O CONCEITO DA PROTECÇÃO DE DADOS NOS ENSAIOS CLINICOS:

Revisão regulamentar

Trabalho Realizado por:

Sandra Casaca

Setembro 2011

Índice

1. Introdução

A evolução da sociedade desde os seus primórdios até aos nossos dias apresenta, em cada época, as suas especificidades. De facto, a sociedade em que vivemos caracteriza-se pela sua ligação cada vez maior às tecnologias da informação – trata-se da, já designada, "Sociedade de informação".

Cada um dos aspetos da nossa vida em sociedade encontra-se, queiramos ou não, associados a um qualquer sistema de informação. Entre todos estes aspetos encontramos, indiscutivelmente, o sistema de saúde onde todos os cidadãos estão inseridos.

A proteção de dados pessoais é um assunto da maior relevância no momento atual, e ainda o é mais particularmente quando se atenta à necessidade de tratamento de dados pessoais efetuados no âmbito de estudos de investigação científica na área da saúde. Assim, este trabalho tem como objetivo detalhar a evolução da sensibilidade e importância para a proteção dos dados de cada um de nós bem como detalhar a evolução legislativa neste âmbito terminando especificamente no tratamento de dados pessoais relacionados com os ensaios clínicos.

A proteção de dados é um tipo de proteção de privacidade que se manifesta mediante uma legislação especial. O direito à proteção de dados garante a um indivíduo o direito de dispor sobre todos os dados relacionados com a sua personalidade, saúde, vida pessoal, convicção política ou religiosa, raça, etc. Desta forma, este serve para sustentar a proteção da privacidade num mundo onde a possibilidade de recolher, armazenar e cruzar os grandes grupos de dados

é amplamente disponível. Nesta situação, o significado de factos e dados que anteriormente eram considerados irrelevantes pela legislação aumenta. Anteriormente devido à falta de tecnologias altamente desenvolvidas para processamento de dados, nenhuma ameaça foi imposta com tornar público este tipo de informação enquanto hoje o processamento, armazenamento e o cruzamento de dados ou a criação de novos dados, contando com os antigos, pode resultar na violação do direito à privacidade.

Consequentemente, o objeto da proteção é novo - dados pessoais - o seu objetivo, no entanto, é o mesmo que foi para a proteção do sigilo, à semelhança do objetivo de outras ferramentas extralegais para proteger a privacidade ou intimidade. Antes de tratar a questão da proteção de dados como um direito específico, é necessário definir o objetivo e interesse a ser protegido: o que é protegido pelo direito à proteção de dados pelas normas de processamento de dados?

O objetivo da lei de proteção de dados é a proteção da privacidade. Esta afirmação é verdadeira, no entanto, diz pouco sobre o que a privacidade é e por que ela precisa de proteção.

2. As primeiras noções de privacidade

Westin[23] salienta que "*praticamente todos os animais buscam períodos de reclusão individual ou intimidade de pequenos grupos. Este é geralmente descrito como a tendência de territorialidade, em que um organismo privado reivindica a uma área de terra, água ou ar e defende-o contra a invasão por membros de sua própria espécie.* " Os mecanismos de fixação de distância podem ser detetados no mundo animal, o que tem sido chamado de "distância pessoal".

Westin[23] diferencia os vários aspetos da privacidade que são características de todos os seres humanos vivendo numa sociedade. Estes são principalmente as

normas relativas à privacidade no nível individual, ao nível da família/lar e na comunidade. De acordo com os resultados apresentados pelas normas de privacidade segundo o mesmo autor, considera como um aspeto especial da vida privada "*as maneiras pelas quais os seres humanos percebem a sua situação quando estão sozinhos*"[23]. Outro elemento, é universal "*a curiosidade e a vigilância*"[23], ou seja, a tendência dos indivíduos e da sociedade de invadir a privacidade dos outros. O fenómeno da curiosidade para seu próprio benefício, de acordo com Westin[23], não está restrito ao homem.

A proteção da honra aparece já no clássico do Direito Romano, e depois de superar a sua história na Idade Média, ela continua sendo uma garantia para assegurar o direito do nome e da proteção do direito de retrato no Direito Suíço, enquanto nos Estados Unidos, é assimilada pela proteção da privacidade.

Warren e Brandeis[22], no célebre artigo publicado em 1890 (The right to privacy), referem a necessidade de conectar o reconhecimento do direito à privacidade, no direito comum.

Warren e Brandeis[22] apoiaram a necessidade do reconhecimento do "direito à privacidade", com a mudança na estrutura de publicidade e o surgimento de novas tecnologias da época. A proteção do indivíduo ganhou um novo fundo substituindo os direitos de propriedade: a privacidade; a proteção não só da privacidade, mas a proteção da autonomia em seu sentido amplo. É um marco importante no desenvolvimento dos direitos de personalidade: o desenvolvimento que se caracteriza "principalmente pelo destacamento de proteção da propriedade"[22]. A proteção do nome, imagem e gravação de som é reconhecida como uma resposta aos desafios de desenvolvimento da tecnologia, e o direito da personalidade em geral é transposta para o direito - em primeiro lugar na Suíça.

O direito geral de personalidade, depois de um declínio temporário durante a Segunda Guerra Mundial, tornou-se novamente o foco do pensamento jurídico.

Apareceram então as primeiras leis de proteção de dados embora ainda de uma forma indireta, a proteção jurídica dos factos (dados) de um indivíduo fora da esfera de proteção da confidencialidade. Como passo seguinte - com base na disposição da Constituição Alemã (Grundgesetz), que declara os direitos da personalidade em geral - o Tribunal Constitucional Alemão formula o direito de autodeterminação informativa (autonomia informativa). A nova legislação garante o direito de dispor sobre todos os dados que podem ser associados a uma pessoa (não importa se os dados fazem parte da esfera de sigilo ou não).

3. A noção da proteção de dados

A noção de proteção de dados Alemã (Datenschutz) tornou-se generalizada, com início na década de setenta, significando um novo tipo de proteção em relação aos direitos da personalidade anterior. Esta nova proteção, de acordo com os regulamentos de proteção de dados, aplica-se, normalmente, a pessoas singulares não só em determinados tipos de dados (imagem e gravação de som), como geralmente não é restrita aos dados sensíveis.

Compete então chegarmos à definição/noção do que é a proteção de dados. O conceito de proteção de dados é muitas vezes tratado como parte da proteção da privacidade, ou bem como o seu contrário, a ela se opõem, como uma solução especificamente europeia (legal) para um problema que contribuiu para o aparecimento do "direito à vida privada". A proteção dos dados pode ser entendida apenas no âmbito da vida privada, sendo utilizada como um instrumento jurídico de proteção da privacidade, nascido num determinado contexto social e técnico. Também não devemos desconsiderar o facto de que a noção de privacidade é usada hoje num sentido muito mais amplo do pensamento jurídico - como já me referi a ele anteriormente, como resultado do desenvolvimento que tem vindo a atravessar desde o fim do século passado, pode ser interpretada como o equivalente do direito geral da personalidade.

Assim, em suma o conceito de proteção de dados surgiu na Europa como uma resposta aos perigos do processamento eletrónico de dados, que foram sendo disseminados através da revolução eletrónica, a partir da década de 70, e o conteúdo da proteção jurídica prevista por ele mudou significativamente várias vezes desde o seu aparecimento, e ainda está atualmente em constante evolução.

A proteção de dados não pode ser identificada como o direito de autodeterminação informativa, uma vez que as leis de proteção de dados iniciais não garantiam uma disposição para qualquer indivíduo sobre seus dados pessoais. A proteção de dados inclui todos os regulamentos que, através da regulamentação do tratamento de dados pessoais de um indivíduo, têm como objetivo a proteção desses dados, independentemente de saber se este regulamento garante o direito de autodeterminação informativa de um indivíduo ou não.

A proteção de dados e a liberdade de informação, a legislação dos dados relativos a indivíduos e os esforços visando a disponibilização ao público de dados do governo, têm sido ligados historicamente. Os dados da primeira geração de normas de proteção de dados não foram dirigidas diretamente a regulamentar o tratamento de dados pessoais, mas sim a uma regulação estatal das aplicações tecnológicas. O tamanho excessivo dos bancos de dados disponíveis para o governo e os sistemas capazes de processar os dados de uma forma eficaz estavam a ameaçar não só a privacidade do indivíduo, mas também a divisão tradicional de poder.

