A DIRETIVA EUROPEIA SOBRE PROTEÇÃO DE DADOS PESSOAIS – uma análise de seus aspectos gerais

Demócrito Reinaldo Filho
(Juiz de Direito, 32ª. Vara Cível)

Sumário: 1. Regulamentação da proteção de dados na Europa – uma introdução. 2. Instrumentos multinacionais. 3. A Diretiva Europeia sobre a proteção de dados pessoais.

1. Regulamentação da proteção de dados na Europa – uma introdução.

A proteção da *privacidade* individual desde muito se inseriu entre as preocupações dos juristas, que sempre a enxergaram como um dos *direitos da personalidade*. Leis específicas de proteção de dados pessoais, no entanto, começaram a surgir só a partir das décadas de 60 e 70, com o advento das tecnologias da informação. O grande poder de processamento de dados pelos computadores foi o fator responsável pela germinação da moderna legislação nessa área. O aumento do poder de controle e processamento de dados prontamente desencadeou a demanda por uma legislação específica para regular a coleta e manuseio de informações pessoais.

Embora o "direito à privacidade" (*right to privacy*) tenha se desenvolvido originalmente na jurisprudência e doutrina norte-americanas, foi a Europa que se notabilizou como a fonte dos principais e mais completos conjuntos de leis sobre proteção de dados pessoais, que emergiram nessas décadas. Em 1970, o Estado alemão de Hesse editou a primeira lei sobre essa matéria. A Suécia conta com o *Datalegen*, Lei 289 de 11 de maio de 1973. Desde 1977, a Alemanha tem uma lei federal de proteção de uso ilícito de dados pessoais. A Dinamarca regulamenta a questão da proteção de dados pelas Leis 243 e 244, ambas de 08 de julho de 1978, que estenderam a proteção também para as pessoas jurídicas. A França tem a Lei 78-77, de 06 de janeiro de 1978. A Espanha tem a peculiaridade de ter uma regra constitucional determinando a regulamentação da proteção da privacidade contra invasões da atividade informática (art. 18, par. 1º.). A Constituição de Portugal de 1977 tem texto ainda mais completo (art. 35), pois contempla a previsão do direito do cidadão de conhecer os dados que lhe são concernentes, de que esses dados sejam utilizados de acordo com a finalidade para o qual foram recolhidos e, ainda, de retificá-los (em caso de erro) e de atualizá-los.

Atualmente, uma expressiva parte dos países europeus possui leis de proteção de dados, incluindo a Áustria, Bélgica, República Checa, Finlândia, Hungria, Irlanda, Itália, Luxemburgo, Holanda, Suécia, Suíça e Inglaterra.

As leis européias de proteção à privacidade e regulamentação do processamento de

dados pessoais distinguem-se por quatro características essenciais[1]. São elas:

a) aplicam-se em geral aos setores públicos e privados;
b) aplicam-se a um largo leque de atividades, incluindo a coleta de dados, armazenamento, uso e disseminação;
c) elas impõem obrigações a qualquer pessoa que se envolva em alguma dessas atividades;
d) têm em geral poucas limitações setoriais, isto é, aplicam-se indistintamente a qualquer categoria de dados.

2. Instrumentos multinacionais.

A edição de leis nacionais de proteção de dados pessoais pelos países individualmente foi um fenômeno seguido e, em alguns casos até antecipado, pela elaboração de textos de caráter multinacional. Em 1980, o Comitê de Ministros da *OECD – Organization for Economic Cooperation and Development*[2], publicou as "Diretrizes sobre Proteção da Privacidade e o Fluxo Transnacional de Informações Pessoais"[3], documento que estabeleceu princípios básicos sobre proteção de dados e sobre o fluxo de informações entre países que possuem leis em conformidade com esses princípios. Essas "guidelines", no entanto, não têm força coercitiva e permitem uma variação muito ampla na sua implementação no direito interno dos países. Um ano mais tarde, em 1981, o *Conselho da Europa*[4] promulgou a Convenção "Para a proteção dos indivíduos com respeito ao processamento automático de dados pessoais"[5], que entrou em vigor em 1985. Dita Convenção é bem similar às "Guidelines" da OECD, embora com foco na proteção de dados para resguardar a privacidade individual. Ela contém regras no sentido de que a proteção das informações pessoais alcança todas as fases da atividade de processamento de dados, desde a coleta e o armazenamento até a disseminação. Especificamente, ela estabelece que: os dados devem ser obtidos e processados de uma maneira justa; que devem ser usados e armazenados somente com propósitos legais; que devem ser processados de forma adequada, relevante e não excessiva em relação à finalidade inicial da coleta; que os dados devem ser exatos, atualizados e armazenados por período não superior que o necessário. Ela confere à pessoa a quem as informações se referem o direito de inquirir o controlador sobre sua existência, de obter uma cópia e de corrigir os dados falsos ou impropriamente processados. A Convenção estabelece, ainda, que todos os países signatários devem editar leis nacionais em conformidade com seus princípios.

