colecção encontros

e

encontros
internacionais
de macau

As novas tecnologias, a sociedade da informação e o direito

MACAU
NOVEMBRO2000

INSTITUTO INTERNACIONAL MACAU
澳門國際研究所

JOSÉ ALVES PEREIRA

Licenciado em Direito pela Faculdade de Direito da Universidade de Lisboa, 1968. Natural de Águeda, 1945. Admitido na Ordem dos Advogados Portugueses em 1971. É Advogado e Árbitro.

Exerceu advocacia em Moçambique no período de 1968-1970, tendo sido admitido como membro efectivo da Ordem dos Advogados de Moçambique em 1996.

Desde 1990 até Janeiro de 2000 exerceu a sua actividade em sociedade com o seu nome, José Alves Pereira e Associados, com escritório em Lisboa, tendo-se esta fundido muito recentemente na sociedade Barrocas & Sarmento, a qual tomou a denominação Barrocas & Alves Pereira.

Foi membro do Conselho Geral e Vice-Presidente da Ordem dos Advogados de Portugal no período de 1992 a 1998. Durante esse período, colaborou activamente na criação das Ordens dos Advogados de Angola e Moçambique e foi representante da Ordem dos Advogados de Portugal em relações internacionais e no âmbito do Conselho das Ordens de Advogados da Comunidade Europeia (C.C.B.E.)

Orador em diversas conferências, debates, entrevistas e artigos sobre temas relacionados com o Direito e a Justiça.

Autor de diversos livros de direito publicados em Portugal e no estrangeiro, designadamente: "Agency and Distribution Agreements in Portugal", "Basic Aspects of Distribution Agreements under Portuguese Law"; "Brief Summary of the Law and Doctrine on Pre-contractual Liability in Portugal", "Insurance Intermediaries"; "The Hague Convention on Taking Evidence Abroad in Civil and Commercial Matters" (capítulo sobre Portugal); "Managing Capital Adequacy (colaboração no capítulo sobre Portugal). Contribuições várias para o "European Law Bulletin" da "American Bar Association".

Membro associado e coordenador por Portugal da "American Bar Association"; Presidente Nacional da "World Jurist Association"; membro da "International Bar Association", da "Union Internationale des Avocats", da "Inter-Pacific Bar Association", da "Association of Trial Lawyers of America", da "Off-Shore Institute" e da "UAE - Union des Avocats Européens".

AS TELECOMUNICAÇÕES E A PROTECÇÃO DA VIDA PRIVADA E DE DADOS PESSOAIS

1 O DIREITO À PRIVACIDADE EVOLUÇÃO HISTÓRICA

1.1. Na longa e sofrida entrada da conquista dos direitos fundamentais da pessoa humana, o reconhecimento, consagração e elaboração doutrinária sobre o Direito à Privacidade ou à Intimidade da Vida Privada é uma conquista relativamente recente [1].

Não vou aqui, obviamente, falar sobre esse longo caminho percorrido desde a Magna Carta de 1215 até aos nossos dias, passando pela Revolução Francesa e a sua Declaração dos Direitos do Homem e do Cidadão de 1789, pelo "Bill of Rights" americano de 1791 até desembocar, após episódios de incrível barbárie e espantosas atrocidades, em pleno Séc. XX, na Declaração Universal dos Direitos do Homem de 1948.

Algumas linhas, apenas, para assinalar a evolução do Direito à Privacidade, neste contexto.

1.2. Necessariamente obscurecido, dentro da hierarquia de valores, por outros direitos considerados mais elementares e fundamentais, como o Direito à Vida, o Direito à Liberdade, o Direito à Segurança, o Direito à Propriedade Privada e outros, só a partir dos finais do Séc. XIX a elaboração jurídica e doutrinal deste direito assume algum significado.

Numa primeira fase, assiste-se à demarcação da sua autonomia perante outros direitos fundamentais como o Direito de Propriedade e o Direito à Honra, reconhecendo-se a necessidade da sua protecção como tal, independentemente da decorrência ou justificação doutrinária derivada daqueles outros direitos.

Alguns radicam o seu nascimento no famoso artigo de 1890 de Louis Brandeis e Samuel Warren na "Harvard Law Review" sobre o título "The Right to Privacy" onde, a propósito da publicação e distribuição de um catálogo que incluía e descrevia quadros e gravuras pintados e desenhados pelo Príncipe Consorte e pela Rainha Vitória, se questiona o direito a essa divulgação com base na "individual's inviolate personality" e se afirma que "The right of privacy is the most comprehensive of rights and the right most valued by civilised men".

Nos princípios do século, pouco a pouco, assiste-se ao reconhecimento judicial desse direito [2].

Após o tumulto e a barbárie das duas guerras mundiais, a Declaração Universal dos Direitos do Homem de 1948 e a Convenção Europeia dos Direitos do Homem de 1950 vem consagrá-lo em termos inequívocos, estabelecendo o direito ao respeito da vida privada e familiar, do domicílio, da correspondência, da honra e da reputação.

De 1950 ao início da década de setenta, a evolução da informática, o tratamento de dados por computador e a sofisticação das comunicações acarretaram a necessidade de re-equacionar e desenvolver não só conceitos mas, sobretudo, formas de protecção.

Tendo este direito nascido, em autonomia, no advento da chamada "Revolução da Informação", ocorrida nos finais do Séc. XIX, com a invenção do telégrafo e do telefone, com o progressivo e contínuo desenvolvimento de novas técnicas de fotografia e impressão [3], é contudo o computador e a sua evolução nas décadas de 70 e 80 que vai provocar o discutir da sua problemática e a necessidade de uma eficaz protecção da vida privada perante a capacidade de intervenção e agressão que esse computador representa.

E, assim, os conceitos, a terminologia, as formas de protecção vão evoluir meteoricamente desde o início da década de 70 até aos nossos dias.