O direito à proteção de dados, especialmente na Hungria, é tratado na literatura com frequência como o direito de acesso aos dados de interesse público, ou seja, como o direito duplo da liberdade de informação (''direitos de informação''): proteção dos dados e a liberdade de informação.

O objeto da legislação em matéria de gestão de informação não é um dado pessoal, mas sim dados (informações) independente do suporte dos mesmos, cuja gestão é regulamentada pelas determinadas áreas da legislação por razões específicas (proteção da privacidade, interesse da segurança nacional, etc.).

4. Evolução da legislação nacional e europeia

4.1 A primeira geração de normas de proteção de dados

Na segunda metade da década de 60 a realidade de gestão e acumulação de dados tornou-se infindável com o inicio da era informática. Estes desenvolvimentos, levaram alguns países a pensarem na controversa e polémica proteção dos dados.

A primeira geração de proteção de dados, nasceu num período em que os computadores já eram usados por alguns, e para o tratamento de dados essencialmente estatal. Houve uma ameaça de que o estado, ligando diversos registos, ganharia uma superpotência informativa sobre o indivíduo. Por conseguinte, ao formular a primeira lei de proteção de dados, os autores tiveram especial atenção aos desafios da nova tecnologia, de forma a tornar a proteção dos dados controlável e transparente. As características da primeira geração de normas no âmbito da proteção de dados são os seguintes:

a) O principal objetivo destas normas é a transparência das grandes bases de dados - principalmente estatais.

b) Estas normas não garantem o direito de dispor sobre os dados de um indivíduo para alcançar este objetivo, mas garantem alguns direitos (principalmente o direito de acesso e retificação), que mais tarde se tornaram partes integrantes do direito de autodeterminação informativa.

c) Obrigações relativas a registar as bases de dados contendo dados pessoais aparecem dentro desta geração de normas de proteção de dados. Assim, é importante salientar que a obrigação do registo surgiu num contexto em que havia poucos grandes bancos de dados.

d) Com os dados da primeira geração das normas de proteção, o legislador quis controlar especificamente o tratamento informático de dados. Estes regulamentos foram instrumentos peculiares de proteção da privacidade na fase inicial da revolução da informação, mas de acordo com a definição acima não podem ser consideradas como normas de proteção de dados no sentido de que o seu objetivo era basicamente a tecnologia ao serviço da manutenção dos registos.

e) É uma característica de algumas normas o direito de ter acesso às informações disponíveis para a administração pública. Isto sustenta a ideia de que o alvo direto das normas de primeira geração não foi a proteção de, mas sim a criação da "divisão de informação do poder", e a supressão do excesso de poder de informação do ramo executivo do governo no interior do estado e da sociedade.

4.2 A decisão do censo e da segunda geração de normas de proteção de dados

A 28 de Janeiro de 1981 foi emitida a Convenção 108 do Conselho da Europa[32] com vista à proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal. Nesta Convenção participaram todos os Estados Membros do Conselho da Europa e teve como objetivo cito: "*garantir que em cada território todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («proteção dos dados»)*"[32].

Tendo como objetivo o supracitado, a mesma Convenção[32] no seu artigo 2º apresenta já algumas definições que marcam o início da compreensão sobre esta temática:

> a) «Dados de carácter pessoal» significa qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação («titular dos dados»);
>
> b) «Ficheiro automatizado» significa qualquer conjunto de informações objeto de tratamento automatizado;
>
> c) «Tratamento automatizado» compreende as operações, efetuadas, no todo ou em parte, com a ajuda de processos automatizados: registo de dados, aplicação a esses dados de operações lógicas e ou aritméticas, bem como a sua modificação, supressão, extração ou difusão;
>
> d) «Responsável pelo ficheiro» significa a pessoa, singular ou coletiva, autoridade pública, serviço ou qualquer outro organismo competente, segundo a lei nacional, para decidir sobre a finalidade do ficheiro automatizado, as categorias de dados de carácter pessoal que devem ser registadas e as operações que lhes serão aplicadas.

Em Dezembro de 1983, o Tribunal Constitucional Federal Alemão declarou inconstitucional (como a violação à Lei Básica), algumas disposições da lei sobre o recenseamento aprovada no mesmo ano, e com esta decisão produziu um efeito global sobre a política de proteção de dados.

Com a evolução dos tempos o Direito da Personalidade inclui a autoridade do indivíduo para se decidir, na base da ideia de autodeterminação, quando e quais os limites com base no princípio da autodeterminação para definir que informações sobre sua vida privada podem ser comunicadas a outros e em que medida. De acordo com o tribunal, a autodeterminação exige maior proteção

devido ao desenvolvimento da tecnologia. Esta é ameaçada principalmente pelo facto de que, contrariamente à prática anterior, não há necessidade de chegar de volta ao arquivo manual de milhares de documentos, desde que os dados sobre as relações pessoais ou materiais de um indivíduo específico possam ser armazenados sem qualquer restrição técnica com a ajuda de processamento automático de dados, e possam ser recuperados a qualquer momento num curto espaço de tempo, independentemente da sua localização. Além disso, no caso da criação de sistemas integrados de informação com outras bases de dados, estes podem ser integrados numa imagem parcial ou totalmente completa de um indivíduo, sem o consentimento informado do detentor dos dados sobre a regularidade e o fim a que se destina o uso dos mesmos. O Tribunal declarou que a situação pode ser perigosa tanto para o direito do indivíduo à autodeterminação como para a sociedade.

No entanto, o Tribunal declarou que o direito à autodeterminação informativa não era ilimitado. Limitações são apenas aceites por razões imperiosas de interesse público tendo que cumprir a exigência de clareza, portanto, serem formuladas de uma forma que os cidadãos conheçam os requisitos e a extensão da limitação. O objetivo da gestão de dados deve ser especificado, e pode ser exigido que sejam adequados e necessários para o efeito. Como mais uma garantia processual a decisão judicial prevê o direito à informação e a obrigação de exclusão de dados uma vez que o objetivo seja alcançado.

A segunda geração de normas para a proteção dos dados, de acordo com Mayer-Schönberger[15] caracteriza-se pelo facto de garantir direitos específicos para o indivíduo sobre todo o processo de tratamento de dados pessoais. Os legisladores perceberam que a decisão dos cidadãos não pode ser restrita para o seu consentimento ou discordância com o tratamento automatizado dos seus dados, já que a tecnologia por esta altura havia permeado a sociedade de uma forma que a divergência implicaria custos excessivos para o indivíduo. As mudanças

tecnológicas do período - o surgimento dos computadores pessoais, e sua posterior ligação às redes - teria tornado impossível a regulamentação da tecnologia.

Em Portugal, a Comissão com autoridade sobre a temática em discussão iniciou o seu primeiro mandato em 7 de Janeiro de 1994, começando a funcionar nas suas atuais instalações em frente à Assembleia da República.

A sua primeira designação foi Comissão Nacional de Proteção de Dados Pessoais Informatizados – CNPDPI.

Contudo, já desde 1976 a Constituição da República Portuguesa tinha consagrado, como direito fundamental, no seu artigo 35º, a proteção dos dados pessoais face à utilização da informática.

No entanto, só quinze anos depois, é aprovada a primeira lei de proteção de dados – Lei 10/91 de 29 de Abril[34], na qual se regulamenta a utilização e o controlo dos dados pessoais e se prevê a criação da CNPDPI.

Esta lei vem a sofrer algumas alterações com a Lei 28/94 de 29 de Agosto[35], que aprova medidas de reforço da proteção de dados pessoais, quando a Comissão já tinha entrado em funcionamento.

4.3 Globalização: documentos internacionais de proteção de dados

A necessidade de harmonização das legislações das várias nações, inevitavelmente, ocorreu após a aprovação dos primeiros Atos sobre a proteção de dados, a fim de assegurar que estas legislações nacionais não eram limites ao fluxo transfronteiriço de dados pessoais.

Como um primeiro desenvolvimento no contexto da globalização da proteção de dados, da Organização para a Cooperação e Desenvolvimento Económico

(OCDE) formulou orientações[36] para a proteção de dados em 1980 (Diretrizes da OCDE para a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais). A especial importância das orientações da OCDE está no facto de que os Estados Unidos da América são um membro da organização, e por isso - ao contrário da convenção CE e da diretiva da UE - as diretivas da OCDE podem ser entendidas como o denominador comum entre a Europa e os Estados Unidos. O principal objetivo das orientações[36] da OCDE é evitar a criação de obstáculos injustificados à proteção de dados para o desenvolvimento das relações económicas e o fluxo transfronteiriço de dados.

