

A importância da segurança e privacidade da informação. Análise do estudo elaborado pelo Estado para a implementação do registo de saúde electrónico

P V Gomes¹, M Jacquinet² & H Curado³

¹Biomatemática, Bioestatística e Bioinformática, Escola Superior de Tecnologia da Saúde do Porto, IPP, V. N. Gaia, Portugal

²CEMRI, Universidade Aberta, Lisboa, Portugal

³Gestão e Administração em Saúde, Escola Superior de Tecnologia da Saúde do Porto, IPP, V. N. Gaia, Portugal

¹pvg@estsp.ipp.pt, ²mjacquinet@classic.univ-ab.pt, ³hct@estsp.ipp.pt

RESUMO

A análise que tem vindo a ser efectuada, paralelamente a experiências diversas de implementação de registos de dados pessoais de utentes das unidades de saúde, em particular no que concerne à protecção da privacidade, enquanto valor intrínseco à pessoa humana, encontra novos contornos face ao recente trabalho realizado no âmbito da Administração Central dos Sistemas de Saúde para a implementação do “Registo de Saúde Electrónico”.

Este trabalho pretende analisar a bipolarização de interesses em questão. Por um lado o interesse público de adopção de um sistema de informação único, por outro lado a necessária protecção à privacidade do ser humano.

Palavras-Chave: Registo de Saúde Electrónico, Privacidade, Sistemas de Informação em Saúde.

ABSTRACT

The analysis that for years has been made, simultaneously with some implementation experiences of personal data records for the health facilities users, particularly as regards of the privacy protection, while intrinsic human value, find new contours in the recent presented work made by the Central Government Health Systems, for the implementations of the electronic health personal data.

In this paper we intend to analyze the unquestioned polarization of interests concerned. On the one hand the public interest in adoption of a single information system, on the other hand the necessary protection of the legal human privacy.

Key-Words: Electronic Health Record, Privacy, Health Information Systems.

1. INTRODUÇÃO

Há alguns anos têm vindo a ser efectuadas diversas experiências para a implementação de registos de dados pessoais de utentes das unidades de saúde^{1,2}. Sobre estas iniciativas incidem algumas análises críticas no que concerne à protecção da privacidade, enquanto valor intrínseco à pessoa humana.

¹ São diversas as experiências e estudos que vão sendo realizados. Quanto àquelas o documento referido no texto (R1) dá-nos uma elucidação clara sobre o estado da arte. Ao nível académico, desde há anos que a temática tem vindo a ser inserida nos currícula de diversas instituições, destacando-se, por colaboração dos autores o Mestrado em Informática

O registo de dados pessoais de utentes das unidades de saúde encontra novos contornos face ao trabalho recentemente apresentado como “*Documento de Estado da Arte*” e, bem assim, as “*Orientações para Especificação Funcional e Técnica do Sistema de RSE*”³, no âmbito da Administração Central dos Sistemas de Saúde (ACSS). Estes documentos, designados “RSE - Registo de Saúde Electrónico”, respectivamente R1 e R2A, constituem a base do trabalho que o Estado se propõe desenvolver para implementar um registo de dados pessoais no âmbito das instituições prestadoras de cuidados de saúde.

Com o presente texto pretende-se analisar o referido trabalho considerando os diversos aspectos inerentes à problemática, tendo em conta a inquestionável bipolarização de interesses em questão.

A existência de um sistema de informação único apresenta vantagens claras para o sistema de saúde, não obstante os rigorosos critérios que devem ser considerados no seu desenvolvimento e implementação (muito embora não uniformemente aceites). No entanto, a protecção necessária da privacidade do ser humano como bem jurídico. Esta, como imanência da pessoa humana, não pode ser objecto de devassa nem, por falta de protecção, suscitar tratamentos discriminatórios ou vexatórios.