Esses dois textos multinacionais tiveram uma profunda influência na edição de leis

---

[1] Segundo Fred H. Cate, em "Privacy in the Information Age", Brookings Institution Press, Washingto D.C., p. 32/33.

[2] A OECD foi fundada em 1960 por vinte países, incluindo os EUA, com o objetivo de "promover o bem estar econômico e social, assistindo os governos de seus membros na formulação e coordenação de políticas; para estimular e harmonizar os esforços de seus membros em favor de países em desenvolvimento; e para contribuir com a expansão do comércio mundial". O endereço do *site* da OECD é http://www.oecd.org/ .

[3] "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*", documento divulgado em 1o. de outubro de 1980. Pode ser encontrado em: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

[4] Hoje com o nome de *Conselho da União Européia*. Site: http://ue.eu.int/

[5] "For the Protection of Individuals with Regard to Automatic Processing of Personal Data" (ETS No. 108, de 1o. de outubro de 1980). O texto pode ser encontrado em: http://www.coe.fr/eng/legaltxt/108e.htm .

de proteção de dados pessoais de diversos países. Aproximadamente 30 países assinaram a Convenção e vários outros estão planejando fazê-lo em breve. Desde 1997, 15 países membros da União Europeia já possuíam uma legislação nacional em conformidade com a Convenção. As "Guidelines" também tiveram influência na legislação de vários países, mesmo aqueles não membros da OECD.

Todavia, a atividade legiferante no âmbito interno dos Estados nacionais não se deu de forma uniforme, ao menos por três razões. A primeira, porque algumas leis nacionais de proteção de dados pessoais já existiam anteriormente à adoção da Convenção. A segunda, porque ela não era auto-executável, permitindo que os países a implementassem de maneiras muito variadas. E, a terceira, porque ela não incorporou definições importantes, como, p. ex., o que constitui um "adequado" nível de proteção de dados pessoais; como resultado, os países membros viram-se livres para implementar suas próprias definições e conceitos, na legislação interna de cada um deles.

Com o nível de proteção à privacidade variando de país a país, fruto da desigual aplicação tanto da Convenção quanto das "Guidelines", a União Européia editou a Diretiva 95/46/EC relativa ao processamento de dados pessoais[6], de forma a harmonizar o grau de proteção existente nas leis nacionais e de assegurar o livre fluxo de informações pessoais entre os países membros. A Diretiva estabelece um conjunto de regras que não somente reforça os direitos anteriormente previstos nas leis nacionais, mas também criou um novo conjunto de direitos, aplicando-se à atividade de processamento de dados quer ela aconteça de forma automatizada, em ambientes eletrônicos, ou na forma tradicional manual.

3. A Diretiva 95/46/EC relativa ao processamento de dados pessoais

Formalmente aprovada em 24 de outubro de 1995, para entrar em vigor 03 anos depois, a Diretiva é um amplo texto legal em matéria de proteção de dados pessoais. Ela exige que cada país membro da União Européia tenha uma agência ou comissário de proteção de dados, este último um agente estatal que supervisione a aplicação dos princípios e leis de proteção à privacidade individual. Ela também exige que cada um deles edite leis sobre o processamento de dados pessoais. A Diretiva estabeleceu um prazo de 03 anos após a data de sua vigência, para que os países membros da União Européia adotem as medidas legislativas e regulamentares necessárias para incorporar suas regras no direito interno deles. Adiante fazemos uma análise mais detalhada do escopo e regras específicas fundamentais da Diretiva.

3.1. Definições contidas na Diretiva

Uma das falhas da Convenção sobre proteção de dados pessoais, conforme já ressaltamos, foi a não inclusão de definições importantes relacionadas com a atividade de processamento de informações. A Diretiva não incorreu no mesmo erro, trazendo, logo no seu art. 2º., um extenso leque de conceitos. Por exemplo, dados pessoais são definidos como "qualquer informação relativa a uma pessoa singular identificada ou identificável" (art. 2º., a). Esse conceito, com a abrangência que lhe foi dada, alcança não somente informações textuais, mas também fotografias, imagens audiovisuais e registros de sons

---

6 "*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*".

relativos a uma pessoa. Além disso, o raio de extensão não se limita a pessoas vivas; os dados referentes a pessoas naturais em geral, quer estejam vivas ou não, incluem-se no conceito legal de "dados pessoais". Outro conceito importante destacado na Diretiva é o de processamento de dados pessoais, que corresponde a "qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a coleta, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição" (art. 2º. b). O controlador (*controller*) dos dados ou pessoa responsável pelo tratamento também é definido na Diretiva, como "a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais" (art. 2º., d). Essa definição é de suma importância porque o controlador dos dados é a pessoa primariamente obrigada pelas regras das Diretiva.

Além dessas definições, a Diretiva traz ainda outras, tais como os conceitos de "fichário de dados pessoais", de "subcontratante", de "terceiro", de "destinatário" e de "consentimento do sujeito dos dados" (art. 2º., "c", "e", "f", "g" e "h"), todos estes também de suma importância para a correta compreensão e aplicação de seus preceitos.