É um atributo progressivo das orientações que se aplicam não apenas para a gestão automatizada de dados, mas toda a gestão de dados que, devido à maneira como são processados, ou por causa de sua natureza ou do contexto em que eles são usados, representam um perigo para a privacidade e para as liberdades individuais.

As recomendações das orientações[36] sobre tratamento de dados privados do sector público incluem os seguintes princípios:

- Existência de limites para a recolha de dados pessoais e estes devem ser obtidos por meios justos e legais e, quando apropriado, com o conhecimento ou consentimento do titular dos dados.
- Os dados pessoais devem ser relevantes para os fins a que se destinam, e, na medida do necessário para o efeito, devem ser precisos, completos e atualizados.
- Os fins para os quais os dados pessoais são recolhidos devem ser especificados, em último caso no momento da recolha dos mesmos, e a sua posterior utilização limitada aos fins a que se destinam.
- Os dados pessoais não devem ser divulgados, comunicados ou utilizados para outros fins que não os especificados acima, exceto com o consentimento do titular dos dados, ou da autoridade competente.

- Os dados pessoais devem ser protegidos por garantias de segurança contra riscos como perda ou acesso não autorizado, destruição, modificação, etc.
- O meio de estabelecer a existência e a natureza dos dados pessoais devem estar prontamente disponíveis, bem como as principais finalidades do seu uso, e a identidade e localização habitual do tratamento dos mesmos.
- Um indivíduo deve ter o direito de obter de um controlador de dados a confirmação da existência ou não de dados que lhe dizem respeito, e que esta informação lhe seja comunicada dentro de um prazo razoável, sem qualquer encargo, e se este existir, não pode ser excessivo; de uma forma que seja possível contestar e desafiar os dados que lhe digam respeito e, se o desafio for bem-sucedido, a ter os dados apagados, retificados, completados ou alterados.
- O controlador de dados deve ser responsável pelo cumprimento das medidas que o obrigam aos princípios acima referidos.

É também da responsabilidade do responsável pelo tratamento dos dados cumprir com as orientações regulamentares no campo dos fluxos transfronteiriços de dados pessoais. Os Estados Membros podem limitar o fluxo de dados específicos regulados por normas de proteção de dados, tendo em conta a natureza dos dados em causa, bem como o facto de o Estado Membro conseguir proporcionar uma proteção dos mesmos.

Na sequência da adoção da Convenção CE, a Comissão Europeia considerou que a Convenção poderia resolver o problema de harmonização na União Europeia: em 1981, foi apresentada uma recomendação que encorajou os Estados Membros a adotar a convenção. Contudo, a relutância existente em relação à legislação não era sem qualquer razão: quando a Comissão se apercebeu da divergência existente entre as legislações nacionais iniciou, em 1990, o desenvolvimento da directiva[31]. Tornou-se então claro, que os Estados Membros estavam fortemente

divididos quanto à questão dos regulamentos de proteção de dados: a Grã-Bretanha, por exemplo, era explicitamente contra a proteção de dados com regulamentação a nível sindical. Ainda assim, a directiva[31] foi finalmente aprovada em 1995, e os Estados Membros tiveram de aplicar as suas disposições até 1998.

A directiva[31] baseia-se no artigo 100º do Tratado da Comunidade Europeia, é uma medida de harmonização que serve a meta incluída no artigo 14º (mercado interno único). O seu objetivo está refletido no seu título: "*Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas relativamente ao tratamento de dados pessoais e à livre circulação desses dados*". Este objetivo também aparece no preâmbulo e no artigo 1º da diretiva (o título do último é "*Objeto da diretiva*").

Em conformidade com esta diretiva, os Estados devem proteger os direitos e liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à privacidade no que diz respeito ao tratamento de dados pessoais. Contudo, os Estados-Membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-Membros por razões relacionadas com a proteção de dados.

Desta forma, a legislação sobre a proteção de dados sofreu uma evolução num curto espaço de tempo. Segue-se um sumário da mesma:

<u>Diretivas</u>

- Diretiva 95/46/EC[31] do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 sobre a proteção de dados individual no que se refere ao processamento de dados pessoais e à sua livre circulação.
- Diretiva 2002/58/EC[37] do Parlamento Europeu e do Conselho de 12 Julho de 2002 referente ao processamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

- Diretiva 2006/24/EC[38] do Parlamento Europeu e do Conselho de 15 Março de 2006 sobre a retenção de dados gerados ou processados em relação à disponibilização de serviços de comunicação eletrónica públicos ou redes de comunicação bem como a adenda Diretiva 2002/58/EC.
- Diretiva 2009/136/EC[39] do Parlamento Europeu e do Conselho de 25 Novembro de 2009 relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e posteriormente Diretiva 2002/22/EC respeitante à utilização de cookies pelos websites.

4.4 A transposição para o direito nacional

Como é de fácil entendimento, e dada a conjetura da altura, a principal preocupação no que se refere à temática da proteção de dados estava na sua proteção face à utilização em meios informáticos, já publicada, desde 1976, na Constituição da República Portuguesa no seu artigo 35º.

Contudo apenas 15 anos mais tarde é aprovada a primeira lei de proteção de dados. Esta Lei 10/91 de 29 de Abril[34], regulamenta a utilização e o controlo dos dados pessoais e prevê a criação da CNPDPI. Em 1994 a Comissão Nacional de Proteção de Dados (CNPD) iniciou o seu primeiro mandato.

1976 PDP na utilização informática (Constituição da Republica)

1980 Diretrizes da OCDE sobre PD e fluxos transfronteiriços

1981 Recomendação pela CE para adoção a convenção

1990 Início do desenvolvimento a Diretiva

1991 1ª Lei de PD: Lei 10/91 (prevê a criação da CNPDPI)

1994 Medidas de reforço: Lei 28/94

1994 Início do 1ª mandato da CNPD

1995 Diretiva 95/46/EC aprovada

1995 Publicação da Diretiva 95/46/EC (PD quanto ao processamento e circulação)

1998 Data limite de implementação pelos EM

1998 Publicação da Lei 67/98

1998 Publicação da Lei 69/98 (Proteção de DP nas telecomunicações)

2002 Publicação da Diretiva 2002/58/EC (PD nas comunicações eletrónicas)

2006 Publicação da Diretiva 2006/24/EC (Disponibilização de serviços de comunicação eletrónica)

2009 Publicação da Diretiva 2009/136/EC

PD- Proteção de dados

PDP- Proteção de dados pessoais

Esta lei 10/91 de 29 de Abril[34] vem sofrer algumas alterações com a Lei 28/94 de 29 de Agosto[35] que visa reforçar e criar medidas de proteção aos dados pessoais.

Foi publicada, em 1995, a Diretiva 95/46/CE[31] do Parlamento e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que impõe aos Estados-Membros um prazo de três anos para a sua transposição para o direito nacional.

A 4ª revisão constitucional, em 1997, levantou algumas alterações ao artigo 35º, de modo a permitir uma adequada transposição da Diretiva de Proteção de Dados. Na nova redação do artigo 35º, a Comissão viu consagrada constitucionalmente a sua existência, como entidade administrativa independente.

Em 1998, foi aprovada a nova Lei de Proteção de Dados Pessoais – Lei 67/98 de 26 de Outubro[30], que transpõe a Diretiva 95/46/CE[31], e vem alargar substancialmente o leque de atribuições e competências da Comissão, que passa desde então a designar-se de CNPD -Comissão Nacional de Proteção de Dados.

Na mesma altura, sai a Lei 69/98 de 28 de Outubro[40], que vem regular a proteção de dados pessoais e a defesa da privacidade no sector das telecomunicações, transpondo a denominada Diretiva das Telecomunicações (Diretiva 97/66/CE[41]), e que também atribui à CNPD competências nesta matéria.

A Lei 10/91[34] e a Lei 28/94[35] são revogadas pela Lei 67/98 de 26 de Outubro[30].

Em 2004, é revogada a Lei 69/98[40], com a publicação da Lei 41/2004, de 18 de Agosto[42], que regula a proteção de dados pessoais no sector das comunicações eletrónicas, transpondo a Diretiva 2002/58/CE[37] para o direito nacional.

É também publicada legislação complementar, que atribui competências à Comissão como autoridade nacional de controlo em matérias de proteção de

dados pessoais relativas a Schengen (Lei 2/94 de 19 de Fevereiro[43]) e à Europol (Lei 68/98, de 26 de Outubro[44]).