Importa perceber que é o Estado, e não a pluralidade quase incomensurável de entidades prestadoras de cuidados de saúde, que deve assumir o papel de uniformização do sistema. Essa é também uma função do Estado Regulador. Emerge aqui a questão da operacionalidade. À mesma procurou responder o grupo de trabalho criado pelo Despacho n.º 10864/2009, de 28 de Abril do Secretário de Estado da Saúde, mediante o “Documento de Estado da Arte”, enquanto reflexão sobre a temática e os trabalhos que têm vindo a ser realizados. Questiona-se, porém, se em sede de “Orientações para Especificação Funcional e Técnica do Sistema de RSE” a abordagem é suficientemente abrangente. Permite-se, assim, fazer alguma reintegração das ideias ali apresentadas, em sede de observações dubitativas.

Depois da introdução ao tema, o segundo capítulo contextualiza a regulação do sector de saúde em Portugal. É feita uma análise sobre a regulação deste sector tendo em conta vários aspectos, a sua evolução, factores económicos e sociais e os actores e intervenientes.

No terceiro capítulo serão abordadas questões relacionadas com a privacidade e protecção de dados no que diz respeito ao registo de saúde electrónico. Será analisada a conflitualidade entre o interesse público e o interesse privado, bem como apontados outros factores importantes a ter em conta.

O quarto capítulo faz uma análise sobre a estrutura e segurança da informação do modelo de informação proposto. São ainda abordadas algumas questões sobre os casos particulares bem como sobre a necessidade de envolvimento de todos os intervenientes no sistema e não apenas os sugeridos pelo documento em análise.

O presente trabalho termina com as principais conclusões, apontando alguns aspectos essenciais a considerar nos processos de desenvolvimento e implementação do registo de saúde electrónico.

2. REGULAÇÃO DO SECTOR DA SAÚDE

O *managerialismo* tem vindo a assumir-se nos estados da Europa e do mundo uma particular preponderância, como forma de assunção das funções do estado. Em Portugal procura-se seguir uma tendência de décadas noutros países, em particular na designada empresarialização das clássicas funções do Estado, de que o sector da saúde tem conhecidos recentes exemplos, como o sejam a reforma do sistema de “gestão hospitalar”, instituído pela Lei n.º 27/2002, de 8 de Novembro, a qual procedeu também a alterações à Lei de Bases da Saúde (Simões, 2004).

Neste contexto de reforma do sector da saúde são recorrentes os conceitos de “utilidade” e “escolha racional”, de “contratos programa”, a reflectir que o “mercado” foi eleito como modelo ideal para prossecução do interesse público, a que se associam as ideias de “concorrência” e “empresa”, procurando-se sustentar a necessidade de reforma na ineficácia dos sistemas existentes, como refere Campos (Campos, 2000, pp. 47-76), na caracterização, da grande maioria dos hospitais públicos portugueses, designado o sistema existente “como pesadamente ineficiente, com baixa produtividade, reduzida responsabilidade social (...)”. Esta espécie de “capitalismo dos serviços”, encontra-se hoje bem ilustrado no *outsourcing* que trespassa o funcionamento dos serviços na prestação de cuidados de saúde, com alguma proletarianização das profissões.

Médica da Faculdade de Medicina da Universidade do Porto e diversos cursos da Escola Superior de Tecnologias da Saúde do Porto.

² Entre outros, Curado e Lapão, 1995.

³ Documentos disponíveis no sítio da Internet da Administração Central do Sistema de Saúde em <http://www.acss.min-saude.pt/>.

Ora, é neste contexto, de evolução não prestadora de serviços, mas de empresarialização, que surge, proposto pelo Estado, um modelo de Registo de Saúde Electrónico, em que se assume a particular função do Estado hetero-regulador. Percebe-se o porquê desta necessidade de intervenção, nesse mesmo contexto de análise do sector da saúde. Com efeito, não se está num clássico domínio de “mercado”, onde as leis da oferta e procura se aplicam. No “mercado da saúde” existem inúmeras falhas de mercado tornando a intervenção do Estado no sector particularmente necessária. Importaria perceber, que não nesta análise, se a salvaguarda do bem público saúde se contenta com esta hetero-regulação, enquanto pura norma pública que define as normas de conduta dos agentes interventores do mercado (Sanches, 2000).

