PRIVACIDADE E PROTEÇÃO DE DADOS NOS CUIDADOS DE SAÚDE DE IDOSOS

Francisco C.P. Andrade*, Ângelo Costa **, Paulo Novais **

* Escola de Direito da Universidade do Minho: fandrade@direito.uminho.pt

** Departamento de Informática, Universidade do Minho: acosta@di.uminho.pt e pjon@di.uminho.pt

INTRODUÇÃO:

Nas últimas décadas, a expectativa de vida aumentou exponencialmente. A combinação desse aumento na esperança média de vida e de uma simultânea diminuição do número de nascimentos acarretou profundas modificações no modo como as pessoas vivem o seu quotidiano[1].

Há uma evidente necessidade de repensar o planeamento e a prestação dos cuidados de saúde, de modo a melhorar a qualidade de vida do ser humano comum, em especial dos idosos. As tecnologias e as ciências da computação vêm progredindo no sentido do desenvolvimento de novas aplicações nos domínios médico e social, como é o caso das aplicações de software de monitorização, passíveis de serem usadas para auxiliar o utilizador na execução das suas tarefas quotidianas[2].

Problema comum à utilização destes sistemas é o facto de requererem total cooperação por parte dos utilizadores e de serem muito baseados na utilização de perfis de utilizador. Estes sistemas necessitam de recolher um elevado número de dados em tempo real, de modo a que se possam ir adaptando às variáveis com que o próprio utilizador se vai confrontando. Esta construção de perfis de utilizador requer a interacção com humanos que formulem questões, cabendo ao sistema avaliar as respostas de modo a criar o respectivo perfil.

Tipicamente, estes sistemas exigem que dados pessoais (e, eventualmente, até dados sensíveis) sejam partilhados entre diferentes pessoas e, em alguns sistemas, os dados e informação poderão ficar disponíveis para uma utilização por parte de outros utilizadores (por exemplo profissionais de saúde e familiares).

---

[1] -- cfr. United Nations “World Population Ageing 1950-2050”, ed. UN 2002

[2] -- cfr. Chisolm, D. & Evans, D. B., “Economic evaluation in health: saving money or improving care?” in “Journal of Medical Economics, 10, 2007, págs. 325-337

MOTIVAÇÃO: CUIDADOS DE SAÚDE E PRIVACIDADE

A Ciência Médica é hoje desenvolvida em colaboração entre humanos e tecnologias. Apesar das decisões mais relevantes serem apenas tomadas por médicos, os computadores providenciam hoje um inestimável apoio (através dos sistemas de apoio à decisão) facultando um fácil acesso a dados, testes e resultados e apresentando até sugestões que facilitam o processo de tomada de decisão relativamente à situação clínica de um determinado paciente. Muitas das sugestões apresentadas pelas aplicações informáticas, e que se baseiam na análise de dados sensíveis como é o caso dos dados médicos, são, em última análise, revistos por pessoal especializado, como médicos e paramédicos. Na verdade, os computadores não devem tomar nenhuma decisão no que concerne aos problemas de saúde dos pacientes. As pessoas profissionalmente envolvidas na relação clínica têm que seguir regras deontológicas de proteção e salvaguarda da vida humana, estando ainda ainda sujeitas a obrigações de sigilo e de respeito pela privacidade, mas a verdade é que dados sensíveis vão sendo partilhados entre pessoas e aplicações.

Todos os dias, técnicos processam dados e informação relativos aos utilizadores/pacientes. Hospitais e unidades de cuidados de saúde confiam na recolha de dados, tendo em vista os objectivos do tratamento dos doentes, sacrificando até os requisitos da privacidade para que se mantenha um fluxo de dados, importante para a disponibilização de serviços de saúde mais eficientes e confiáveis[3]. Esta situação não é desejável, mas também deve-se reconhecer que inviabilizar totalmente este tipo de ações também o não seria. Há que estabelecer um equilíbrio entre os direitos e legítimas preocupações dos utilizadores e os requisitos de funcionamento eficiente de hospitais e unidades de saúde[4]. A recolha e partilha de dados e informação[5] entre hospitais, médicos e outros profissionais é muito importante para a

---

[3] -- cfr. Baltussen, R., Adams, T., Torres, T.T., Hutubessy, R., Acharya, A., Evans, D., Murray, C. "Making Choices in Health: WHO Guide to Cost-Effectiveness Analysis", World Health Organization 2003, e ainda Chisholm & Evans, 2007, referido.

[4] -- Ball, M.J., Lillis, J. (2001). E-health: transforming the physician/patient relationship. International Journal of Medical Informatics 61: 1-10, e ainda Hospital Waiting Times team, "Inpatient and Outpatients Waiting Lists", Department of Health, 2010

[5] -- aceitamos aqui a distinção estabelecida por Peter Jones / David Marsh in "Essentials of EDI Law", Electronic Data Interchange Council of Canada, 1993, pág. 7, que referiam a diferença entre informação e dados, sendo a primeira "the communication of instructive knowledge, information or news", por contraposição a dados, entendidos como "a more restrictive word which means things assumed as fact and made the basis of reasoning or

prestação de bons serviços de saúde, mas também importa nunca esquecer que a privacidade e a protecção de dados pessoais são direitos fundamentais constitucionalmente garantidos[6].

ASSISTENTES COGNITIVOS NAS PERDAS DE MEMÓRIA

As perdas de memória de longo prazo podem constituir um problema complexo e de difícil resolução, com particular incidência na população idosa. As disfunções cognitivas podem ser divididas em três diferentes estados: ausência de limitações cognitivas, ligeiras limitações cognitivas ou severas limitações cognitivas. Estes tipos de limitações traduzem diferentes estados de perda de memória. No primeiro estado, não há limitações ou estas são muito ligeiras[7]. Num segundo estado, a pessoa enfrenta já alguns problemas na sua vida quotidiana, e as falhas de memória começam já a afetar a execução de simples tarefas diárias. O terceiro estado significa que a pessoa necessita de constante vigilância, já que não consegue executar quase nenhuma das mais simples tarefas do quotidiano. As pessoas que estão no primeiro e segundo estados referidos são as que poderão ser ajudadas pela tecnologia, entendida enquanto meio auxiliar que contribui para suprir as referidas falhas de memória.

Atualmente, há vários projectos e aplicações, que lidam com este tipo de problemas. Como exemplos, podemos apontar os projectos "Hermes" e "SenseCam"[8]. Os assistentes cognitivos podem ser descritos do seguinte modo[9]: são sistemas que auxiliam o utilizador na execução

---

calculation". Enquanto a informação requer uma interpretação e processamento por humanos, os dados podem ser processados sem intervenção humana.