Em 1974, em alguns países da Europa e nos Estados Unidos, com o "Privacy Act", inicia-se a elaboração de leis destinadas a assegurar uma protecção adequada. As constituições da quase totalidade dos países civilizados passam a incluir nos direitos fundamentais formas de protecção da vida privada face à informática e ao tratamento por esta de dados pessoais.

A mera referência ao direito ao respeito da vida privada e familiar, como enunciação genérica e difusa, aparece agora concretizada com conceitos e instrumentos claramente inovadores.

Desde logo, a sofisticação emerge da ênfase na identidade pessoal, na personalidade e na dignidade humana. A pessoa, com a sua identidade

---

[1] Sobre a evolução histórica do Direito à Privacidade ver M. Januário Gomes "O Problema da Salvaguarda da Privacidade Antes e Depois do Computador" em "BMJ nº 319 (1982)".

[2] Sobre o reconhecimento judicial do Direito cfrs. Arthur R. Miller, Ann Arbor "The Assault on Privacy", The University of Michigan Press, 1971.

[3] Como afirma Januário Gomes, ob.e loc. citados "o nascimento da necessidade de tutelar juridicamente a existência duma zona intima ou privada nasceu duma particular evolução da técnica".

e dignidade, não só adquire maior relevo como requer uma maior protecção.

Mas, e sobretudo, aparecem conceitos totalmente novos, centrados na sociedade de informação dos nossos dias. A comunicação global substitui-se à clássica correspondência. As telecomunicações adquirem relevância própria. E surgem as noções de "dados pessoais informatizados" de "tratamento e conexão de dados" de "rede informáticas" de "fluxos transfronteiras" etc.

O homem manteve-se o mesmo, mas o mundo, em 50 anos, mudou radicalmente.

E esse novo ambiente, com técnicas de comunicação e informação cada vez mais rápidas, eficazes e não localizadas, gera necessariamente uma imensidade de novos problemas e exige uma muito maior protecção da vida provada.

Foi Artur R. Miller que o disse, quasi profeticamente, em momento em que o computador ainda era utilizado de forma incipiente:

"A computer is not simply a machine in a fixed position in a building. It can be that, but it often will be much more. It can also be the heart of a surveillance system". [4]

Desde então, o computador deixou de estar fixo e a sua portatibilidade e eficácia aumentaram exponencialmente. Desde então, a transmissão de dados e imagens acontece, instantaneamente, ao simples tocar de uma tecla. Desde então, a vida de todos e de cada um, os seus dados pessoais, o tratamento desses dados e a sua utilização, podem percorrer um cada vez mais pequeno mundo à velocidade da luz.

Surgem problemas a níveis completamente inimagináveis, mesmo no domínio da ficção cientifica, há cinquenta anos.

Surge a Internet, sem pátria nem fronteiras, descentralizada técnica e territorialmente. Surge uma nova noção de espaço, o ciberespaço, onde os dados se recolhem e não deixam traços visíveis e localizados. Surge, como alguns já disseram, uma área de "não direito", onde os conceitos jurídicos tradicionais não são aplicáveis ou transponíveis. Navega-se, instantaneamente à distância de um "clique".

E o mundo alerta-se e interroga-se.

Não foi tudo isto feito em nome do homem e para o homem? Não tem esta anarquia tecnológica de respeitar a privacidade e a dignidade humanas? Mas não acarretará esse respeito e protecção o cercear de um progresso científico e tecnológico que todos os dias nos abre novos mundos e novas fronteiras? Onde, nesta área, os limites dos interesses privados, do interesse público e do interesse científico?

É sobre tudo isto que me proponho reflectir convosco nesta breve comunicação.

2 O CONCEITO DE DADOS PESSOAIS. OS DADOS SENSÍVEIS

2.1. Correlativamente com a evolução dos conceitos do Direito à Privacidade, a noção do que deve ser objecto de protecção, traduzida pelo novo conceito de "dados pessoais", regista igualmente uma enorme evolução, quer no tempo quer no espaço [5].

Começou-se pelos conceitos clássicos da vida privada e familiar, domicílio e correspondência.

O conceito de vida privada, tendo partido simplesmente do que cada indivíduo fazia na tranquilidade e solidão da sua casa e do seu ambiente familiar, expande-se, subsequentemente, para o direito de comunicar com privacidade, devendo ser assegurado o carácter confidencial dessa comunicação.

E essa comunicação, inicialmente confinada ao conceito clássico de correspondência, adquire, com a evolução da técnica e das formas informatizadas de comunicação, um conceito extremamente mais vasto e abrangente.

Da comunicação passa-se para o conceito de informação. A informação é facultada, recolhida e tratada por formas altamente sofisticadas e eficazes. Os dados, ou seja, o conjunto de informações recolhidas, podem ser tratados e circular à velocidade da luz.

Numa primeira fase, assistimos à preocupação de assegurar a protecção desses dados perante as entidades públicas, a quem deviam ser obrigatoriamente fornecidas, por razões fiscais, de providencia social ou estatísticas, abordando-se uma óptica estrita de protecção do particular perante a administração pública, que aparecia como o principal consumidor de meios e dados informáticos.

Mas rapidamente se evoluiu para outros patamares.

[4] Arthur R. Miller, ob. e loc. citados.

[5] Sobre o conceito de dados pessoais cfrs. Helena Moniz "Notas sobre a Protecção de Dados Pessoais Perante a Informática R.P.C.C. 7 (1997) e bibliografia aí citada.

A expansão e portatibilidade dos meios e o seu aparecimento como poderoso intermediário na recolha e tratamento de dados, sobretudo, agora, com fins comerciais, a interactividade entre os consumidores e os meios, ampliaram a noção de dados pessoais e passaram a exigir um conceito mais alargado.