5. Conceito de proteção de dados no âmbito dos ensaios clínicos

De forma a clarificar a LPD (Lei de Proteção de Dados), Lei 67/98[30], no que concerne a proteção de dados no âmbito dos ensaios clínicos, foram, em 2007, publicadas duas deliberações por parte da CNPD:

- Deliberação nº 333/2007[28]: Princípios aplicáveis aos tratamentos de dados pessoais, no âmbito de ensaios clínicos com medicamentos de uso humano.
- Deliberação nº 227/2007[27]: Princípios aplicáveis aos tratamentos de dados pessoais efetuados no âmbito de estudos de investigação científica na área da saúde

Iremos então abordar cada uma destas deliberações em pormenor.

A Lei nº 46/2004, de 19 de Agosto[33] transpõe para a ordem jurídica nacional a Diretiva 2001/20/CE[45], do Parlamento Europeu e do Conselho, de 4 de Abril, a regulamentação dos ensaios clínicos. Ao abrigo desta lei define-se ensaio clínico como: "*qualquer investigação conduzida no ser humano, destinada a descobrir ou verificar os efeitos clínicos, farmacológicos ou os outros efeitos farmacodinâmicos de um ou mais medicamentos experimentais, ou identificar os efeitos indesejáveis de um ou mais medicamentos experimentais, ou a analisar a absorção, a distribuição, o metabolismo e a eliminação de um ou mais medicamentos experimentais, a fim de apurar a respetiva segurança ou eficácia*".

5.1 Ensaios Clínicos Intervencionais

5.1.1 Introdução e breves definições

Tendo em atenção que ensaios clínicos intervencionais têm a definição acima descrita onde a utilização de determinado fármaco é avaliada, dada a importância expressada pela própria CNPD quanto à necessidade de realização dos mesmos, e consequentemente, a recolha de dados pessoais, o tratamento/utilização dos mesmos está dependente de vários pressupostos.

Compete ainda acrescentar que sob o ponto de vista da CNPD, de acordo com a Lei 46/2004[33], na sua secção II, consideram-se responsáveis pela realização de um ensaio clínico o Promotor, o Investigador bem como o Monitor. Contudo, perante a CNPD a entidade responsável pelo Ensaio Clínico é o Promotor uma vez que é este que determina a finalidade do tratamento e os meios para a sua realização. O Investigador detém as responsabilidades de prestação de informação, obtenção do consentimento informado, garantia do processamento dos dados pessoais e da confidencialidade durante o ensaio. Este co-responsabiliza-se com o Promotor pelos danos patrimoniais e não patrimoniais sofridos pelos participantes.

Salienta-se ainda a participação nos Ensaios Clínicos de Subcontratantes. Estes últimos atuam em nome e sob a responsabilidade do Promotor. Um exemplo de um subcontratante é o Monitor, que serve o propósito de acompanhar o Ensaio Clínico mantendo o Promotor devidamente e permanentemente informado. Garante ainda o correto e completo registo dos dados recolhidos. Considera-se também subcontratante o próprio Investigador que se responsabiliza pela realização dos ensaios clínicos nos centros de ensaio.

Assim, deve-se levar em consideração as seguintes definições citadas na legislação (artigo 3º da Lei nº 67/98[30] de 26 de Outubro):

- Dados pessoais: qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;
- Tratamento de dados pessoais: qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;
- Responsável pelo tratamento: é "*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 de dados pessoais; sempre que as finalidades e os meios de tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa*."
- Promotor: é a entidade responsável, perante a CNPD, na medida em que determina a finalidade e os meios do tratamento. É responsável pelos danos causados aos participantes.
- Investigador: pratica atos materiais típicos da entidade responsável: presta o dever de informação (alínea b) do artigo 10º da Lei 46/2004[33] e artigo

10º da LPD), obtém o consentimento dos participantes (alínea c) do artigo 10º da Lei 46/2004[33] e nº 2 do artigo 7º da LPD), assegura o processamento dos dados pessoais (alínea f) do artigo 10º da Lei 46/2004[33]) e garante a confidencialidade durante o ensaio. É também responsável pelos danos causados aos participantes.

5.1.2 Dados Pessoais e Dados Pessoais Sensíveis

Carece ainda de compreensão, nesta primeira fase, o significado de dados pessoais sensíveis bem como a permissibilidade da citada legislação para a recolha dos mesmos. Assim, de acordo com o artigo 5º, Capitulo II Secção I da Lei 67/98[30], os dados pessoais devem ser:

- Tratados de forma lícita e com respeito pelo princípio da boa fé;
- Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades;
- Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados;
- Exatos e, se necessário, atualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente;
- Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

Assim sendo, e desde que devidamente autorizados pelo titular dos dados e pela CNPD estes podem ser recolhidos.

No entanto, a lei já não é permissiva quanto à recolha dos seguintes dados pessoais sensíveis:

- convicções filosóficas ou políticas,
- filiação partidária ou sindical,
- fé religiosa,
- vida privada
- origem racial ou étnica,
- tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos.

A recolha de qualquer um destes dados tem que ser aceite por parte do titular dos dados através da assinatura de um consentimento informado e tem que ser aprovado por parte da CNPD única e exclusivamente se estes forem de interesse público e imprescindíveis para o decorrer do ensaio clínico. Contudo a sua necessidade de recolha em determinados ensaios clínicos é normalmente aprovada quando devidamente justificada. Por exemplo a recolha da Raça/Etnia é uma prática comum nestes estudos, fazendo parte da informação demográfica recolhida. Esta informação é essencial devido à necessidade de provar que os resultados obtidos são válidos independentemente da origem étnica do doente e por isso transponíveis para outros grupos populacionais. O mesmo se passa com a vida privada, um outro exemplo em que de acordo com a Deliberação 333/2007[23] emitida pela Comissão Nacional de Proteção de Dados, no capítulo "V - Categorias e qualidades dos dados pessoais" refere-se quais os dados de vida privada passíveis de recolha:

"*7. De igual modo, dados da vida sexual, dados da vida privada (como sejam dados pessoais comportamentais, ligados aos usos pessoais, dados pessoais psicológicos e volitivos, entre muitos outros), dados pessoais da origem racial ou étnica apenas devem ser tratados quando estiver cabalmente demonstrada a sua*

pertinência, adequação, indispensabilidade e não excessividade face à finalidade do ensaio"[23].

A recolha deste tipo de dados é levada a cabo através de questionários. Estes questionários são preenchidos pelos doentes, ou seja, as respostas são fornecidas de forma voluntária. O objetivo é recolher informação sobre os hábitos associados à toma da medicação, para se avaliar a adesão à terapêutica e avaliar a influência da patologia na qualidade de vida do doente. Sendo que a pertinência desta recolha está cabalmente demonstrada em virtude de permitir a condução do estudo e atingir o seu objetivo principal que é avaliar a segurança e eficácia das terapêuticas em estudo. Esta informação é assim crucial para a realização deste ensaio. Não podemos nunca esquecer que apesar da aprovação da CNPD o doente, por meio do consentimento esclarecido, deverá também dar a sua autorização para tal recolha.

Dados como a data de nascimento, são considerados demográficos, devem ser devidamente fundamentados quanto à necessidade de recolha apesar de não ser considerado um dado pessoal sensível uma vez que não é um dado de saúde. Para os ensaios clínicos a recolha da data de nascimento com DD/MM/YY é indispensável em todo e qualquer estudo relacionado com a saúde.

Ao desenvolver ensaios clínicos em qualquer parte do mundo, as empresas devem assegurar a recolha de determinadas características mínimas como sendo o sexo, a data de nascimento completa e correta e um código individual. Isto irá permitir que os dados recolhidos nos ensaios clínicos sejam credíveis, que permitam a confirmação da existência do indivíduo e possibilitem as várias análises necessárias (exemplo: baseadas no sexo, idade/ grupo de idades).

Este tipo de dados pode ainda ser recolhido se cumprir com as seguintes cláusulas aqui incluídas como citação do artigo 7º alínea 3 da LPD[30] (cito):

- *Ser necessário para proteger interesses vitais do titular dos dados ou de uma outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento;*
- *Ser efetuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas atividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares;*
- *Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos;*
- *Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efetuado exclusivamente com essa finalidade*.

No que respeita à recolha de dados de saúde e vida sexual, incluindo dados genéticos, apenas é permitida para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD, nos termos do artigo 27º, e sejam garantidas medidas adequadas de segurança da informação.