[6] -- cfr. Catarina Sarmento e Castro "Direito da Informática, Privacidade e Dados Pessoais", Almedina, 2005, págs. 22-29 e Carlos Ruiz Miguel "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea", in "Temas de Direito da Informática e da Internet", Coimbra Editora, 2004, págs. 17-71

[7] -- (paradigma "*where are my keys?"*) cfr. Luck, M., Ashri, R. & d'Inverno, M. "Agent-Based Software Development", Artech House Publishers, 2004.

[8] -- cfr. Jiang, J., Geven, A. & Zhang, S. "HERMES: A FP7 Funded Project towards Computer-Aided Memory Management Via Intelligent Computations" in "3rd Symposium of Ubiquitous Computing and Ambient Intelligence", vol. 51, págs. 249-253, 2008 Springer, Berlin/Heidelberg. Cfr. ainda Hodges, S., Williams, L., Berry, E., Izadi, S., Srinivasan, J., Butler, A., Smyth, G., Kapur, N. & Wood, K. "SenseCam: A retrospective memory aid" in "8th International Conference on Ubicomp", 2006, págs. 177-193.

[9] -- cfr. Tucker, G. "Age-Associated Memory Loss: Prevalence and Implications" in "Journal Watch Psychiatry"; Geda, Y.E., Roberts, R. O., Knopman, D.S., Petersen, R.C., Christianson, T.J.H., Pankratz, V.S., Smith, G.E., Boeve, B.F., Ivnik, R.J., Tangalos, E.G., & Rocca, W.A. "Prevalence of Neuropsychiatric Symptoms in Mild Cognitive Impairment and Normal Cognitive Ageing: Population Based Study", Arch Gen Psychiatry, 65 (10), 2008, págs. 1193-1198; Charness, N. "Ageing and Human Performance. Human Factors" in "The Journal of the Human Factors and Ergonomics

das suas tarefas diárias apresentando sugestões relacionadas com aquilo que o utilizador vai fazendo em cada momento ou procedendo, no final do dia, a uma revisão das ações do utilizador e dos lugares onde este esteve. No entanto, ainda não podemos falar em projetos direccionados para uma real interatividade e total automação. O que isto quer dizer é que os projetos até agora desenvolvidos ainda requerem uma grande atenção por parte do utilizador, tanto no que respeita à configuração de todas as opções como à correção dos erros decorrentes da respectiva execução.

UM ASSISTENTE COGNITIVO: IGENDA

O Projeto iGenda tem vindo a ser desenvolvido na Universidade do Minho (Portugal)[10]. Trata-se de um projeto baseado em ambiente AAL ("Ambient Assisted Living") e que integra uma agenda inteligente que automaticamente procede à marcação e calendarização de eventos e de atividades livres. Os eventos podem resultar da marcação por terceiras pessoas e o sistema processa a calendarização das tarefas e atividades na agenda do utilizador. Este desenvolvimento tem como principal objetivo a resolução de um problema muito comum que afeta as pessoas idosas, o problema das falhas de memória.

O iGenda opera em dois patamares distintos: por um lado, a calendarização de eventos; por outro, a gestão de tempos livres. A calendarização de eventos processa-se através da recepção de novos eventos pelo sistema e, usando um sistema de resolução de conflitos, procede à calendarização nos espaços livres, corrigindo erros e procurando ultrapassar incompatibilidades que possam decorrer deste processo. A função de gestão de tempos livres, por seu turno, assegura a calendarização, na agenda do utilizador, de actividades de lazer e de tempos livres, procurando assim manter o utilizador ocupado e activo.

O iGenda tem três núcleos internos: o "Agenda Manager", o "Conflicts Manager" e o "Free Time Manager". O "Agenda Manager" é o portal do sistema para recepção e envio de informação. É constituído por um receptor de mensagens, gestor de segurança e distribuidor de tarefas. As mensagens recebidas integram um mecanismo de assinatura electrónica segura com chave de encriptação gerada para cada utilizador, criando-se assim um nível de

---

Society", 2008, 50 (3), págs. 548-555; National Institute for Health and Clinical Excellence, 2011 "Dementia: supporting people with Dementia and their carers in health and social care".

[10] -- Costa, A., Novais, P., Corchado, J.M., Neves, J. "Increased performance and better patient attendance in an hospital with the use of smart agendas", in "Logic Journal of IGPL.", 2011

segurança que apenas permite ao destinatário da mensagem a sua desencriptação e consequente acesso ao seu conteúdo. Integra um gestor de tarefas que, de acordo com as mensagens recebidas, envia os dados para o respectivo agente electrónico, servindo ainda como activador do "Free Time Manager". O "Agenda Manager" atua ainda como sistema de segurança do sistema, mantendo protegidos os restantes agentes, e assegura uma importante função de proteção: não interage diretamente nem com os dados do utilizador nem com o calendário, sendo um elemento chave para a proteção global do sistema[11]. O "Agenda Manager" integra na sua base de dados todas as pessoas autorizadas a estabelecer ligação com o utilizador, servindo também como porta de proteção contra intrusões. Por outro lado, o "Agenda Manager" mantém um registo de todas as ligações ao sistema, através de um sistema de registo de entrada (*"Login"*) que assegura o registo de todas as entradas e saídas do sistema e comunicações.

O "Conflicts Manager" é fundamental para a calendarização de eventos. Utiliza um processo de inferência lógica que permite a tomada de decisões. Existem várias abordagens possíveis para a questão da seleção e escalonamento dos eventos a calendarizar. A nossa abordagem baseia-se numa pilha de processos. É utilizado um sistema de classificação que utiliza valores numéricos para classificar a importância de um dado evento. Em seguida, o sistema verifica se há espaço para calendarizar o evento. Depois segue-se um intricado processo. Os eventos recebidos são hierarquizados de acordo com critérios de reputação do utilizador. O utilizador que agendou o evento é verificado na base de dados da pessoa que recebe a indicação do evento, sendo-lhe atribuída uma classificação. Este valor será fundamental para a determinação do valor a atribuir pelo sistema.

Um exemplo: "se o médico pessoal do utilizador marca uma consulta, então ao evento será atribuída uma "Prioridade 1". Mas se o próprio médico declara uma prioridade baixa, então o valor passa para "Prioridade 2". Mas se é um amigo do utilizador a agendar um evento, então este poderá atingir um valor mínimo de "Prioridade 4", dependendo da reputação do amigo no sistema.

A pessoa que agenda o novo evento pode atribuir, ela própria, um valor de importância ao evento, mas o sistema irá sempre verificar qual o valor base que é atribuído àquele utilizador.

