Privacidade dos dados em ambientes de interoperabilidade – a área da saúde

Secundino Domingos Marques Lopes

Tese apresentada à Universidade de Évora
para obtenção do Grau de Doutor em Gestão

ORIENTADOR: *Professor Doutor. Rui Filipe Cerqueira Quaresma*

ÉVORA, FEVEREIRO DE 2016

INSTITUTO DE INVESTIGAÇÃO E FORMAÇÃO AVANÇADA

À Fátima, Madalena e Tiago

Agradecimentos

Felizmente um percurso desta natureza não se faz sozinho, apesar dos muitos momentos de trabalho solitário. Foram muitas as pessoas que contribuíram para manter a motivação, a criatividade e o equilíbrio necessários a um percurso que sabíamos à partida que ia ser longo e difícil.

O apoio da família foi sem dúvida fundamental. Apesar de todo o esforço efetuado para retirar ao mínimo os tempos em família, nos momentos decisivos a prioridade teve que ser o estudo. Tenho orgulho na minha família, valeu a pena.

Um agradecimento muito especial ao orientador deste trabalho, Prof. Dr. Rui Quaresma, pelas suas capacidades únicas e imprescindíveis de orientação, objetividade, exigência e rigor. Nos momentos decisivos do percurso coube-lhe a tarefa de indicar o caminho a seguir. Sem a qualidade da sua orientação dificilmente teria sido possível terminar este estudo.

A colaboração e o apoio dos responsáveis do Instituto Politécnico de Portalegre, na conjugação do percurso de investigação com as tarefas diárias de docente na Escola Superior de Tecnologia e Gestão, foram sem dúvida importantes, através de todos os meios que me foram disponibilizados.

Um agradecimento também muito especial aos responsáveis da SPMS, e de todas as unidades de saúde abrangidas pelo estudo, sem os quais não teria sido possível operacionalizar o mesmo.

Por fim, um obrigado a todos os amigos e colegas de trabalho pelo seu incentivo constante.

Resumo

A partilha de dados entre organizações através de iniciativas de interoperabilidade entre múltiplos sistemas de informação é fundamental à colaboração e integração de serviços, à agilidade das organizações e ao aumento na disponibilidade e qualidade da informação. Sistemas que inicialmente foram construídos para funcionarem de forma isolada, por diversos fatores evoluem para uma situação em que a sua sobrevivência depende da interoperabilidade com outros sistemas, mesmo que tecnologicamente heterogéneos. Contudo, ao nível dos dados, o aumento considerável na intensidade de utilização e na sua exposição a riscos adicionais, assim como a perda do controlo e de rastreabilidade sobre a sua utilização, impõem uma atenção especial para com as questões relacionadas com a privacidade, a proteção e a segurança destes dados.

Para a área da saúde, onde a partilha de dados de saúde é hoje uma realidade a nível nacional, a privacidade dos dados é uma questão central, que carece de soluções, de acordo com o nível de interoperabilidade acordado entre as organizações. Este contexto está na base da decisão de estudar os fatores com influência sobre a privacidade dos dados num contexto de interoperabilidade na área da saúde (promovido pela implementação da Plataforma de Dados da Saúde), através de uma investigação qualitativa e interpretativa, com base no método de *estudo de caso*. No sentido de compreender a evolução destes fatores de acordo com o nível de interoperabilidade a implementar, é utilizado um modelo de maturidade de interoperabilidade, numa perspetiva organizacional.

Os resultados finais da investigação permitiram identificar, compreender e validar com sucesso dez subdomínios de fatores com influência sobre privacidade dos dados em contextos de interoperabilidade, que devem estar na origem do desenvolvimento de um programa conjunto de proteção, orientado para as questões associadas à privacidade dos dados.

Palavras-chave: privacidade dos dados, interoperabilidade, área da saúde, PDS.

Abstract

Data privacy in interoperability contexts – the area of health

Data sharing among organizations through interoperability initiatives among multiple information systems is fundamental to the collaboration and integration of services, to the agility of organizations and to increase the availability and quality of information. Systems originally built to operate isolatedly have evolved, for different reasons, into a situation where in which their survival depends on the interoperability with other systems, even if technologically heterogeneous. However, in terms of data, the considerable increase in the intensity of its use and its exposure to additional risks, as well as the loss of control and traceability of its use, require a special attention to issues related to privacy, protection and security of these data.

For the health sector, where the sharing of health data is nowadays a reality at national level, data privacy is a central issue, which needs solutions according to the agreed level of interoperability among organizations. This context led the authors to study the factors with influence on data privacy in a context of interoperability in the healthcare sector (promoted by the implementation of the Health Data Platform), through a qualitative and interpretative research, based on the method of case study. In order to understand the evolution of these factors in terms of the level of interoperability to implement, an interoperability maturity model is used, in an organizational perspective.

The final results of the research made it possible to successfully identify, understand and validate 10 subdomains of factors with influence on data privacy in interoperability contexts, which should be the basis for the development of a joint protection program, targeted at issues associated with data privacy.

Keywords: data privacy, interoperability, health sector, PDS.

Índice

Índice de Figuras

Índice de Tabelas

Índice de Gráficos

Lista de Abreviaturas e Siglas

ACSS - Administração Central do Sistema de Saúde

AMA - Agência para a Modernização Administrativa

CE – Comissão Europeia

C2 - Command and Control

C2S - Command and Control Support

CEN - European Committee for Standardization

CIC - Comissão para a Informatização Clínica

CNPD – Comissão Nacional de Proteção de Dados

CNPDPI – Comissão Nacional de Proteção de Dados Pessoais Informatizados

CPO - Chief Privacy Officer

CPR - Computerized Patient Record

DDRS - Defense Data Repository System

DoD - Departamento da Defesa dos EUA

DoD IRDS - DoD Information Resource Dictionary System

DSTO - Australian Defence Science and Technology Organization

EHR - Electronic Health Record

EIF - Framework de Interoperabilidade Europeia

EMR - Electronic Medical Record

ENISA - European Union Agency for Network and Information Security

epSOS - Smart Open Services for European Patients

FEUP - Faculdade de Engenharia do Porto

GIG - Global Information Grid

HES - Hospital do Espírito Santo E.P.E

HFF - Hospital Professor Doutor Fernando Fonseca E.P.E.

HITSP - Healthcare Information Technology Standards Panel

HL 7- Health Level 7

IAM - Interoperability Assessment Methodology

IAPP - International Association of Privacy Professionals

ICO - Information Commissioner's Office

INEM - Instituto Nacional de Emergência Médica

i-Score - The Layered Interoperability Score

LCI - Layers of Coalition Interoperability

LCIM - Levels of Conceptual Interoperability Model

LISI - Levels of Information System Interoperability

M&S - Modelação e simulação

MCISI - Military Communications and Information Systems Interoperability

NMI - NATO C3 Technical Architecture Reference Model for Interoperability

OASIS - Advancement of Structured Information Standards

OCDE - Organização para a Cooperação e Desenvolvimento Económico

OECD - Organization for Economic Cooperation and Development

OIAM Organizational Interoperability Agility Model

OIM - Organizational Interoperability Maturity Model for C2

PbD - Privacy by Design

PDS - Plataforma de Dados da Saúde

PIA - Privacy Impact Assessment

PIAF - Privacy Impact Assessment Framework

QoIM - Quantification of Interoperability Methodology

RALC - Restricted Access/Limited Control

RIS - Rede de Informação da Saúde

SAML - Security Assertion Markup Language

SGBD - Sistemas de Gestão de Bases de Dados

SI – Sistema(s) de Informação

SIC - Sistemas de Informação e Comunicação

SNS - Serviço Nacional de Saúde

SoIM - Spectrum of Interoperability Model

SoSI - System-of-Systems Interoperability Model

SPMS – Serviços Partilhados do Ministério da Saúde

SSO - Single Sign-ON

TI – Tecnologias de Informação

TIC – Tecnologias de Informação e Comunicação

UE – União Europeia

ULSNA - Unidade Local de Saúde do Norte Alentejano

UML – Unified Modeling Language

USF – Unidade de Saúde Familiar

WAN - Wide Area Network

XML - Extensible Markup Language

XSPA - Cross-Enterprise Security and Privacy Authorization

Capítulo I - Introdução

A Internet alterou e introduziu mudanças profundas nos sistemas, no sentido em que as decisões dependem em tempo real dos dados, informação ou conhecimento, disponíveis noutro sistema (Winters, Gorman, & Tolk, 2006). Como grande parte da sua arquitetura são dados, estes constituem a força vital da *era da informação*, sendo de assinalar que grande parte destes são dados pessoais.