3.2. Escopo da Diretiva

No seu art. 3º., a Diretiva trata de definir seu âmbito de aplicação, estabelecendo que se aplica a qualquer forma de processamento de dados, quer este se realize de maneira automatizada (ainda que parcial) ou não (item 1). Ficam excluídas do seu raio de alcance: a) as atividades não sujeitas à aplicação do direito comunitário; b) o tratamento de dados que tenha por objeto a segurança pública e a defesa e segurança do Estado; c) as atividades do Estado voltadas à aplicação da lei penal (prevenção, investigação e repressão de infrações penais); e c) o tratamento de dados "efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas" (item 2). Além dessas, outras exceções e restrições, em relação a direitos e obrigações específicos, são feitas no art. 13 da Diretiva.

3.3. Princípios e direitos básicos contidos na Diretiva em relação ao processamento de dados

3.3.1. Princípio da finalidade (*purpose limitation principle*)

Os dados pessoais somente podem ser recolhidos de acordo com finalidades determinadas, explícitas e legítimas e não podem, posteriormente, ser utilizados de maneira diferente daquelas previstas inicialmente (art. 6º., b). Como efeito, o tratamento de dados pessoais implica o máximo de transparência, não podendo ser feito com base em razões ocultas. Os propósitos que justificam o processamento têm que ser explícitos, claramente identificados.

3.3.2. Princípios relativos à qualidade dos dados

Os dados submetidos a tratamento:

a) têm que ser processados de uma maneira leal e lícita (art. 6º., I, a);
b) têm que ser adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente (art. 6º, I, c);
c) têm que ser exatos e atualizados (art. 6º., I, d);
d) devem ser conservados apenas durante o período necessário para o atingimento das finalidades para as quais foram recolhidos (art. 6º., I, e).

3.3.3. Princípios relativos à legitimidade do processamento dos dados

O art. 7º. enumera situações que justificam o processamento de dados pessoais. Para ser considerado legítimo, o tratamento de dados necessita se enquadrar em uma das circunstâncias descritas.

O tratamento de dados somente se justifica se (art. 7º.):

a) o sujeito ou titular dos dados tiver dado seu consentimento;
b) para execução de um contrato do qual seja parte;
c) for necessário para o cumprimento de uma obrigação legal;
d) para a proteção de direitos vitais do sujeito;
e) para realizar interesses legítimos da pessoa responsável pelo processamento.

3.3.4 Regras relativas ao tratamento de categorias específicas de dados

O tratamento de dados considerados sensíveis, ou seja, aqueles que se referem a origem racial ou étnica de uma pessoa, suas opiniões políticas, credos religiosos, filiações a sindicatos, convicções éticas ou filosóficas, bem como os concernentes à sua saúde e vida sexual, em regra é proibido (art. 8º., I), salvo quando:

a) a pessoa em causa tiver dado seu inequívoco consentimento (a não ser quando a legislação nacional prevê que a proibição não pode ser retirada pelo consentimento)
b) o tratamento é necessário para o cumprimento de obrigações trabalhistas do controlador (desde que a legislação nacional estabeleça garantias adequadas);
c) o tratamento for necessário para proteger interesses vitais do sujeito dos dados;
d) o tratamento for efetuado por uma entidade sem fins lucrativos, relativamente a seus membros ou a pessoas com as quais mantenha relacionamento periódico, desde que os dados não sejam comunicados a terceiros sem o consentimento deles;
e) o tratamento disser respeito a dados tornados públicos ou for necessário à defesa de um direito em processo judicial (art. 8º, item 2);
f) for necessário para fins de tratamento médico ou de saúde, desde que o responsável por ele esteja submetido ao sigilo profissional (art. 8º., item 3).

A Diretiva ainda prevê que os Estados-membros podem estabelecer outras exceções à regra geral do não processamento de dados sensíveis (art. 8º., item 4) e que o tratamento de informações relativas a condenações penais deve ficar sob o controle de autoridades

públicas, podendo essa mesma regra se aplicar às infrações cíveis e administrativas (item 5).

3.3.5. Garantias básicas do titular (sujeito) dos dados

A Diretiva estabelece uma série de direitos básicos da pessoa a respeito de quem os dados são coletados, direitos esses que, se vistos de outro ângulo, constituem deveres imputados aos processadores (controladores) das informações pessoais. De fato, os controladores, aqueles responsáveis pelo tratamento de dados pessoais, estão obrigados a fornecer à "pessoa em causa" uma série de informações, que se constituem em direitos básicos do sujeito, em relação ao processamento de seus dados pessoais.

3.3.5.1 O direito de ser informado (arts. 10 e 11)

Os dados referentes a uma pessoa podem ser recolhidos diretamente junto a ela ou por meio de terceiros, que disponham desses mesmos dados. Na primeira hipótese, a Diretiva (no seu art. 10) estabelece que o controlador tem que prestar à "pessoa em causa" as seguintes informações:

a) a identidade do responsável (ou do seu representante, se for o caso) pelo tratamento dos dados;
b) a finalidade do tratamento dos dados.

