



## DIRECTIVAS PARA A HARMONIZAÇÃO DA PROTECÇÃO DE DADOS NA COMUNIDADE IBERO-AMERICANA

Sumário: 1. Introdução; 2. Conteúdo essencial do direito à protecção de dados pessoais. Critérios de harmonização; 3. Directivas (princípios, direitos e obrigações) que uma Lei nacional de protecção de dados de carácter pessoal deverá conter.

### I. Introdução

O documento sobre desenvolvimentos legislativos e harmonização, elaborado pelo Grupo de Trabalho Permanente de Desenvolvimento Normativo da Rede Ibero-Americana de Protecção de Dados, na reunião celebrada em Santa Cruz de la Sierra (Bolívia), de 3 a 5 de Maio de 2006, considera como uma das prioridades máximas nos trabalhos da Rede a elaboração de uma proposta de Directivas que contribua para as iniciativas reguladoras da Protecção de dados que surjam na Comunidade Ibero-Americana.

O estabelecimento de um quadro harmonizado de protecção de dados a nível global tem sido o principal alicerce da adopção dos diferentes instrumentos internacionais actualmente existentes em matéria de protecção de dados.

Trata-se assim de garantir que o desenvolvimento do comércio a nível mundial seja compatível com a protecção dos direitos das pessoas, especialmente no que se refere à protecção da informação que lhes diz respeito.

Deste modo, o estabelecimento de um quadro homogéneo de regulamentação do direito à protecção de dados, quer mediante a adopção de instrumentos supranacionais de carácter vinculativo, quer mediante a promulgação de leis nacionais que consagrem o conteúdo essencial deste direito, garantirá o desenvolvimento do comércio na zona, facilitando o intercâmbio de informação entre os diferentes operadores sedeados nos Estados Ibero-americanos e entre estes e países terceiros, em particular os Estados-membros da União Europeia, em condições que não sejam restringidas em consequência do diferente nível de protecção do direito fundamental à protecção de dados de carácter pessoal.

Assim, o Preâmbulo da Recomendação do Conselho da OCDE, relativa às directivas que regem a protecção da privacidade e a circulação transfronteiriça de dados de



carácter pessoal, aprovada a 23 de Setembro de 1980, reconhece expressamente que “a circulação transfronteiriça de dados pessoais contribui para o desenvolvimento económico e social”, mas, ao mesmo tempo, recorda que “a legislação nacional relativa à protecção da privacidade e da circulação transfronteiriça de dados pessoais pode obstaculizar tal circulação transfronteiriça”.

Por este motivo, a Recomendação tem por objectivo essencial “fomentar a livre circulação de informação entre os países membros e evitar a criação de obstáculos injustificados ao desenvolvimento das relações económicas e sociais entre os países membros”. Pretende-se assim que o intercâmbio transfronteiriço de informação não possa ser limitado pela legislação nacional de protecção de dados, garantindo porém a adequada protecção deste direito fundamental.

Ainda mais claramente, se possível, a Directiva 95/46/CE, do Conselho e do Parlamento Europeu, 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, exprime esta ideia nos pontos 6 a 9 dos seus Considerandos, afirmando o seguinte:

*“ (6) Considerando, além disso, que o reforço da cooperação científica bem como a introdução coordenada de novas redes de telecomunicações na Comunidade exigem e facilitam a circulação transfronteiras de dados pessoais;*

*(7) Considerando que as diferenças entre os Estados-membros quanto ao nível de protecção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, no domínio do tratamento de dados pessoais, podem impedir a transmissão desses dados do território de um Estado-membro para o de outro Estado-membro; que estas diferenças podem, por conseguinte, constituir um obstáculo ao exercício de uma série de actividades económicas à escala comunitária, falsear a concorrência e entravar o exercício pelas administrações das funções que lhes incumbem nos termos do direito comunitário; que esta diferença de níveis de protecção resulta da disparidade das disposições legislativas, regulamentares e administrativas nacionais;*

*(8) Considerando que, para eliminar os obstáculos à circulação de dados pessoais, o nível de protecção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados deve ser equivalente em todos os Estados-membros; que a realização deste objectivo, fundamental para o mercado interno, não pode ser assegurada unicamente pelos Estados-membros, tendo especialmente em conta a dimensão das divergências que se verificam actualmente a nível das legislações nacionais aplicáveis na matéria*



*e a necessidade do coordenar as legislações dos Estados-membros para assegurar que a circulação transfronteiras de dados pessoais seja regulada de forma coerente e em conformidade com o objectivo do mercado interno nos termos do artigo 7º A do Tratado; que é portanto necessária uma acção comunitária com vista à aproximação das legislações;*