A interoperabilidade e a cooperação podem ser consideradas como facilitadores da integração de serviços e de organizações. Um pré-requisito, ou mesmo o "objetivo final" para qualquer sistema integrado ou de colaboração, é a *partilha de informações ou dados* (Otjacques, Hitzelberger, & Feltz, 2007). Não se trata apenas de movimentar os dados de modo contextualizado, mas também fazê-lo com segurança, qualidade de serviço, e permitindo uma experiencia de utilização na apresentação e atuação ou navegação sobre os dados apresentados, uniforme, evitando ao utilizador confrontar-se com vários interfaces aplicativos distintos (APDSI, 2013). Contudo, uma maior interoperabilidade traz consigo alguns inconvenientes. A possibilidade de, em determinadas situações, a interoperabilidade poder reduzir a privacidade individual está entre as preocupações mais apontadas à interoperabilidade. O aumento dos níveis de interoperabilidade pode aumentar o número de utilizadores que podem plausivelmente ter acesso a dados pessoais, partilhados através de sistemas interoperáveis (Gasser & Palfrey, 2007). Esta partilha deve acontecer num ambiente seguro e de proteção da privacidade destes dados, sendo necessário garantir que a velocidade destas inovações não apresenta efeitos colaterais negativos em matéria de segurança e privacidade (ENISA, 2011).

A importância da privacidade nas sociedades contemporâneas globalizadas e de informação, tem sido amplamente discutida e é hoje inquestionável. O trabalho realizado em diversas áreas tem melhorado imenso a nossa compreensão da privacidade ao nível individual, organizacional e social (Xu, Dinev, Smith, & Hart, 2008). No setor da saúde a privacidade é particularmente importante, devido à sensibilidade, potencial ou real dos dados clínicos (NETHA, 2006); neste setor, a utilização de grandes quantidades de dados, acedidos cada vez mais por um número maior de profissionais, coloca um enorme desafio à sua segurança e privacidade (Ernst & Young, 2012b). Este facto limita inclusive o livre fluxo de dados, por preocupações com a sua privacidade (Otjacques et al., 2007; Gottschalk, 2009a).

A problemática da privacidade é uma realidade complexa e subjetiva. Organizações com iniciativas de interoperabilidade em curso, nomeadamente do setor da saúde, resolvem com facilidade os requisitos técnicos e de sistemas, para que de uma forma ágil os dados possam fluir. O mesmo não acontece com as questões da proteção de dados e da privacidade de dados. Frequentemente, a privacidade não é incorporada nos sistemas e tecnologias de processamento de dados, nem os níveis superiores de gestão, em geral, estão suficientemente conscientes deste problema (Art. 29 WP, 2009). A investigação em novas ferramentas de proteção da privacidade dos dados é tão importante quanto o aumento na quantidade e técnicas mais sofisticadas de recolha de dados sobre indivíduos. Nunca foi tão importante e desafiador proteger a privacidade, face à proliferação de informações pessoais na Internet e ao crescente poder analítico que as instituições têm disponível (Weitzner et al., 2008).

Este estudo centra-se na dimensão da privacidade dos dados, com o objetivo de identificar os fatores críticos que influenciam a sua proteção em contextos de interoperabilidade entre sistemas sociotécnicos. Não se pretende identificar e solucionar problemas técnicos de interoperabilidade, mas sim contribuir para o conhecimento da problemática da privacidade, para que através da colaboração necessária entre organizações, possam ser implementadas medidas de proteção adequadas ao ambiente de partilha de dados.

Uma proteção completa da privacidade dos dados só será uma realidade quando tivermos medidas efetivas de proteção aplicadas e monitorizadas num processo contínuo de melhorias, aos dados, aos processos e às pessoas. E aqui está a maior das dificuldades – saber por onde começar, o que contemplar, como aplicar, assim como o que depende da iniciativa individual ou conjunta com outras organizações. A dificuldade de visualizar os riscos e o seu impacto sobre a organização, dificulta a afetação de meios e recursos ao desenvolvimento de um programa de proteção de dados.

Esta lacuna no domínio dos sistemas de informação (SI) justifica a necessidade de realização de uma investigação para identificar e compreender os fatores com influência sobre a privacidade dos dados em contextos de interoperabilidade.

1.1 Enquadramento

> "*A privacidade está para a era da informação como o ambiente esteve para a era industrial. O impacto da utilização indevida de dados é semelhante à má utilização dos recursos ambientais no início da era industrial. E nós vamos pagar um custo elevado, se não fizermos nada agora …*". (Bamberger & Mulligan, 2011, p.14).

O desenvolvimento de projetos que envolvem dados pessoais ou tecnologias intrusivas para a privacidade da pessoa, inevitavelmente dão lugar a preocupações com a privacidade. O efeito nefasto de muitas destas iniciativas durante as últimas décadas resultou em danos na confiança pública e na reputação das organizações (ICO, 2009). A privacidade de dados refere-se à evolução do relacionamento entre a tecnologia e o direito legal de, ou expectativa pública de, privacidade na recolha, armazenamento, tratamento e partilha de dados (Jericho Forum, 2007b). Este relacionamento é frequentemente questionado/desafiado pelo ambiente dinâmico, complexo, crescente e global de informação (Hunton & Williams, 2009). Existem problemas de privacidade de dados sempre que dados identificáveis relativos a uma ou mais pessoas são recolhidos e armazenados, em formato digital ou noutro suporte (Jericho Forum, 2007b). Estamos coletivamente a criar, utilizar, transmitir e armazenar dados pessoais a uma taxa de crescimento quase exponencial, com as ameaças à privacidade a espalharam-se a uma ampla gama de indústrias e organizações, e a atravessarem ilimitadamente através de fronteiras jurisdicionais (Cavoukian, 2009). A informação que é recolhida para um determinado propósito legítimo é cada vez mais utilizada em propósitos completamente diferentes, e às vezes incompatíveis, e este problema apresenta uma tendência de crescimento (Art. 29 WP, 2009). Para muitas organizações que dependem de dados pessoais, a privacidade tornou-se um fator estratégico (ICO, 2009).

Durante a última década, mudanças significativas na abordagem à privacidade têm aumentado a tensão entre indivíduos e organizações, com consequências na redefinição do conceito de gestão da privacidade[1] e a redefinição do conceito de invasão da privacidade face à evolução tecnológica (Ernst & Young, 2012b). Por

[1] A fraude, a economia global e a legislação, são os três principais fatores apontados com influência na forma como as organizações a nível global gerem a privacidade de dados pessoais.

exemplo, as preocupações relacionadas com a privacidade são a causa mais frequente de abandono das redes sociais, segundo um estudo de Stieger et al. (2013). O efeito que as tecnologias de informação apresentam para a privacidade pessoal, pode, segundo Tavani (2008), ser analisado com base na *quantidade* e no *tipo* de dados pessoais que podem ser recolhidos, na *velocidade* com que os dados pessoais podem ser partilhados e, no *tempo* de duração de retenção dos dados. A nível global, os reguladores procuram responder ao ritmo de mudanças que exigem mais proteção da privacidade. Mas para cada passo que dão em frente, a tecnologia parece, no mínimo, dar dois. A tecnologia está a evoluir a um ritmo tal que os principais reguladores não conseguem acompanhar (Ernst & Young, 2013). Muitas leis são reativas e ultrapassadas no momento em que são promulgadas, não conseguindo acompanhar a evolução das tecnologias e os novos modelos de negócios (Culnan, 2011).

Quando a Diretiva 95/46/CE (CE, 1995) foi adotada, o contexto do tratamento de dados ainda era relativamente claro e simples, ao contrário do contexto atual, devido à tendência crescente no sentido da diferenciação organizacional na maioria dos setores relevantes, em que se aposta cada vez mais na criação de cadeias de prestação de serviços ou numa prestação de serviços que envolve várias organizações e no recurso à subcontratação ou externalização de serviços, a fim de beneficiar de especialização e de possíveis economias de escala (Art. 29 WP, 2010a).

Embora as regras de proteção de dados sejam relativamente bem reconhecidas na União Europeia (UE), a dinâmica da era da informação está a provocar uma distância entre a lei e as práticas de negócios no mundo digital (Cleff, 2007). A proteção de dados tem de passar da "teoria à prática". Os requisitos jurídicos têm de ser traduzidos em medidas reais de proteção dos dados. O quadro jurídico da UE em matéria de proteção de dados necessita de mecanismos adicionais para incentivar a proteção de dados na prática (Art. 29 WP, 2010b).

A violação dos dados pessoais pode, se não forem adotadas medidas adequadas e oportunas, dar origem a prejuízos económicos e sociais substanciais, nomeadamente através da usurpação de identidade, danos físicos, humilhação ou danos significativos para a reputação da pessoa em causa (GDPR, 2012). Apesar do conteúdo de um novo regulamento geral para a proteção de dados (GDPR, 2012) ainda estar em discussão no seio da UE, é essencial que as empresas e organizações coloquem a privacidade e

proteção de dados pessoais na sua agenda. Este é seguramente um investimento que compensará (APDSI, 2014).

Ao longo do tempo as instituições de saúde foram sentindo a necessidade de olhar para os SI como um suporte à sua atividade diária, quer em termos clínicos, quer administrativos, ou contabilísticos. Esta necessidade foi sentida em momentos diferentes, e as soluções encontradas foram sendo diferentes de instituição para instituição, permitindo-se o crescimento de uma realidade complexa e heterogénea (Reis, 2012). A nova era dos cuidados de saúde está centrada na gestão dos serviços de saúde, desenvolvendo estratégias para o equilíbrio simultâneo da qualidade e dos custos, promovendo o desenvolvimento da integração de sistemas que permitem o desenvolvimento da capacidade de colaboração na prestação de cuidados de saúde, de capacidades analíticas, e permitindo uma relação mais próxima do paciente com os serviços. Todas estas frentes só são verdadeiramente possíveis através do acesso a dados e a partilha de dados (Patrício & Brito, 2012). Os recentes avanços tecnológicos tornaram assim possível aos profissionais de saúde exportar e partilhar dados clínicos agregados eletronicamente, com outros profissionais de saúde e inclusive com os pacientes. Ainda recentemente, a capacidade de partilhar dados clínicos eletronicamente entre prestadores de cuidados de saúde estava limitada por questões de interoperabilidade (Kahn & Sheshadri, 2008).