Todavia, o sector da saúde tem características muito particulares. Com efeito, a saúde constitui um bem público. Os cuidados de saúde não são equiparáveis, em termos de necessidade àquelas que emergem de outros serviços públicos que, por serem de apropriação individual, o Estado possa deixar a cada cidadão a sua procura, ainda que incentivando a sua apropriação. Não é equiparável a percepção de cuidados de saúde ao benefício concedido pelo Estado na prestação de serviços de cultura mediante museus, escolas de ensino não obrigatório e outros. A saúde constitui um bem público, cuja existência, em termos de bem-estar social é superior à soma do bem-estar de todos os indivíduos. Tal percepção é clara se pensarmos nos efeitos dum surto pandémico em termos de produtividade nacional. Os custos sociais de inactividade seriam incalculáveis.

3. PRIVACIDADE E PROTECÇÃO DE DADOS

Existem, actualmente, distintos modelos de registo de dados dos utentes das unidades de saúde, quer a nível do sector público, como do privado. São conhecidas as dificuldades inerentes à sua compatibilização, bem como as desvantagens da utilização dos referidos distintos modelos. A busca de um modelo uniformemente aplicado, que emerge da vontade política, impõe que se reflecta sobre os contornos dos interesses em confronto. Com efeito, tratando-se dum modelo assente nas tecnologias da informação e comunicação (TIC), pressupondo o tratamento⁴ de dados pessoais, veio trazer à colação a indispensabilidade de se efectuar uma reflexão sobre tais operações face à necessária protecção da privacidade (Curado & Lapão, 2005).

Os contornos, na área da saúde são particularmente relevantes, porquanto se trata de dados sensíveis dotados de protecção constitucional. A Constituição Portuguesa reconhece, por um lado, o direito dos cidadãos à identidade pessoal e à reserva da intimidade da vida privada, mas também consagra os direitos do cidadão face à utilização da informática¹. “As informações sensíveis são aquelas que se referem às questões intimamente ligadas ao núcleo da personalidade e dignidade humana” (Domínguez, 2005). Não pode deixar de se referir que merece o mesmo relevo e protecção jurídica o tratamento não informatizado dos dados pessoais, porquanto o que releva é a natureza dos dados independentemente do suporte. Todavia, o modelo proposto, em análise, tem subjacente o tratamento informatizado dos dados pessoais.

Em matéria de registo electrónico de dados dos utentes das unidades de saúde há a considerar, como dados pessoais, aqueles que relevam do domínio público, mas são informação pessoal, tais como o nome, morada, telefone, mas também dados biométricos (peso, altura, cor da pele, do cabelo, dos olhos) e toda a informação clínica de carácter genérico (grupo sanguíneo, alergias, diabetes, hipertensão) que possa ser condicionante da prescrição médica, assim como o historial clínico (resultados de análises, exames médicos, intervenções cirúrgicas). Dados pessoais são, em suma, de acordo com a Lei de Protecção de dados pessoais, bem como no âmbito normativo, da União Europeia, dados pessoais são, em suma, “qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular, identificada ou identificável”ⁱⁱ.