2.2. O sector das telecomunicações, tendo a sua quota parte de influência nas mutações acima descritas, é, também, profundamente influenciado pelas mesmas. A massificação das relações humanas, na sua globalização, não pode deixar de ser condicionada por este estado de coisas.

Este sector vem assumindo uma enorme importância [6], sobretudo a partir do início da década de oitenta, com o desenvolvimento de novas aplicações tecnológicas e consequente redução do custo das redes e serviços, possibilitando a aparição de novos operadores, num movimento que, concomitantemente, permitiu ao consumidor beneficiar do funcionamento dos mecanismos inerentes à concorrência e, em geral, do mercado.

Ao mesmo tempo que os preços eram reduzidos, aumentou a procura internacional, quer dos serviços clássicos de telecomunicações, quer de novas aplicações, por forma a satisfazer necessidades concretas, tendo este movimento levado à progressiva superação do monopólio natural e sua substituição pelo sistema da concorrência.

2.3. Mas é indiscutivelmente o computador e a evolução do mesmo, com o aumento gigantesco na sua capacidade de recolha, armazenamento e tratamento de dados pessoais que vem exigir, de forma gritante, a adopção de sistemas e meios de protecção eficazes das pessoas e da sua privacidade.

Recentemente, a capacidade de armazenamento, tratamento e difusão de dados articula-se com as telecomunicações, em simbiose técnica tão estreita que se torna difícil delimitar claramente os dois sectores, operando sob a capa abrangente da tecnologia de informação.

Aparece o fenómeno Internet, como ambiente ambíguo, sem base territorial e sem lei, onde a transmissão de dados não é linear, mas eminentemente difusa, onde a distinção clássica entre correspondência privada e comunicação audiovisual acessível a todos, se interliga e confunde.

Constata-se também que, ao contrário do que se passa geralmente em matéria de telecomunicações, a Internet não está centralizada tecnicamente. Repare-se ainda que não existe uma entidade que desempenhe o papel de operador comercial (nem sequer a Internet Society nem a IETF assumem semelhante função), e até mesmo a qualificação desta como uma rede chega a ser discutível, não o sendo, contudo, a sua inserção no mundo das telecomunicações [7].

A capacidade que os modernos telemóveis, da segunda ou terceira geração, possuem para actuar como verdadeiros e potentes computadores de portabilidade extrema, ligados a um meio de telecomunicação por excelência, mais não faz que acentuar esta problemática e os problemas que podem suscitar ao nível de protecção da vida privada num mundo cada vez mais aberto e transparente.

2.4. Tudo isto exige, assim, uma noção abrangente de dados pessoais, sujeitos a protecção.

Vamos socorrer-nos, como em outros pontos desta intervenção, do que é uniformemente considerado como a maior e mais abrangente intervenção legislativa no campo da protecção de dados pessoais, a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995.

Refira-se que esta Directiva foi complementada, para o domínio específico das telecomunicações, pela Directiva 97/66/CE do mesmo Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997 [8].

Aí se definem "Dados pessoais" como "qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa)" adiantando-se que "é considerado identificável todo aquele que possa ser identificado, directo ou indirectamente, nomeadamente por referência a um número de

[6] A indústria das telecomunicações ocupa, actualmente, o terceiro lugar a nível mundial, sendo apenas suplantada pela assistência na área da saúde e pela Banca.

[7] Sobre interessantes e específicos problemas suscitados pela Internet veja-se o interessante relatório apresentado pela Secção de Business Law do American Bar Association à reunião anual de 2000 em Londres intitulado "Achieving Legal and Business Order in Cyberspace: Jurisdictional Issues Created by the Internet".

[8] Ambas as Directivas estão disponíveis em http://europa.eu.int/eur-lex.pt

identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social; [9]

Trata-se, assim, de uma definição extremamente abrangente: "Toda e qualquer informação relativa a pessoa singular".

Desde logo, a exclusão das pessoas colectivas do âmbito da protecção. Foi entendido que a privacidade e os dados pessoais só fazem sentido em função do Homem, como pessoa física. No entanto, já alguns autores se pronunciaram – e insistem – [10] pela extensão destes direitos às pessoas colectivas, uma vez que a livre utilização de ficheiros contendo dados pessoais referentes às mesmas pode constituir uma grave agressão não só ao normal desenvolvimento da sua actividade mas até à sua própria personalidade jurídica.

Por outro lado, os dados tem que ser relativos à pessoa, enquanto tal.

De fora ficam dados diferentes, como os de ordem técnica ou científica.

Finalmente a imputação à pessoa tem de ser directa. Esta tem que estar identificada ou ser identificável. Se os mesmos se referirem a um grupo, a uma raça, a um povo, sem que seja possível o seu relacionamento com uma pessoa física, os dados deixarão de ser pessoais.

2.5. Tendo partido assim, de uma noção global e abrangente, urge no entanto delimitá-la um pouco mais, para se poder definir quais desses dados carecem de protecção.

E assim, é consistente nas leis e doutrina, que, para beneficiarem da protecção os dados devem ser:

- **objecto do tratamento**
- **estruturados em ficheiros**

Só estas operações, por assim dizer, tornam perigosa a sua divulgação sem regras específicas de protecção.

Só esse tratamento, sistemático em ficheiros, com todos os recursos da técnica, pode constituir uma grave ameaça à privacidade.

Mas em que consiste esse tratamento e esses ficheiros?

Uma vez mais, as noções da Directiva são abrangentes:

Tratamento é "qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, 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". [11]

Por **Ficheiros**, entende-se "qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico". [12]

Pela enorme abrangência destas definições se verifica que foi intenção sujeitar a uma protecção definida por princípios e regras específicas toda e qualquer operação sobre dados pessoais estruturados ou arquivados.

2.6. Cumpre, ainda, falar numa determinada categoria de dados pessoais que, pelo seu conteúdo, pelo risco que acarretam para as pessoas a que dizem respeito, devem ser objecto de uma protecção muito especial.