Assistimos atualmente à construção de sistemas em que a sua sobrevivência depende precisamente do fator interoperabilidade com outro ou outros sistemas, numa colaboração traduzida na prática na partilha de dados e serviços entre sistemas heterogéneos (Tolk & Aaron, 2010). Sem o desenvolvimento da interoperabilidade, a adoção de tecnologias no domínio da saúde, irá apenas promover o desenvolvimento de silos de dados e informação, à semelhança do que acontece com os registos médicos em suporte papel (Appari & Johnson, 2010).

Para o ambiente distribuído que caracteriza os projetos de interoperabilidade entre SI, coloca-se assim o desafio de como conseguir acomodar e harmonizar os parâmetros de sensibilidade dos dados e os requisitos de segurança dos processos que são definidos e exigidos por cada um dos organismos envolvidos e, assim, construir um ambiente cooperativo de confiança entre todos eles (Fugini & Mezzanzanica, 2003). Apesar da sua importância, a interoperabilidade não deve ser abordada apenas como uma questão puramente técnica, considerando os riscos que

podem surgir da interligação dos sistemas, que podem ter um impacto profundo sobre a privacidade e a proteção de dados (Art. 29 WP, 2009). Os desafios de investigação em privacidade e segurança estão longe de ser resolvidos, especialmente os relacionados com a gestão dos dados, sendo necessárias soluções de apoio à definição, aplicação, monitorização e negociação de políticas entre organizações.

No setor da saúde, em particular, as quebras de segurança são um enorme desafio, dado que existem muitas situações em que os pacientes e os profissionais de saúde podem ser afetados (Ernst & Young, 2012b). Este é um ambiente complexo mas promissor, em que os profissionais de saúde são confrontados com novos desafios no sentido de protegerem o paciente, assim como novas abordagens que lhes permitam a utilização dos dados e a sua partilha para outros objetivos (investigação, auditorias, saúde pública) (CALLIOPE, 2009). Os recursos ubiquamente disponíveis de computação e de rede, existentes a nível mundial para a transmissão de todas as variedades de dados, vão-nos permitir considerar novos tipos de SI para os cuidados de saúde, incluindo novos tipos de vigilância da saúde, e também novas oportunidades para a análise de dados biométricos e de saúde (Haux, 2006).

As situações tradicionais de um conjunto relacionado de dados ser da única e exclusiva utilização de uma organização, estão a alterar-se face à evolução tecnológica que aumentou consideravelmente a disponibilidade e multiutilização destes dados ao exterior de uma organização. Neste processo de evolução, o valor associado aos dados conseguiu apenas desencadear preocupações e medidas concretas de segurança. A privacidade destes dados nunca foi uma prioridade.

Num ambiente de partilha de dados, como é o caso do domínio da saúde, tecnicamente complexo, é urgente uma interoperabilidade organizacional, que mantendo a autonomia de processos e de dados, promova a partilha de conhecimento e soluções, a sua utilização, no sentido de melhorar o funcionamento conjunto das organizações, através do alinhamento de procedimentos e práticas, orientados à privacidade dos dados.

A proteção da privacidade dos dados para o ambiente de colaboração depende desta dinâmica.

1.2 Problemática e motivação

Uma consulta à base de dados de doutoramentos realizados em Portugal, permite verificar que existem poucos estudos sobre o desenvolvimento de projetos de interoperabilidade e de proteção de dados na área dos SI. Pela dimensão e complexidade que estes dois temas apresentam, assim como pela sua importância no desenvolvimento de serviços públicos de qualidade, quer ao nível nacional quer ao nível europeu, considera-se que estes domínios merecem e devem ser objeto de estudo e de mais trabalhos de investigação.

A interoperabilidade entre SI, com estruturas e contextos organizacionais diferentes, apresenta-se como um processo longo e complexo. Em alguns domínios específicos, a interoperabilidade apresenta-se como o principal fator da eficiência operacional das organizações em causa, vital para uma "eficiência coletiva", nomeadamente para projetos em rede (IDABC, 2010).

Soares (2009, p.447) considerou a privacidade e a proteção de dados pessoais como um dos fatores com influência no processo de implementação de interoperabilidade entre SI na administração pública em Portugal, concluindo que a "*privacidade e proteção de dados é uma força cuja ponderação e consideração no decorrer de iniciativas de interoperabilidade é incontornável*".

Contudo, a atenção dada pelas organizações a estes assuntos está longe de ser a necessária e exigível, face à importância crescente dos dados e da sua privacidade para a organização. Este e outros fatores, contribuem para que a privacidade dos dados não faça parte da cultura e práticas das organizações, com consequências que, na maioria dos casos, só são visíveis com a danificação da sua reputação face à exposição não controlada de dados pessoais confidenciais.

A alteração desta situação passa por compreender a dinâmica e complexidade da privacidade dos dados, ao nível local de um SI e em simultâneo em contextos de partilha de dados e serviços com outros sistemas, e desenvolver ferramentas com base neste conhecimento que permitam o desenho e operacionalização de um programa de proteção para as questões da privacidade dos dados.

De acordo com os dados da PORDATA[2], o número de processos entrados na Comissão Nacional de Proteção de Dados (CNPD), a solicitar autorização para o tratamento de dados pessoais, era de 442 em 1996 (ainda antes da publicação da Lei nº 67/98 para a proteção de dados pessoais), e 13.504 em 2012. É um número representativo do aumento considerável das situações que envolvem a utilização e o armazenamento digital de dados pessoais em Portugal, e da necessidade crescente de existirem práticas de proteção de dados nas organizações.

Assim, associado ao domínio da interoperabilidade, pretende-se estudar as questões da privacidade dos dados, num contexto de informação sensível, na certeza de que a privacidade dos dados constitui uma barreira condicionante à sua implementação, e que necessita de ser estudada.

Existem em Portugal vários contextos de interoperabilidade no setor público, nomeadamente nas áreas da justiça, finanças, administração interna, ensino e saúde, em que a confidencialidade e também a privacidade dos dados são atualmente dois temas muito presentes. O acesso a algumas destas áreas e às suas organizações é contudo muito complexo, sendo que em algumas, a investigação só é viável, se partir do seu interior. A maior abertura para a realização deste estudo, face aos objetivos do mesmo, surgiu na área da saúde. Na área da saúde a partilha de dados pessoais e sensíveis é hoje uma realidade a nível nacional e europeu, e onde o risco para a privacidade dos dados é maior que em outras áreas, pelo que, apresentou-se como a oportunidade ideal e privilegiada para a realização deste estudo.

O conhecimento resultante deste estudo pode auxiliar as organizações no planeamento dos SI e no desenvolvimento e operacionalização de soluções para a proteção da privacidade dos dados, assim como na sua adaptação ao período de transição para um novo ambiente regulador de proteção de dados para todo o espaço europeu.

[2] Dados relacionados com o tema justiça e segurança, disponíveis e consultados em 7 de julho de 2015 no URL: http://www.pordata.pt/Portugal/Comiss%c3%a3o+Nacional+de+Protec%c3%a7%c3%a3o+de+Dados+processos+entrados++findos+e+pendentes-405.

1.3 Objetivos

A interoperabilidade entre SI é um fenómeno recente. Anteriormente os sistemas eram desenhados e desenvolvidos numa perspetiva intra-organizacional, não existindo intenção da sua integração com outros sistemas. A prestação de serviços públicos orientados para o cidadão, e a necessidade de reduzir as "ilhas" de informação, obrigaram a uma reorientação gradual dos sistemas, no sentido de partilharem dados e serviços.

A interoperabilidade criou assim condições para que os sistemas consigam hoje utilizar os dados de outro sistema, com a mesma facilidade com que utilizam os dados gerados localmente. É sem dúvida um requisito inquestionável, que no mínimo está a obrigar as organizações a repensarem a estratégia pretendida para os seus SI. Contudo, também está na base do aumento verificado na intensidade de utilização de dados e na sua maior exposição a riscos adicionais. Estas situações estão a colocar problemas às organizações, nomeadamente ao nível da privacidade dos dados. Se o desenvolvimento de um programa de proteção destinado ao interior das organizações já é uma tarefa complexa, o seu desenvolvimento concertado para o conjunto das organizações parece, à partida, uma tarefa impossível de atingir com o sucesso pretendido. O conhecimento científico resultante deste estudo pode assim diminuir a complexidade desta tarefa.

A partilha de dados e informação, mesmo que em suporte papel, apresentou-se sempre como um processo complexo quando a natureza da informação obriga a procedimentos de segurança que permitam assegurar a sua privacidade. Contudo, este requisito ganha outra dimensão quando se apresenta como um componente primordial e fundamental em ambientes de interoperabilidade, constituídos essencialmente por SI heterogéneos e cada vez mais com dimensão mundial.