*(9) Considerando que, devido à protecção equivalente resultante da aproximação das legislações nacionais, os Estados-membros deixarão de poder levantar obstáculos à livre circulação entre si de dados pessoais por razões de protecção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada; que é deixada aos Estados-membros uma margem de manobra que, no contexto da aplicação da directiva, poderá ser utilizada pelos parceiros económicos e sociais; que os Estados-membros poderão, pois, especificar na sua legislação nacional as condições gerais de licitude do tratamento de dados; que, ao fazê-lo, os Estados-membros se esforçarão por melhorar a protecção actualmente assegurada na respectiva legislação nacional; que, nos limites dessa margem de manobra e em conformidade com o direito comunitário, poderão verificar-se disparidades na aplicação da directiva, o que poderá reflectir-se na circulação de dados quer no interior de um Estado-membro, quer na Comunidade;*

A maior parte das Constituições dos Estados que integram a Comunidade Ibero-Americana contém disposições que garantem à pessoa o direito fundamental à protecção dos seus dados pessoais e o "habeas data". Estas previsões são completadas além disso pelas resoluções saídas dos Tribunais de Justiça e, em particular, dos Tribunais Constitucionais.

Reconhece-se assim, através dos canais constitucional e jurisprudencial um direito fundamental das pessoas à protecção dos seus dados de carácter pessoal, independente e autónomo do direito à privacidade, consistindo no direito do cidadão a dispor livremente da informação que lhe respeita.

Tendo isso em conta, é preciso que os poderes públicos adoptem as medidas necessárias para garantir às pessoas a salvaguarda do direito fundamental, como garantia essencial do Estado de direito.

No entanto, o reconhecimento do direito fundamental deveria, como foi afirmado, ser complementado com o estabelecimento de um quadro legal uniforme, que permitisse garantir um nível equivalente de protecção deste direito, através do reconhecimento legal dos princípios, direitos e deveres que o configuram. Deste modo poder-se-á assegurar que, encontrando-se plenamente garantido o direito



fundamental, os Estados Ibero-americanos beneficiem do enriquecimento económico, social e cultural que pode derivar do livre intercâmbio transfronteiriço da informação que contenha dados de carácter pessoal.

O presente documento tem por objecto delimitar esses perfis essenciais que configuram o direito fundamental à protecção de dados pessoais, com o objectivo de oferecer aos poderes públicos dos Estados Ibero-americanos critérios orientadores que possam ser úteis ao desenvolvimento das iniciativas legislativas a adoptar, facilitando assim o estabelecimento de um quadro homogéneo de protecção que facilite o intercâmbio dos fluxos de informação entre todos eles e entre eles e Estados terceiros que adoptaram padrões similares de protecção.

## 2. Conteúdo essencial do direito à protecção de dados pessoais. Critérios de harmonização.

Como já se disse, a maioria dos Estados Ibero-americanos reconhece, tanto por referência directa na Constituição, como em consequência de decisões dos seus órgãos jurídicos, o direito do cidadão à protecção de dados de carácter pessoal, essencialmente mediante o reconhecimento do recurso ao "*habeas data*", através do qual o cidadão pode tomar conhecimento dos dados que se lhe referem e da finalidade para a qual são tratados por um determinado responsável pelo tratamento, podendo exigir a sua rectificação, eliminação ou actualização.

O exercício deste direito deu origem a uma rica jurisprudência que evoluiu para o reconhecimento de uma série de princípios a que devem submeter-se as Administrações Públicas e as entidades privadas que tratam dados de carácter pessoal.

Na Colômbia, a Corte [Tribunal] Constitucional definiu, através de mais de 140 sentenças, o alcance e características do *habeas data* bem como as condições que devem rodear o tratamento dos dados pessoais consagrado no artigo 15 da Constituição de 1991.

Desde a primeira sentença (T 414/92), o Tribunal estabeleceu que a pessoa é o titular e proprietário do dado pessoal. Portanto é obrigação dos responsáveis de bancos de dados administrar correctamente e proteger os arquivos e bases de dados que contenham informação pessoal ou socialmente relevante e não atentar contra os direitos fundamentais das pessoas. A Corte Constitucional declarou, de maneira geral, que "*a função de administrar uma base de dados deve fundamentar-se nos princípios de liberdade, necessidade, veracidade, integridade, incorporação, finalidade, utilidade, circulação restrita, caducidade e individualidade*".