Se necessário, outras informações ainda devem ser prestadas, "tendo em conta as circunstâncias específicas do recolhimento dos dados, para garantir à pessoa em causa um leal tratamento dos dados"[7]. Essas informações adicionais incluem:

a) os destinatários dos dados[8];
b) o caráter obrigatório ou facultativo de sua resposta (do controlador dos dados), bem como as conseqüências se não responder;
c) a existência do direito de acesso aos dados e do direito de retificá-los.

O texto da Diretiva não indica quais circunstâncias específicas são essas, que fazem surgir para o controlador ou processador dos dados o dever de prestar informações adicionais. Uma situação exemplificativa da necessidade de serem prestadas as informações adicionais pode ser encontrada na utilização de *cookies* por parte de um operador de *website*. Pela razão de que seu uso nem sempre é aparente para o internauta (a pessoa a respeito de quem os dados são coletados), ou, mesmo sendo, as implicações decorrentes da utilização de dados pessoais coletados por meio deles não podem ser precisamente avaliadas, o operador está obrigado a prestar as informações adicionais no caso de utilização de *cookies*. A mera presença de um aviso no *site* alertando sobre a existência de

---

[7] O conceito de "processamento leal" (fair processing) deve ser buscado em conformidade com a exigência de transparência, posta no art. 6.1.b da Diretiva.

[8] O "destinatário" (*recipient*) dos dados é definido no art. 2o., "g", da Diretiva, como "a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que receba comunicações de dados, independentemente de se tratar ou não de um terceiro".

cookies, por si só, não atende os padrões de conteúdo informacional exigido pela Diretiva[9].

Praticamente as mesmas informações (requeridas no art. 10) devem ser prestadas quando os dados pessoais não são recolhidos junto à "pessoa em causa" (art. 11)[10]. E devem ser prestadas, diz a Diretiva, "no momento em que os dados forem registrados ou, se estiver prevista a comunicação a terceiros, o mais tardar quando da primeira comunicação desses dados" (item 1 do art. 11).

No contexto dos ambientes eletrônicos, essas provisões legais têm especial relevo. Como se sabe, a arquitetura das redes informáticas de comunicação facilita a coleta e transmissão de dados pessoais. Os operadores de sistemas informáticos, tais como provedores de acesso à Internet e outros prestadores de serviços *on line*, estão obrigados ao respeito a essas regras sempre que atuarem no processamento de dados. Tomemos, por exemplo, um operador de *website*. Na eventualidade de coleta de algum dado de caráter pessoal – seja através de *cookies* ou outro método -, na medida em que um internauta visite sua página, está obrigado a prestar as informações previstas na Diretiva. Isso pode ser feito por meio de um aviso que apareça na página eletrônica, ao início do processo de coleta, dando conhecimento ao internauta dessa atividade. As mesmas informações devem ser prestadas no caso de os dados pessoais não serem colhidos diretamente da "pessoa em causa". Como também é notório, nos ambientes eletrônicos atuam uma série de agentes intermediários, desde provedores de acesso à Internet, provedores de serviços, operadores de páginas *web*, simples usuários, enfim, uma série de atores que podem, dependendo das circunstâncias, participar do processo de tratamento e transmissão de dados alheios. O dever de prestar informações ao titular dos dados também se aplica, sempre que, recebendo-os de terceiro, a pessoa fizer uso deles ou pretender repassá-los adiante. Empresas de e-marketing ou que exploram o comércio eletrônico, por exemplo, que têm a necessidade de transferir dados alheios (de seus clientes ou não), como decorrência de sua própria atividade, devem informar o "sujeito" sobre a transmissão dos dados. As informações obrigatórias podem ser prestadas utilizando-se a própria rede de comunicação por meio do qual os dados foram colhidos ou repassados, sempre que isso se fizer possível.

Embora essas sejam as regras, o seu cumprimento às vezes pode ser de difícil aplicação prática. Nos ambientes das redes telemáticas abertas, saber precisamente quem teve acesso a uma categoria de dados nem sempre é possível.

O item 2 do art. 11 trata das exceções ao direito à informação, nos casos em que os dados não são coletados junto ao "sujeito em causa". Prevê que a obrigatoriedade da prestação das informações ao "sujeito dos dados" (*data subject*) não se aplica sempre que o processamento for feito com "finalidades estatísticas, históricas ou de investigação científica", e desde que esse dever se mostre "impossível ou implicar esforços desproporcionais"[11]. Essa exceção serve, por exemplo, para os casos em que o operador colhe os dados em uma base de dados na Internet, e não tem qualquer contato com a pessoa a quem eles se referem. Seria um peso excessivo exigir que o controlador prestasse informações a uma pessoa que ele não tem contato direto, ou nem sequer saberia como

---

[9] Essa também é a opinião de Sophie Louveaux, em seu artigo "Principles on Directive 95-46-CE", parte do "Sprit Project – Electronic Commerce Legal Issues Platform – Privacy Issues".

[10] O art. 11 estabelece também, para a hipótese que especifica, que o controlador deve informar o titular a respeito das categorias de dados envolvidos (letra "c").