A existência de distintos sistemas de informação, de controlo público, detendo dados pessoais, torna o risco de violação da privacidade exponencial, em particular se não for acompanhado das adequadas medidas de segurança, porquanto possibilita uma vigilância quotidiana da vida de qualquer pessoa. Não obstante, a Lei de protecção de dados pessoais permite o seu tratamento sem o consentimento do seu titular, se for necessário para “*execução de uma missão de interesse público*” (cf. alí. d) do art. 6º). Para acrescentar, em

⁴ “Tratamento de dados pessoais” («tratamento»), face à alínea b) do art. 2º da Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, constitui “qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas 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”. Esta mesma redacção veio a ser acolhida pela alínea b) do art. 3º da Lei n.º 67/98, de 26 de Outubro.

matéria de dados sensíveis, onde relevam “*dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica*”, que muito embora sendo o seu tratamento proibido (cf. Art. 7º da Lei 67/98), se admitem exceções, ainda que carecendo de mediação da Comissão Nacional de Protecção de Dados, ou do legislador, “*quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, (...) com garantias de não discriminação*” devendo ser acompanhada de especiais medidas de segurança (em referência ao art. 15º).

Importa efectuar uma análise da compatibilização entre os interesses em confronto. Por um lado o iminente interesse público da recolha e tratamento de informação pessoal, por questões de interesse público. Por outro, a necessária tutela da personalidade, porquanto esta pressupõe o direito à privacidade, a qual só será garantida se o sistema for dotado de mecanismos de segurança da informação.

3.1 A Tutela da Privacidade

A privacidade é, em si mesma, uma imanência da personalidade humana e um corolário da sua autonomia, compreendendo o direito à reserva sobre a intimidade da vida privada e honra pessoais. Consequentemente, é “*o individuo que tem o direito de decidir que as suas informações pessoais sejam mantidas sob o seu exclusivo controlo, como tem o direito de comunicar a quem, quando, onde e em que condições as informações pessoais devem ser reveladas*” (Fortes & Spinetti, 2004).

Na esteira da Comissão Nacional de Protecção de Dados, o eventual conflito dos interesses públicos e privado pressupõe uma leitura jurídica da tutela constitucional da personalidade consentânea com os demais interesses, na sua harmonização, ou, na subordinação ao interesse público da protecção da privacidade, sempre que “*as restrições aos direitos fundamentais não constituam, relativamente ao fim prosseguido, uma intervenção desproporcionada e intolerável que atente contra a essência do próprio direito protegido*” (CNPD, 1)ⁱⁱⁱ. Para acrescentar que o interesse que reconheceu o direito à confidencialidade deve ceder “*perante outro interesse público mais forte*”.

Danilo Doneda, citando Stefano Rodotà refere que “*Havendo dano, seja a uma colectividade ou a indivíduos, o certo é que a protecção mais adequada para a privacidade não reside mais na garantia do isolamento e segredo, mas sim em uma perspectiva de amplo controlo da circulação de informações pessoais. Pode-se considerar, emblematicamente, uma transformação na definição do direito à privacidade, do “direito a ser deixado em paz” “para o direito a controlar o uso que outros fazem das informações que me digam respeito*” (Doneda, 2000).

O que está então em causa não é tanto o valor absoluto da privacidade, antes sim da garantia de segurança da privacidade. Como refere Gutiérrez (2004), “*a recolha e tratamento automatizado de dados garças às técnicas informáticas (bases de dados) e a transmissão de dados pessoais através da Internet (via correio electrónico, (...)) entre outros) pressupõe a inclusão de mecanismos de defesa para a protecção de dados*”. Deste modo se compatibiliza o valor da privacidade, enquanto valor iminentemente privado, com o tratamento de dados necessários à defesa dum outro valor, também constitucional, a segurança (e igualmente de interesse individual).

A garantia da privacidade está não no “*right to be let alone*” mas na segurança da informação respeitante à pessoa humana. Ora, esta segurança, sob o ponto de vista técnico-jurídico, é uma “*qualidade do ordenamento jurídico, que implica a certeza das suas normas e, consequentemente, a previsibilidade da sua aplicação*” (Iglesias, 2004).