Concretamente, precisou que os administradores devem: (1) Obter previamente a autorização da pessoa cujos dados se pretende incluir na base; (2) Notificar a pessoa sobre a inclusão dos seus dados no banco e informá-la de que vai concentrar a sua informação numa base de dados, para que o titular possa desde o início exercer os seus direitos de rectificação e actualização; (3) Actualizar permanente e oficiosamente a informação para que esta seja verdadeira, completa e não se omitam factores que possam alterar o bom nome da pessoa; (4) Eliminar *ex officio* a informação negativa que tenha caducado com o tempo; (5) Indemnizar os prejuízos causados por negligência ou por possíveis falhas no manuseamento, tratamento ou gestão de dados pessoais; (6) Garantir o direito de acesso, actualização e correcção.

Estes direitos implicam que o cidadão tenha *"a possibilidade (...) de saber de forma imediata e completa, como, porquê e onde aparece qualquer dado relacionado com ele"*; (...) *se a informação é errónea ou inexacta, o indivíduo pode solicitar, com direito a resposta também imediata, que a entidade responsável do sistema introduza nele as pertinentes correcções, aclarações ou eliminações, a fim de preservar os seus direitos fundamentais prejudicados"*. Finalmente, a Corte precisou que, por regra geral, *"não pode ser recolhida informação sobre dados "sensíveis" como, por exemplo, a orientação sexual das pessoas, a sua filiação política ou o seu credo religioso, quando isso, directa ou indirectamente, possa conduzir a uma política de discriminação ou marginalização"*.

Em Espanha, a Sentença 292/2000, de 30 de Novembro, depois de desvincular o direito à protecção de dados do direito à privacidade, declara que *"o conteúdo do direito fundamental à protecção de dados consiste num poder de disposição e de controle sobre os dados pessoais, que faculta à pessoa a capacidade para decidir quais desses dados entende proporcionar a um terceiro, seja o Estado ou um particular, ou quais pode este terceiro recolher, e que também permite ao indivíduo saber quem possui esses dados pessoais e para quê, podendo opor-se a essa posse ou uso"*, acrescentando que *"estes poderes de disposição e controle sobre os dados pessoais, que constituem parte do conteúdo do direito fundamental à protecção de dados se concretizam juridicamente na faculdade de consentir a recolha, a obtenção e o acesso aos dados pessoais, seu posterior armazenamento e tratamento, bem como o seu uso ou usos possíveis, por um terceiro"*. Assim, conclui-se que *"são elementos característicos da definição constitucional do direito fundamental à protecção de dados pessoais os direitos do afectado a consentir ou negar a recolha e uso dos seus dados pessoais e a saber dos mesmos. E resultam indispensáveis para tornar efectivo esse conteúdo o reconhecimento do direito a ser informado de quem possui os seus dados pessoais e com que fim, e o direito a poder opor-se a essa posse e uso requerendo a quem de direito que ponha fim à posse e utilização dos dados. Isto é, exigindo do responsável do tratamento que o informe que dados possui sobre a sua pessoa, acedendo aos registos e entradas relevantes, e que destino tiveram, o*



*que também cobre possíveis concessões a terceiros; e, em caso disso, requerer-lhe que os rectifique ou os elimine".*

No México, o direito à protecção de dados pessoais aplica-se no âmbito dos ficheiros públicos a nível federal na Lei Federal de Transparência e Acesso à Informação Pública Governamental (LAI), e cada legislatura estatal, no quadro das suas leis de acesso à informação, inclui capítulos *ad-hoc*.

Actualmente, existem duas iniciativas de reforma constitucional, a primeira apresentada à Câmara de Senadores que acrescenta o artigo 16º da Constituição Política dos Estados Unidos Mexicanos para reconhecer o direito à protecção de dados pessoais, como um direito fundamental, o qual foi aprovado na anterior legislatura e enviado à Câmara de Deputados para os efeitos constitucionais correspondentes, estando ainda pendente a sua discussão e aprovação nesta última. A segunda iniciativa foi apresentada no passado dia 27 de Março de 2007 e veio reforçar a anteriormente referida, já que dota o Congresso de faculdades expressas para aprovar uma lei sobre a matéria, argumentando que é relevante não apenas por se tratar de um tema de protecção de direitos humanos e liberdades fundamentais, mas também pelos efeitos essenciais que estes têm sobre a economia nacional. *Finalmente, é de sublinhar que o Plenário do IFAI, na sua sessão de 25 de Abril de 2007, aprovou por unanimidade que seja criado um grupo de trabalho entre o sector privado e esta instituição, para a elaboração de um esboço de projecto de Lei em matéria de Protecção de Dados Pessoais.*

No Peru, o Tribunal Constitucional tem-se pronunciado através de jurisprudência diversa sobre o reconhecimento do direito à autodeterminação informativa que o artigo 2º, número 6) da Constituição Política de 1993 reconhece e, tem afirmado também o objecto deste direito, sua natureza relacional e marcado as diferenças entre este e outros direitos humanos como os direitos à intimidade, à imagem e à identidade pessoal.