5.1.3 Os direitos dos Titulares dos dados

De modo a obter informação necessária acerca da eficácia e segurança de um determinado medicamento é essencial proceder à recolha e processamento de dados pessoais dos participantes (titulares dos dados). Esta recolha de dados será feita com o consentimento esclarecido por parte dos participantes, havendo uma secção específica no documento, onde os seus direitos relativamente ao

tratamento de dados pessoais são explicados. Nos termos do artigo 11º da Lei de Proteção de Dados[30], o participante titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos, a confirmação da existência do tratamento dos seus dados pessoais, conhecimento sobre a finalidade desse tratamento, sobre as categorias de dados pessoais tratados, sobre os destinatários dos seus dados pessoais, a lógica subjacente ao tratamento, bem como a retificação, o apagamento ou bloqueio dos dados e da notificação dos destinatários dessa retificação. Por tudo isto, deve ficar devidamente esclarecido que o titular dos dados tem todo o direito de acesso, retificação e eliminação que deve estar devidamente mencionado no consentimento informado.

O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos informação no que respeita à existência ou não de tratamento dos seus dados (incluindo as suas categorias),

Os titulares dos dados devem ser devidamente informados da identidade do responsável pelo tratamento ou seu representante legal (se aplicável); finalidade do tratamento bem como outro tipo de informação como:

- Os destinatários ou categorias de destinatários dos dados;
- O carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder;
- A existência e as condições do direito de acesso e de retificação, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir ao seu titular um tratamento leal dos mesmos.

Caso os dados estejam presentes em redes abertas, e o responsável pelo tratamento dos mesmos daí os recolha, tem sempre que informar o titular dos

dados exceto se este já tiver conhecimento que os seus dados podem andar a circular na rede sem condições de segurança. Ora coloca-se então aqui uma dificuldade, uma vez que o responsável pelo tratamento dos dados poderá não ter acesso à informação se o titular deu ou não autorização para a publicação dos seus dados em rede aberta. Carece assim sempre da autorização da CNPD.

Contudo, caso esta recolha de dados seja feita com finalidades estatísticas, históricas ou de investigação científica e a informação do titular dos dados se revelar impossível ou obrigar a esforços despropositados por parte da entidade que vai tratar os dados ou quando a lei assim o determinar, a CNPD pode em deliberação dispensar da obrigação de informação ao titular dos dados.

5.1.4 A Interconexão de dados pessoais

Apesar de a LPD (Lei de Proteção de Dados)[30] ser de alguma forma restritiva quanto à interconexão de dados pessoais, no que respeita aos ensaios clínicos a necessidade da mesma ocorrer deve ser devidamente explicada. Um dos objetivos da realização destes estudos é recolher informação relativamente ao perfil de um medicamento, que permita avaliar segurança e eficácia, e desta forma provar que o mesmo é uma alternativa terapêutica válida para uma patologia específica. Frequentemente são necessários vários ensaios clínicos e estudos observacionais para conseguir a aprovação de um medicamento para cada patologia. Verifica-se ainda que ao longo do tempo, o perfil de segurança e eficácia que estiveram na base da aprovação de um medicamento vai sendo atualizado, resultando do cruzamento dos dados existentes com a informação recolhida dos estudos mais recentes. Assim, sendo e para bem da saúde publica, é necessário a permissividade da ocorrência de interconexões em virtude de estas permitirem uma mais correta avaliação do perfil clínico e de segurança do medicamento.

5.1.5 Medidas de segurança e comunicação dos dados

O responsável pelo tratamento dos dados deve colocar em prática, à luz da LPD[30], todas e quaisquer medidas que garantam a proteção dos dados por ele tratados. Assim, estes dados devem estar protegidos para que pessoas não autorizadas sejam impedidas de aceder aos mesmos e que os acessos estejam devidamente controlados.

No caso de se tratar de dados pessoais sensíveis, as medidas de segurança devem incluir:

- Diferentes níveis de acesso;
- Mecanismos de autenticação;
- Registo de todos os acessos e introduções de dados;
- Separação lógica dos dados pessoais de saúde dos dados pessoais administrativos;
- Acesso diferenciado pelos diferentes médicos e profissionais envolvidos, segundo necessidade (ex: especialidades);
- Medidas especiais transporte e acesso pelos auxiliares administrativos;
- Os dados pessoais de saúde, vida sexual e genéticos devem ser separados lógica e fisicamente dos restantes dados pessoais;
- Existência de “packs” de dados pessoais dedicados com informação selecionada.

Da mesma forma, os dados pessoais devem estar seguros contra destruição (acidental ou não), alteração ou divulgação. Por conseguinte, aquando da sua divulgação os mesmos devem ser encriptados de forma a garantir que se existir uma fuga de informação a mesma está protegida. Quaisquer entidades/pessoas encarregues do tratamento dos dados pessoais (pertencentes ao responsável pelo tratamento ou a uma entidade terceira) ficam obrigados a sigilo mesmo após cessarem as suas funções. Caso o tratamento dos dados pessoais envolva a

comunicação dos mesmos a terceiros esta deverá ser alvo de aprovação prévia pela CNPD.

Para além de tudo isto, os dados pessoais dos indivíduos participantes num ensaio clínico devem ser devidamente codificados impedindo a sua direta identificação (sendo assim anonimizados). Por conseguinte apenas devem ter acesso aos dados pessoais de cada participante os intervenientes no ensaio para os quais esta informação seja crucial no exercício das suas funções (i.e.: investigador e pessoal da sua equipa). No caso das Comissões de Ética, estas apenas poderão ter acesso a determinados dados pessoais no âmbito da verificação da conformidade dos procedimentos quanto aos consentimentos informados assinados pelos titulares dos dados participantes no ensaio clínico.

5.1.6 Fluxos transfronteiriços e suas diferenças

Tratando-se de dados pessoais de saúde, objeto de rigorosas regras éticas e legais ligadas ao sigilo e à confidencialidade, sendo dados pessoais sensíveis, merecedores de especiais regras de segurança o responsável pelo tratamento dos dados deve garantir assim a obtenção de autorização prévia da transferência de dados pessoais dos participantes para um país fora da União Europeia através do consentimento livre, específico, informado, expresso, escrito, datado e assinado para essa transferência: nº 1 do artigo 20º, nº 2 do artigo 7º, alínea h) do artigo 3º da LPD[30], nº 3 do artigo 4º da Lei 12/2005[29], alínea o) do artigo 2º da Lei 46/2004[33].

Existem no entanto 2 tipos de fluxos transfronteiriços: dentro da UE e fora da UE.

Sendo livre dentro da UE a circulação de dados pessoais (sem prejuízo do disposto nos atos comunitários de natureza fiscal e aduaneira), já para fora da UE o mesmo não se verifica. A adequação do nível de proteção de um Estado que não pertença à UE deve ser avaliado caso a caso. A transferência de dados pessoais para um país que não pertença à UE apenas se pode realizar se esse

assegurar ter um nível adequado de proteção de dados. Esta proteção é avaliada em função da:

- Natureza dos dados;
- Finalidade do tratamento;
- Duração do tratamento;
- País de origem;
- País de destino;
- Leis de proteção de dados no país de destino.

As Diretiva da Comissão Europeia[31] sobre a proteção de dados que entrou em vigor em Outubro de 1995 proíbe a transferência de dados pessoais para países fora da União Europeia que não cumpram o padrão de proteção de dados da União Europeia (UE). Enquanto os Estados Unidos e a UE partilham o objetivo de melhorar a proteção da privacidade dos seus cidadãos os EUA tem uma abordagem diferente à privacidade daquelas tomadas pela UE.

A fim de colmatar estas abordagens diferentes de privacidade e fornecer um meio simplificado para organizações dos EUA darem cumprimento à diretiva o Departamento de Comércio dos EUA juntamente com a Comissão Europeia desenvolveu um ponto de trabalho -"porto seguro" – Safe Harbour.

Dadas as diferenças entre os países, muitas organizações têm vindo a expressar indecisão sobre o impacto que a legislação Europeia poderá ter nos seus procedimentos no que respeita à adequabilidade da transferência de dados pessoais para fora da EU.

