e dos riscos específicos apresentados pelo tratamento de dados. As orientações do Grupo de trabalho do artigo 29.º sobre as medidas também podem incluir orientações relativas a este aspecto.

IV.3 Ligação com outros requisitos

Notificações prévias

54. Podia reflectir-se sobre o possível impacto sobre as notificações prévias numa situação em que as garantias adequadas são definidas a nível do responsável. Podia prever-se que determinados mecanismos de responsabilidade substituam ou limitem as exigências administrativas da actual legislação em matéria de protecção de dados, como foi já sugerido pelo Grupo de trabalho do artigo 29.º no seu parecer sobre o futuro da privacidade.

Transferências internacionais de dados

55. As regras empresariais obrigatórias são um exemplo da forma de aplicar princípios de protecção de dados com base no princípio da responsabilidade. É uma forma de proporcionar garantias adequadas às transferências efectuadas fora

[10] Documento de trabalho n.° 153 do Grupo de trabalho do artigo 29.º que estabelece uma tabela com os elementos e princípios retomados das regras empresariais obrigatórias, e documento de trabalho n.° 154 que estabelece um quadro para a estrutura das regras empresariais obrigatórias.

da União Europeia e que é reconhecida e aceite pelo Grupo de trabalho do artigo 29.º.

56. Este domínio beneficiaria de uma análise mais aprofundada à luz da revisão da Directiva 95/46. Em particular, seria importante analisar se o artigo 26.º, n.º 2, da Directiva (*um Estado-membro pode autorizar uma transferência...desde que o responsável pelo tratamento apresente garantias suficientes...; essas garantias podem, designadamente, resultar de disposições contratuais adequadas*) abrange plenamente as regras empresariais obrigatórias e eventualmente outros mecanismos de responsabilidade vinculativos enquanto ferramentas que permitem assegurar as garantias adequadas.

57. Neste contexto, é extremamente relevante avaliar, entre outros, os mecanismos utilizados internamente para pôr em prática os princípios e obrigações da protecção de dados entre os responsáveis pelo tratamento de dados, bem como os sistemas de verificação. Importa discutir também os mecanismos de melhoramento do actual sistema com base na autorização de transferências de dados por parte das autoridades nacionais de protecção dos dados.

IV.4 O papel das autoridades de protecção de dados

58. Uma questão a abordar é se o princípio da responsabilidade proposto no presente parecer irá afectar os poderes das autoridades de protecção de dados, especialmente no domínio da execução. Como será descrito infra, o princípio não elimina quaisquer poderes das autoridades de protecção de dados. Pelo contrário, trará benefícios às referidas autoridades.

59. No que diz respeito à execução, o princípio, tal como é proposto, reconhece a competência das autoridades de protecção de dados para solicitar ao responsável pelo tratamento provas da conformidade com o princípio da responsabilidade, pelo que se insere nas actividades de execução levadas a cabo pelas autoridades. Assegura-se deste modo que as autoridades continuam competentes para a qualquer momento aplicarem medidas coercivas. Convém esclarecer que as autoridades de protecção manteriam sempre a competência para controlar não só as medidas tomadas pelos responsáveis pelo tratamento, mas sobretudo, a conformidade com os princípios e obrigações subjacentes.

60. Por outro lado, a aplicação do princípio da responsabilidade irá proporcionar às autoridades de protecção de dados informação útil para a monitorização dos níveis de conformidade. Com efeito, uma vez que os responsáveis pelo tratamento terão de ser capazes de demonstrar às autoridades se, e de que forma, aplicaram as medidas, as autoridades ficarão na posse de informações em matéria de conformidade muito relevantes, que poderão utilizar no contexto das suas medidas coercivas. Além do mais, se essas informações não forem prestadas quando solicitado, as autoridades de protecção de dados terão um motivo imediato para agir contra os responsáveis pelo tratamento de dados, independentemente da alegada violação de outros princípios de protecção de dados subjacentes.

61. Este princípio também seria útil para as autoridades de protecção de dados na medida em que as ajudaria a ser mais selectivas e estratégicas, permitindo-lhes investir os recursos de forma a gerar a maior conformidade possível.