---

[11] -- cfr. Moreno, A., Valls, A. & Viejo, A., "Using JADE-LEAP to implement agents in mobile devices", in http://jade.tilab.com/papers/EXP/02Moreno.pdf ; e Gawinecki, M. & Frackowiak, G. "Multi-Agent Systems with JADE: A Guide with Extensive Study", IEEE Distributed Systems Online, 9, 2008.

Quanto aos eventos, serviços médicos e similares terão prioridade nos rankings, enquanto as actividades recreativas terão um valor inferior.

O Projecto iGenda assenta ainda na ideia de ajudar o utilizador na programação dos tempos livres, a partir de uma recolha de eventos e actividades. Isto é realizado com base numa execução automatizada de eventos e na sua adição a um calendário atribuído a cada utilizador. O objetivo do "Free Time Manager" é assegurar uma calendarização de actividades de tempos livres nos espaços livres do calendário do utilizador. Esta função é importante porque mantém o utilizador activo e ligado a outros utilizadores, ajudando-o a alcançar uma integração social.

A base de dados irá conter indicações sobre diferentes tipos de actividades de que o utilizador gosta e que possam ser realizadas quer individualmente, quer em conjunto com outras pessoas. O "Free Time Manager" irá verificar o espaço livre que o utilizador tem no seu calendário e, utilizando funções lineares de distribuição, procederá ao agendamento de actividades nesses espaços. E se a actividade em causa envolver outras pessoas, o iGenda fará a necessária ligação com as aplicações iGenda dos outros utilizadores, por forma a compatibilizar a calendarização das actividades.

A decisão será tomada em tempo real ou através do preenchimento de um questionário que vai permitindo ao utilizador a avaliação da eficiência do sistema. Os resultados serão recolhidos e utilizados pelo sistema, permitindo modificar os valores de prioridade das actividades e adaptar a actuação do sistema de modo a que este se vá tornando mais eficiente.

As funções utilizadas para agendar actividades nos espaços livres de calendário são lineares mas introduzem uma variável aleatória pelo que nem sempre será a mesma actividade a ser escolhida. Naturalmente, a actividade preferida será mais vezes escolhida, mas outras actividades disponíveis poderão também ser escolhidas, de modo a manter um quadro equilibrado de distribuição de actividades e a evitar a monotonia e a repetição.

Conectividade e Interfaces

Normalmente o uso será assegurado a partir de um dispositivo móvel que o utilizador trará sempre consigo. Este aparelho terá acesso a toda a informação disponibilizada pelo servidor e providencia um inestimável conjunto de informações captadas por sensores presentes neste aparelho móvel, tais como o posicionamento através de GPS. O sistema permite ainda o estabelecimento de ligações com os familiares do utilizador, podendo estes agendar novos eventos ou visualizar o calendário do utilizador, de modo a que possam até avaliar se os eventos calendarizados são os mais adequados.

Os interfaces disponíveis são simples quanto possível e construídos de acordo com as normas mais comuns de utilização[12], apresentando características amigas do utilizador (“*user-friendly”*). O utilizador poderá manter aberta uma janela com informações (por exemplo sobre as actividades recentemente agendadas) podendo ter uma janela adicional para o envio de mensagens com campos específicos. O dispositivo móvel utiliza uma plataforma Android (sistema operativo da Google), sendo o interface desenhado de modo a que o utilizador possa facilmente interagir com o sistema. O sistema utiliza o máximo de serviços providenciados pelos sistemas operativos, minimizando o número de aplicações suplementares.

Os módulos são basicamente constituídos por agentes sofisticados que comunicam através da rede (LAN, WiFi, 3G) e que, pelas suas características, poderão estar presentes em diferentes servidores ou até em diferentes países. O mesmo se passa com as interface do iGenda que pode operar automaticamente com o “Agenda Manager”, receber actualizações do calendário e estar disponível para o envio de mensagens em tempo real.

Sensing Module

Com a criação do iGenda, verificou-se que diferentes módulos poderiam estar ligados ao sistema, permitindo a extenção das funções de calendarização automática e inteligente. Tal foi o caso do “Sensing Module” (Modulo de Sensorização - SM). Este tem como objectivo a monitorização móvel do utilizador[13] e utiliza um conjunto de sensores corporais que recolhem dados vitais, processando remotamente os dados e enviando para o médico informação atualizada sobre o estado de saúde do utilizador. Os sensores podem recolher dados de electrocardiograma, pressão arterial, oximetria e deteção de quedas (modificações abruptas do Sensor G), entre outros, sendo estes dados processados com vista a agregar informação sobre o estado geral de saúde do utilizador. Os dados são posteriormente enviados para o médico do utilizador para uma análise mais detalhada. Esta monitorização permite libertar o utilizador do hospital, sem deixar de providenciar a monitorização que os hospitais normalmente

[12] -- cfr. Wu, M. & Baecker, R. “Participatory Design of an Orientation Aid for Amnesics”, in “Proceedings CHI 2005”, ACM Press, 2005, págs. 511-520.

[13] -- Carneiro, D., Novais, P., Costa, R., Gomes, P., Neves, J. “Emon: Embodied Monitorization”, in M. Tscheligi, B. De Ruyter, P. Markopoulos, R. Wichert, T. Mirlacher, A. Meshterjakov & W. Reitberger (eds.) “Ambient Intelligence”, Vol. 5859, págs. 133-142, Springer, Berlin / Heidelberg; DeLong, P. “Interoperability & Sensor Fusion”, in “Naval Engineers Journal”, 2003, 115 (2), págs. 89-104; Corchado, E., Arroyo, A., Tricio, V. “Soft Computing models to identify typical meteorological days”, in “Logic Journal of IGPL”, 2010; Triantafyllidis, A., Koutkias, V., Chouvarda, I., Maglaveras, N. “An open and reconfigurable wireless sensor network for pervasive health monitoring”, in “Methods of Information in Medecine”, 2008, 47 (3), págs. 229-234.

asseguram. Por outro lado, os médicos também ficarão mais disponíveis para os casos de verdadeira emergência, sem deixarem de manter o controlo diário, a partir dos relatórios, e de tomar decisões com base nos seus conteúdos.

Neste cenário, o interesse da integração do iGenda é evidente, pois assegura a manutenção da ligação médico-utilizador. Se após um relatório diário, o médico decide chamar o utilizador para uma consulta, tudo o que tem a fazer é abrir o iGenda e agendar uma consulta. O evento será automaticamente calendarizado e o utilizador será notificado. O mesmo se poderá dizer nos casos em que é o utilizador quem pretende marcar a consulta. Neste caso, o médico recebe uma notificação da pretensão do utilizador, deixando-se para o médico a decisão de marcação bem como a possibilidade de uma resposta fundamentada.