[11] O dispositivo ainda excepciona o controlador do dever de prestar informações "quando a lei impõe o registro dos dados ou a sua divulgação".

contactá-la. Para situações como essa, é que a Diretiva proveu a dita exceção. Isso não significa, entretanto, que o processador nesses casos não esteja submetido a outros princípios e regras estabelecidos na Diretiva. Ele está submetido, por exemplo, aos princípios da finalidade e da adequação, insculpidos no art. 6º.

A exceção ao direito à informação prevista no item 02 do art. 11 acena, claramente, no sentido de que o controle sobre os dados pessoais (por parte do sujeito dos dados) fica bastante reduzido, sempre que eles não são coletados junto ao titular. É certo que a exceção somente se aplica às hipóteses em que os dados são coletados para fins "estatísticos, históricos ou de pesquisa científica", mas a regra pode ser uma porta aberta para o titular perder o controle sobre seus dados pessoais, já que não saberá quem os detém[12].

3.3.5.2 O direito de acesso e de correção

O *direito de acesso* e o *direito de correção* dos dados pessoais são disciplinados mais detalhadamente no art. 12 da Diretiva, que estabelece a obrigação dos Estados-membros editarem leis que garantam à *pessoa em causa* (sujeito dos dados) o direito de obter, mediante requisição, com periodicidade razoável e sem demora ou custos excessivos:

a) confirmação da existência de dados pessoais;
b) informações sobre os fins a que se destina o tratamento;
c) as categorias de dados objeto do tratamento e sua origem;
d) os destinatários dos dados;
e) a lógica do sistema, em caso de tratamento automatizado de dados.

Como corolário do *direito de acesso*, as leis nacionais devem assegurar também o direito do sujeito dos dados de retificar, apagar ou bloquear a transferência daqueles que sejam indevidamente processados, especialmente os incompletos ou inexatos. O sujeito (titular) dos dados deve ter ainda assegurado o direito de notificação aos terceiros (a quem os dados hajam sido transferidos) de qualquer retificação, eliminação ou bloqueio de dados inexatos ou indevidamente processados.

Esse último direito do "sujeito dos dados", de notificação a terceiros das alterações eventualmente produzidas, pode se mostrar excessivamente oneroso, ou mesmo impossível de ser realizado na prática, quando se tratar dos ambientes eletrônicos. Tome-se o exemplo de um controlador de uma base de dados disponibilizada na Internet. Ele em regra não tem conhecimento de quantas e quais pessoas acessaram os dados que disponibilizou, não tendo, por conseguinte, como notificá-los de eventuais alterações solicitadas pela pessoa a quem os dados se referem. Por isso mesmo, a Diretiva ressalva que o *direito de notificação* não pode ser exigido quando "isso for comprovadamente impossível ou implicar um esforço desproporcional" (art. 12, letra "c").

3.3.5.3 O direito de objeção

Ao titular dos dados é assegurado o direito, desde que fundado em relevantes e legítimas razões de ordem particular, de se opor ao processamento das informações que lhe digam respeito, salvo quando as leis nacionais dispuserem em contrário. Sempre que

[12] Essa advertência é feita por Sophie Louveax (ob. cit.), que reclama que as leis nacionais sobre proteção de dados têm que definir melhor o escopo dessa exceção.

houver uma objeção justificada, o processamento dos dados, ainda que iniciado, deve ser suspenso em relação às informações que disser respeito ao interessado (art. 14, "a").

O *direito de objeção* é incondicional quando disser respeito ao processamento de dados para fins de marketing. Nesses casos, não se leva em consideração os motivos para objeção do titular dos dados. Tem ele o direito de se insurgir contra o processamento de suas informações pessoais, não sendo necessário invocar os motivos de sua recusa. Além disso, tem o direito de ser informado antes que seus dados sejam transferidos a terceiros com esses fins (de marketing), de modo a poder manifestar sua oposição a tal comunicação (art. 14, "b").

3.3.5.4 O direito de não ser submetido a processos automatizados de decisão

Em seu artigo 15, sob o título "Decisões individuais automatizadas", a Diretiva estabelece uma regra especial e extremamente inovadora, não presente na maioria dos outros textos legais de proteção a dados pessoais. Trata-se de norma que objetiva regular a construção de perfis de forma automatizada, métodos conhecidos como "automated profiling practices". Tem a seguinte redação o dispositivo em questão:

> "Artigo 15º
> Decisões individuais automatizadas
> 1. Os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento".