2.7. Convencionou-se chamar a tais dados "dados sensíveis" [13]. São eles os dados que revelam a origem racional ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, o estado de saúde ou a vida sexual.

Aqui não se trata de disciplinar e regular a forma por que devem ser tratados. Trata-se, antes de mais, de proibir "tout court" o seu tratamento, pelos perigos que tal tratamento acarreta.

Conforme as legislações, só se admitem excepções em casos extremamente limitados e perfeitamente identificados.

Não vamos, no âmbito desta comunicação, debruçar-nos sobre estes dados mas, tão somente, sobre a restante massa de dados pessoais, despidos da sensibilidade que lhes assegure tal protecção restritiva.[14]

---

[9] Cfrs. artº 2º da Directiva

[10] Quanto à não inclusão das pessoas colectivas e no sentido dessa inclusão ver Dr. Jorge Bacelar Gouveia "Os Direitos Fundamentais à Protecção dos Dados Pessoais Informatizados" in "Revista da Ordem dos Advogados" Ano 51 (1991), vol. III, pgs. 709 e sgs.

[11] cfrs. artº 2º g)

[12] cfrs. art. 2º c)

[13] cfrs. artº 8º nº 1 da Directiva

[14] Sobre os dados "sensíveis" ou "pessoalismos", ver J. J. Gomes Canotilho e Vital Moreira, Constituição da República Portuguesa Anotada, I, pág. 227 e Isabel Reis Garcia, "Do Direito da Informática a um anteprojecto de lei de protecção de dados pessoais", in Revista da Ordem dos Advogados, 1989.

3 OS PRINCÍPIOS BASE APLICÁVEIS À PROTECÇÃO DE DADOS PESSOAIS NA INFORMÁTICA E NAS TELECOMUNICAÇÕES

3.1. A evolução legislativa [15] e a prática seguida na protecção de dados pessoais permitiram definir um conjunto de direitos pessoais, aplicáveis a esta área específica e que hoje se podem considerar como universalmente aceites.[16]

São eles:

a) O **Direito de Informação** da pessoa sobre a existência de um tratamento de dados pessoais que lhe diga respeito.

De acordo com este direito tem que ser prestada ao titular dos dados informação suficiente relativamente à finalidade para a qual os dados são recolhidos; se os dados se destinam a ser transmitidos ou revelados a terceiros; a identidade do responsável pelo tratamento; e, ainda, se a resposta relativa aos dados pessoais tem carácter obrigatório ou facultativo, e possíveis consequências em caso de não responder.

b) O **Direito de Oposição** ao tratamento de dados pessoais. Certas legislações exigem, mesmo, um consentimento inequívoco e expresso, não só no caso de dados sensíveis, mas sempre no caso destes.

c) O Direito de que os princípios da **Lealdade** e **Licitude** e **Finalidade** sejam respeitados na recolha e tratamento de dados. E, assim:

– que o tratamento seja necessário para prosseguir fins ou interesses legítimos e explícitos.

– os dados pessoais recolhidos sejam adequados, pertinentes e não excessivos em relação ao fim para o qual os dados serão processados.

– que o processamento dos dados seja feito com total respeito dos direitos do titular dos dados.

d) O **Direito de Acesso** à integralidade dos dados pessoais objecto do Tratamento e o **Direito de Rectificação** de tais dados.

e) O **Direito à Limitação Temporal** dos dados tratados.

Assim, os dados devem ser conservados apenas pelo período de tempo considerado necessário para as finalidades da recolha e tratamento, exceptuados casos autorizados para fins históricos, estatísticos ou científicos.

f) O Direito à Segurança dos dados pessoais tratados

Quer isto dizer que o responsável pelo tratamento deve tomar as medidas consideradas necessárias, através de uma ponderação que entre em linha de conta com a natureza dos dados e os riscos causados pelo tratamento, para prevenir:

– a destruição ou perda de forma acidental ou ilícita de quaisquer dados pessoais;

– a alteração, difusão ou acesso não autorizados aos dados pessoais, devendo ainda o responsável pelo tratamento tomar especiais cuidados com o pessoal encarregado do tratamento dos dados pessoais;

– qualquer forma de tratamento ilícito dos dados pessoais.

No caso de o tratamento dos dados ser feito por um subcontratante, deve tal ser feito nos termos de contrato ou acto jurídico que vincule o subcontratante ao responsável pelo tratamento, sendo naquele estipulado que o subcontratante actua exclusivamente em obediência de instruções recebidas do responsável pelo tratamento e que assume as obrigações de segurança acima referidas.

No caso de os dados circularem na Internet, caso paradigmático de uma rede aberta, impende também sobre o responsável pelo tratamento o dever de informar o titular de que os dados poderão circular sem condições de segurança e, como tal, poderão ser vistos e utilizados por um terceiro não autorizado.

g) **Direito ao controlo do tratamento dos dados** por um organismo independente.

Só assim o particular pode estar seguro de que não está sujeito a critérios ocasionais de conveniência política na definição e

[15] A lei portuguesa nesta matéria é constituída pela Lei nº 68/98, de 26 de Outubro e 69/98 da mesma data, a primeira transpondo a Directiva 95/96/CE e a segunda a Directiva 97/66/CE.

[16] O elencar dos direitos segue o sistematização elencada por Marcel Pinet no seu artigo "La mise en ouvre sur Internet de la "transparence" au regard de la proteccion dos données a caractere personel". Disponível em WWW.garanteprivacy.it

protecção dos seus direitos fundamentais.

É assim que a Directiva 95/46/CE, atrás citada, estabelece, no seu preâmbulo:

– que a criação nos Estados-Membros de autoridades de controlo que exerçam as suas funções com total independência constitui um elemento essencial da protecção das pessoas no que respeita ao tratamento de dados pessoais.