O sistema de processamento será ainda capaz de tomar algumas decisões proativas, baseadas nas condições normalizadas de saúde, por exemplo, se houver uma significativa mudança de alguns índices de saúde do utilizador, o SM pode pedir ao iGenda que calendarize um evento tanto na agenda do utilizador, como na agenda do médico.

O SM é capaz de detetar fatores que não são detetáveis a partir de um exame de rotina, criando um sistema mais eficiente de agregação de dados. Por outro lado, dada a natureza dos sensores, o SM e o iGenda podem ser executados a partir de um mesmo dispositivo móvel, criando-se assim uma forte sinergia entre ambos.

AMEAÇAS À PRIVACIDADE E À PROTEÇÃO DE DADOS

Este projeto assenta numa intensa utilização de dados pessoais e privados e, dada a sua natureza, os dados recolhidos têm que ser revistos por especialistas para que o sistema possa ser fiável e eficiente. Também a componente social pode requerer que a informação se torne visível para outros utilizadores. É possível também que em muitos casos tenha que ser garantido um total acesso a familiares ou àqueles que têm responsabilidades de cuidar do utilizador.

Perfis

Para que haja um ajustamento às necessidades do utilizador, foi construída uma plataforma de personalização que guarda o perfil do utilizador e as escolhas que ele foi realizando ao longo do tempo. Estes perfis contêm dados privados e pessoais dos utilizadores, os quais são

utilizados para criar uma base de dados de preferências e automação, criando assim um modelo padrão que pode muito facilmente ajudar a formular sugestões. Os dados recolhidos são revistos por um técnico (sujeito a uma obrigação de sigilo) que os insere num modelo, atribuindo pesos e relacionando os dados, de modo a torná-lo mais efetivo. O perfil também aloja um estado clínico do utilizador de modo a tornar atividades proativas mais eficientes[14].

Este sistema de perfis recolhe uma grande variedade de dados. Mas a associação entre dados e informação não é totalmente confiável. Estas operações podem por vezes induzir o sistema em erro e apontar para resultados totalmente imprevistos. Para corrigir esta situação, os técnicos têm que rever de novo toda a informação e, se necessário com a ajuda do utilizador, atribuir aos dados um significado correto.

Um sistema de aprendizagem também irá recolher, ao longo do tempo, dados sobre as escolhas e actividades do utilizador. O sistema vai aprendendo aquilo que o utilizador faz, quais as suas actividades preferidas, de modo a poder modificar eficazmente os algoritmos de decisão.

Módulos de Recolha de Dados

O iGenda integra vários módulos que integram diferentes sensores e aparelhos que lêem e processam informação pessoal relativa ao utilizador. O SM recolhe dados dos sensores implantados no corpo do utilizador. Os dados são processados e analisados através de definições médicas logicamente definidas. Estas definições suportam um fluxo de decisão que se vai traduzir num diagnóstico médico inicial. Caso ocorra uma emergência, o sistema notifica de imediato o Serviço de Emergência, transmitindo-lhe os dados vitais e a localização do utilizador.

O conjunto dos dados vitais captados pelos sensores é transferido para o servidor principal, de modo a ser processado e a criar um mapa clínico das condições de saúde do utilizador que o médico pessoal do utilizador possa consultar. Com a utilização deste mapa de saúde do utilizador, o sistema é capaz de identificar eventuais problemas e automaticamente agendar uma consulta, tanto na agenda do utilizador como do médico, procedendo de imediato à notificação de ambos.

---

[14] -- cfr. Robinson, L., Bamford, C., Beyer, F., Clark, A., Dickinson, C., Emmet, C., Exley, C., Hughes, J., Robson, L., Rousseau, N. “Patient preferences for future care – how can Advance Care Planning become embedded into dementia care: a study protocol”, in “BMC Geriatr”, 2010, 10, 2.

Partilha de Dados

Os dados passam por vários técnicos para que possam ser revistos e inseridos no sistema. O pessoal autorizado pode ser mais ou menos vasto e qualquer técnico autorizado poderá proceder às necessárias operações técnicas.

A possibilidade de partilha de dados clínicos é também uma importante característica. Estado clínico e ficheiros de saúde podem ser partilhados entre diferentes entidades e organizações médicas, ou projetos, com módulos associados ao iGenda. Dados, tais como os ficheiros electrónicos de saúde, podem ser partilhados em projetos como VirtualECare[15] e distribuídos a vários hospitais e centros médicos.

Relativamente a outras pessoas envolvidas, os dados podem ser partilhados com vários elementos da família e até amigos. As pessoas podem ser previamente autorizadas pelo utilizador e ter diferentes tipos de acesso aos dados, para ver os dados ou até para adicionar novos eventos, alterar eventos existentes ou até ver eventos que o utilizador considera privados.

Os dados são enviados dos aparelhos e sensores que os recolhem para o iGenda, passando por uma série de processos de recepção e transmissão, suportados por sistemas de comunicações como GSM, UMTS e WiFi, entre outros. Isto implica que uma terceira parte, como será o caso do prestador do serviço móvel, também tenha acesso à informação transmitida.

Para uma adequada execução do sistema, torna-se necessário que toda a informação recebida seja armazenada. Isto significa que todos os dados serão armazenados, de modo permanente,. Estes sistemas comportam um evidente e permanente risco de perda de privacidade e de acesso por terceiros a dados pessoais e sensíveis do utilizador.

Garantias Técnicas e Jurídicas

Esta aplicação gere dados e informação vitais e pessoais do utilizador, tornando-os acessíveis a terceiros e permitindo até identificar em cada momento a sua localização. Assim sendo, este projeto acarreta um elevado risco de perda de privacidade. A este respeito, necessário se torna

[15] -- cfr. Novais, P., Costa, R., Carneiro, D., Neves, J. "Inter-Organization Cooperation for Ambient Assisted Living", in "Journal of Ambient Intelligence and Smart Environments", 2010, 2 (2) págs. 179-195; e Novais, P., Costa, A., Costa, R., & Lima, L. "Collaborative Group Support in E-Health", in T. Matsuo, N. Ishii, R. Lee (eds.), "ACIS-ICIS", 2010, págs. 177-182, IEEE Computer Society.