A proteção e a privacidade dos dados são, como sabemos, um assunto sempre presente. Todos os dias o desenvolvimento tecnológico apresenta novas situações problemáticas para a utilização de dados no geral, e em particular para os dados pessoais. As organizações, especialmente as que dependem de dados pessoais para o seu normal funcionamento, como é o caso da área da saúde, vêem-se obrigadas a desenvolver e adaptar de uma forma contínua os seus programas de segurança, como forma de lidar com toda esta dinâmica. A segurança é, contudo, insuficiente para dar resposta à complexidade dos requisitos de proteção da privacidade.

As organizações, ao acordarem partilhar dados de uma forma contínua, necessitam de planear o desenvolvimento dos seus SI e acomodar níveis semelhantes e integrados de proteção destes dados. Neste sentido, consideramos como o objetivo principal para este trabalho de investigação, a ***identificação dos fatores com influência sobre a privacidade dos dados, em ambientes onde, por força da interoperabilidade estabelecida entre sistemas, estes são partilhados de uma forma estruturada e contínua***. A compreensão desta problemática requer um trabalho de investigação alinhado com um conjunto de objetivos específicos, que consideramos essenciais à orientação da investigação, nomeadamente:

a. A identificação e estudo dos principais fatores com influência sobre a dinâmica da privacidade dos dados em contextos de interoperabilidade entre sistemas sociotécnicos.

b. A seleção e utilização de um modelo de interoperabilidade, ferramenta essencial para lidar com a complexidade dos vários níveis de exigência de interoperabilidade entre sistemas, neste caso em relação às questões associadas à privacidade dos dados, e no apoio aos responsáveis pelos sistemas no planeamento da evolução da interoperabilidade com outros sistemas para níveis de maturidade superiores.

c. A validação dos fatores com influência sobre a privacidade dos dados identificados, através da recolha da opinião e experiência de várias categorias de profissionais, num cenário privilegiado para o estudo da privacidade dos dados, dada a sensibilidade dos dados utilizados e o ambiente de partilha de dados em desenvolvimento – a área da saúde.

d. Compreender em relação à privacidade dos dados para o contexto de interoperabilidade, por onde as organizações devem iniciar um programa de proteção, os componentes que este programa deve apresentar, e a interoperabilidade organizacional necessária ao desenvolvimento conjunto destes componentes.

1.4 Metodologia

A complexidade das questões da privacidade dos dados em ambientes de interoperabilidade está mais associada a questões organizacionais e culturais, do que a questões técnicas ou tecnológicas, apesar de estas apresentarem uma influência significativa sobre o controlo da utilização dos dados.

O desenvolvimento de ligações permanentes entre as organizações, que implicam a partilha de dados de uma forma estruturada, está a contribuir para que a complexidade da proteção dos dados aumente. As TI atuam como protetoras dos dados, garantido o cumprimento das regras existentes, mas em simultâneo facilitam o acesso aos dados e, consequentemente, aumentam os riscos de violação da sua privacidade. Apenas com o desenvolvimento de uma visão conjunta de todas as organizações, se pode garantir um ambiente confiável e seguro para processos de partilha de dados. Isolar a atitude das organizações não é solução, apenas contribuiria para o desenvolvimento de um contexto desequilibrado de proteção. Este é um problema transversal que exige uma maior responsabilidade das organizações.

Ao não existirem ainda profissionais nas organizações especializados e dedicados à questão da proteção dos dados, através dos quais se poderia estudar esta problemática, a utilização de um contexto real de partilha de dados entre organizações, que surgiu da interoperabilidade entre sistemas, e em que a privacidade dos dados é um requisito de primeira ordem, foi a solução encontrada para viabilizar a investigação.

Considerando os objetivos da investigação, e os condicionalismos existentes para a recolha de dados, decidiu-se optar pelo método *estudo de caso* no suporte à validação dos pressupostos previamente construídos e fundamentados da investigação, num contexto organizacional. Foi assim possível recolher dados que resultam da experiência e da opinião dos vários profissionais com responsabilidades sobre a proteção de dados, assim como estudar o trabalho das organizações em domínios como a segurança e a proteção de dados. O método *estudo de caso* permitiu desta forma a preparação e estruturação daquilo que se quer investigar, da fase de recolha dos dados, e da análise e apresentação dos resultados finais. É um estudo perfeitamente identificado com a perspetiva filosófica interpretativa, de abordagem qualitativa, como uma estratégia de investigação de estudos de caso.

1.5 Estrutura do trabalho

Além deste capítulo, este documento está organizado em mais cinco capítulos, os anexos e as referências bibliográficas.

Neste primeiro capítulo é enquadrado o estudo, e apresentados de forma sucinta a problemática em estudo e a motivação subjacente, os objetivos do estudo, a metodologia de investigação, e a estrutura da tese refletida neste documento.

A primeira fase do processo de revisão bibliográfica está na origem do Capítulo II, o qual apresenta para os dois temas principais deste estudo – a privacidade e a interoperabilidade – a sua base teórica, a sua relação, assim como os principais desafios que surgem para a privacidade dos dados num ambiente de interoperabilidade.

No Capítulo III, é apresentado o resultado da segunda fase da revisão da bibliografia, focada na privacidade dos dados, e que identificou e fundamentou dez subdomínios de fatores, que pensamos de forte influência sobre a privacidade dos dados, e que constituem os fundamentos teóricos do *estudo de caso* a construir.

No Capítulo IV, são apresentados e justificados o enquadramento filosófico para o estudo, a metodologia e método adotados, e os vários componentes do *estudo de caso* de suporte ao processo de investigação, nomeadamente o projeto de pesquisa (que inclui a questão de estudo, as proposições e respetivas variáveis dependentes, e a estratégia e método utilizado para análise dos dados), a operacionalização da recolha de dados, e o instrumento desenhado para proceder à análise dos dados.

O Capítulo V é dedicado na íntegra à apresentação dos resultados da investigação. A apresentação dos resultados finais é realizada em duas partes: na primeira são apresentados os resultados da análise dos dados ao nível das variáveis dependentes de cada proposição, e na segunda, os resultados ao nível da proposição. No final do capítulo consta a versão final da *framework* conceptual do estudo.

O último capítulo, o Capitulo VI, é dedicado às conclusões do processo de investigação, refletindo-se sobre os objetivos definidos para a investigação, e sobre as limitações surgidas na realização do estudo. São ainda sugeridas algumas propostas de oportunidades futuras de investigação no domínio da privacidade dos dados e da interoperabilidade entre sistemas.

Capítulo II – Privacidade e Interoperabilidade

O presente capítulo apresenta a revisão realizada sobre os dois temas que estão na base da problemática em estudo - a privacidade dos dados e a interoperabilidade.

Num primeiro momento, será enquadrado o conceito de privacidade dos dados, a sua relação com os conceitos de proteção e de segurança dos dados, assim como, e com base na legislação atual, apresentados os *princípios gerais de proteção de dados*, os *atores envolvidos*, os *direitos* e as *obrigações,* essenciais à compreensão deste conceito, e da sua importância em registos de saúde eletrónicos.

Num segundo momento, a atenção é dirigida para o conceito de interoperabilidade, para o seu estudo com base numa abordagem baseada num modelo de interoperabilidade, e no modelo de interoperabilidade selecionado para suporte ao estudo.

O capítulo termina com a apresentação dos principais desafios que surgem quando está em causa a necessidade de proteger a privacidade dos dados, sempre que partilhados através de um ambiente controlável de interoperabilidade.

2.1 Privacidade

2.1.1 O conceito de privacidade

A privacidade só se tornou uma questão social importante depois de 1960, com a atenção política que emergiu face a uma enorme expansão de ameaças (Clarke, 2009). Apesar do debate bastante intenso desde o final da década de 60, ainda não existe uma definição universalmente aceite de privacidade (Introna, 1997; Wuyts et al., 2009). Constitui atualmente um conceito abrangente, que engloba (entre outras coisas) a liberdade de pensamento, o controlo sobre o corpo, o controlo sobre informações pessoais, a liberdade de vigilância, a proteção da reputação de alguém, e proteção contra buscas e interrogatórios (Solove, 2008). Tem sido descrita como algo que pode ser "invadida", "violada", "quebrada", "perdida", "diminuída", e assim por diante (Tavani, 2007). As ideias fundamentais da privacidade são que ela envolve pessoas e informações (Wuyts et al., 2009). Para muitos académicos constitui um valor e um direito fundamental, ligada a ideias de autonomia, dignidade pessoal e

independência. É muitas vezes vista como condição necessária para separar aquilo que é pessoal do que é público (Waldo, Lin, & Millett, 2007).

Interpretada de forma mais ampla, a privacidade tem a ver com a integridade do indivíduo, e abrange todos os aspetos das suas necessidades sociais (Clarke, 2006). O objeto da privacidade pode ser uma pessoa, um grupo de pessoas, ou uma organização formal através da qual pessoas e grupos cooperam. Por exemplo, no contexto específico da colaboração interempresarial, podemos distinguir diferentes níveis de privacidade, como a privacidade das pessoas, da empresa, da colaboração e de todo o ecossistema de serviços (Moen, Ruohomaa, Viljanen, & Kutvonen, 2010).