– que essas autoridades devem ser dotadas dos meios necessários para a realização das suas funções, incluindo poderes de inquérito ou de intervenção, especialmente em caso de reclamações, e poderes para intervir em processos judiciais; que essas autoridades devem ajudar a garantir a transferência do tratamento de dados efectuados no Estado-membro sob cuja jurisdição se encontram;

– que as autoridades dos diferentes Estados-Membros deverão prestar-se mutuamente assistência no desempenho das suas funções por forma a assegurar integralmente o respeito das regras de protecção em toda a União Europeia.

h) Finalmente, e no respeito pelos princípios gerais de direito, conforme a violação seja considerada um ilícito civil ou criminal, um **Direito à Reparação** pelos danos causados.

3.2. Convém complementar esses direitos, especificamente aplicáveis no campo dos dados pessoais informatizados, com alguns princípios específicos aplicáveis ao Sector das Telecomunicações.

Nesse sector são plenamente aplicáveis os direitos acima referidos, competindo ainda acentuar alguns deveres específicos, como decorrência do Direito à Segurança já acima referido.

É usual, nas leis mais evoluídas que ao assunto se dedicam nas várias jurisdições, e na sequência da Directiva 97/66/CE atrás citada, encontrarmos deveres especificados de segurança dos prestadores de serviços a nível técnico e organizacional, um dever estrito de assegurar a confidencialidade das comunicações, proibindo escutas, intercepções e vigilância [17], consagrar-se o direito à recepção de uma factura detalhada [18], consagrar-se o direito de apresentação e restrição da identificação da linha chamadora e da linha conectada[19], consagrar-se o direito de reencamihamento automático de chamadas [20], fixar-se as condições em que o assinante pode constar em listas de assinantes ou opor-se a tal e estabelecer-se um direito de oposição à recepção de chamadas não solicitadas, no âmbito de acções de marketing directo [21].

Para melhor análise dos termos em que esses direitos e deveres são consagrados remete-se para a Directiva 97/66/CE já citada.

4 AS FORMAS DE ASSEGURAR A PROTECÇÃO. A VIA LEGISLATIVA E ADMINISTRATIVA E A AUTO-REGULAÇÃO

4.1. Entre as vias debatidas e implementadas para assegurar a protecção das pessoas e da sua privacidade em caso de tratamento de dados pessoais, as várias jurisdições adoptam duas diferenciadas:

– ou uma via legislativa, procurando regular por lei expressa a protecção de dados;

– ou uma via de auto-regulação, pela qual os próprios operadores ou responsáveis pelo Tratamento aderem livremente a um conjunto de princípios e regras de conduta que se comprometem a aceitar.

Quer numa quer noutra das vias se encontram, em maior ou menor grau, soluções de controlo por via administrativa, quer através de entidades independentes, quer de organismos judiciais ou estatais.

4.2. Ainda na via legislativa, a protecção aparece assegurada ou por Convenções Internacionais (cfrs. Convenção nº 108 para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal), quer por instrumentos do Direito Comunitário (cfrs. as Directivas 95/46/CE de 24 de Outubro de 1995 e 97/66/CE de 15 de Dezembro de 1997, acima mencionadas) ou pelas Constituições e leis nacionais dos diversos países.

[17] Cfrs. art. 5º da Directiva citada. De um modo geral, este Direito tem protecção penal, cfrs. o artº 384º do C. Penal Português

[18] Cfrs. artº 7º da Directiva

[19] Cfrs. artº 8

[20] Cfrs. artº 10

[21] Cfrs. artº 12

4.3. Como exemplo e paradigma da auto-regulação encontramos o que se passa nos Estados Unidos da América. De notar que a par de diversos códigos de conduta e mecanismos de auto-regulação pura, aí se adoptou, recentemente, e por efeito do disposto na Directiva Comunitária de que a transferência de dados pessoais para o exterior da União Europeia está condicionada à existência de um nível adequado de protecção dos dados pessoais no Estado de destino, um documento, por várias vezes alterado que, mantendo a preferência por um sistema que privilegia a auto-regulação, contém uma série de princípios aplicáveis a empresas americanas que pretendam "importar" dados pessoais da União Europeia. Esse conjunto de princípios é designado por "Safe Harbor Principles" (SHP). [22]

Acentue-se, ainda, que ao contrário das Constituições mais recentes da quasi generalidade dos países da Europa Ocidental, não há um direito explícito à privacidade na Constituição dos Estados Unidos da América. Os princípios relativos ao Direito à Privacidade têm sido construídos através de decisões do Supremo Tribunal baseadas em disposições do "Bill of Rights".

Igualmente no que concerne à existência de uma entidade independente para fiscalização e execução dos direitos de privacidade no âmbito da protecção de dados pessoais, o sistema é escasso e passa por departamentos e comissões federais, com poderes limitados e dispersos.

Acentue-se, no entanto, que existe um debate significativo e uma corrente de opinião que tende a prevalecer a curto prazo, no sentido da implementação por via legislativa da protecção de dados pessoais no sector privado, sobretudo em face dos fenómenos da Internet e do comércio electrónico. Contudo, a enorme força de "lobying" do sector privado informático dos Estados Unidos tem, até agora, feito prevalecer a tese de que a auto-regulação é suficiente.

4.4. De uma forma sumária, pode dizer-se que o funcionamento dos SHP consiste no seguinte: desnecessidade de sujeição a um processo de autorização para ser levada a cabo uma transferência de dados pessoais de um Estado comunitário para os Estados Unidos, uma vez que uma empresa europeia que queira proceder a tal tem conhecimento que está a enviar dados pessoais para uma organização norte-americana que aderiu aos SHP através da consulta da lista de aderentes aos SHP que é disponibilizada no site do Department of Commerce norte-americano. Nesta lista, que só estará operacional em Novembro de 2000, constarão os nomes de todas as empresas norte-americanas que aderiram aos SHP e a qualquer documentação adicional, sendo esta lista regularmente actualizada.