estabelecer quais as esferas da personalidade do utilizador que vão ser afectadas. A Jurisprudência Alemã considera, para além de uma esfera pública ou de publicidade, a existência de uma esfera pessoal, uma esfera privada e uma esfera íntima[16]. Por outro lado, foi expressamente reconhecida pelo artigo 8º da Convenção Europeia de Direitos Humanos a existência de um Direito Fundamental à Privacidade. E, posteriormente, também a Carta de Direitos Fundamentais da União Europeia consagrou, no seu artigo 7º, este mesmo direito, claramente dirigido para a protecção do indivíduo contra intrusões ilegítimas por parte de autoridades públicas ou de outros indivíduos[17]. Para além das questões relativas à privacidade, também o problema da protecção de dados pessoais tem hoje que ser repensado, já que o artigo 8º da Carta de Direitos Fundamentais da União Europeia elevou a protecção de dados pessoais ao estatuto de Direito Fundamental[18]. Mas estes dois temas, Privacidade por um lado, Protecção de Dados Pessoais por outro, ainda que comummente interligados e frequentemente tratados em conjunto até pela doutrina jurídica, podem exigir diferentes abordagens. Por exemplo, enquanto o direito à privacidade pode exigir uma proibição relativa à vigilância em certos espaços ou situações[19], já a protecção de dados pessoais poderá implicar outro tipo de restrições relativamente aos procedimentos de recolha e processamento de dados[20].

A questão fulcral será a de saber quais as obrigações legais (e protecção jurídica) decorrentes da situação acima referida. A questão é particularmente delicada, já que envolve a recolha, armazenamento e transmissão de dados de saúde, que são considerados pelo direito europeu como "dados sensíveis". Neste aspecto, é importante olhar para o respectivo enquadramento legal e tentar perceber até que ponto serão admissíveis excepções a esta consideração dos dados de saúde como dados sensíveis e se a consideração dos dados como sensíveis estará ou não relacionada com o respectivo contexto. A incidência de questões como a distribuição de dados, a necessária monitorização através de câmaras e sensores, o estabelecimento de perfis

---

[16] -- cfr. Farinho, D. "Intimidade da Vida Privada e Media no CiberEspaço", Almedina, 2006, pág. 45-53.

[17] -- cfr. Rouvroy, A., "Privacy Data Protection and the Unprecedented Challenges of Ambient Intelligence", in "Studies in Ethics, Law and Technology", 2008, 2 (1), pág. 8.

[18] -- cfr. Rouvroy, idem, pág 9 e Carlos Ruiz Miguel, citado, que no entanto, a págs. 65, aponta a existência de uma ampla margem de aprciação dos Estados relativamente à regulação deste direito.

[19] -- "prohibition against surveillance in certain spaces or situations (e.g., in bathrooms)", Hert, P.D., Gutwirth, S., Moscibroda, A., Wright, D., Fuster, G.G., "Legal safeguards for Privacy and Data Protection in Ambient Intelligence", in "Personal and Ubiquitous Computing", 2008, 13 (6), págs. 435-444.

[20] -- cfr. Catarina Sarmento e Castro, citado, aponta quer os princípios fundamentais de tratamento de dados pessoais (págs. 229-238), quer os direitos dos titulares dos dados (págs. 239-262). Cfr. ainda, Carlos Ruiz Miguel, citado, págs 56-64.

de utilizador, poderão ou não tornar-se uma porta aberta para intromissões na privacidade e utilização de dados pessoais do utilizador. Para além disso, há que não perder de vista que não são apenas os dados recolhidos que são importantes, mas também o conhecimento gerado a partir dele. A questão do conhecimento torna-se realmente importante, já que permite a transformação dos dados em informação e a sua relacionação com o contexto, atribuindo assim um significado aos elementos recolhidos. Para além disso, poderemos ter diferentes perspectivas sobre o sistema e a utilização que dele é feita.

Privacidade

O direito à intimidade e à vida privada estão intimamente ligados à personalidade[21]. Trata-se do direito que cada pessoa tem a poder decidir por si só o quê (e quando) deve ser partilhado com terceiras pessoas, permitindo ao indivíduo o controlo da sua própria vida e experiências, nas esferas em que não é permitida uma intromissão, nem por parte do Estado nem por parte de terceiras pessoas[22]. Este é um direito intimamente ligado à liberdade pessoal, à construção da identidade, ao controlo que cada um deve ter sobre os aspectos da identidade que deseja projetar para o mundo[23]. No Ordenamento Jurídico Português, este direito à privacidade aparece expressamente reconhecido e consagrado pelos artigos 26º nº 1 da Constituição da República Portuguesa e 70º do Código Civil (aqui entendido como um direito de personalidade).

Este direito à privacidade aparece agora, devido aos desenvolvimentos tecnológicos, como particularmente ameaçado. Aumentam as possibilidades tecnológicas de monitorização constante do individuo, especialmente pela utilização dos RFIDs e outras tecnologias que possibilitam seguir tudo o que fazemos e onde quer que vamos[24], ou seja, uma constante observação e monitorização, o estabelecimento de relações entre pessoas e objectos que permitem seguir a pessoa. Acrescem ainda as possibilidades de recolha ou mineração de dados (data mining) e de construção de perfis de utilizador, a utilização de sensores capazes de monitorar aspectos como a pressão arterial, a temperatura do corpo, os batimentos cardíacos, as expressões faciais, incluindo até a possibilidade de uma constante observação de

[21] -- cfr. Catarina Sarmento e Castro, citado, págs. 22-28. cfr. Janeiro, D.B., "La protección de datos de carácter personal en el derecho comunitario", in "Estudos de Direito da Comunicação", Instituto Jurídico da Comunicação, Faculdade de Direito, Universidade de Coimbra, 2002, que, a págs. 44 e nota 37 refere a existência de direitos fundamentais de terceira geração.

[22] -- cfr. Janeiro, D.B., citado, págs. 46/47.

[23] -- cfr. Rouvroy, citado, págs. 8/9.

[24] -- " to follow whatever we do and wherever we go ", Hert et. al. 2008, citado.

escolhas, comportamentos, emoções, tornando as pessoas cada vez menos capazes de viver de acordo com as suas escolhas e comportamentos totalmente livres e autónomos[25]. E, para além do mais, este aumento das possibilidades de monitorização traz consigo um progressivo esbatimento da distinção entre esfera pública e esfera privada e o perigo da "Vigilância de Dados" ou "Dataveillance"[26]. Pelo que se sente hoje em dia uma enorme necessidade de protecção da intimidade e da vida privada, procurando assegurar as garantias de confidencialidade e fortalecer dois aspectos diferenciados da intimidade: o aspecto negativo da intimidade, excluindo-se o conhecimento por terceiros daquilo que é próprio do indivíduo; o aspecto positivo da intimidade, assegurando-se um controlo do indivíduo sobre a informação que lhe é própria[27].