Sob o ponto de vista técnico, a garantia de segurança da informação confidencial resultará de dois aspectos. O primeiro respeitante à definição de níveis de acesso à informação (quem pode aceder a que informação e em que condições), e, um segundo que resulta da implementação e manutenção de um sistema de registo dos acessos à informação (quem acedeu a que informação e quando). “*É, pois, de extrema importância que o tratamento de dados pessoais, neste contexto, seja rodeado dos mais elevados mecanismos de segurança, porquanto somente esta é susceptível de salvaguardar a privacidade e, consequentemente, suscitar a confiança no sistema como um todo*” (Curado & Lapão, 2005).

A não compreensão da pessoa enquanto ser social, que simultaneamente reclama privacidade, mas também segurança, privilegiando aquela em total detrimento desta, apenas contribuirá para uma visão individualista dos direitos de personalidade, contrária à própria natureza humana, que ao pressupor sociabilidade tem necessariamente que compreender cedências individuais. A não se entender assim, como refere Ascensão (Ascensão, 1995), “*o direito de personalidade transforma-se no direito de egoísmos privados. Contradiz o que deveria ser a sua base fundamental, que é a consideração da pessoa. A pessoa é convivência e sociedade. Nenhuma consideração de intimidade pode ser mais forte que esse traço essencial da personalidade*”.

Não obstante o próprio conceito de liberdade imponha que se assegure a tutela máxima da privacidade, o facto de se viver em sociedade reclama, numa compressão da liberdade individual, a recolha e partilha de dados pessoais, como garante dum valor que sendo colectivo, também é um valor individual, a saúde pública.

4. ESTRUTURA E SEGURANÇA DO SISTEMA DE INFORMAÇÃO

A segurança de um sistema de informação deve ser abordada através de uma perspectiva multidimensional que considere todas partes envolvidas. É importante referir que um sistema de informação é um sistema social de actividades humanas que pode ou não envolver computadores. O sistema de informação reúne, guarda, processa e distribui informação relevante para a organização (ou sociedade), de modo a que esta seja acessível e útil para quem a utiliza (Buckingham, Hirschheim, & Land, 1987).

A percepção de que sistema de informação é diferente de tecnologia de informação permite destacar o conceito de sistema de comunicação entre pessoas, o qual está envolvido na obtenção, processamento, distribuição e utilização de Informação para suportar sistemas de actividades humanas (Beynon-Davies, 2002).

Actualmente os sistemas de informação utilizam as tecnologias de informação como um dos seus componentes essenciais, no entanto, os sistemas de informação incluem diferentes elementos heterogéneos, humanos, tecnológicos (software, hardware), informação, procedimentos (normas, regras, processos) e relações (Avison & Fitzgerald, 1995).

Cada um dos elementos heterogéneos referidos é designado por Law (1992) e Underwood (1998) como um actuante. Um actuante pode ser considerado como uma rede simplificada de interacções e associações de elementos heterogéneos, que constituem eles próprios uma rede.

Pode então definir-se um sistema de informação como um conjunto de componentes inter-relacionados que recolhem, reúnem, processam, armazenam e distribuem informação para suportar a tomada de decisão, coordenação e controlo numa organização. Os sistemas de informação ajudam a analisar problemas, a visualizar situações complexas e criar novos produtos (Laudon & Laudon, 2002).

O Registo de Saúde Electrónico deve ser visto como parte integrante de um sistema de informação global de saúde. Deve interagir e ter uma interoperabilidade plena com os outros sistemas de informação para o cidadão.

Dada a complexidade que engloba a implementação do Registo de Saúde Electrónico, é necessário que esta se enquadre numa estratégia global de gestão de informação e de gestão de conhecimento.

A implementação do Registo de Saúde Electrónico irá gerar um volume de informação e de conhecimento considerável. Quanto maior é o volume de conhecimento, maior é o grau de especialização necessário para lidar com ele (Kock, 2005). Resultando numa espiral em que o processo de informação e conhecimento cresce gradualmente com a especialização originada pelo próprio conhecimento.