Como se observa, a regra em comento atribui ao indivíduo o direito de não se submeter a certos processos de decisão automatizados. Tem aplicação aos sistemas informatizados de construção de perfis, cada dia mais presentes em grandes empresas privadas. A criação de perfis (*profiling*) consiste em sistema ou método de inferir características (geralmente comportamentais) sobre uma pessoa a partir da coleta de determinados dados e, então, tratá-la de acordo com essas características. Sistemas automatizados e programas específicos são capazes de, a partir de padrões e sequências de dados pessoais, estabelecer um conjunto de indicações comportamentais (o perfil), baseado em probabilidades. A partir do tipo de "perfil" gerado, o programa, então, é utilizado para a tomada de decisões em relação à pessoa pesquisada. Por meio de diferentes técnicas e abordagens, esses sistemas tornam o processo de tomada de decisões mais otimizado e estável, substituindo a decisão humana por decisões automatizadas. As decisões podem envolver diferentes aspectos da vida da pessoa (que tem os dados processados), como performance no trabalho, histórico creditício, conduta pessoal, desempenho em certas áreas de atuação etc. Pretendentes a cargo, à compra de um determinado bem ou à obtenção de financiamento preenchem questionários que são utilizados para tomadas de decisões com base nas respostas fornecidas. A norma da Diretiva (art. 15) proíbe as decisões automáticas nos casos em que possam afetar a vida das pessoas. O processador dos dados não deve tomar decisões automatizadas em relação às pessoas submetidas ao processo de coleta de informações, a não ser dentro de certas condições estabelecidas no item 2 do art. 15, como

por exemplo, quando o processo automático de decisões ocorre para propiciar a execução de um contrato, quando se confere ao sujeito dos dados a oportunidade de dar sua opinião ou outras salvaguardas são aplicadas[13].

Os sistemas automáticos de processamento de informações e tomada de decisões fazem aumentar o risco do abuso das tecnologias para regular o comportamento humano. A norma da Diretiva procura minimizar essa tendência, ao colocar nas mãos do sujeito dos dados a possibilidade de se contrapor a que decisões que afetem sua órbita de interesses e sua pessoa sejam tomadas com base exclusivamente em processos automatizados.

3.3.6 Exceções e limitações dos direitos do titular (sujeito) dos dados

Dentro de certas circunstâncias e para atingir determinadas finalidades, os Estados-membros da UE podem adotar medidas legislativas para restringir o alcance de alguns direitos garantidos aos titulares dos dados. Com efeito, o art. 13 da Diretiva estabelece a possibilidade de restrição de direitos sempre que o processamento ou coleta de dados envolver um interesse público relevante. Assim, especificamente os direitos estipulados no nº 1 do artigo 6º, no artigo 10º, no nº 1 do artigo 11º e nos artigos 12º e 21º, podem ser relativizados quando o processamento de dados pessoais for necessário para segurança e defesa do Estado, para fins de segurança pública, para prevenção, investigação e repressão de infrações penais, para atingir um importante interesse financeiro ou econômico do Estado-membro ou da União Européia, para possibilitar o exerício de determinadas funções públicas ou ainda para proteger direitos e liberdades alheias. O direito de acesso e correção (referidos no art. 12) também podem ser restringidos quando os dados pessoais forem utilizados para fins de investigação científica, desde que certas garantias jurídicas sejam observadas.

3.4 Segurança e confidencialidade dos dados

As entidades privadas e públicas devem implementar medidas técnicas e organizacionais apropriadas à proteção dos dados pessoais que processam e armazenam. As medidas têm que ser adequadas aos riscos que a atividade representa e à natureza dos dados tratados, de modo a protegê-los contra destruição (acidental ou ilícita), perda acidental, alteração, difusão ou acesso não autorizado (art. 17).

Além de manter um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger, o responsável pelo processamento, ou pessoa a ele subordinada, deve também manter a confidencialidade do tratamento.

3.5 Obrigação de notificação à autoridade supervisora e controle prévio

[13] O citado item 2 do art. 15 da Diretiva tema a seguinte redação: "2. Os Estados-membros estabelecerão, sob reserva das restantes disposições da presente diretiva, que uma pessoa pode ficar sujeita a uma decisão do tipo referido no nº 1 se a mesma:a) For tomada no âmbito da celebração ou da execução de um contrato, na condição de o pedido de celebração ou execução do contrato apresentado pela pessoa em causa ter sido satisfeito, ou de existirem medidas adequadas, tais como a possibilidade de apresentar o seu ponto de vista, que garantam a defesa dos seus interesses legítimos; ou b) For autorizada por uma lei que estabeleça medidas que garantam a defesa dos interesses legítimos da pessoa em causa."

Os representantes das empresas que atuam na coleta e processamento de dados pessoais devem notificar previamente a autoridade pública responsável pela supervisão dessa atividade. Como se sabe, a Diretiva impôs aos Estados-membros da União Europeia a obrigação de criação de cargos a serem preenchidos por agentes públicos responsáveis pela fiscalização da aplicação de suas normas. Esses agentes públicos, chamados de comissários para proteção de dados pessoais, têm poderes para fiscalizar empresas que processam dados pessoais, aplicar multas e ingressar com processos judiciais quando verificam alguma irregularidade ou inobservância das normas e princípios da Diretiva 95/46/EC. Nenhuma entidade, portanto, pode iniciar alguma atividade automatizada de tratamento de dados pessoais sem antes notificar o comissário ou agente público responsável pela supervisão dessa atividade (art. 18). Essa notificação pode ser feita de maneira simplificada ou mesmo dispensada se, em face do tipo de tratamento ou da natureza dos dados, o processamento não é suscetível de prejudicar direitos ou liberdades da pessoa que tem os dados tratados.