Dados Pessoais

Dados pessoais são dados relativos a uma pessoa singular, identificada ou identificável, considerada titular dos dados[28]. Já dados de saúde são dados relativos a todos os aspectos, físicos e psicológicos, relevantes para a saúde de uma pessoa, tal como foi referido pelo Tribunal de Justiça da União Europeia a propósito da interpretação do artigo 8º nº 1 da Diretiva nº 95/46/CE[29]. Sendo os dados de saúde considerados dados sensíveis, de acordo com o direito europeu e português (art. 7º da Lei 67/98), o seu tratamento, em princípio, não será autorizado, a não ser que o titular dos dados consinta e que sejam disponibilizadas medidas de segurança adicionais, como por exemplo a separação lógica entre os dados de saúde e outros dados pessoais (art. 15º nº 3 da Lei 67/98).

Existe no ordenamento jurídico português uma proibição geral de tratamento de dados pessoais. A Constituição da República Portuguesa, no artigo 35º, proíbe expressamente a utilização da informática para o tratamento de dados relativos à vida privada[30]. Por outro lado, a Lei 67/98, em conformidade com a Diretiva Europeia 95/46/CE, especificou esta proibição de modo a incluir no âmbito dos dados sensíveis os dados relativos à vida privada, saúde, vida sexual e dados genéticos (art. 7º nº 1 Lei 67/98) .

---

[25] -- cfr. Rouvroy, A. e Poullet, Y. "The right to informational self-determination and the value of self-development. Reassessing the importance of Privacy for Democracy", in "Reinventing Data Protection", Springer, 2009, págs. 45-76.

[26] -- cfr. Hert et. al. 2008, citado.

[27] -- cfr. Janeiro, D., citado, pág. 30.

[28] -- cfr. Catarina Sarmento e Castro, citado, pág. 71.

[29] -- cfr. Processo C-101/01, decidido a 6 de Novembro de 2003.

[30] -- para uma análise da evolução constitucional portuguesa sobre esta questão, cfr. Garcia Marques & Lourenço Martins "Direito da Informática", Almedina, 2000, págs. 167-183.

No entanto, permanece uma excepção evidente a esta proibição geral: trata-se do caso em que o titular dos dados expressamente consente (art. 7º nº 2 Lei 67/98), através de manifestação de vontade concreta, livre e informada (art. 3º h) Lei 67/98)[31].

Assim, ainda que medicamente justificável, o tratamento de dados de saúde requer necessariamente o consentimento livre e expresso do titular dos dados através de uma manifestação de vontade concreta, livre e informada[32]. O que implica um reconhecimento de um princípio de informação, ou melhor da existência de um direito à informação, dado que o titular tem o direito de saber exatamente que dados sobre si estão contidos nos ficheiros. Por outro lado, o requisito do consentimento não se considerará preenchido enquanto for precedido apenas pela indicação de uma finalidade vaga e genérica. Por maioria de razão, este requisito haverá de integrar necessariamente um direito de controlo por parte do titular dos dados, no sentido de que este terá o direito de remover, atualizar ou retificar os dados. Finalmente, como corolário de um princípio de lealdade, os dados devem ser mantidos corretos, precisos e serem utilizados de acordo com a finalidade que foi invocada no momento da recolha, de um modo seguro e confidencial[33]. E sempre que a finalidade que preside à utilização seja alterada, necessário se tornará um novo consentimento do titular[34].

Este requisito de um consentimento livre e expresso tem de estar em permanente relação com os princípios reconhecidos pela lei e pela doutrina para a permissão do tratamento de dados pessoais: em primeiro lugar, um princípio geral de transparência, o que quer dizer que a pessoa responsável pelo tratamento dos dados tem que estar claramente identificada, tendo que informar também claramente o titular dos dados sobre as finalidades e prazos para o tratamento e conservação dos dados ou sobre a sua comunicação a terceiros. Para além disto, este princípio de transparência claramente implica a existência de um direito à informação e de um direito de acesso aos dados (que tem que ser assegurado ao titular dos dados) e, sempre

---

[31] -- devendo, no caso dos dados sensíveis, ser necessariamente expressa. Catarina Sarmento e Castro, citado, pág. 206. A exteriorização da vontade "será livre se manifestada sem a intervenção de qualquer tipo de coação, direta ou indireta; será específica se concreta e precisa, afastando, deste modo, qualquer tipo de manifestação de vontade implícita. Será informada quando o titular dos dados esteja ao corrente dos efeitos que derivam da sua manifestação de vontade", Catarina Sarmento e Castro, citado, págs. 261-262.

[32] -- cfr. Catarina Sarmento e Castro, citado, pág. 207. Refere esta autora a necessidade de o consentimento ser "expressão de uma manifestação de vontade específica...dado em função de um período temporal restrito, e para finalidade e circunstâncias conhecidas antecipadamente". Cfr. ainda Helena Moniz "Notas sobre a protecção de dados pessoais perante a informática – o caso especial dos dados pessoais relativos à saúde", in "Revista Portuguesa de Ciência Criminal", Ano 7, Fascículo 2º, Abril-Junho 1997, págs. 231-238.

[33] -- cfr. Carlos Ruiz Miguel, citado, pág. 57.

[34] -- cfr. Catarina Sarmento e Castro, citado, pág. 207.

que tal seja legalmente exigido, o cumprimento de obrigações de registo, autorização, notificação à Comissão Nacional de Proteção de Dados[35]. Também de enorme relevo é a obrigação de conformidade com o princípio da finalidade. O que quer dizer que os dados só podem ser usados de acordo com a finalidade que foi considerada no momento da sua recolha. E que esta finalidade há de ser determinada, explícita, legítima (não contrária à lei). Os objetivos precisos e concretos do tratamento dos dados têm que ser indicados e os dados não podem ser utilizados contrariamente à referida finalidade. Tudo isto considerado, poderemos afirmar que o consentimento tem que ser inequívoco e informado[36]. Mas deve ser sempre realçado que os princípios de proteção de dados têm que ser sempre aplicados[37].

Mas a consideração deste princípio de finalidade não pode ser dissociado de outro requisito extremamente importante a ser observado no tratamento e processamento de dados: os dados recolhidos têm que ser apenas os necessários e adequados atendendo à referida finalidade e o tratamento e processamento não podem exceder aquilo que é realmente necessário para a prossecução das referidas finalidades. Ou seja, tem que ser respeitado o princípio da proporcionalidade, entre os dados que são colhidos e a finalidade que presidiu à sua recolha[38]. Por outro lado, há que reconhecer que os critérios para apreciar a necessidade da recolha de dados hão de ser objetivos e de acordo com as finalidades expressas[39].