A adesão aos SHP é, sublinhe-se, puramente voluntária, e as organizações que decidem aderir aos mesmos têm que cumprir determinados requisitos, respeitar os SHP e declarar publicamente que o fazem. Por forma a beneficiar das vantagens inerentes aos SHP, uma organização tem que declarar anualmente ao Department of Commerce, por escrito, que adere aos SHP, e declarar na sua política de privacidade divulgada publicamente que aderiu aos SHP, regendo-se pelos mesmos [23].

4.5. Os princípios constantes do SHP obedecem, de uma forma geral, aos atrás descritos como direitos dos titulares dos dados pessoais.

Dado, contudo, reflectirem a opinião prevalente nos Estados Unidos da América quanto à protecção de dados pessoais e considerada a enorme importância que os Estados Unidos da América assumem no âmbito do tratamento de dados e emissão de fluxos transfronteiras, convém enunciá-los, embora de forma sumária.

Os SHP são sete princípios, que podem ser descritos da seguinte forma:

1º. **Notificação/Informação**: as organizações devem notificar os titulares dos dados acerca das finalidades para as quais recolhem e utilizam a informação relativa àqueles. Devem fornecer informação acerca do modo de contactar a organização relativamente a quaisquer dúvidas ou queixas, identidade de quaisquer terceiros a quem os dados sejam transmitidos, bem como as escolhas e meios que a organização dispõe para limitar a utilização e divulgação.

2º. **Escolha**: as organizações devem dar aos titulares dos dados a oportunidade de escolher (**opt out**) se desejam que os seus dados sejam

[22] Ver os princípios e a lista de aderentes no site do Department of Commerce norte-americano, cujo endereço é WWW.ita.doc.gov/ecom

[23] Para se poder "qualificar" para os SHP, uma organização pode: (I) associar-se a um programa de protecção da privacidade que adira aos SHP; (ii) desenvolver a sua própria política de protecção da privacidade, em conformidade om os SHP; (iii) estar na dependência de uma entidade administrativa (ou outra) que efectivamente proteja a privacidade.

divulgados a terceiros ou utilizados para um fim incompatível com aquele para o qual foram de início recolhidos, ou posteriormente autorizados pelo titular dos dados. Relativamente à informação considerada sensível, deve ser dada ao titular a possibilidade de uma opção afirmativa ou explícita (**opt in**), no caso de a informação se destinar a ser divulgada a terceiros ou utilizada para um fim diferente do originalmente afirmado ou posteriormente autorizado pelo titular dos dados.

3º. **Transferência para terceiros**: para divulgar as informações a terceiros, as organizações interessadas deverão respeitar os princípios da Notificação e Escolha. No caso de uma organização querer transferir dados para um terceiro que actue como agente, podê-lo-á fazer, se assegurar que o terceiro aderiu aos SHP, ou está sujeito à Directiva ou outras regras similares. Em alternativa, a organização interessada poderá celebrar um acordo escrito com o terceiro, nos termos do qual o terceiro se compromete, pelo menos, a conferir um nível de protecção da privacidade similar ao conferido pelos princípios aplicáveis.

4º. **Acesso**: os titulares dos dados deverão ter acesso aos seus dados pessoais, que sejam detidos por uma organização, e ter a possibilidade de os corrigir, aditar, ou apagar quando incorrectos, a não ser que o custo de acesso seja desproporcionado em relação aos riscos que corre a privacidade do indivíduo (ou de outrém) no caso concreto.

5º. **Segurança**: as organizações deverão tomar precauções razoáveis por forma a proteger dados pessoais em relação a perdas, utilização indevida e acesso não autorizado, divulgação, alteração e destruição.

6º. **Integridade dos dados**: os dados pessoais recolhidos deverão ter relevância para o fim pretendido. Uma organização deverá tomar medidas razoáveis para assegurar que os dados são aptos para cumprir a função pretendida, e que são exactos e completos.

7º. **Fiscalização de cumprimento**: Como forma de assegurar o cumprimento dos SHP, devem ser:

(a) assegurados mecanismos de recurso independentes e acessíveis que permitam aos titulares dos dados ver as suas queixas e litígios investigados e resolvidos, bem como indemnizados (se a lei aplicável o prever);

(b) previstos mecanismos de verificação do cumprimento dos SHP por parte das organizações que se comprometeram a tal;

(c) previstas obrigações de solucionar problemas surgidos de uma falha no cumprimento dos SHP. As sanções deverão ser rigorosas em medida suficiente para assegurar o cumprimento dos princípios. As organizações que não apresentem a declaração anual de respeito pelos SHP serão excluídas da lista do Department of Commerce e deixarão, consequentemente, de poder beneficiar das vantagens inerentes aos SHP.

Para além dos princípios acima referidos, o Department of Commerce elaborou ainda um conjunto de quinze perguntas e respostas ("FAQ"), que pretendem complementar o enunciado dos princípios. [24] [25]

4.6. Finalmente, cumpre perguntar. Como se pode assegurar a protecção de dados no caso de fluxos transfronteiras para países onde não exista qualquer protecção ou a mesma não seja adequada?

Já vimos que a Directiva da União Europeia o proíbe, como regra. Se o País não assegura um nível de protecção adequado, que existirá se os direitos base que atrás enunciámos foram respeitados, a transferência de dados pessoais é proibida. [26]

Contudo, a própria Directiva admite derrogações no seu artigo 26º em caso de consentimento inequívoco do titular dos dados, do cumprimento contratual, da protecção de um interesse público relevante ou de defesa dos interesses da pessoa em causa.