Alguns tratamentos que ofereçam um elevado risco às liberdades e direitos da pessoa titular dos dados não podem ser iniciados antes da obtenção da aprovação pela autoridade supervisora. Nesses casos, o responsável pelo processamento de dados deve consultar previamente a autoridade supervisora. A Diretiva prevê que os Estados-membros devem, através de regulamento, indicar os tipos de tratamentos que apresentam elevado risco às pessoas e que, portanto, necessitam de aprovação prévia (art. 20).

3.6 Cadastro

O art. 21 da Diretiva estabelece que as autoridades supervisoras das atividades de processamento de dados pessoais (*data protection authorities*), conhecidas como comissários para proteção de dados, devem manter uma espécie de cadastro das entidades que processam dados de forma massificada, para acesso ao público. Esse cadastro abrange somente empresas que, pela forma do tratamento ou tipo de dados processados, estão obrigadas a notificar a autoridade de proteção de dados, na forma do art. 18.

3.7 Sanções administrativas e ações judiciais

Sem prejuízo de multas e outras sanções aplicadas pela autoridade pública, a qualquer pessoa é assegurado o direito de ingressar em juízo quando ocorrer violação dos seus direitos garantidos pelas normas e princípios da Diretiva. Em ocorrendo um prejuízo, de ordem patrimonial ou moral, decorrente de tratamento ilícito de dados, a pessoa prejudicada tem direito a buscar reparação. A entidade que executa a atividade de processamento só não será responsabilizada se provar que o fato que causou o dano não lhe pode ser imputado (arts. 22 a 24).

3.8 Transferência de dados pessoais a países não integrantes da União Européia

O artigo 25 da Diretiva contém regra que tem servido como fonte de problemas diplomáticos com países não membros da União Europeia. A norma em questão proíbe a

transferência de dados pessoais de cidadãos europeus a países que não possuam "um nível de proteção adequado" (item 1). A adequação ao nível de proteção exigida na Diretiva é examinada tomando-se por base uma série de fatores[14], mas sobretudo as regras de direito em vigor no país para onde se pretende transferir os dados. De um modo geral, a legislação de um país é considerada adequada quando suas normas internas ou tratados e convenções internacionais que tenha subscrito se igualarem às normas da Diretiva, em termos de proteção de dados pessoais.

A regra que exige um nível adequado de proteção legislativa, para transferência de dados pessoais a um determinado país, não é absoluta, admitindo exceções. Em algumas hipóteses restritas, como, *v.g.*, a pessoa titular dos dados tenha manifestado seu consentimento, a transferência for necessária para a execução de um contrato, para o exercício ou defesa de um direito em processo judicial ou outros interesses vitais da pessoa em causa ou para atingir interesse público relevante, é admitida a transferência de dados para um terceiro país que não tenha o mesmo nível legal de proteção de dados pessoais (art. 26). É possível também a transferência de dados pessoais para países com baixo nível de proteção legal quando o responsável pelo tratamento dos dados apresenta garantias suficientes de proteção da vida privada, que podem ser dadas através de cláusulas contratuais adequadas (art. 26, item 2).

Um órgão da União Européia que tem funções executivas, a Comissão Europeia (*European Comission*)[15], fica encarregado de examinar quais países possuem um nível adequado de proteção de dados. A Diretiva exige que a transferência de informações pessoais, contidas em bases de dados de entidades privadas ou órgãos públicos situados em países do bloco europeu, só podem ser transferidas para um Estado não integrante da comunidade se este oferecer um nível adequado de proteção. A *Comissão*, por força dessa exigência, edita decisões indicando quais países adotam o nível de proteção adequado[16]. Esse expediente é utilizado como forma de conferir maior segurança jurídica para as empresas da União Europeia, na questão da transferência de dados, além de contribuir para o livre fluxo das informações, que é um dos objetivos da Diretiva. Quando a *Comissão Européia* reconhece que um determinado país tem nível de proteção adequado, a decisão tem o efeito de permitir que dados pessoais contidos em bases de dados de empresas e órgãos públicos europeus sejam transferidos para entidades sediadas naquele país, sem necessidade de outras garantias, conforme previsto na Diretiva Européia sobre proteção de dados[17].

A *Comissão Europeia* também tem a função de elaborar modelos de cláusulas contratuais (*cláusulas contratuais-tipo*) para transmissão de dados pessoais a países não membros da UE. Essas cláusulas-modelo devem ser utilizadas para transações comerciais e inseridas em contratos quando o responsável pelo tratamento dos dados não residir ou não tiver a base de suas operações em país integrante da União Europeia. Em relação a países cujos sistemas de leis conferem um nível de "proteção adequada" a dados pessoais, já

---

[14] Tais como a natureza dos dados a ser transferidos e a finalidade e duração do tratamento (item 2 do art. 25).