Não surpreendentemente, a privacidade como conceito e como direito sofre mudanças constantes, mudanças a que temos que nos adaptar continuamente. Devemos preservar os ideais do passado e adaptarmo-nos a novos contextos nunca contemplados pelos autores das leis de privacidade (Cavoukian, 2009).

Atendendo à complexidade na definição de privacidade, bem como às questões ou dimensões envolvidas, autores como Introna (1997) e Clarke (2006) sugerem a sua definição com base em quatro categorias distintas, as quais não se excluem mutuamente, nomeadamente: a privacidade da pessoa, a privacidade do comportamento e da esfera pessoal, a privacidade nas comunicações pessoais, e a privacidade da informação pessoal.

> A *privacidade da pessoa*, por vezes referida como "privacidade corporal", diz respeito à integridade do corpo do indivíduo (Clarke, 2006). São os casos da vacinação obrigatória, transfusão de sangue sem o consentimento prévio, assim como a recolha de dados biométricos (ICO, 2009).
>
> A *privacidade do comportamento e da esfera pessoal* relaciona-se com o direito à não observação, utilização e invasão da atividade de um indivíduo ou do seu "espaço privado", relevante tanto em "espaços privados" como em "locais públicos" (Clarke, 2006; Introna, 1997). Relaciona-se com questões sensíveis, tais como as preferências e hábitos sexuais, atividades políticas e práticas religiosas (Clarke, 2006). Para Johnson (1989), a verdadeira questão da privacidade reside no julgamento da pessoa, por outros, ou seja, dos aspetos da vida pessoal culturalmente reconhecidos como imunes ao julgamento de outros. É o conhecimento sobre a pessoa através do qual outros a julgam de um modo particular, talvez com base em ideias e normas preconcebidas, que

faz com que exista o desejo individual de espaço pessoal e privado de imunidade (Introna & Pouloudi, 1999).

A *privacidade das comunicações pessoais*, relacionada com a liberdade de comunicação, através de vários meios, sem que estas sejam intercetadas por outras pessoas ou organizações (Clarke, 2006). São os casos da monitorização de caixas de correio eletrónico, o controlo de determinados tipos de tráfego no local de trabalho, a interceção telefónica, entre outras (ICO, 2009).

A *privacidade de dados pessoais*, referida muitas vezes como a "privacidade dos dados" e "privacidade das informações". Mesmo quando os seus dados são recolhidos por uma outra parte, o indivíduo deve ser capaz de exercer um significativo controlo sobre os seus dados e sobre a sua utilização (Clarke, 2006). A ideia de controlo sobre a distribuição de dados pessoais é determinante em situações em que é importante determinar se o direito à privacidade do indivíduo foi ou não violado (Introna, 1997).

Tavani (2008), com base na evolução do significado de privacidade, inicialmente entendida em termos de liberdade de intrusão (física), até à atualidade, em que a privacidade surge cada vez mais associada à preocupação constante sobre como proteger dados pessoais, distingue quatro tipos de privacidade: (1) privacidade como a não intrusão no espaço físico pessoal: *privacidade física/acessibilidade*; (2) privacidade como a não interferência nas escolhas individuais: *privacidade de decisão*; (3) privacidade como a não invasão/interferência no pensamento e identidade pessoal: *privacidade psicológica/mental*; e (4) privacidade como ter controlo sobre/limitar o acesso à informação pessoal: *privacidade informacional*[3].

Do ponto de vista da teoria ética, a privacidade é um valor curioso, afirma Moor (1997). Por um lado, parece ser algo de grande importância e a sua defesa é vital, e, por outro lado, a privacidade parece ser um assunto de preferência individual, relativa culturalmente, e no geral difícil de justificar. Tavani (2007) questiona mesmo, o que é, exatamente, a privacidade? Segundo este autor, ao ser de difícil definição, a privacidade é muitas vezes descrita como, ou confundida com noções como liberdade, autonomia, sigilo e solidão.

[3] A preocupação incide nos problemas de privacidade que surgem da quantidade de dados pessoais recolhidos e armazenados, da velocidade à qual os dados são transferidos e partilhados, e do período que dura a retenção destes dados.

Face à dificuldade de uma definição simples e global de privacidade, Introna (1997) identificou certos aspetos da privacidade, importantes à sua compreensão: (i) a privacidade é um conceito relacional, emerge numa comunidade quando as pessoas interagem; (ii) a privacidade visa o domínio pessoal; o que é considerado pessoal é, em certa medida, definido culturalmente. No geral pode-se afirmar que os aspetos pessoais ou privados são os aspetos que não afetam, ou tendem a não afetar, significativamente os interesses de outros; (iii) reivindicar privacidade significa reivindicar o direito de limitar ou controlar o acesso ao domínio pessoal ou privado da pessoa; (iv) o controlo da distribuição de imagens textuais ou informação verbal sobre uma pessoa constitui uma forma eficaz de controlar o acesso à sua esfera pessoal; (v) reivindicar privacidade significa reivindicar o direito ao domínio (pessoal) de imunidade contra o julgamento de outros; (vi) a privacidade é um conceito relativo. Uma privacidade total pode ser tão indesejável como uma total transparência. É uma questão de adequação à situação em causa. É, infelizmente ou felizmente, uma questão de julgamento (Moor, 1997).

2.1.2 Privacidade e proteção de dados

> "*O tratamento dos dados pessoais é concebido para servir as pessoas; os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais devem respeitar, portanto, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, particularmente o direito à proteção dos dados pessoais*" (RGPD, 2012, p.15).

O direito fundamental à proteção de dados pessoais baseia-se essencialmente no Artigo 8.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (Conselho da Europa, 1950) e no Artigo 8.º da Carta dos Direitos Fundamentais da UE (UE, 2010), que estabelece que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhe digam respeito (CNPD, 2012b). Mais especificamente, a Diretiva 95/46/CE relativa à proteção de dados (CE, 1995), a Diretiva 2002/58/CE sobre a privacidade e comunicações eletrónicas (CE, 2002) e as legislações nacionais dos Estados-Membros que implementam estas diretivas estabelecem regras mais precisas (Art. 29 WP, 2007a). A privacidade como

(enquanto) autodeterminação informativa foi adotada em quase todos os regulamentos e legislações de proteção de dados (Haas, Wohlgemuth, Echizen, Sonehara, & Müller, 2011).

A privacidade está relacionada com a capacidade do indivíduo em exercer um controlo sobre a recolha, utilização, divulgação e retenção dos seus dados pessoais, tendo por base necessariamente um aviso claro sobre que dados serão recolhidos e como serão utilizados e/ou partilhados (IPC, 2009). Em situações em que os seus dados pessoais estão na posse de terceiros, o seu titular deve ser capaz de exercer um grau significativo de controlo sobre os dados e sobre a sua utilização (ICO, 2009). A privacidade é desta forma um valor e um direito (Amicelle, 2012). A privacidade é o direito de uma entidade (normalmente uma pessoa), agindo em nome próprio, em determinar o grau em que irá interagir com o seu ambiente, incluindo o grau em que a entidade está disposta a partilhar informações sobre si mesma, com os outros (The Internet Society, 2000), ou seja, controlar a disponibilidade e exposição dos seus dados pessoais (Lilien & Bhargava, 2006).

Nos últimos 30 anos houve uma profunda mudança de escala no papel dos dados pessoais na nossa economia, sociedade e vida diária, devido às mudanças que surgiram causadas pelo aumento: (1) no *volume* dos dados pessoais recolhidos, utilizados e armazenados; (2) na *gama de análises* que envolvem dados pessoais, que fornecem uma perceção sobre tendências, movimentos, interesses e atividades individuais e de grupos; (3) nas *ameaças* à privacidade; (4) no número e variedade de *atores* capazes de colocar em risco a privacidade ou proteger a privacidade; (5) na *frequência e complexidade das interações* que envolvem dados pessoais; e (6) na *disponibilidade global* de dados pessoais, suportada por plataformas e redes de comunicação globais (OCDE, 2013).

A proteção de dados, como proteção jurídica específica, surgiu como resultado do enfraquecimento ou do desaparecimento de alguns limites naturais que anteriormente asseguravam a proteção da privacidade (Jóri, 2007). É, desta forma, um processo de natureza legal (Amicelle, 2012), e está relacionada com a garantia de que os dados não são corrompidos, são acessíveis apenas para fins autorizados, e está em conformidade com os requisitos legais aplicáveis (Dutch, 2010). A proteção de dados está, assim, relacionada com uma forma especial de privacidade – a privacidade informacional/privacidade de dados pessoais. Neste sentido, como

conceitos, privacidade e proteção de dados estão inequivocamente relacionados um com o outro (Amicelle, 2012).

É importante realçar que quase todos os dados, uma vez ligados a um indivíduo identificável, tornam-se dados pessoais. Assim, a definição de "privacidade" pode ser bastante mais abrangente, fazendo com que desafios à privacidade e à proteção de dados sejam igualmente mais amplos.