Assim, por exemplo, a sentença com data de 29 de Janeiro proferida no Proc. N° 1797-2002-HD/TC, declara que *"o direito reconhecido na alínea 6) do artigo 2º da Constituição é denominado pela doutrina direito à autodeterminação informativa e tem por objecto proteger a intimidade, pessoal ou familiar, a imagem e a identidade face ao perigo que representa o uso e a eventual manipulação dos dados através dos computadores. Por outro lado, ainda que o seu objecto seja a protecção da intimidade, o direito à autodeterminação informativa não pode ser identificado com o direito à intimidade, pessoal ou familiar, reconhecido, por sua vez, na alínea 7) do mesmo artigo 2º da Constituição (...) por sua própria natureza, o direito à autodeterminação informativa, sendo um direito subjectivo tem a característica de ser, prima facie e de modo geral, um direito de natureza relacional, pois as exigências que obrigam ao seu respeito, se encontram muitas vezes vinculadas à*



protecção de outros direitos constitucionais." A referida sentença ratifica o expresso na sentença proferida no Proc. N.º. 666-1996-HD/TC, precisando o que abarca a protecção do direito à autodeterminação informativa através do *habeas data*, declarando que compreende: *"em primeiro lugar, a capacidade de exigir juridicamente a possibilidade de aceder aos registos de informação, computadorizados ou não, qualquer que seja a sua natureza, nos quais se encontrem armazenados os dados de uma determinada pessoa. Tal acesso pode ter por objecto que seja possível saber o que se encontra registado, para quê e para quem se realizou o registo de informação, assim como a (ou as) pessoa (s) que recolheram tal informação. Em segundo lugar, o habeas data pode ter a finalidade de acrescentar dados ao registo existente, quer seja pela necessidade de actualizar os que se encontram registados, quer com o fito de incluir os dados não registados. mas necessários para que se tenha uma referência cabal sobre a imagem e identidade da pessoa afectada. Da mesma forma, com o direito em referência, e na sua ausência, através do habeas data, um indivíduo pode rectificar a informação, pessoal ou familiar, que se encontre registada; impedir que esta seja difundida para fins distintos daqueles que justificaram o seu registo ou, inclusive, tem a capacidade de cancelar aqueles que razoavelmente não devam encontrar-se armazenados."*

Por seu lado, na Europa, o direito fundamental à protecção de dados de carácter pessoal é expressamente reconhecido como direito fundamental e claramente diferenciado do direito à intimidade pessoal e familiar das pessoas pelo artigo 8º da Carta de Direitos Fundamentais da União Europeia, que estabelece o seguinte:

*"1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.*

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

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

Os números 2 e 3 deste preceito delimitam o conteúdo essencial de que deve revestir-se a legislação que regule o direito fundamental à protecção de dados pessoais. Deste modo:

- Os dados deverão ser tratados de forma leal.
- Os dados deverão ser tratados para fins específicos.



- O tratamento deverá efectuar-se com base no consentimento do interessado ou como consequência de algum outro fundamento legítimo e previsto legalmente.
- Todas as pessoas terão direito de acesso, rectificação e eliminação do tratamento.
- Deverá existir uma autoridade independente encarregada de zelar pela garantia do direito.

Por outro lado, diferentes instrumentos internacionais, emanados de Organismos Supranacionais dos quais são membros todos ou grande parte dos Estados Ibero-americanos têm vindo a estabelecer os princípios básicos que configuram o direito à protecção de dados pessoais.

Assim, a já citada recomendação da OCDE delimita estes princípios, enumerando como básicos os seguintes:

1. Aplicação aos tratamentos de dados do sector público e privado;
2. Interpretação restritiva das possíveis excepções à aplicação dos princípios;
3. Princípio da limitação da recolha;
4. Princípio da qualidade dos dados;
5. Princípio da especificação da finalidade;
6. Princípio da limitação de uso;
7. Princípio das medidas de segurança;
8. Princípio da transparência;
9. Princípio da participação individual (*Habeas data*)
10. Princípio da responsabilidade
11. Garantias da circulação transfronteiriça, ininterrupta e segura, dos dados pessoais, entre os Estados que observem estes princípios;
12. Estabelecimento de sanções e recursos suficientes em caso de incumprimento.

Por sua vez, devem ser tidas em conta as Directivas para a regulação dos arquivos de dados pessoais informatizados, adoptadas através da Resolução 45/95 da Assembleia Geral das Nações Unidas, de 14 de Dezembro de 1990, que consideram como garantias mínimas a previsão pelas legislações nacionais dos seguintes princípios:

1. Princípio da legalidade e lealdade
2. Princípio da exactidão
3. Princípio da especificação da finalidade
4. Princípio do acesso do titular dos dados



5. Princípio da não discriminação;
6. Limitação da faculdade para abrir derrogações;
7. Princípio da segurança;
8. Supervisão e sanções, através de uma autoridade que deverá oferecer garantias de imparcialidade, independência e competência técnica;
9. Fluxo transfronteiriço de dados baseado na semelhança das garantias;
10. Campo mínimo de aplicação geral a todos os arquivos informatizados públicos e privados.