62. O Grupo de trabalho do artigo 29.º lembra que o princípio da responsabilidade pode contribuir para o desenvolvimento de conhecimentos técnicos e jurídicos no domínio da aplicação de requisitos de protecção de dados. Pessoas com profundos conhecimentos e compreensão dos aspectos técnicos e jurídicos no domínio da protecção de dados, com aptidões para comunicar, dar formação a colaboradores, criar e aplicar políticas e realizar auditorias serão indispensáveis neste domínio. Estes conhecimentos especializados serão necessários quer internamente, quer sob a forma de serviço externo contratado por empresas. Esta evolução será vital para assegurar que os responsáveis pelo tratamento de dados consigam realizar as suas obrigações incluindo, se necessário, a realização de auditorias internas e externas. Simultaneamente, tal evolução seria benéfica para as autoridades de protecção de dados pois, na medida em que o sistema contribuirá para a conformidade geral, as autoridades terão ao seu dispor mais informação segura sobre as práticas internas das empresas, e a formação de profissionais em matéria de protecção de dados altamente qualificados facilitará certamente a sua interacção com os responsáveis pelo tratamento de dados.

63. Pode concluir-se que a actividade das autoridades de protecção de dados está centrada num papel mais *ex post* do que *ex ante*. Como a responsabilidade coloca a tónica na obtenção de resultados específicos em termos de boa governação da protecção de dados, é uma actividade centrada nos resultados, sendo a sua ênfase de natureza *ex post* (ou seja, intervém após o início do tratamento de dados).

IV. 5 Sanções

64. O sistema proposto só pode funcionar se as autoridades de protecção de dados estiverem investidas de poderes de sanção efectivos. É necessário aplicar sanções efectivas sempre que os responsáveis pelo tratamento de dados não conseguirem respeitar o princípio da responsabilidade, por exemplo, deverá ser possível punir um responsável que não honre as declarações prestadas sobre políticas internas vinculativas. Obviamente, tratar-se-ia de um complemento à actual violação dos princípios substantivos da protecção de dados.

65. Para além do exposto, o Grupo de trabalho do artigo 29.º considera que os poderes das autoridades nacionais de protecção de dados deviam incluir a possibilidade de impor instruções precisas aos responsáveis pelo tratamento de dados sobre os seus sistemas de conformidade.

IV.6 Desenvolvimento de sistemas de certificação

66. A longo prazo, a disposição relativa à responsabilidade pode incentivar o desenvolvimento de programas ou selos de certificação. Esses programas contribuiriam para comprovar que um responsável pelo tratamento de dados cumpriu a disposição e, por conseguinte, definiu e implementou medidas adequadas que foram periodicamente auditadas. Vários factores podem favorecer essa evolução:

67. Em geral, é previsível que, por razões de diferenciação, os serviços de protecção de dados/auditoria/avaliação do impacto sobre a privacidade proponham oferecer certificados/selos como forma de se destacarem gradualmente no mercado e de oferecerem uma vantagem competitiva. Os responsáveis pelo tratamento de dados podem decidir optar por serviços de certificação fidedignos. À medida que determinados sistemas de atribuição de selos se tornem conhecidos pelos seus testes rigorosos, é provável que mereçam a preferência dos responsáveis pelo tratamento de dados, pois proporcionarão um maior «conforto» em termos de conformidade, para além de oferecerem uma vantagem competitiva.

68. O uso das BCR como base jurídica para as transferências internacionais de dados exige dos responsáveis pelo tratamento de dados a aplicação de garantias adequadas para que as autoridades de protecção de dados possam autorizar as transferências. Os serviços de certificação podiam ser úteis neste domínio, analisando as garantias proporcionadas pelo responsável pelo tratamento de dados e emitindo o selo relevante. Na sua análise das BCR e da avaliação das garantias proporcionadas para efeitos de transferências internacionais de dados, as autoridades de protecção de dados podiam valorizar a certificação atribuída por um determinado programa de certificação, contribuindo dessa forma para simplificar o processo de autorização das transferências internacionais de dados.