Não podemos esquecer aqui os direitos legalmente consagrados do titular dos dados: em primeiro lugar, o direito ao esquecimento e o direito a ser deixado sozinho[40]: os dados devem ser conservados apenas durante o período necessário de acordo com as finalidades da recolha e do tratamento (art. 5º nº 1 e) Lei 67/98). Bem entendido, há que estabelecer um prazo adequado para a conservação dos dados, de modo a evitar uma apropriação perpétua de aspectos muito vastos da vida pessoal do titular dos dados[41]. O que faz com que alguns autores expressamente refiram a necessidade de ser assegurada uma auto-determinação

---

[35] -- cfr. Catarina Sarmento e Castro, citado, pág. 229.

[36] -- cfr. Hert et al. citado.

[37] -- "the individual should always be informed of the presence of tags and readers, the purposes for which data are collected and processed, who is the responsible controller, whether the data (and what kind of data) are stored, the means to access and to rectify data, and whether the data will be made available to third parties", Hert et al. citado.

[38] -- cfr. Catarina Sarmento e Castro, citado, págs. 236-237.

[39] -- cfr. Catarina Sarmento e Castro, citado, págs. idem.

[40] -- cfr. Catarina Sarmento e Castro, citado, págs. 239-242.

[41] -- "perpetual appropriation of quite broad aspects of personal life", De la Cueva, M.D. & Lucas, P. "Informática e protección de datos personales", Centro de Estudios Constitucionales, 1993, pág. 69.

informativa[42] ou até um Direito à auto-determinação informacional[43]. Para que este direito seja considerado, necessária se torna a existência de um direito de acesso do titular aos dados (um direito de consulta que não necessita de ser justificado), mas sobretudo a existência de um direito de retificação e atualização dos dados e, com vista ao cumprimento de um verdadeiro controlo pelo titular, o direito à correção dos dados dentro de prazos determinados. Quer isto dizer que o titular dos dados deve ter o direito de verificar se os dados relativos à sua pessoa estão ou não corretos e, caso não estejam, deve ter o direito de retificação e atualização dos dados. Por outro lado, há que não esquecer que os dados não podem ser conservados para além do prazo necessário (ou do prazo fixado). Se os dados estão incorretos ou se são conservados para além do prazo limite, o titular tem o direito que os mesmos sejam eliminados ou, pelo menos, o acesso aos mesmos bloqueados[44].

Uma excepção ao requisito do consentimento livre e informado ocorrerá quando o titular dos dados estiver temporariamente impedido de expressar o consentimento (por estar em coma ou inconsciente) e, no entanto, o tratamento dos dados seja essencial para proteger interesses vitais do titular dos dados (art. 7º nº 3 a) Lei 67/98). Este poderá ser o caso de situações de monitorização de pessoas em coma ou em unidades de cuidados intensivos[45] (Castro 2005).

Uma outra excepção importante à proibição de tratamento de dados de saúde é a contemplada pelo artigo 7º nº 4 da Lei 67/98. De acordo com esta norma, o tratamento de dados de saúde (embora esse dados sejam sensíveis) será admitido quando necessário por razões de medicina preventiva, diagnóstico médico, cuidados e tratamentos médicos, desde que estes sejam assegurados por médico ou profissional de saúde sujeito a obrigação de sigilo e que a CNPD – Comissão Nacional de Proteção de Dados seja notificada e sejam contempladas as necessárias garantias de segurança da informação (Castro 2005). A Comissão Nacional de Proteção de Dados já veio, até, confirmar que as operações de telemedicina são consideradas como tratamento de dados para efeito do artigo 7º nº 4 da Lei 67/98 (Autorização nº 73/2000, publicada no ano 2000 pela CNPD). Este reconhecimento não deixa de constituir uma janela aberta para o desenvolvimento das possibilidades de intervenção da telemedicina, desde que os requisitos acima referidos sejam respeitados. De todo o modo, este tratamento de dados de saúde só será admissível quando efetuado por profissional de saúde ou por outro profissional sob obrigação de sigilo. E, de todo o modo, os dados relativos à saúde, vida sexual ou dados

[42] -- "Recht auf informationelle Selbstbestimmung", cfr. Catarina Sarmento e Castro, citado, págs. 24-29.
[43] -- cfr. Rouvroy et al. 2009, citado.
[44] -- cfr. Catarina Sarmento e Castro, citado, pág. 251.
[45] -- cfr. Catarina Sarmento e Castro, citado, pág. 222.

genéticos terão que estar logicamente separados dos outros dados pessoais, nos termos do previsto no art. 15º nº 3 da Lei 67/98[46].

Mas, mesmo considerando que a recolha e tratamento destes dados podem ser não apenas admissíveis como até altamente benéficos para o titular dos dados, não se deve esquecer a necessária obrigação de observância de princípios fundamentais no domínio do tratamento de dados pessoais, sobretudo os relativos ao princípio da finalidade da recolha e tratamento dos dados: a finalidade terá que ser previamente conhecida, tem que ser legal e legítima, e a utilização dos dados tem que respeitar tal finalidade.

Algumas dificuldades podem decorrer da necessária consideração dos direitos fundamentais do titular dos dados, sobretudo no que se refere ao direito ao esquecimento ou ao direito a ser deixado só, significando que os dados só podem ser conservados enquanto tal for necessário, atendendo às finalidades que presidiram à recolha e tratamento dos dados. Em Portugal, a Comissão Nacional de Protecção de Dados determinará os prazos de utilização dos dados, de acordo com as finalidades do tratamento. No final do prazo, os dados devem ser eliminados, assim se assegurando o direito ao esquecimento do titular dos dados (embora a CNPD possa autorizar a conservação dos dados para finalidades científicas ou de mera estatística)[47]. Outro importante direito do titular dos dados que deve ser referido é o direito a que os dados sejam eliminados ou o acesso a estes seja bloqueado, quando os dados não estejam atualizados ou sejam conservados para lá do prazo limite fixado (art. 5º nº 1 c) e art. 11º nº 1 d) da Lei nº 67/98). Por outro lado, deve ficar claro que o titular dos dados deve sempre ser informado sobre a presença de etiquetas e leitores, sobre as finalidades para as quais os dados são recolhidos e processados, sobre quem é o responsável pelo controle, se os dados (e que dados) são armazenados, sobre os meios para acesso e retificação dos dados, e se os dados serão disponibilizados a terceiros[48]. Por fim, claro está que o titular dos dados tem assegurado, nos termos do artigo 12º da Lei nº 67/98, o chamado "direito de oposição"[49]