Juntamente com estes instrumentos, não deve ser esquecida a análise produzida no âmbito da União Europeia em cumprimento da Directiva 95/46/CE. A importância da Directiva no âmbito supra-europeu revela-se essencial, em primeiro lugar, dado que se trata do texto internacional que regula com maior precisão e detalhe os princípios, direitos e deveres que configuram o direito fundamental à protecção de dados.

Além disso, deve recordar-se que o fundamento da Directiva, como já se disse, consiste em estabelecer um quadro harmonizado do direito à protecção de dados pessoais que garanta o livre fluxo de informação no âmbito da União Europeia, favorecendo assim o comércio e o enriquecimento derivado dos fluxos de informação.

Por último, não se deve esquecer que os artigos 25 e 26 da Directiva estabelecem um regime específico para os fluxos transfronteiriços de dados de carácter pessoal, exigindo, como ponto de partida, que o Estado a que se destinem os dados ofereça um nível adequado de protecção de dados. Deste modo, a Directiva dá cumprimento ao princípio essencial de equilíbrio entre a livre transmissão de informação e a protecção do direito das pessoas.

Nesse sentido, a assunção de princípios que possam considerar-se “adequados” aos previstos na Directiva pode constituir um ponto de partida apropriado para facilitar os fluxos transfronteiriços de informação entre ambos os lados do Atlântico, mantendo as garantias adequadas do direito fundamental à protecção de dados pessoais. Não se trata assim de obter uma aplicação transfronteiriça da legislação europeia, mas sim de conseguir uma adequada conciliação entre ambos.

No contexto Ibero-americano, devem citar-se os esforços realizados no âmbito da UNESCO e a Estratégia Latino-americana da Sociedade da Informação (ELAC) levada a cabo no seio da CEPAL, com o objectivo de alcançar a criação de mecanismos de harmonização legal no âmbito da privacidade e protecção de dados pessoais.



Deve sublinhar-se ainda que alguns Estados adoptaram nos últimos anos iniciativas neste sentido. Assim, devem referir-se os desenvolvimentos legislativos levados a cabo pela Argentina, que culminaram na adopção da Decisão da Comissão de 30 de Junho de 2003, segundo a qual se considera que esse Estado garante um nível adequado de protecção no que respeita aos dados pessoais transferidos a partir da Comunidade.

Neste quadro, pode ser interessante analisar a actividade desenvolvida pelo Grupo de Trabalho criado pelo artigo 29 da Directiva 95/46/CE; em particular o seu Parecer 4/2002, de 3 de Outubro, sobre o nível de protecção de dados na Argentina.

Os diversos pareceres aprovados pelo mencionado Grupo de Trabalho relativos ao nível de protecção de dados em Estados terceiros tiveram como referência o documento de trabalho do Grupo sobre Transferências de Dados Pessoais para Países Terceiros: aplicação dos artigos 25 e 26 da Directiva sobre protecção de dados na UE, aprovado a 24 de Julho de 1998, cujo Capítulo 1 analisa o que se deve entender por “protecção adequada”.

Para esse efeito, o documento delimita dois tipos de análises que têm de ser efectuadas à legislação do Estado destinatário dos dados, a fim de poder determinar se a mesma é adequada: uma análise ao seu conteúdo substantivo e outra relacionada com os mecanismos e procedimentos de aplicação da legislação substantiva.

Quanto ao conteúdo substantivo, a legislação do Estado de destino deve conter os princípios básicos de protecção de dados que tradicionalmente têm vindo a ser reconhecidos pelos acordos e directivas internacionais adoptados neste âmbito, e que foram já referidos, considerando-se como tais os seguintes:

1. Limitação da finalidade
2. Qualidade e proporcionalidade dos dados
3. Transparência
4. Segurança e confidencialidade
5. Direitos de acesso, rectificação, supressão e bloqueio dos dados
6. Restrições a transferências subsequentes
7. Categorias especiais de dados
8. Marketing directo
9. Decisão individual automatizada

Estes princípios devem, no mínimo, estar presentes na legislação do Estado destinatário dos dados para que se possa considerar que o mesmo oferece um nível adequado de protecção.