Definir uma estratégia de gestão de informação permite aproveitar os recursos e capacidades de informação para que possa existir uma aprendizagem e adaptação ao meio ambiente em permanente mudança (Choo, 1998). Este factor de adaptação é vital quando se fala em segurança. Para que essa adaptação seja efectiva é necessário aprender a lidar com os dados, a informação, o conhecimento e com a própria mudança.

A existência de uma estratégia de gestão do conhecimento permite capturar, armazenar, distribuir e aplicar o conhecimento (implícito, tácito e explícito) de maneira a alcançar de modo mais eficiente os objectivos propostos (Tochtermann & Maurer, 2000). Ao incorporar e explorar o potencial do conhecimento a implementação do Registo de Saúde Electrónico trará vantagens consideráveis, não só em termos organizacionais, mas também ao nível do enriquecimento científico e técnico dos profissionais de saúde.

O documento em análise, “RSE - Registo de Saúde Electrónico, R2A: Orientações para Especificação Funcional e Técnica do Sistema de RSE” (Ministério da Saúde. Administração Central de Sistema de Saúde, 2009) descreve, entre outros aspectos, o modelo de informação para o registo de saúde electrónico.

A estrutura do modelo de informação proposta apresenta três níveis de informação. Dois níveis integram o RSE, são designados por “Tronco Comum” e “Partilhado”. O Tronco Comum contém o conjunto de dados resumido que contém informação geral sobre a saúde do Cidadão e um índice para a informação do nível partilhado. O nível Partilhado inclui o conjunto de conteúdos partilhados com relevância para a prestação de cuidados de saúde de qualidade (Ministério da Saúde. Administração Central de Sistema de Saúde, 2009).

O terceiro nível designado por “Específico” engloba o conjunto de dados detidos por cada entidade, sendo cada uma responsável pela gestão dos seus sistemas operacionais. No entanto o documento em análise

apresenta um défice de orientações para este nível. É necessário clarificar quais as classes de dados pertencentes a este nível de modo a evitar a redundância com os outros níveis.

Nos níveis Tronco Comum e Partilhado é necessário especificar de forma mais clara e completa alguns aspectos relacionados com a segurança da informação, nomeadamente no que diz respeito à confidencialidade e privacidade.

É necessária uma definição clara de níveis de acesso à informação, bem como meios de monitorização e controlo. O sistema deve registar quem acede a quê, quando e porquê. Nem todos os profissionais, independentemente da sua categoria, devem aceder a toda a informação. Nem todos os episódios de atendimento justificam o acesso a toda a informação por parte do profissional de saúde.

Na implementação de um sistema deste tipo um dos aspectos importantes a considerar é a forma como o sistema vai reagir perante casos particulares que eventualmente possam surgir. O documento R2A no ponto 4.7 e) prevê acessos em caso de emergência (página 38). Se numa primeira fase a prioridade de uma unidade de saúde, perante um doente não identificado, será salvar a sua vida, estabilizar, tratar, etc. é importante que com a maior brevidade possível toda essa informação seja integrada no sistema. O documento R2A não especifica como o sistema deverá reagir perante situações em que não seja possível identificar o doente (situações de emergência, doente inconsciente, amnésia, etc.).

Se por um lado a constituição do grupo de trabalho foi abrangente e multidisciplinar, por outro lado o documento revela alguma inconsistência quando no ponto 4.3 “Articulação com as Ordens Profissionais” apenas se refere ao envolvimento das Ordens Profissionais no processo. Nem todas as profissões envolvidas têm Ordem Profissional e não devem por isso deixar de ter um papel activo em todo o processo. É fundamental integrar, envolver, ouvir e considerar todos os intervenientes. Importante lembrar que os utentes também são intervenientes.