[15] Link para o site da *Comissão Européia*: http://ec.europa.eu/

[16] Periodicamente, a *Comissão Européia* emite decisões reconhecendo países não membros que oferecem proteção adequada a dados pessoais. Suíça, Canadá, Estados Unidos e Argentina são alguns países que já receberam esse atestado de excelência na proteção de dados pessoais

[17] A respeito dessa questão, sugerimos a leitura do nosso artigo **Argentina possui sistema adequado de proteção a dados pessoais**, publicado no site Consultor Jurídico, em 10.07.03, acessível em: http://www.conjur.com.br/2003-jul-10/argentina_possui_sistema_adequado_protecao

reconhecidos pela Comissão Européia, não há necessidade do emprego das cláusulas contratuais-modelo nas relações que empresas européias travarem com empresas desses países. Quanto aos demais, sem reconhecido regime jurídico de "proteção adequada", o uso das cláusulas contratuais-modelo é uma solução viável para transferência de informações pessoais[18].

A fórmula da utilização de cláusulas contratuais padronizadas, não tem sido suficiente, entretanto, para evitar problemas diplomáticos que surgem entre a representação da União Européia e governos de outros países, no que tange à transferência de dados pessoais de cidadãos europeus. Só para exemplificar, pode ser lembrado o embaraço diplomático surgido com os EUA, ao requisitaram que as empresas européias de aviação repassassem os dados dos passageiros de suas aeronaves, com o alegado propósito de prevenir ações terroristas. Desde o fatídico ato terrorista às torres do *World Trade Center*, o Governo americano vem coletando dados dos passageiros de aeronaves com vôos internacionais com destino aos EUA. Os dados incluem os nomes dos passageiros, itinerário, números de cartão de crédito e até a preferência gastronômica da comida servida a bordo dos aviões. A União Européia resistiu muito a esse repasse, alegando que a entrega dos dados requisitados poderia violar as leis européias de proteção de dados pessoais. O impasse só foi resolvido depois que o Governo do EUA se comprometeu a dar algumas garantias sobre a forma como as informações seriam processadas[19].

3.9 Códigos de conduta

A Diretiva incentiva o processo de auto-regulação de certos segmentos do empresariado, prevendo a possibilidade de implementação, no âmbito das associações de classe, de códigos de conduta, desenhados em observância aos seus princípios. Os códigos de conduta, nessa acepção, contribuem para a adequada disseminação das normas de proteção de dados pessoais (art. 27). Os códigos de conduta podem ser submetidos à autoridade supervisora nacional de proteção de dados, para emitir parecer sobre a adequação às normas da Diretiva.

3.10 Autoridade supervisora da proteção de dados pessoais e grupo de trabalho

A Diretiva impõe a cada um dos Estados-membros a criação, no âmbito de sua administração, de pelo menos um cargo de autoridade supervisora (*supervisory authority*) da proteção de dados pessoais, com poderes para monitorar a aplicação das suas normas dentro do território do país (art. 28). A autoridade supervisora deve ser consultada quando da adoção de alguma medida administrativa ou elaboração de algum regulamento

---

[18] Para saber mais sobre cláusulas contratuais modelo, sugerimos a leitura de nosso artigo "**Comissão Européia aprova novos modelos de cláusulas contratuais para a transmissão de dados pessoais a países não membros da UE**, publicado no site Boletim Jurídico (ISSN 1807-9008), em 04.04.05, como parte integrante da Edição n. 121, código de publicação 565, disponível em: http://www.boletimjuridico.com.br/doutrina/texto.asp?id=565

[19] Ver, a respeito desse problema diplomático, nosso artigo intitulado **A crise entre os EUA e a UE em relação ao repasse de dados dos passageiros de aviões**, publicado no site Consultor Jurídico, em 20.09.03, disponível em: http://www.conjur.com.br/2003-set-20/crise_repasse_dados_passageiros_avioes

relacionado à proteção de dados pessoais (art. 28, item 2). A Diretiva ainda prevê que a autoridade supervisora deve estar investida de poderes de intervenção em empresas, para fins de determinar eventualmente a cessação definitiva ou temporária de alguma atividade de processamento de informações pessoais, para notificar o controlador dos dados ou ainda comunicar outras autoridades legislativas ou instituições públicas, para adoção de outras medidas. A autoridade para proteção de dados pessoais também deve ter poder de investigação, para abrir inquérito em caso de violação das normas da Diretiva, bem como para receber reclamações por parte de alguém que se sinta violado em seus direitos. A autoridade para proteção de dados pessoais de um país pode trabalhar em cooperação com a de outro, na extensão que for necessária para atingir seus objetivos institucionais. As decisões da autoridade supervisora poderão ser contestadas na via judicial.

A Diretiva instalou um Grupo de Trabalho (*Working Party*) com funções consultivas, formado por representantes das autoridades nacionais de proteção de dados, que elegem um presidente para mandato de dois anos, podendo ser renovado (art. 29). Cabe a esse Grupo de Trabalho basicamente emitir opiniões e recomendações sobre matéria de proteção de dados pessoais.

Recife, 05.02.13