A realidade do mundo actual é a de que a vasta maioria dos Estados, sobretudo dos países não industrializados, não dispõe, ainda, de legislação adequada para a protecção de dados pessoais.

E é um facto que, por vezes, essa transferência de dados é inevitável, num mundo cada vez mais próximo e globalizado.

[24] Ver as FAQ no referido site WWW.ita.doc.gov/ecom

[25] Para uma análise crítica da Safe Harbor Principles ver Yves Poullet "Les Safe Harbor Principles". Une protection adéquate?... Disponível em http://www.droit.fundp.ac.be/crid.htm

[26] cfrs. Artº 25º da Directiva 95/46/CE

Tem-se discutido, exaustivamente, a forma de suprir essa falta de protecção por via contratual [27]. Procuram-se disposições contratuais exaustivas e eficazes que, inseridas em contrato entre o exportador e o importador de dados, mitiguem essa falta de protecção. A elaboração de um contrato-modelo está em estudo pelo Conselho da Europa, pela Comissão Europeia, pela Câmara Internacional de Comércio e pela OCDE.

Se bem que esses contratos possam constituir a protecção possível, convém assegurar que:

– os contratos contenham cláusulas em benefício de terceiro, a saber, a pessoa em causa.

– os contratos sejam complementados por declarações unilaterais vinculativas do importador de dados para com a pessoa em causa, reconhecendo os direitos-base já acima referidos.

– os contratos sejam completos e explícitos no concernente à protecção de dados e não a tratem como mera decorrência das relações comerciais entre as partes.

– os contratos se fundem nos princípios e direitos consignados nas Directivas Comunitárias, como forma mais perfeita e sofisticada de protecção disponível. Alternativamente, e em caso de conexão mais relevante, devem usar-se os Safe Harbour Principles, aplicáveis nos E.U.A.

– a exequibilidade das obrigações contratuais esteja assegurada. Se as instâncias judiciais do País em causa se revelarem inadequadas, deve prever-se o recurso a Tribunais arbitrais e assegurar-se, por exemplo, através de garantias bancárias, o pagamento de possíveis indemnizações [28].

5 ALGUMAS QUESTÕES CONTROVERSAS EM SEDE DE PROTECÇÃO DA VIDA PRIVADA E DE DADOS PESSOAIS. UMA VISÃO DO FUTURO

5.1. É evidente que a natureza de uma intervenção deste tipo, a multifacetada complexidade da matéria e o pouco tempo de que disponho me obrigam a não fazer uma abordagem exaustiva do assunto. Qualquer dos pontos abordados esquematicamente constituiria matéria suficiente para um seminário autónomo.

Não queria, porém, terminar sem deixar para discussão algumas questões que me parecem particularmente aliciantes e controversas emitindo, quanto a elas, uma visão pessoal mas evitando, como o aconselha a prudência, assumir posições definitivas em matéria tão nova, tão fluída e tão mutável como esta.

Essas questões prendem-se com o futuro da protecção de dados pessoais. Vencerá a tese de que só a lei expressa, acompanhada de uma autoridade independente e interventora, pode assegurar uma protecção adequada? Ou, pelo contrário, será a auto-regulação, através de formas mais abrangentes e sofisticadas, aquilo que vamos encontrar no futuro?

5.2. Desde logo uma advertência sobre quanto é arriscado falar de futuro nesta matéria.

A evolução tecnológica, a crescente rapidez na transmissão e tratamento de dados, a utilização da Internet para uma cada vez maior actividade comercial "on line", desenham, todos os dias, novas fronteiras.

Se nos anos 70 e 80, o objectivo primário se centrava na protecção do indivíduo perante os estáticos e gigantescos computadores de governos e organizações públicas, hoje é claramente no sector privado, na área comercial, no consumo resultante de um mercado emergente, agressivo e anárquico, que as maiores questões se colocam.

5.3. Depois, convém notar que se assiste a uma interligação ou entre-ajuda entre as duas vias de protecção que não se assumem como suficientes.

E é natural que assim aconteça.

Por um lado, um sistema de auto-regulação não é lei, e a sua eficácia depende, sobretudo, de uma aceitação e execução generalizadas.

Por outro, a eficácia da lei, em ambiente de contactos puramente electrónicos, sem localização territorial, como acontece no que se convencionou chamar ciberespaço, é, no mínimo, duvidosa.

A noção de âmbito de aplicação territorial é inerente à lei. Porém, na Internet, as partes que obtêm e usam dados pessoais não têm, muitas vezes, um estabelecimento estável ou mesmo fisicamente determinável ou, sequer, elementos de

[27] A Directiva, no seu artº 26º nº 2, admite uma derrogação à proibição de transferência para país terceiro que não assegure um nível de protecção adequado, quando garantias suficientes de protecção resultem "de cláusulas contratuais adequadas".

[28] Ver, a este respeito, a interessante comunicação de Waltraut Kotschy à recente "22nd. International Conference on Privacy and Personal Data Protection. Veneza 2000" sob o título "Model Contracts for securing data protection in cases of transborder data flow to countries without adequate data protection". Disponível em WWW.garanteprivacy.it

conexão identificáveis com a jurisdição onde o consumidor ou a pessoa em causa residem. Não se podendo, assim, definir o território onde o ilícito, civil ou criminal, ocorreu, não se estabelece a jurisdição aplicável e a exequibilidade da lei é posta em causa.

Talvez por isso as leis (e nomeadamente a Directiva 95/46/CE) alargam extraordinariamente os elementos de conexão e a aplicação extra-territorial, no sentido de colmatar essas lacunas.

Alarga-se, de forma amplíssima, a noção de "tratamento de dados pessoais" [29], de "responsável pelo tratamento" [30], de actividades com utilização de meios situados num determinado território [31] e, como já vimos, proíbe-se a transferência de dados para países sem protecção adequada [32]. Mas na prática, como poderá uma jurisdição europeia forçar todos os operadores da "web", à volta do mundo, que não tenham associações relevantes ou estejam estabelecidos na Europa, a aderir às normas da Directiva?