Embora o documento R2A refira no ponto 1. “Arquitectura Aplicacional e Tecnológica” como uma das principais orientações o “*Foco no Cidadão, como centro do sistema*”, não está claro no capítulo em que é feita a apresentação do grupo de trabalho e indicada de forma genérica a sua composição, que faça parte do referido grupo alguma entidade que represente o cidadão.

Não obstante, a preocupação demonstrada pelo documento R2A no ponto 4.1 “Protecção de dados Pessoais e acesso aos dados de saúde”, em que reconhece a “*Titularidade da informação pela pessoa titular dos dados, o que leva ao impedimento do acesso aos dados fora do RSE*”, o documento não clarifica como o utente pode aceder à sua própria informação.

Outro ponto importante a considerar relacionado é a utilização de dados para investigação. O documento R2A não especifica como o utente, sendo proprietário dos seus próprios dados, possa ter um papel activo quando estes são utilizados para fins de investigação. Podendo autorizar ou não essa utilização, saber quando são utilizados, quem os utilizou, com que finalidade e quais os resultados obtidos.

5. CONCLUSÕES

É num contexto de evolução não prestadora de serviços, mas de empresarialização, que surge, proposto pelo Estado, um modelo de Registo de Saúde Electrónico, em que se assume a particular função do Estado hetero-regulador. Percebe-se o porquê desta necessidade de intervenção. Com efeito, não se está num clássico domínio de “mercado”, onde as leis da oferta e procura se aplicam. No “mercado da saúde” existem inúmeras falhas de mercado tornando a intervenção do Estado no sector particularmente necessária.

A privacidade é, em si mesma, uma imanência da personalidade humana e um corolário da sua autonomia, compreendendo o direito à reserva sobre a intimidade da vida privada e honra pessoais. Todavia, a não compreensão da pessoa enquanto ser social, que simultaneamente reclama privacidade, mas também prestações do Estado, privilegiando aquela em total detrimento desta, apenas contribuirá para uma visão individualista dos direitos de personalidade, contrária à própria natureza humana, que ao pressupor sociabilidade tem necessariamente que compreender cedências individuais. Não obstante o próprio conceito de liberdade imponha que se assegure a tutela máxima da privacidade, o facto de se viver em sociedade reclama, numa compressão da liberdade individual, a recolha e partilha de dados pessoais, como garante dum valor que sendo colectivo, também é um valor individual, a saúde pública.

A garantia da privacidade está não no “*right to be let alone*” mas na segurança da informação respeitante à pessoa humana.

É fundamental que a integração e interconexão dos sistemas de informação e conhecimento, muitas vezes recorrendo a artefactos tecnológicos que possibilitam a colaboração entre diferentes actantes, integrem

rigorosos mecanismos de segurança sobre a partilha de informação sensível e considerem um conjunto de medidas que permitam definir níveis de acesso, auditoria, controlo e avaliação.

A partilha de informação e conhecimento é essencial na interconexão entre os diferentes intervenientes. É uma necessidade com riscos associados, quer na segurança da informação, quer na salvaguarda da privacidade e liberdade individual.

Dada a complexidade da implementação do Registo de Saúde Electrónico é fundamental o envolvimento de todos os intervenientes, não só na fase de desenvolvimento e implementação, mas também ao longo de todo o seu ciclo de vida.

A intenção de colocar o “*Foco no Cidadão, como centro do sistema*” não será nunca concretizada se não forem criados mecanismos claros e efectivos para que o cidadão possa participar e interagir com o sistema.