Em resumo, há que salientar que a Diretiva 95/46/CE expressamente refere importantes requisitos relativos à qualidade dos dados, salientando que estes devem ser:

a) Processados de modo leal e legal;

---

[46] -- cfr. Catarina Sarmento e Castro, citado, pág. 92.
[47] -- cfr. Catarina Sarmento e Castro, citado, pág. 251.
[48] -- cfr. Hert et al. citado.
[49] -- "faculdade concedida ao titular de se opor ao tratamento dos seus dados pessoais, com base em razões ponderosas e legítimas relacionadas com a sua situação particular", Catarina Sarmento e Castro, citado, pág. 254.

b) Recolhidos para finalidades específicas, explícitas e legítimas, e nunca de modo incompatível com essas finalidades;
c) Adequados, relevantes e não excessivos, com relação às finalidades para as quais foram recolhidos e processados;
d) Precisos, corretos e, sempre que necessário, atualizados; todas as medidas razoáveis devem ser tomadas para assegurar que dados incorretos ou incompletos, atendendo às finalidades para que foram recolhidos ou processados, sejam corrigidos ou apagados.
e) Mantidos de modo a que permitam a identificação dos titulares dos dados apenas pelo tempo necessário à prossecução das finalidades que presidiram à recolha ou processamento dos dados.

No domínio da proteção de dados, a principal preocupação prende-se com o controlo que cada indivíduo terá (ou não) sobre os seus próprios dados, considerando-se para tal tanto a lei como a tecnologia, sobretudo as chamadas tecnologias indutoras de transparência[50]. Neste sentido, reveste-se de primordial importância um direito a que alguma doutrina se vem referindo ultimamente, tendo em vista o integral cumprimento dos requisitos do direito à auto-determinação informativa: trata-se do direito que cada indivíduo tem a não ser sujeito a decisões individuais automatizadas tomadas apenas por sistemas aplicativos[51].

As preocupações jurídicas aqui deixadas relacionam-se com a necessária regulação da transmissão de dados pessoais (e sua proteção) através dos vários serviços do Igenda. A questão é que sistemas orientados à pessoa que utilizam informação sensível sobre o utilizador não sejam pura e simplesmente proibidos com base em razões legais ou de uma exagerada invocação de direitos de protecção da pessoa e dos direitos humanos. O que se torna vital é a protecção do utilizador e dos dados que fluem no sistema, de modo a que o utilizador possa beneficiar dos serviços disponibilizados sem deixar de estar, ao mesmo tempo, legalmente protegido.

[50] -- ou “Transparency Enhancing Technologies”, cfr. Hert et al. citado.
[51] -- cfr. Catarina Sarmento e Castro, citado, pág. 251-253.

CONCLUSÕES E DESAFIOS

O progressivo envelhecimento da população nas sociedades actuais requer novos tipos de intervenção e de prestação de serviços aos idosos. Novas aplicações têm surgido de modo a que alguns desses serviços possam ser disponibilizados em casa do idoso (ou do paciente) libertando estes da necessidade de permanência em unidades hospitalares. Mas, uma resposta neste domínio adequada às necessidades dos utilizadores implicará uma elevada utilização de dados e informação pessoal, incluindo a criação e gestão de perfis de utilizador, de modo a alimentar o sistema com a informação e conhecimento necessários à intervenção proativa do sistema na calendarização de eventos e atividades em que o idoso possa participar. Por outro lado, a prestação de cuidados de saúde frequentemente requer que dados pessoais e sensíveis sejam armazenados em sistemas de informação, disponibilizados aos profissionais médicos e paramédicos e até a outros utilizadores (como será o caso dos familiares). No ordenamento jurídico português, o processamento de dados da saúde (considerados dados sensíveis) pode ser admitido quando necessário para cuidados preventivos, diagnóstico e tratamento médico, desde que assegurados por médico ou profissional de saúde sujeitos a obrigação de sigilo. Neste contexto, poderão ser enquadradas as operações de telemedicina, o que constituirá uma janela aberta para um aproveitamento das possibilidades oferecidas por este novo método de intervenção clínica, desde que sejam respeitados os requisitos legalmente exigidos. Poderá haver aqui possibilidades de proceder à monitorização e à criação de perfis de utilizador de acordo com os requisitos legalmente exigidos. Torna-se, no entanto, necessária uma constante focalização nos direitos do titular dos dados numa perspectiva de plena garantia do exercício do direito à auto-determinação informativa. Para tanto, deve ser exigida uma permanente cooperação e participação do utilizador, com a única excepção admissível das situações em que este não esteja em condições de prestar o seu consentimento livre e esclarecido (por exemplo, por estar inconsciente ou em coma) e o tratamento dos dados pessoais seja absolutamente necessário para proteger interesses vitais do titular dos dados.

Apesar de podermos admitir que estes sistemas possam respeitar os requisitos legais relativamente aos direitos e garantias dos titulares dos dados, há que reconhecer sempre os riscos daquilo que hoje poderíamos classificar de "dataveillance"[52] (ou vigilância a partir dos

[52] -- Cfr. Clarke, R. "Information Technology and Dataveillance", in "Communications of the ACM", 1988, 31 (5), págs. 498-512 "the massive collection, aggregation and algorithmic analysis of data on everyone and everything", "and of profiling, allowing the gathering of

dados). Por outro lado, há também que distinguir entre requisitos atinentes à privacidade e requisitos atinentes à proteção de dados, bem como entre garantias de opacidade e garantias de transparência[53]. Assim sendo, importante se torna perceber que não é suficiente a consagração legal de direitos; torna-se ainda necessário assegurar a efetividade destes. E aqui haverá que reconhecer também o importante papel que poderá desempenhar a tecnologia a este respeito[54]. Será assim interessante observar que se a tecnologia, por um lado, comporta inúmeras ameaças ao direito à privacidade e à proteção de dados, por outro lado poderemo-nos questionar legitimamente se a mesma tecnologia não poderá ser considerada como uma parte da solução dos problemas, ao potenciar ela própria uma utilização conforme com os requisitos legais em termos de privacidade e proteção de dados[55].

---

data and construction of knowledge about citizen-consumers in order to achieve certain purposes", Hert et. al. citado.

[53] -- Hert et al. citado.

[54] -- "privacy-enhancing technologies and transparency-enhancing technologies", Hert et al. citado.

[55] -- "Just as technical standards make networked communications possible, increasing the risk that data may be processed without regard to the requirements of data protection law, they may also lower the cost of compliance with data protection laws and increase access to privacy-enhancing technologies", Jane Winn, "Technical Standards as Data Protection Regulations", in "Reinventing Data Protection?", Springer, 2009, págs. 191-206.