De forma a diminuir esta incerteza e fornecer uma base de trabalho mais esperada, o Departamento do Comércio desenvolveu um documento contendo os princípios sob a autoridade estatutária para promover e desenvolver o comércio entre os EUA e a UE. A estes princípios as empresas têm que obedecer para

poderem estar dentro da lista do Safeharbour. Ao reunir estes 7 princípios as empresas dos EUA podem receber dados pessoais provenientes de empresas da UE. Os sete princípios são os seguintes:

- **Informação**

Uma organização deve informar os cidadãos sobre os fins para os quais recolhe e usa informações sobre eles, como entrar em contacto com a organização relativamente a qualquer questão ou queixa, os tipos de empresas terceiras a quem divulga a informação, e as escolhas e meios que a organização oferece aos cidadãos para limitarem a utilização e divulgação dos seus dados pessoais. Esta informação deve ser dada em linguagem clara sempre que os titulares dos dados sejam convidados a fornecer informações pessoais ao responsável pelo tratamento dos dados. Sempre que a finalidade do tratamento dos dados ou o fluxo da informação (ex. com a inclusão de uma entidade terceira para processamento dos dados) seja alterada, o responsável pelo tratamento dos dados deverá informar novamente os titulares dos dados e obter o seu consentimento.

- **Escolha**

O responsável pelo tratamento dos dados deve oferecer aos titulares dos dados a oportunidade de escolherem (opt out – oportunidade de exclusão) a) serem expostos a uma entidade terceira ou b) seus dados serem utilizados para um fim diferente do originalmente acordado. Os titulares dos dados devem ter acesso rápido, fácil e sem custos excessivos para puderem exercer o seu direito de escolha.

No caso de dados pessoais sensíveis deve ser dado um consentimento explícito (opt in – oportunidade de inclusão) por parte do titular dos dados no

caso de a informação vir a ser partilhada com uma entidade terceira ou utilizada para outro fim além do que estava inicialmente proposto.

- **Transferência de dados**

Para poder transferir dados para outra empresa o responsável pelo tratamento dos dados deve aplicar os dois princípios anteriores. A entidade terceira deverá: a) cumprir também com estes sete princípios; b) ter um contrato assinado com o responsável pelo tratamento dos dados de forma a garantir que cumpre com estes sete princípios ou c) cumprir com a diretiva. Se o responsável pelo tratamento dos dados cumprir com estes requisitos, mesmo que a entidade terceira não cumpra, não pode ser considerado responsável se a entidade terceira não proceder da maneira acordada, a não ser que o responsável pelo tratamento de dados tiver ocorrente dessa divergência e não tenha tomado as providências cautelares necessárias.

- **Segurança**

Todas as entidades que criem, mantenham, utilizem ou disseminem dados pessoais devem tomar as precauções necessárias de forma a os proteger de quaisquer perdas, utilização errada, acesso não autorizado, revelação, alteração ou destruição.

- **Integridade dos dados**

Deve ser consistente com os sete princípios. Os dados pessoais recolhidos devem ser relevantes para os fins a que se destinam. Uma organização não pode tratar informações pessoais de uma forma que seja incompatível com os fins para os quais tenham sido recolhidos ou posteriormente autorizados pelo indivíduo. Na medida necessária para esses fins, um responsável pelo tratamento deve tomar medidas razoáveis para garantir que os dados são fiáveis para a utilização pretendida, precisos, completos e atuais.

- **Acesso**

Os indivíduos devem ter acesso às informações pessoais sobre eles que um responsável pelo tratamento detém e ser capaz de corrigir, alterar ou excluir essas informações, quando incorretas, salvo se os encargos ou despesas de fornecimento de acesso forem desproporcionados em relação aos riscos para a privacidade do indivíduo, ou se os direitos de outras pessoas para além do titular dos dados sejam violados.

- **Execução**

A proteção eficaz da privacidade deve incluir mecanismos que garantam a conformidade com estes Princípios, o recurso para os indivíduos a quem se referem os dados afetados por não-conformidade com os Princípios e as consequências para a organização quando os princípios não são seguidos. No mínimo, tais mecanismos devem incluir (a) estar prontamente disponíveis e acessíveis mecanismos de recurso independentes pelo qual as queixas de cada indivíduo e as disputas são investigadas e resolvidas com referência aos Princípios e indemnizações caso a lei aplicável ou as iniciativas privadas o prevejam; (b) procedimentos de acompanhamento para verificar se as afirmações que as empresas fazem sobre suas práticas de privacidade são verdadeiras e que estas foram implementadas, tal como apresentado, e (c) a obrigação de resolver os problemas decorrentes de não cumprimento com os Princípios por organizações anunciando a sua adesão a elas e as consequências para essas organizações. As sanções devem ser suficientemente rigorosas para garantir o cumprimento pelas organizações.

5.1.7 O tempo de conservação dos dados

De acordo com a legislação nacional e internacional, os dados pessoais devem ser mantidos apenas pelo período de tempo estritamente necessário. Este princípio revela a importância da preservação dos direitos dos participantes, no

entanto, também se encontra prevista a necessidade de preservar a informação recolhida por largos períodos, devido a motivos históricos, estatísticos ou científicos. Devido à natureza dos dados recolhidos nestes estudos, estes são tornados anónimos no ato da recolha pelo investigador. O envio dos dados para processamento ocorre obrigatoriamente após esta operação, garantindo-se assim que a identidade do participante se encontra protegida e que os dados enviados mantêm um elevado valor científico. Por estes motivos, uma vez que a sua destruição é planeada após a perda do valor científico dos mesmos, é virtualmente impossível definir a data de destruição a priori. Assim sendo nos ensaios clínicos por vezes os dados são mantidos durante um longo período de tempo (podendo até chegar ao tempo de vida do medicamento em si no mercado). Quando devidamente justificado, a CNPD aceita que não seja definida uma data para a conservação dos dados. Esta justificação prende-se na sua generalidade com a contínua avaliação risco/benefício do fármaco ao longo de toda a sua vida (subentende-se por vida o tempo que medeia o inicio dos ensaios clínicos e a manutenção em comercialização do mesmo).

5.2 Ensaios Clínicos Observacionais

5.2.1 Introdução

Além da LPD, a CNPD emitiu também uma deliberação nº 227/2007[27] aplicável aos tratamentos de dados pessoais efetuados no âmbito de estudos de investigação científica na área da saúde, doravante designados por estudos observacionais ou não intervencionais.

De acordo com o Decreto-Lei nº 46/2004[33] de 19 de Agosto, os ensaios clínicos observacionais também designados de não intervencionais têm a seguinte definição:

"O estudo no âmbito do qual os medicamentos são prescritos de acordo com as condições previstas na autorização de introdução no mercado desde que a

inclusão do participante numa determinada estratégia terapêutica não seja previamente fixada por um protocolo de ensaio, mas dependa da prática corrente; a decisão de prescrever o medicamento esteja claramente dissociada da decisão de incluir ou não o participante no estudo; não seja aplicado aos participantes qualquer outro procedimento complementar de diagnóstico ou de avaliação, e sejam utilizados métodos epidemiológicos para analisar os dados recolhidos."

Assim estes estudos podem ter várias finalidades, serem apenas observacionais ou epidemiológicos, retrospetivos e/ou prospetivos.

Independentemente do tipo de Ensaios Clínicos de que estejamos a tratar, estes seguem sempre regras explicitas integradas na LPD[30] e carecem sempre de uma avaliação por parte da CNPD. Grande parte dos requisitos são transversais aos Ensaios Clínicos intervencionais e aos Observacionais. Seguidamente salientarei as diferenças.

5.2.2 O papel da proteção de dados

Tal como acontece para os estudos intervencionais o objetivo da avaliação por parte da entidade reguladora é garantir a proteção dos dados dos participantes neste tipo de ensaio especialmente no que respeita à qualidade dos dados e à admissibilidade do tratamento. É aferida pela CNPD a necessidade e não excessividade dos dados recolhidos de acordo com a finalidade do estudo.

A recolha dos dados deve garantir que estes são pertinentes, adequados e não excessivos no que respeita à finalidade do tratamento dos mesmos. No que diz respeito à admissibilidade do tratamento, este deve ser levado a cabo de forma lícita, com princípios de boa fé garantindo que os dados apenas são utilizados para o fim a que inicialmente se destinaram. A manutenção destes dados deve apenas ser feita durante o tempo necessário para permitir o cumprimento da sua finalidade.

No entanto, contrariamente ao que acontece nos ensaios clínicos intervencionais, neste tipo de ensaios poderá haver legitimidade para o tratamento de dados pessoais, com a finalidade de investigação na saúde, sem que para isso tenha que existir um consentimento esclarecido ou informado do titular dos dados. Nestes casos tem que ficar provado o interesse público legítimo. Esta recolha de dados deve ser ponderada em detalhe e o interesse do tratamento dos dados devidamente avaliada.