As preocupações legítimas sobre privacidade surgem quando a velocidade e conveniência levam à exposição indevida de informação (Moor, 1997). Sendo a informação capturada eletronicamente para uma finalidade, esta é "lubrificada" e fica pronta para qualquer outra finalidade. Num mundo informatizado podemos deixar pegadas eletrónicas em vários lugares, e os dados recolhidos para uma finalidade podem ser "ressuscitados" e usados noutro lugar. O problema da privacidade da informação consiste em manter uma vigilância adequada sobre onde esta informação pode e deve ir.

A segurança está normalmente associada à disponibilidade e resiliência dos sistemas e infraestruturas tecnológicas e, no domínio da informação, à garantia da sua confidencialidade e integridade. Envolve a aplicação e gestão de medidas de segurança adequadas, tendo por base o conhecimento de uma ampla gama de ameaças, com o objetivo de minimizar os impactos e garantir o sucesso e a continuidade de um processo de negócio sustentado (ISO/IEC, 2009). É, sem qualquer dúvida, um componente crítico de qualquer sistema informático, devendo fornecer as garantias necessárias à proteção dos dados, sendo que numa situação ideal deve ser desenvolvida como um serviço quase invisível, mas forte (Liberty Alliance, 2003).

No que respeita aos dados, o estudo das questões da sua privacidade não pode ser dissociado das questões associadas à proteção e à segurança destes dados. A Tabela 1 sintetiza esta relação. Apesar da temática em estudo ser a privacidade dos dados, esta determina que as outras duas dimensões, proteção e segurança, sejam igualmente abordadas, dada a sua influência sobre a eficácia das medidas ao nível da proteção da privacidade, assim como sobre a criação de um ambiente seguro de recolha e utilização de dados pessoais. Neste sentido, quando nos referimos à privacidade dos dados inclui-se implicitamente a proteção e a segurança dos dados.

Tabela 1 - Relação entre privacidade, proteção e segurança dos dados

Privacidade	• Focada no indivíduo ou grupo de indivíduos, e nos dados pessoais identificáveis, assim como no subconjunto de dados sensíveis. • Constitui uma reclamação, um direito de um individuo à proteção, ao controlo e à limitação de utilização, dos seus dados pessoais em situações normativas.
Proteção	• Focada no indivíduo, grupo de indivíduos ou organização. • É um meio, um instrumento legal, de garantia da privacidade. • Ajusta a compatibilidade dos processos de tratamento de dados com as finalidades para que foram recolhidos. • Serve para sustentar a proteção da privacidade num mundo onde a possibilidade de recolha, armazenamento e cruzamento de grandes conjuntos de dados está amplamente disponível.
Segurança	• É um meio de garantia da disponibilidade, confidencialidade, integridade, não-repúdio, e confiança dos dados. • Relacionada com as questões (técnicas) de segurança da informação e das infraestruturas de armazenamento e comunicação. • Capacidade de um sistema resistir a eventos acidentais ou a acessos maliciosos ou ilícitos que comprometem os dados.

Não devemos usar o termo privacidade dos dados como sinónimo de "confidencialidade dos dados" ou "serviço de confidencialidade dos dados", pois são conceitos diferentes. A privacidade é um motivo de segurança, e não um tipo de segurança. Por exemplo, um sistema que armazena dados pessoais tem que proteger os dados e impedir danos, constrangimentos, inconveniências ou injustiças a qualquer pessoa sobre a qual os dados são mantidos, e para proteger a privacidade da pessoa. Por esta razão, o sistema necessita de disponibilizar um serviço de confidencialidade dos dados (The Internet Society, 2000).

2.1.3 Legislação de suporte à privacidade e proteção de dados

As novas tecnologias, ao permitirem um acesso mais fácil e mais generalizado a dados pessoais do que as formas tradicionais de tratamento, levaram à aprovação das primeiras leis de proteção de dados (Art. 29 WP, 2007b). Nos anos 50, o Conselho da Europa reconheceu a privacidade como um direito fundamental. Foi definido no Artigo 8º da Convenção Europeia para a Proteção dos Direitos do Homem e Liberdades Fundamentais (Conselho da Europa, 1950), e estabeleceu que todas as pessoas têm direito ao respeito da sua vida privada e familiar, da sua casa e da sua

correspondência (Guarda & Zannone, 2009). Contudo, o direito à privacidade só é introduzido nas várias legislações Europeias muito mais tarde[4].

Os princípios de privacidade publicados pela Organização para a Cooperação e Desenvolvimento Económico (OCDE) em 1980 (OCDE, 1980) constituem a primeira *framework*[5] de privacidade amplamente usada, com influência sobre as leis de proteção de dados e da privacidade existentes e emergentes, assim como na criação dos principais programas práticos de privacidade e na definição de princípios adicionais (OCDE, 2013). Estes princípios foram adotados por vários países, quer explicitamente através de legislação própria, quer através de vários códigos éticos (Barker et al., 2009), destacando-se[6]: (1) o *U.S. Privacy Act*; (2) a *framework* de privacidade da *Asia-Pacific Economic Cooperation* (APEC); (3) o *Health Insurance Portability and Accountability Act – HIPAA*[7]; (4) o *Children's Online Privacy Protection Act*[8]; e (4) a Diretiva 95/46/CE (Breaux & Antón, 2008).

A proteção de dados foi introduzida no quadro jurídico da UE como um problema do mercado interno, através da Diretiva 95/46/CE baseada no Artigo 95/EC (Art. 29 WP, 2009), a qual constitui o bloco principal da legislação de proteção de dados na UE. Pretendeu-se com esta diretiva proteger o direito fundamental à proteção de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros (Otjacques et al., 2007). A Diretiva 2002/58/CE[9], a Decisão-Quadro

---

[4] Os primeiros casos surgem na Alemanha Ocidental na legislação da Assia (7 de outubro de 1970) e na Baviera (12 de outubro de 1970), e em seguida, uma lei federal sobre proteção de dados (Bundesdatenschutzgesetez, BDSG) em 1977. As legislações nacionais de vários países foram também alteradas como é o caso da Suécia (1973), França (1978), Luxemburgo (1979), Dinamarca (1979), Áustria (1980), Noruega (1980), Islândia (1982), Reino Unido (1984), Finlândia (1988), Holanda (1990), Portugal (1991), Espanha (1993), Bélgica (1993), e Suíça (1993). Além disso, países como Espanha, Portugal, Áustria, Holanda, Alemanha e Grécia alteraram a sua própria constituição onde incluíram cláusulas de privacidade (Guarda & Zannone, 2009).

[5] Em 11 de julho de 2013, o Conselho da OCDE adotou e publicou uma revisão desta *framework* com base na recomendação do *OECD Working Party on Information Security and Privacy* (WPISP, 2011) para revisão das diretrizes que regem a proteção da privacidade e fluxos transfronteiriços de dados pessoais.

[6] Mais informação sobre a legislação de proteção de dados, as definições associadas à proteção de dados e a identificação da autoridade local de proteção de dados, em relação a 63 jurisdições a nível mundial pode ser obtida na obra do grupo DLA Piper (2013).

[7] Informação detalhada sobre a legislação HIPAA pode ser consultada no URL: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[8] Informação detalhada no URL: http://www.coppa.org/comply.htm

[9] Relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas). Informação disponível do

2008/977/JHA[10], a Diretiva 2009/136/CE[11] (que altera a Diretiva 2002/22/CE, a Diretiva 2002/58/CE, e o Regulamento (CE) nº 2006/2004) constituem outros instrumentos legislativos importantes de proteção de dados (ENISA, 2011).

A Diretiva 95/46/CE constitui um regulamento de privacidade abrangente, em que a privacidade da informação está muito ligada ao conceito de proteção dos dados, aplicando os princípios da privacidade ao processamento de informações pessoais (ICO, 2008). Países como os EUA optaram por uma abordagem setorial, diferente da adotada pela UE, que se baseia numa mistura de legislação, regulamentação e autorregulamentação (Hamidovic, 2010).

As Diretivas da UE apenas definem princípios gerais, deixando que cada Estado-Membro implemente as suas medidas específicas nacionais (Guarda & Zannone, 2009). Em Portugal, a proteção de dados pessoais e da privacidade tem consagração constitucional desde 1976, e o legislador nacional optou por oferecer, na Lei de Proteção de Dados, um âmbito de proteção mais abrangente do que o prescrito pela Diretiva 95/46/CE, e no qual já se inclui o tratamento de dados policiais (CNPD, 2012b). Na Tabela 2 é possível identificar a legislação nacional que faz a transposição das diversas diretivas europeias que referimos.

Tabela 2 – Identificação da legislação nacional que faz a transposição das Diretivas Europeias

Diretiva UE	**Portugal**
Diretiva 95/46/CE	Lei 67/98
Diretiva 2002/58/CE	Lei 41/2004
Diretiva 2006/24/CE	Lei 32/2008
Diretiva 2009/136/CE	Lei 46/2012

site da Comissão Europeia dedicado à proteção de dados, consultado em 18.julho.2012. URL: http://ec.europa.eu/justice/data-protection/law/index_en.htm.

[10] Para a proteção de dados pessoais no âmbito da cooperação policial e judiciária em matéria penal (GDPR, 2012).