Logicamente, para que se possa considerar que existe um efectivo reflexo legal destes princípios na legislação do Estado em questão, será preciso que a lei tenha um âmbito geral de aplicação aos tratamentos efectuados pelos sectores público e privado, de forma a que não se estabeleçam limites à sua aplicação para além dos relacionados com a actividade meramente pessoal ou familiar de quem os leva a cabo ou as limitações ao direito fundamental no quadro da actividade de uma sociedade democrática.

Por outro lado, quanto à análise aos procedimentos de aplicação das normas substantivas, o documento considera que a existência dos mesmos é indispensável para que um sistema de protecção de dados possa, na prática, outorgar um nível adequado de protecção, dado que pressupõe a existência de mecanismos de controle dos princípios contidos nas leis nacionais.

Como o documento indica, este elemento materializa-se geralmente no estabelecimento de uma autoridade independente de protecção de dados e na regulação de procedimentos adequados que permitem aos afectados obter a protecção dos seus direitos ou a reparação dos prejuízos que lhes tenham sido causados.

Assim, como regra geral, poderá considerar-se que um Estado outorga um nível de protecção adequado quando o mesmo conte com uma norma reguladora da protecção de dados que contenha os princípios substantivos que foram enumerados e quando exista uma autoridade encarregada de velar pelo seu cumprimento, à qual os indivíduos possam dirigir as suas reclamações e que tenha poderes de inspecção e investigação dos tratamentos de dados.

Um último requisito essencial dessa autoridade será a sua capacidade para impor medidas que garantam a efectividade do direito, tais como sanções em caso de incumprimento ou, no mínimo, a capacidade para exigir aos Tribunais a imposição dessas medidas nas situações em que do uso dos seus poderes de investigação se verifique que existem violações da lei de protecção de dados.

A análise descrita permitiu ao Grupo avaliar favoravelmente a adequação do nível de protecção de dados pessoais dos Estados relativamente aos quais posteriormente foi adoptada uma Decisão neste sentido por parte da Comissão Europeia. Basta analisar o já citado Parecer 4/2002, referente ao nível de protecção de dados na Argentina, para comprovar que a sua estrutura e análise se fundamenta no que o citado documento de trabalho estabelece.



3. Directivas (princípios, direitos e obrigações) que deverá conter uma Lei nacional de protecção de dados de carácter pessoal:

1. Âmbito de aplicação

1.1. As presentes directivas serão aplicadas a qualquer tratamento manual ou automatizado de dados pessoais, entendendo-se por tal qualquer informação referente a pessoas físicas identificadas ou identificáveis. Por conseguinte, as directivas serão aplicáveis aos tratamentos levados a cabo por todas as entidades dos sectores público e privado.

1.2. Não obstante, será possível excluir das directivas o tratamento manual ou não automatizado, quando os dados objecto de tratamento não se destinem a ser incorporados num ficheiro estruturado, de acordo com critérios que permitam a identificação das pessoas cujos dados são sujeitos a tratamento.

1.3. Da mesma forma, as directivas não serão aplicáveis ao tratamento de dados de carácter pessoal, automatizado ou manual, que uma pessoa física realize para fins exclusivamente relacionados com a sua vida privada ou familiar.

1.4. Será possível a exclusão da aplicação dos números 2, 3, 4, 5, 6.1, 6.2, 6.3 e 8 das presentes directivas numa lei nacional que regule determinados tratamentos de dados pessoais, na medida em que a sua aplicação possa constituir um risco para a protecção da segurança nacional ou ordem pública, para a saúde pública ou para a moralidade e tal medida seja estritamente necessária e não excessiva no âmbito de uma sociedade democrática.

2. Princípios relacionados com a finalidade e qualidade dos dados

2.1. Tratamento leal e lícito: os dados só poderão ser recolhidos e tratados de boa fé, no estrito respeito da Lei e dos direitos das pessoas e em conformidade com o previsto nas presentes directivas.

2.2. Limitação da finalidade: os dados só poderão ser recolhidos e tratados para o cumprimento das finalidades determinadas, explícitas e legítimas relacionadas com a actividade de quem os trate.

Não poderão ser tratados para fins distintos daqueles que motivaram a sua obtenção a menos que exista legitimação suficiente para tal, conforme o estabelecido no número 3 destas directivas.



2.3. Princípio da proporcionalidade: Só poderão ser sujeitos a tratamento os dados que resultem adequados, pertinentes e não excessivos em relação às finalidades a que se refere o ponto anterior.

2.4. Princípio da exactidão: os dados deverão manter-se exactos, completos e actualizados, correspondendo à verdadeira situação da pessoa a que se refiram.

2.5. Princípio da conservação: os dados deverão ser eliminados ou tornados anónimos quando tenham deixado de ser necessários para o cumprimento das finalidades que justificaram a sua obtenção e tratamento.