A importância do interesse público deve ser declarada pela entidade que avalia as instituições públicas ou privadas que estão autorizadas a realizar investigação clínica, bem como pelo Ministério responsável pela tutela das áreas da Ciência e da Tecnologia (Lei 125/99 de 20 de Abril[46]) no caso de Ensaios Clínicos abrangidos por um programa de financiamento público a longo prazo. No caso de instituições particulares não integradas nos programas de financiamento público deve, na mesma, ser demonstrado inequivocamente o interesse público. As entidades pertencentes ao Serviço Nacional de Saúde podem também ser consideradas responsáveis pelo tratamento de dados sendo neste caso o Comité de Ética Hospitalar ou o Comité de Ética para a Investigação os avaliadores do legítimo interesse público.

Contudo o mesmo já não pode acontecer no âmbito de teses académicas. Nestes casos, e tratando-se de uma pessoa individual como sendo responsável pelo tratamento dos dados, é necessária a recolha do consentimento informado dos titulares dos dados.

Nos demais casos a legitimidade do tratamento terá de decorrer do consentimento livre, específico, informado (alínea h do artigo 3º da LPD)[30] expresso do titular (nº 2 do artigo 7º da LPD[30]) e escrito (nº 3 do artigo 4º da Lei 12/2005[29]). Chamo então a atenção para o seguinte texto retirado da deliberação nº 227/2007[27] e que define o significado deste tipo de consentimento:

"O consentimento livre significa que o titular não conhece nenhuma condicionante ou dependência no momento da sua declaração que afete a formação da sua vontade e, ainda, que pode revogar, sem penalizações e com efeitos retroativos, o consentimento que haja prestado.

O consentimento específico significa que o consentimento se refere a uma contextualização factual concreta, a uma atualidade cronológica precisa e balizada e a uma operação determinada. O consentimento específico afasta os casos de consentimento preventivo e generalizado, prestado de modo a cobrir uma pluralidade de operações.

O consentimento informado significa que ao titular foi dado conhecimento, não apenas dos elementos do artigo 10º da LPD, mas ainda de todas as informações relevantes para a compreensão de todos os elementos ligados ao tratamento. O dever de informação por parte do responsável inclui o dever de esclarecer e a obrigação de se certificar que o titular conheceu e apreendeu todos os elementos do conteúdo do direito de informação. A existência ou possibilidade de ocorrência de riscos para o titular, quer para a sua saúde, quer para a sua privacidade, deve ser comunicada.

O consentimento expresso significa que a sua prestação tem de visar diretamente o tratamento de dados pessoais de saúde, não podendo ser inferido ou extraído implicitamente de outras declarações ou comportamentos.

O consentimento escrito significa que deve constar de texto lavrado ou subscrito pelo próprio titular."

Em estudos retrospetivos, quando existe uma necessidade de aceder a dados pessoais existentes nas instituições de saúde deverá o investigador contactar com a mesma (na pessoa do médico assistente ou outro) para que este último possa recolher o consentimento esclarecido do titular dos dados. No entanto, ao abrigo

da Lei 12/2005[29] no nº6 do artigo 19º, quando se trata da utilização de material biológico e amostras de ADN para as quais não tenha sido recolhido o consentimento esclarecido do titular dos dados nem possa ser obtido o mesmo (pela quantidade de dados ou pela morte do titular) é permitido que o material e os dados possam ser processados, mas apenas para fins de investigação científica ou obtenção de dados epidemiológicos ou estatísticos.

5.2.3 O Responsável pelo tratamento dos dados e medidas de segurança

Tal como nos Ensaios Clínicos Intervencionais, nos Ensaios Clínicos Observacionais e de acordo com a Lei 125/99 de 20 de Abril[46], podemos ter como responsáveis pelo tratamento dos dados um Laboratório do Estado ou de outra Instituição Publica ou de Instituições Privadas de investigação.

Sempre que o Responsável pelo tratamento dos dados recorrer a uma entidade terceira, esta prestação deve ser regida por um contrato/ato jurídico que vincule a entidade subcontratante ao responsável pelo tratamento. O subcontratante desenvolve a sua ação mediante instruções do responsável e isso deve ficar claramente escrito no contrato/ato jurídico de forma a proteger os dados pessoais recolhidos contra possíveis destruições acidentais, perda, alteração, difusão ou acessos não autorizados e proteção do tratamento dos dados.

Tal como para os Ensaios Clínicos Intervencionais, o acesso aos dados recolhidos deve ser diferenciado por níveis com palavras passe que permitam acessos e perfis de utilizador diferenciados, sendo que os dados pessoais e os dados de saúde devem estar separados.

Especial precaução deve ser tida para a investigação sobre o genoma humano, que carece de confidencialidade reforçada sobre a identidade e as características das pessoas estudadas individualmente. Este tipo de investigação carece de consentimento informado bem como de aprovação por parte dos comités de ética

das instituições hospitalares, universitárias ou de investigação bem como da CNPD.

Quer os dados pessoais sejam recolhidos informaticamente ou em papel, cabe ao responsável pelo tratamento dos mesmos garantir a segurança dos dados.

5.2.4 Tipos de dados que podem ser tratados e sua recolha

Tal como acontece nos ensaios clínicos intervencionais, os dados pessoais tratados devem ser adequados, pertinentes e não excessivos no que respeita à sua finalidade. Os seguintes tipos de dados foram identificados como podendo ser necessários para a realização de tais estudos:

- Dados de identificação;
- Dados de saúde incluindo história clínica, medicação e resultados dos meios complementares de diagnóstico;
- Informação de saúde e genética no que respeita à história familiar;
- Hábitos pessoais;
- Dados que concernem a vida profissional;
- Dados relativos aos parâmetros clínicos em estudo.

Estes dados podem ser diretamente obtidos pela aplicação de questionários aos titulares dos dados (pela via do investigador/outros profissionais de saúde que colaborem no estudo) ou pelo médico assistente sendo que nestes casos normalmente não existe a necessidade de identificação dos dados (os dados devem ser disponibilizados de forma anónima).

No caso de não se poder conduzir o estudo recorrendo à utilização de dados pessoais anonimizados, estes devem ser codificados e a sua descodificação ter acesso limitado. Nestes casos deve ser sempre devidamente justificada a necessidade, bem como nos casos em que a anonimização é de todo impossível,

e esta necessidade, terá de ser avaliada e aprovada pela CNPD antes do início da recolha dos mesmos dados.

Por tudo isto e ao abrigo da LPD[30] no nº 2 do artigo 7º é permitido o tratamento dos dados pessoais sensíveis nas seguintes situações:

- Consentimento esclarecido do titular e/ou interesse publico devidamente comprovado
- Autorização da CNPD

Em qualquer dos casos deve ser garantida a anonimização dos dados.

6. O que nos reserva o futuro

Crime cibernético, perda de dados, redes sociais, utilização da Internet por crianças, são algumas das realidades recentes às quais as normas sobre proteção de dados têm de se adaptar. Os progressos técnicos constantes e as novas aplicações criadas com esses progressos. A Web 2.0, as redes sociais, os serviços de localização geográfica e os telefones inteligentes não existiam quando a atual legislação de proteção de dados foi aprovada. Ou seja, para dar resposta aos desenvolvimentos técnicos e garantir a proteção de dados dos cidadãos europeus no futuro, é necessário rever a legislação em vigor. A diretiva de 1995 é uma boa base mas tem sido implementada pelos Estados-Membros de formas muito díspares; o que faz com que as empresas tenham de se adaptar a uma pletora de diferentes leis da privacidade. É necessária uma lei unificada em toda a União Europeia. A importância da sua aplicação, independentemente do local onde o processamento de dados dos cidadãos europeus seja realizado. Esta questão é importante se pensarmos na quantidade de serviços em linha disponíveis a partir de países asiáticos ou dos EUA.

Cada vez são cometidos mais crimes através da Internet e a experiência diz-nos que é muito difícil levar os autores dos crimes a tribunal. Os cidadãos europeus têm responsabilidade sobre os seus próprios dados. É preciso consciencializar as pessoas para aquilo que fazem quando utilizam a Internet e para os perigos existentes, para que não divulguem facilmente os seus dados pessoais. A melhor proteção é sempre a que é feita pelos próprios e as pessoas tendem, a deixar os seus traços digitais sem cuidado. A culpa não é só dos consumidores e existe uma proposta para que a revisão da legislação contemple a introdução de um princípio de responsabilidade para os controladores de dados, ou seja, as empresas. Além disso, deverá também ser implementada as "notificações das violações de dados", tal como já sucede em relação ao sector das telecomunicações. Se, por exemplo, as informações constantes dos cartões de crédito de alguns milhões de pessoas estiverem a ser desviadas dos servidores da empresa, os responsáveis deverão informar imediatamente os cidadãos afetados por esse desvio, para que os mesmos possam ser ressarcidos das perdas e tomar as medidas necessárias para proteger a sua privacidade. Recentes escândalos relacionados com dados pessoais demonstraram que não é isso que acontece.