[11] 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 setor 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. Informação disponível do *site* da Comissão Europeia dedicado à proteção de dados, consultado em 18.julho.2012. URL: http://ec.europa.eu/justice/data-protection/law/index_en.htm.

Contudo, e apesar de os princípios e objetivos sobre os quais assenta o quadro jurídico atual continuarem a ser válidos, não foi possível evitar uma fragmentação na execução da proteção dos dados pessoais na UE (Eurobarometer, 2011), bem como a insegurança jurídica e o sentimento generalizado na opinião pública de que subsistem riscos significativos (GDPR, 2012). A harmonização inicial obtida pela Diretiva 95/46/CE tornou-se insuficiente (Costa & Poullet, 2012).

A Comissão Europeia está atualmente num processo de revisão[12] do quadro jurídico geral relativo à proteção dos dados pessoais com o objetivo: (1) de modernizar o sistema jurídico da UE para a proteção dos dados pessoais, em particular para fazer face aos desafios decorrentes da globalização e do uso das novas tecnologias; (2) de reforçar os direitos dos indivíduos e, ao mesmo tempo, reduzir as formalidades administrativas para garantir uma livre circulação de dados pessoais dentro e fora da UE; e (3) de melhorar a clareza e coerência das regras comunitárias de proteção de dados pessoais, e alcançar uma implementação e aplicação coerentes e eficazes do direito fundamental à proteção de dados pessoais em todas as áreas de atividade da UE. A proposta de regulamento em discussão será aplicada a qualquer processador de dados dentro da UE, incluindo qualquer organização fora da Europa que ofereça bens e serviços aos residentes da UE (Ernst & Young, 2013). As estruturas políticas enfrentam a este nível um enorme desafio, que vai exigir mudanças, no sentido de identificar soluções que permitam aplicar os princípios da privacidade a um mundo cada vez mais convergente, dada a aproximação entre o mundo virtual e o mundo real (Wright et al., 2009).

Apesar de se encontrar em discussão pública uma proposta de regulamento geral para a proteção de dados (GDPR, 2012) para todo o espaço europeu, ainda não aprovado, decidiu-se neste estudo pela sua consideração, tal são as alterações propostas com impacto sobre a problemática em estudo – a privacidade dos dados. Neste sentido, é importante um conhecimento sobre os princípios que atualmente

---

[12] A Comissão Europeia (CE), na sua Agenda Digital para a Europa, uma iniciativa da Estratégia da Europa 2020, identificou a revisão do quadro regulamentar da UE de proteção de dados, como ação essencial para uma maximização dos benefícios da utilização das TIC (ENISA, 2011). Em 9 de julho de 2009, a CE iniciou o processo de revisão do quadro jurídico geral relativo à proteção dos dados pessoais que deu origem a uma proposta de regulamento geral sobre a proteção de dados (GDPR, 2012), que se pretende substitua a Diretiva 95/46/CE, e que na opinião de Costa & Poullet (2012) pode constituir a solução adequada para assegurar uma harmonização da proteção de dados pessoais em todos os Estados-membros da UE. Informação consultada em 23.julho.2012 no URL: http://ec.europa.eu/justice/data-protection/review/index_en.htm

estabelecem como deve funcionar um processo de tratamento de dados, assim como é importante considerar as principais alterações que se preveem para breve através do novo regulamento de proteção de dados. O mesmo se aplica a atores, direitos e deveres associados.

Os regulamentos relativos à proteção de dados na UE foram vitais para a definição dos *princípios*, *atores, direitos e obrigações* associados ao conceito de proteção de dados, para todos os Estados-Membro da UE (Guarda & Zannone, 2009). Estes quatro elementos são fundamentais para o estudo da problemática da privacidade dos dados em contextos de interoperabilidade.

Princípios

A Diretiva 95/46/CE (CE, 1995) foi essencial ao definir os sete princípios gerais (identificados na Tabela 3) que orientaram o tratamento de dados pessoais até ao presente (ENISA, 2012). Seguem os princípios orientadores publicados pela OCDE, que já contemplavam a recolha limitada de dados, a garantia da qualidade dos dados, a especificação da finalidade do processo de recolha, a utilização limitada, as garantias de segurança, a transparência, a participação individual, e a responsabilidade do responsável pela recolha de dados pelo cumprimento destes princípios (Hamidovic, 2010).

Tabela 3 - Princípios associados ao tratamento de dados pessoais

Princípio	**Diretiva 95/46/CE**	**RGPD (2012)**
Tratamento lícito e equitativo	●	○
Limitação da finalidade	●	●
Minimização de dados	●	○
Qualidade da informação	●	●
Consentimento	●	○
Sensibilidade	●	●
Segurança do tratamento	●	○
Transparência	⊗	●
Responsabilidade	⊗	●

● - Existe

○ - Existe e foi melhorado

⊗ – Não existe

A recente proposta de regulamento geral para a proteção de dados (GDPR, 2012) acrescenta dois novos princípios para o tratamento de dados pessoais, a *transparência* e a *responsabilidade* global do responsável pelo tratamento, e

melhora os princípios do *tratamento lícito e equitativo*, da *minimização de dados,* do *consentimento* e da *segurança do tratamento* (GDPR, 2012).

> *Tratamento lícito e equitativo* – a recolha e tratamento de dados pessoais não devem intrometer-se injustificadamente na privacidade do titular dos dados, nem exageradamente intervir com a sua autonomia e integridade, devendo estar de acordo com o quadro jurídico global (Artigo 6.º da Diretiva 95/46/CE (CE, 1995); Artigo 5.º da Lei 67/98 (AR, 1998)). A proposta de regulamento (GDPR, 2012) melhora consideravelmente este princípio, ao propor no Artigo 6.º "*os critérios para um tratamento de dados lícito, que são melhor especificados quanto ao critério do equilíbrio de interesses e ao respeito das obrigações legais e de interesse público*".
>
> *Limitação da finalidade* – os dados pessoais serão recolhidos para finalidades determinadas, legais e legítimas, e não serão tratados de formas não compatíveis com estas finalidades (Artigo 6º da Diretiva 95/46/CE (CE, 1995); Artigo 5.º da Lei 67/98 (AR, 1998)). Só devem ser tratados se, e desde que as finalidades não puderem ser alcançadas através do tratamento de informações que não envolvam dados pessoais (GDPR, 2012).
>
> *Minimização de dados* – a recolha e tratamento de dados pessoais devem ser limitados ao mínimo necessário para se atingir um objetivo específico. Enquadra-se neste princípio a conservação dos dados pessoais[13], os quais serão retidos apenas durante o tempo necessário para que seja atingido o objetivo especificado (Artigo 6.º da Diretiva 95/46/CE (CE, 1995); Artigo 5.º da Lei 67/98 (AR, 1998)). Na proposta de regulamento, à semelhança da Diretiva 95/46/CE, os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de investigação histórica, estatística ou científica, mas é acrescentada a exigência de uma revisão periódica, para avaliar esta necessidade (GDPR, 2012).
>
> *Qualidade da informação* – os dados pessoais devem ser exatos, relevantes e completos[14] no que diz respeito aos fins para os quais são recolhidos e

[13] Deve ser regulada pela Portaria nº 247/2000, de 8 de Maio (CNPD, 2004).

[14] Entende-se por dados incompletos, dados inexatos, sendo que devem ser tomadas todas as medidas razoáveis para assegurar que para estes dados, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou retificados (CE, 1995).

processados (Artigo 6.º da Diretiva 95/46/CE (CE, 1995); Artigo 5.º da Lei 67/98 (AR, 1998)).

Consentimento – os dados pessoais só podem ser recolhidos e processados, apenas se a pessoa em causa tiver dado o seu consentimento explícito para o seu processamento (*Artigo 7.º da Diretiva 95/46/CE* (CE, 1995); Artigo 6.º da Lei 67/98 (AR, 1998)). O artigo 7.º da proposta de regulamento (GDPR, 2012) clarifica as condições para que o consentimento seja válido enquanto fundamento jurídico para o tratamento lícito.

Sensibilidade – o tratamento de dados pessoais, que são particularmente sensíveis para a pessoa em causa, deve ser objeto de medidas de proteção mais estritas do que outros dados pessoais (Artigo 8.º da Diretiva 95/46/CE (CE, 1995); Artigo 7.º da Lei 67/98 (AR, 1998)).

Segurança do tratamento – medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede. Estas medidas devem assegurar um nível de segurança adequado aos riscos inerentes ao tratamento e à natureza dos dados (Artigo 17.º da Diretiva 95/46/CE (CE, 1995); Artigos 14.º e 15.º da Lei 67/98 (AR, 1998)). Quando o propósito do processamento é cumprido, o controlador de dados, deve apagar, destruir ou anonimizar[15] os dados pessoais (Guarda & Zannone, 2009).