### 3. Legitimação para o tratamento

3.1. Os dados só poderão ser recolhidos ou tratados no caso de se ter obtido o consentimento do titular dos dados.

3.2. Não obstante, a Lei poderá estabelecer situações em que não será necessário o consentimento do titular para o tratamento dos seus dados pessoais, atendendo às circunstâncias que envolvam cada situação e, em todo caso, sempre que tal excepção não prejudique os direitos fundamentais do titular. Em particular, a Lei poderá permitir o tratamento de dados sem haver consentimento do titular quando o mesmo se realize no quadro de uma relação jurídica ou por uma Administração no exercício das competências que lhe tenham sido atribuídas.

3.3. Os dados que revelem a ideologia, a filiação sindical, religião ou convicções do titular só poderão ser tratados com o seu consentimento, a menos que a pessoa os tenha tornado públicos de forma manifesta.

3.4. Os dados relacionados com a saúde, a origem étnica e a vida sexual do titular só poderão ser recolhidos e tratados nas condições mencionadas no parágrafo anterior ou quando uma Lei assim o disponha.

3.5 Em todo o caso, as presentes directivas não representarão obstáculos ao adequado tratamento médico do titular dos dados nem a defesa urgente do seu interesse vital.

### 4. Transparência e informação ao titular

4.1 O indivíduo do qual se recolhem os dados deverá ser informado no momento da recolha da identidade do responsável pelo tratamento, dos fins para os quais os dados vão ser tratados e do modo de tornar efectivos os direitos a que se referem os números 5 e 6 destas directivas, assim como de qualquer outra informação necessária



para garantir um tratamento lícito dos dados. Esta obrigação só será exceptuada se o interessado tiver já sido antecipadamente informado destas circunstâncias.

4.2. Quando os dados não tiverem sido obtidos junto do titular deverá o mesmo ser informado do previsto no parágrafo anterior num prazo de tempo razoável e, em qualquer caso, antes de os dados serem comunicados a terceiros.

#### 5. Direitos de acesso, rectificação e cancelamento dos interessados

O interessado cujos dados sejam objecto de tratamento poderá, através de procedimentos claros, expeditos e gratuitos ou sem gastos excessivos:

5.1 Recolher junto do responsável pelo tratamento confirmação da existência ou inexistência de tratamento de dados que lhe diga respeito, assim como informação mínima dos fins de tais tratamentos, das categorias de dados a que se referem e dos destinatários ou das categorias de destinatários a quem tais dados vão ser transmitidos.

5.2. Recolher informação junto do responsável pelo tratamento, de forma inteligível, dos dados objecto dos tratamentos, bem como toda a informação disponível sobre a origem dos dados.

5.3. Exigir, no seu caso, a rectificação ou eliminação dos dados que se revelem incompletos, inexactos, inadequados ou excessivos, como previsto nas presentes directivas.

5.4. Exigir que se notifiquem os terceiros a quem os dados tenham sido comunicados de qualquer rectificação ou eliminação efectuada de acordo com o parágrafo anterior.

#### 6. Outros direitos dos titulares

Além dos direitos a que se refere o número anterior, o titular terá os seguintes:

6.1. Não ser submetido a decisões com efeitos jurídicos sobre si mesmo ou que o afectem de forma significativa, baseadas unicamente num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como o seu rendimento laboral, crédito, fiabilidade ou conduta. No entanto, será possível a adopção de tais decisões quando estas se verificarem no quadro de uma relação jurídica livremente aceite pelo titular, em que se concede ao mesmo a possibilidade de efectuar alegações acerca do resultado da avaliação.



6.2. Opor-se ao tratamento dos seus dados, por motivos não excluídos por Lei, como consequência da ocorrência de uma razão excepcional e legítima derivada da sua situação pessoal concreta.

6.3. Opor-se, a seu pedido e sem gastos, ao tratamento de dados pessoais que lhe digam respeito, destinados a actividades ligadas à publicidade e à prospecção comercial.

6.4. Recorrer ao auxílio dos tribunais e das autoridades a que se refere o número 9 destas directivas, caso considere que o tratamento dos seus dados está a ser realizado em contravenção das mesmas.

6.5. Ser indemnizado por qualquer dano ou lesão que tenha sofrido nos seus bens ou direitos em consequência do tratamento de dados levado a cabo contra o disposto nestas directivas.

## 7. Segurança e confidencialidade no tratamento

7.1. Deverão adoptar-se as medidas técnicas e organizativas que resultem necessárias para proteger os dados contra a sua adulteração, perda ou destruição acidental, ou acesso não autorizado ou uso fraudulento.

7.2. Os intervenientes em qualquer fase do tratamento de dados pessoais estão obrigados ao segredo profissional relativamente aos mesmos. Tal obrigação subsistirá mesmo depois de terminada a sua relação com o responsável do tratamento.