E é por isso que a Directiva 95/46/CE, no seu artigo 27º., realça a necessidade da elaboração de códigos de conduta sectoriais, bem como estabelece no artº 29º um "Grupo de protecção das pessoas", encarregado de importantes funções consultivas e de vigilância.

Por outro lado, os Safe Harbour Principles americanos contém elementos de controlo e definição administrativa que estão longe de constituir uma auto-regulação pura, levando os autores a designá-los como instrumentos de co-regulação [33].

5.4. Assistimos, hoje, a um muito maior esforço de eficácia por parte da auto-regulação que se conjuga com o aparecimento de autoridades independentes de controlo [34].

A ninguém é lícito ignorar o problema. Nem às organizações internacionais, nem aos Estados, nem às sociedades comerciais, nem aos consumidores. Nunca a protecção de dados assumiu, como hoje, uma tão grande relevância política e comercial [35].

A auto-regulação faz-se não somente por declarações unilaterais vinculativas dos operadores destinados aos consumidores, mas por códigos de conduta, quer de organizações [36], quer de sectores, quer de tipos de comércio, quer de profissões. Por outro lado, as organizações certificadoras e que atribuem "standards" como o ISO, a CSA o JIS e outras, começam a atribuir certificados de protecção de privacidade, bem como marcas e selos, que os responsáveis pelo tratamento de dados tem dificuldade, senão mesmo impossibilidade, de ignorar, sob pena de serem evitados e discriminados por parte de consumidores cada vez mais exigentes.

Hoje, o dispôr de um nível de protecção adequado tornou-se um factor de **concorrência** e **credibilidade**, que não pode ser ignorado.

5.5. As diferentes vias, exploradas por diferentes países, a relutância dos maiores responsáveis pelo tratamento de dados, como os Estados Unidos e o Japão em adoptarem leis abrangentes, procurando ao contrário uma maior sofisticação na auto-regulação, obstaram até agora ao aparecimento de uma legislação uniforme ou de um Código de Conduta global [37].

Mas é inevitável, a meu ver, que a protecção de dados se irá solidificar num abrangente Tratado Internacional, a que aderirão todos os países do mundo industrializado e todos aqueles que com estes tenham relações comerciais significativas. [38] E uma vez estabelecidos e aceites os princípios, será o próprio mercado e a própria evolução tecnológica que se encarregarão de assegurar a

[29] cfrs. Art. 2º

[30] idem

[31] cfrs. Artº 4º.1 (c)

[32] Cfs. Art. 25º

[33] Sobre a auto-regulação, ver o interessante artigo do Professor Colin J. Bennett intitulado "Privacy self-regulation in a global economy: a race to the top, the bottom or somewhere else"? produzido na International Conference of Privacy and Data Protection de Veneza, no corrente ano, e disponível em WWW.garanteprivacy.it

[34] Se os Estados Unidos continuam a resistir ao estabelecimento de uma autoridade independente de controlo, vários países e regiões da Ásia Pacífico, como a Nova Zelandia, Hong-Kong e Autrália já reconheceram a sua necessidade e procederam à sua implementação.

[35] Ver o excelente artigo no "The Economist" de Maio 1 a 7 de 1999 sob o título "The End of Privacy".

[36] Ver em WWW.privacyexchange.org exemplos de códigos de conduta adoptados por organizações.

[37] Registem-se, no entanto, os esforços neste sentido da "International Commerce Exchange". Consultar WWW.icx.org

[38] Cfrs., neste sentido, a proposta apresentada pelo ministro francês François Filion, em Abril de 1996, por ocasião do Conselho Informal dos Ministros Europeus. Propôs aquele ministro a celebração de uma Convenção Internacional, preparada num quadro multilateral, que versasse sobre os princípios mínimos de deontologia aplicáveis aos serviços Internet e sobre os princípios-base de cooperação judiciária nesse domínio.

sua aplicação prática. Os computadores do futuro conterão sistemas de controlo e protecção de tratamento de dados cada vez mais sofisticados. O mercado, por seu turno, tratará como párias e indesejáveis todos aqueles que não respeitem essa protecção.

E assim, no final, as vias legislativas e de auto-regulação confluirão num patamar comum. Talvez não o ideal, dados os enormes interesses tecnológicos, de mercado e políticos em confronto. Mas, certamente, um nível civilizado de protecção que permita uma adesão global ao que a Directiva definiu, em parágrafo particularmente feliz, no seu preâmbulo, ao referir "que os sistemas de tratamento de dados estão ao serviço do Homem, que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos".

O mesmo se diga quanto às telecomunicações, relativamente às quais diz o preâmbulo da Directiva 97/66/CE "que estão actualmente a ser introduzidas nas redes públicas de telecomunicações da Comunidade Europeia novas tecnologias digitais avançadas, que suscitam requisitos específicos de protecção de dados pessoais e da privacidade do utilizador; que o desenvolvimento da sociedade de informação se caracteriza pela introdução de novos serviços de telecomunicações; que o desenvolvimento transfronteiras bem sucedido desses serviços, como o vídeo a pedido e a televisão interactiva, depende em parte da confiança dos utilizadores na garantia da sua privacidade".

5.6. No fundo, o futuro nesta matéria, prende-se com a reflexão sobre o futuro do desenvolvimento económico, do desenvolvimento tecnológico, da globalização, da noção de mercado, da liberdade de informação, dos segredos e do próprio conceito da vida privada.

Mas nunca poderemos esquecer que todo o progresso, toda a tecnologia, todo o comércio, toda a informação, só existe do Homem, para o Homem e em função do Homem.

E é por isso que acredito que os valores e direitos fundamentais do Homem acabarão por se fazer respeitar.