Durante a passada Conferencia sobre a Proteção de Dados na Europa em Bruxelas (5 de Abril 2011), foram dados os primeiros passos no que respeita à uniformização da Proteção de Dados pela Europa. Existem no entanto desafios que têm que ser abordados no âmbito da revisão da atual legislação:

- Consequências da globalização e dos fluxos transfronteiriços dos dados pessoais
- Os avanços da tecnologia
- A importância da proteção efetiva

No âmbito dos ensaios clínicos existem cumulativamente outros desafios. O facto de o promotor do estudo ser considerado o controlador dos dados representa um viés. Não é o promotor que tem acesso aos dados pessoais dos participantes mas

sim o Investigador, que coordena os estudos. O Investigador é responsável por selecionar os participantes para os ensaios clínicos, recolher e processar os dados pessoais. Sendo o promotor o principal responsável por garantir a proteção dos dados, isto torna-se difícil quando na realidade não é ele o controlador dos mesmos. Adicionalmente, parte do trabalho de reunião e tratamento dos dados é feita por empresas subcontratadas. Desta forma, a aplicação direta da Diretiva e da LPD deverá ser objeto de revisão tendo em consideração este tipo de constrangimentos.

Do ponto de vista do participante, o acesso aos seus dados bem como os direitos associados de retificação e eliminação, irão também ser alvo de revisão uma vez que é difícil garantir que estes sejam levados a cabo de forma transparente. Os dados recolhidos no âmbito dos ensaios clínicos, são para sempre guardados e utilizados, por isso se um participante desejar retirar o seu consentimento este apenas é possível a partir da altura da tomada de decisão sendo que toda a reunião da informação para traz não é eliminada.

Assim, provavelmente fará sentido que os ensaios clínicos obedeçam a uma legislação de proteção de dados própria e não estarem inseridos na atual contextualização legislativa que como já se viu tem algumas restrições e lacunas de aplicação neste contexto.

7. Bibliografia

1. *Agre, Philip E. – Rotenberg, Marc (eds.) 1997.* Technology and Privacy: The New Landscape. Cambridge, Massachusetts, The MIT Press.
2. *Bennett, Colin J. 1992.* Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaca, Cornell University Press.
3. *Bennett, Colin J. 1997.* Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? *Bennett, Colin J. 1997* In Agre – Rotenberg (eds.).
4. *Bergkamp, Lucas 2002.* The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-driven Economy. Computer Law and Security Report, vol. 18 no. 1
5. *Burkert, Herbert 1997.* Privacy-Enhancing Technologies: Typology, Critique, Vision. In Agre–Rotenberg
6. *Cranor, Lorrie Faith.* Proceedings of the Twelfth Conference on Computers, Freedom and Privacy, April 16–19. 2002, San Francisco
7. *Dumortier, Jos – Goemans Caroline 2000.* Data Privacy and Standardization.
8. Discussion Paper prepared for the CEN/ISSS Open Seminar on Data Protection. http://www.law.kuleuven.ac.be/icri/papers/doctrine/cen-paper.pdf
9. *Gelman, Robert G. 1998.* Protecting yourself online. New York, HarperEdge .
10. *Guadamuz, Andrés 2000.* Habeas Data vs the European Data Protection Directive. Journal of Information, Law and Technology, Vol. 2.
11. *Jay, Rosemary – Hamilton, Angus 1999.* Data Protection Law and Practice. London, Sweet and Maxwell.
12. *Koops, Bert-Jaap 1999.* The Crypto Controversy: A Key Conflict in the Information Society. The Hague, Kluwer Law International.
13. *Korff, Douwe 2002.* EC Study on the Implementation of the Data Protection Directive (Comparative Summary of National Laws). Colchester, University of Essex Human Rights Centre.
14. *Lessig, Lawrence 1999.* Code and Other Laws of Cyberspace. *Lessig, Lawrence 1999.* New York, Basic Books
15. *Mayer-Schönberger, Viktor 1997.* Generational Development of Data Protecton in Europe. In Agre–Rotenberg.
16. *Posner, Richard M. 1984.* An Economic Theory of Privacy. In Schoeman 1984.
17. *Reidenberg, Joel R. – Schwartz, Paul M. 1998.* On-line Serives and Data Protection and Privacy.
18. Anexo ao Relatório Anual de 1998 do Grupo de Trabalho instituído pelo artigo 29 º da Directiva 95/46/CE. Bruxelas, Comissão Europeia, DG Mercado Interno e Serviços Financeiros.
19. *Schoeman, Ferdinand D. (ed.) 1984.* Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press.
20. *Schoeman, Ferdinand D. 1984a.* Privacy: Philosophical Dimensions of the Literature. In Schoeman.
21. *Schwartz, Paul M. 2002.* Privacy, Participation, Cyberspace: An American Perspective. In Baeriswyl–Rudin.
22. *Warren, Samuel D. – Brandeis Louis D. 1984.* The right to privacy [The implicit made explicit]. In Schoeman.
23. *Westin, Alan 1984. The Origins of Modern Claims to Privacy. In Schoeman.*
24. *DECISÃO DA COMISSÃO de 5 de Fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho*

25. *DECISÃO DA COMISSÃO de 27 de Dezembro de 2001 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros, nos termos da Diretiva 95/46/CE*
26. DECISÃO DA COMISSÃO de 27 de Dezembro de 2004 que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros
27. DELIBERAÇÃO Nº 227 /2007 Aplicável aos tratamentos de dados pessoais efetuados no âmbito de estudos de investigação científica na área da saúde
28. DELIBERAÇÃO Nº 333 / 2007 Sobre a proteção de dados pessoais nos ensaios clínicos com medicamentos de uso humano
29. Lei n.o 12/2005 de 26 de Janeiro Informação genética pessoal e informação de saúde
30. Lei n.o 67/98 de 26 de Outubro Lei da Proteção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Diretiva n.o 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados).
31. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Jornal oficial no. L 281 de 23/11/1995 P. 0031 – 0050
32. Convenção 108 do Conselho da Europa de 28 de Janeiro de 1981
33. Decreto-Lei nº 46/2004 de 19 de Agosto, Aprova o regime jurídico aplicável à realização de ensaios clínicos com medicamentos de uso humano
34. Lei 10/91 de 29 de Abril, Lei da Proteção de Dados Pessoais face à Informática
35. Lei 28/94 de 29 de Agosto, Aprova medidas de reforço da proteção de dados pessoais
36. Diretrizes da OCDE para a proteção da privacidade e fluxos transfronteiriços de dados pessoais
37. DIRECTIVA 2002/58/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 12 de Julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações
38. DIRECTIVA 2006/24/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 15 de Março de 2006 relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE
39. DIRECTIVA 2009/136/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 25 de Novembro de 2009 que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) nº 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor
40. Lei nº 69/98 de 28 de Outubro REGULA O TRATAMENTO DOS DADOS PESSOAIS E A PROTECÇÃO DA PRIVACIDADE NO SECTOR DAS TELECOMUNICAÇÕES (TRANSPÕE A DIRECTIVA 97/66/CE, DO PARLAMENTO EUROPEU E DO CONSELHO, DE 15 DE DEZEMBRO DE 1997)
41. DIRECTIVA 97/66/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações

42. Lei 41/2004 de 18 de Agosto, Transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.
43. Lei n.º 2/94, de 19 de Fevereiro. Estabelece os mecanismos de controlo e fiscalização do Sistema de Informação Schengen
44. Lei nº 68/98 de 26 de Outubro. Determina a entidade que exerce as funções de instância nacional de controlo e a forma de nomeação dos representantes do Estado Português na instância comum de controlo, previstas na Convenção, fundamentada no artigo K.3 do Tratado da união Europeia, que cria um serviço europeu de polícia (EUROPOL).
45. DIRECTIVA 2001/20/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 4 de Abril de 2001 relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados - Membros respeitantes à aplicação de boas práticas clínicas na condução dos ensaios clínicos de medicamentos para uso humano
46. Decreto-Lei n.º 125/99 de 20 de Abril