## 8. Limitações à transferência internacional de dados

8.1. Como regra geral só poderão efectuar-se transferências internacionais de dados para o território de Estados cuja legislação recolha o disposto nas presentes directivas.

8.2. Não obstante, a Lei poderá estabelecer pressupostos em que, excepcionalmente, seja possível a transferência internacional de dados para outros Estados, atendendo às circunstâncias que concorram em cada pressuposto. De qualquer modo, deverá ter-se em conta os direitos e interesses do titular e, em particular, se o mesmo deu o seu consentimento à transferência em causa.

8.3. Fora dos pressupostos mencionados nos dois parágrafos anteriores, só será possível a transferência internacional de dados no caso de se obter autorização da autoridade a que se refere o número 9, para o que será necessário que o exportador



dos dados forneça garantias suficientes que assegurem que o importador dos dados cumprirá o disposto nestas directivas.

## 9. Autoridades de controlo

9.1. A garantia do cumprimento destas directivas deverá ficar sujeita ao controlo de uma ou várias autoridades de protecção de dados. As autoridades poderão ter personalidade própria ou serem integradas na Administração Pública ou num Organismo Público pré-existente. Também poderão ter como função exclusiva o cumprimento das normas de protecção de dados ou exercer tal competência juntamente com outras atribuídas pela sua legislação.

A organização territorial do Estado não poderá constituir um obstáculo para que as garantias derivadas da existência da ou das autoridades de protecção de dados sejam reais e efectivas em relação a todos os tratamentos realizados tanto pelo sector público como pelo privado.

9.2. As autoridades de protecção de dados deverão actuar com plena independência e imparcialidade, não podendo estar submetidas no exercício das suas funções ao mandato de nenhuma autoridade pública. Deverão estabelecer-se mecanismos que garantam a independência e inamovibilidade das pessoas a cujo cargo se encontre a direcção de tais autoridades.

9.3 As autoridades deverão ter no mínimo as seguintes competências:

- Tomar conhecimento das reclamações que lhes sejam dirigidas pelas pessoas, em particular quanto ao exercício dos direitos a que se refere o número 5 destas directivas.
- Realizar as averiguações e investigações que sejam necessárias para o cumprimento das directivas, podendo aceder aos dados que sejam objecto de um tratamento e recolher toda a informação necessária para o cumprimento da sua missão de controlo.
- Adoptar as medidas que sejam necessárias para evitar a persistência do incumprimento das directivas.
- Manter um registo dos tratamentos levados a cabo pelos sectores público e privado, a que possam aceder os titulares dos dados, a fim de poderem exercer os direitos reconhecidos nas presentes directivas. O pedido de inscrição realizar-se-á mediante modelos simplificados e baseados em padrões



técnicos, respeitando o princípio da neutralidade tecnológica, utilizando-se sempre que possível técnicas ou meios electrónicos.

- Autorizar, quando for necessário, as transferências internacionais de dados para Estados cuja legislação não contemple o disposto nas presentes directivas.
- Promover o uso de mecanismos de auto-regulação como instrumento complementar de protecção de dados pessoais que: (I) represente um valor acrescentado no seu conteúdo relativamente ao disposto nas leis, (II) contenha ou seja acompanhado de elementos que permitam medir o seu nível de eficácia quanto ao cumprimento e ao grau de protecção dos dados pessoais e (III) consagre medidas efectivas no caso do seu incumprimento.
- Dar parecer sobre os projectos de disposições legislativas que possam afectar o direito fundamental das pessoas à protecção de dados pessoais.
- Divulgar junto dos indivíduos e dos poderes públicos o conteúdo do direito fundamental à protecção de dados pessoais.
- Cooperar com as autoridades de protecção de dados para o cumprimento das suas competências e gerar os mecanismos de cooperação bilateral e multilateral para assistência mútua e prestar o devido auxílio mútuo sempre que ele seja necessário.

## 10. Sanções

10.1. O incumprimento das disposições que reflectem o previsto nestas directivas deverá ser sancionado em conformidade com a legislação interna. A competência para a imposição das respectivas sanções poderá ser atribuída à autoridade de protecção de dados a que se refere o número 9 ou aos órgãos judiciais.

10.2 Em todo o caso, as autoridades de protecção de dados deverão ter capacidade suficiente para recorrerem à via judicial competente para conseguir a adopção das medidas necessárias que garantam o cumprimento destas directivas e, em particular, a imposição das sanções que se apliquem.

10.3. Se as autoridades de protecção de dados forem directamente competentes para a imposição de sanções, as suas resoluções deverão ser passíveis de recurso para os Tribunais.