5. REFERÊNCIAS

- Ascensão, J. O. (1995). *Teoria Geral do Direito Civil*. Lisboa, Faculdade de Direito. 1995/96 (pg. 121).
- Avison, D., & Fitzgerald, G. (1995). *Information Systems Development: Methodologies, Techniques and Tools* (2th ed.). London: McGraw-Hill International.
- Beynon-Davies, P. (2002). *Information Systems: An Introduction to Informatics in Organizations*. Hampshire: Palgrave.
- Buckingham, R. A., Hirschheim, R. A., & Land, F. F. (1987). Information systems curriculum: a basis for course design", in Buckingham, R.A., Hirschheim, R.A., Land, F.F., Tully, C.J. (Eds), *Information Systems Education: Recommendations and Implementation*. Cambridge: Cambridge University Press.
- Campos, A. (2000). Novos Modelos de Gestão de Hospitais. In *Forum de Economia da Saúde*. Livro de comunicações: Porto.
- Choo, C. (1998). *Information Management for the Intelligent Organization - The Art of Scanning the Environment*. American Society for Information Science.
- Curado, H., & Lapão, L. V. (2005). Lições do Sistema de Garantia de Privacidade e Segurança Americano - HIPAA - para o Sistema Nacional de Saúde Português. *Actas do 3º Congresso Nacional da Administração Pública*. AIP. Lisboa.
- Domínguez, A. (2005). Reflexiones sobre la protección de los datos genéticos. *Apuntes sobre la discriminación por razones genéticas desde el derecho europeo*. Espanha: Universidad de Vigo.
- Doneda, D. (2000). Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In G. T. (org.), *Problemas de direito civil-constitucional* (pp. 111-136). Rio de Janeiro: Renovar.
- Fortes, P. A., & Spinetti, S. R. (2004). O Agente comunitário de Saúde e a privacidade das Informações dos Usuários. *Cadernos de Saúde Pública*, Vol. 20 n.º5. Rio de Janeiro. Set/Out 2004.
- Gutiérrez, L. (Júlio de 2004). La protección de datos personales y su necesaria incorporación en los ordenamientos jurídicos de América Latina. *Revista de Derecho Informático*, No. 084.
- Iglesias, A. (Marzo de 2004). Algunos apuntes técnicos y jurídicos sobre los principales protocolos de seguridad en Internet. *Revista de Derecho Informático*, No. 068.
- Kock, N. (2005). *Business Process Improvement Through E-Collaboration: Knowledge Sharing Through de Use of Virtual Groups*. Hershey, PA, USA, Idea Group Publishing .
- Laudon, K. C., & Laudon, J. P. (2002). *Management Information Systems, Managing the Digital Firm* (7th ed.). New Jersey: Prentice Hall.
- Law, J. (1992). Notes on the Theory of the Actor Network: Ordering, Strategy and Heterogeneity. Centre for Science Studies, Lancaster University.
- Ministério da Saúde. Administração Central de Sistema de Saúde, R. (2009). RSE – Registo de Saúde Electrónico. R2A: Orientações para Especificação Funcional e Técnica do Sistema de RSE. Portugal: Ministério da Saúde.
- Sanches, J. (2000). A Regulação: História Breve de um Conceito. *Revista da Ordem dos Advogados*. Ano 60. ISSN: 0870-8118 , pp. 5-22.

Simões, J. (2004). *Retrato Político da Saúde - Dependência do Percurso e Inovação em Saúde: da Ideologia ao Desempenho*. Coimbra: Almedina.

Tochtermann, K., & Maurer, H. (2000). Knowledge Management and Environmental Informatics. *Journal of Universal Computer Science*, pp. 517-536.

Underwood, J. (1998). Not Another Methodology: what ANT tells us about systems development. 6th International Conference on Information Systems Methodologies. Salford UK.

i Cf., respectivamente artigos 26.º e 35.º da Constituição da República Portuguesa.

ii Resulta ainda da Lei n.º 67/98, de 26 de Outubro, art.º 3º - a delimitação de outros conceitos particularmente relevantes, para além do já referido sobre o que se entende por “tratamento de dados pessoais”, com particular relevância para o tema em apreço, é o de “ficheiro de dados pessoais”.

iii A referência do Ac. de 5/10/94 citado in *Pereceres da PGR*, Vol.VII, pág. 40, é feita na Deliberação N.º 51/2001 da CNPD.