IV.7 Regulamentação dos mecanismos de certificação

69. As mesmas razões que favorecem o desenvolvimento de serviços de certificação sustentam a necessidade da sua regulamentação. Com efeito, para que esses serviços possam comprovar com fiabilidade a conformidade da protecção de dados (perante as autoridades de protecção de dados, os responsáveis pelo tratamento e os consumidores em geral) e operar correctamente no mercado interno, será necessário instituir regras que estabeleçam os requisitos de prestação desses serviços. As autoridades de protecção de dados deviam desempenhar um papel fundamental no desenvolvimento dessas regras (em termos de referências, modelos, etc.) e ter competência para fazer cumprir a sua aplicação, o que impõe, por sua vez, que lhes sejam afectados recursos suficientes. As autoridades de protecção de dados também deviam desempenhar um papel na certificação dos certificadores, uma função que pode ser especialmente relevante no domínio das transferências internacionais de dados. Uma vez que a qualidade dos serviços e a necessidade de operarem no mercado interno são critérios-chave, a legislação terá de criar as condições que permitam atingir essa qualidade, pois não parece possível deixar essa matéria a cargo do mercado. A experiência noutros domínios, como a certificação de produtos, revelou um nivelamento por baixo, em que a concorrência entre fornecedores de serviços pode levar a uma redução dos preços e a uma certa flexibilidade ou relaxamento dos procedimentos. Em resumo, quer se trate de um ambiente transfronteiras ou não, as regras parecem ser necessárias para assegurar a qualidade dos serviços e condições equitativas.

70. O Grupo de trabalho do artigo 29.º recorda que a legislação existente em matéria de acreditação[11] pode ser aplicável no domínio dos serviços de certificação em matéria de protecção de dados. Essa legislação já disponibiliza a estrutura necessária para o estabelecimento de regras relativas à organização e ao funcionamento dos organismos de acreditação. Estas regras aplicam-se à acreditação voluntária e também aos casos específicos em que a acreditação é obrigatória.

71. É óbvio que este tipo de serviço também impulsiona a harmonização das normas subjacentes com base nas quais as entidades seriam avaliadas. As orientações atrás mencionadas (prestadas pelo Grupo de trabalho do artigo 29.º ou pela Comissão), que estabeleceriam programas modelo de conformidade de dados, seriam da máxima relevância.

V. CONCLUSÕES

72. O desenvolvimento de novas tecnologias e a contínua globalização da economia e da sociedade levaram a uma multiplicação da informação pessoal que é recolhida, organizada, transferida ou conservada e à consequente multiplicação dos riscos para esses dados.

73. O Grupo de trabalho do artigo 29.º está convicto que o aumento dos riscos e do valor dos dados pessoais *per se* justifica a necessidade de reforçar o papel e a responsabilidade dos responsáveis pelo tratamento de dados. Um quadro legislativo que sirva esta nova realidade deve conter as ferramentas necessárias para incentivar os responsáveis pelo tratamento de dados a aplicarem medidas adequadas e eficazes que concretizem os princípios da protecção de dados. Os procedimentos que garantem a identificação de todas as operações de tratamento de dados, a resposta aos pedidos de acesso, a distribuição de recursos, incluindo a designação de pessoas responsáveis pela organização da conformidade da protecção de dados, são alguns exemplos dessas medidas.

74. Para incentivar a protecção de dados na prática, o Grupo de trabalho do artigo 29.º sugere, como primeira prioridade, a inclusão nas propostas de alteração da Directiva Protecção de Dados de uma nova disposição que exija dos responsáveis pelo tratamento de dados a aplicação de medidas adequadas e eficazes para assegurar o cumprimento dos princípios e obrigações da referida directiva e a sua demonstração às autoridades, quando solicitado. Essas medidas iriam melhorar a conformidade com os princípios e obrigações em matéria de protecção de dados e minimizar os riscos de acesso não autorizado, abuso, perda, etc. A obrigação de demonstrar a aplicação das medidas necessárias quando solicitado, seria uma ferramenta útil que auxiliaria as autoridades de protecção de dados na sua missão de execução.

---

[11] Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de Julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93.

75. A obrigação de implementar tais medidas deve aplicar-se aos responsáveis pelo tratamento de dados de todos os sectores (público e privado) e ser adaptável, para que o tipo de medidas seja proporcional aos riscos associados ao tratamento e à natureza dos dados.

Feito em Bruxelas, em 13 de Julho de 2010.

Pelo Grupo de trabalho
O Presidente
Jacob KOHNSTAMM