Transparência – os dados pessoais devem ser "*objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados*" (Artigo 5.º da proposta de regulamento (GDPR, 2012)), devendo o responsável pelo tratamento "*aplicar regras transparentes e de fácil acesso relativamente ao tratamento de dados pessoais e ao exercício dos direitos pelos titulares de dados*", assim como "*fornecer quaisquer informações relativas ao tratamento de dados pessoais ao titular dos dados de forma inteligível, numa linguagem clara e simples, adaptada à pessoa em causa, em especial*

[15] O processo de anonimização consiste em retirar identificadores pessoais. Uma vez removidos todos os identificadores pessoais, os dados deixam de identificar um indivíduo e deixam de poder ser considerados como dados pessoais.

quando as informações são dirigidas especificamente a uma criança" (Artigo 11.º da proposta de regulamento (GDPR, 2012)).

Responsabilidade global do responsável pelo tratamento – os dados pessoais devem ser "*tratados sob a autoridade e responsabilidade do responsável pelo tratamento, que deve assegurar e demonstrar a conformidade de cada operação de tratamento*" (Artigo 5.º da proposta de regulamento (GDPR, 2012)).

Atores

No processamento de dados podem estar envolvidos diferentes atores, necessários para definir as responsabilidades e poderes impostos pelos princípios da privacidade apresentados (Guarda & Zannone, 2009). Nos Artigos 2.º e 28.º da Diretiva 95/46/CE (CE, 1995) são identificados e definidos cinco atores associados ao processamento de dados pessoais (apresentados na Tabela 4), não sendo contudo reconhecido o *titular de dados* como um ator, apesar de lhe serem atribuídos um conjunto de direitos, na figura da "*pessoa em causa*".

Tabela 4 - Atores relacionados com a proteção de dados

Atores	**Diretiva 95/46/CE**	**RGPD (2012)**
Responsável pelo tratamento	●	○
Subcontratante	●	●
Terceiros	●	⊗
Destinatário	●	●
Autoridade de controlo	●	○
Pessoa em causa - Titular de dados	⊗	●
Representante	⊗	●
Empresa	⊗	●
Grupo de empresas	⊗	●
Criança	⊗	●

● - Existe
○ - Existe e foi melhorado
⊗ – Não existe

Na proposta de regulamento em discussão, o *titular de dados* é reconhecido como um ator, sendo-lhe inclusivamente atribuídos mais direitos, assim como é proposto o reconhecimento de outros atores como a *empresa*, *grupo de empresas* e a *criança*.

Responsável pelo tratamento - constitui "*a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que,*

individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais …" (Artigo 2.º da Diretiva 95/46/CE (CE, 1995); Artigo .3º da Lei 67/98 (AR, 1998)). Também identificado como *controlador de dados*, o qual é competente em decidir sobre o conteúdo e utilização de dados pessoais (OCDE, 2013).

Subcontratante – constitui "*a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento*" (Artigo 2.º da Diretiva 95/46/CE (CE, 1995); Artigo 3.º da Lei 67/98 (AR, 1998)). O conceito de «subcontratante» desempenha um papel importante no contexto da confidencialidade e da segurança do tratamento (Artigos 16.º e 17.º da Diretiva 95/46/CE (CE, 1995)), na medida em que serve para identificar as responsabilidades daqueles com um envolvimento mais direto no tratamento de dados pessoais, quer sob a autoridade direta do responsável pelo tratamento ou por sua conta. A distinção entre *responsável pelo tratamento* e *subcontratante* serve essencialmente para diferenciar os responsáveis pelo tratamento, em sentido estrito, das entidades que agem por conta destes. Trata-se de uma questão relacionada com a atribuição da responsabilidade (Art. 29 WP, 2010a).

Terceiros – qualquer pessoa, singular ou coletiva, que não o titular de dados, o responsável pelo tratamento e o subcontratante que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão habilitados a tratar os dados (Artigo 2.º da Diretiva 95/46/CE (CE, 1995); Artigo 3.º da Lei 67/98 (AR, 1998)). Este tipo de ator não tem continuidade na proposta de regulamento (GDPR, 2012).

Destinatário – qualquer pessoa a quem os dados são divulgados (Guarda & Zannone, 2009), ou a "*pessoa singular ou coletiva, a autoridade pública, serviço ou qualquer outro organismo que receba comunicações de dados pessoais*" (Artigo 2.º da Diretiva 95/46/CE (CE, 1995), Artigo 3.º da Lei 67/98 (AR, 1998)), Artigo 4.º da proposta de regulamento (GDPR, 2012)).

Autoridade de controlo[16] – autoridades especiais designadas para supervisionar a implementação das leis de proteção de dados (Guarda & Zannone, 2009), responsáveis pela fiscalização da aplicação no seu território das disposições adotadas pelos Estados-Membros nos termos da Diretiva 95/46/CE (CE, 1995). Cada Estado-Membro deve estabelecer que uma ou mais autoridades públicas sejam responsáveis pela fiscalização da aplicação do presente regulamento e por contribuir para a sua aplicação coerente no conjunto da União, a fim de proteger os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados na União (GDPR, 2012).

Titular de dados – uma pessoa singular identificada ou identificável, direta ou indiretamente, por meios com razoável probabilidade de serem utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa singular ou coletiva, nomeadamente por referência a um número de identificação, a dados de localização, a um identificador em linha ou a um ou mais elementos específicos próprios à sua identidade física, fisiológica, genética, psíquica, económica, cultural ou social (Artigo 4.º da proposta de regulamento (GDPR, 2012)).

Representante – alguém designado pelo responsável pelo tratamento que pode atuar em seu nome e pode responder inclusive a uma autoridade de controlo (Artigo 4º da proposta de regulamento (GDPR, 2012)). Na Diretiva 95/46/CE este ator não estava definido de uma forma clara (Guarda & Zannone, 2009).

Empresa – "*qualquer entidade que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo, nomeadamente, as pessoas singulares e coletivas, as sociedades ou associações que exercem*

[16] De acordo com a Lei 67/98, Capítulo IV, a Comissão Nacional de Proteção de Dados (CNPD), constitui a autoridade de controlo em Portugal, de acordo com a Diretiva 95/46/CE. Esta comissão iniciou atividades a 7 de janeiro de 1994, com a designação Comissão Nacional de Proteção de Dados Pessoais Informatizados (CNPDPI). Em 1998, é aprovada a nova Lei de Proteção de Dados Pessoais – Lei 67/98 de 26 de Outubro, que transpõe a Diretiva 95/46/CE, e vem alargar substancialmente o leque de atribuições e competências da Comissão, que passa desde então a designar-se Comissão Nacional de Proteção de Dados. Informação consultada em 23 de julho de 2012 no *URL*: http://www.cnpd.pt/bin/legis/leis_nacional.htm.

regularmente uma atividade económica" (Artigo 4.º da proposta de regulamento (GDPR, 2012)).

Grupo de empresas – "*um grupo composto pela empresa que exerce o controlo e pelas empresas controladas*" (Artigo 4.º da proposta de regulamento (GDPR, 2012)).

Criança – qualquer pessoa com menos de 18 anos (Artigo 4.º da proposta de regulamento (GDPR, 2012)).

Direitos do titular de dados

A recolha de dados é essencial, pois não é apenas a porta de entrada num sistema de informação, mas também o primeiro ato que coloca uma pessoa (isto é, os seus dados) em contacto com o SI. Consequentemente, a legislação aplica cuidados especiais à recolha de dados, estabelecendo obrigações sobre o controlador para que disponibilize informação de qualidade ao titular dos dados em causa, antes mesmo de a recolha dos dados ocorrer (Costa & Poullet, 2012). Para estes autores, as circunstâncias e o momento em que ocorre a recolha de dados são significativas para definir a legitimidade do processamento de dados.

À semelhança dos princípios que suportam a conformidade dos processos de tratamento de dados pessoais, a Diretiva 95/46/CE introduziu um conjunto de direitos fundamentais que assistem o titular dos dados na sua relação com as organizações, nomeadamente o direito ao consentimento, de informação, acesso e oposição (apresentados na Tabela 5).

Tabela 5 - Direitos do titular de dados

Direitos do titular de dados	**Diretiva 95/46/CE**	**RGPD (2012)**
Direito ao consentimento	●	○
Direito de informação	●	○
Direito de acesso	●	●
Direito de oposição *e de definição de perfis*	●	○
Direito de retificação	⊗	●
Direito de eliminação dos dados	⊗	●
Direito de portabilidade dos dados	⊗	●

● - Existe

○ - Existe e foi melhorado

⊗ – Não existe

Relativamente aos direitos dos titulares, reconhece-se haver na proposta de regulamento, de uma maneira geral, importantes melhoramentos por comparação com o atual regime, mormente quanto a uma melhor clarificação das obrigações do responsável pelo tratamento, a uma maior transparência perante o titular dos dados e aos mecanismos propostos para um melhor exercício dos direitos (CNPD, 2012b).

Direito ao consentimento – é definido como "qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objeto de tratamento" (Artigo 2.º da Diretiva 95/46/CE (CE, 1995), Artigo 3.º da Lei 67/98 (AR, 1998)), mediante uma declaração ou um ato positivo inequívoco (Artigo 4.º da proposta de regulamento (GDPR, 2012)). O Artigo 7.º da proposta de regulamento, clarifica as condições para que o consentimento seja válido enquanto fundamento jurídico para o tratamento lícito (GDPR, 2012).

Direito de informação – em situações em que os dados foram recolhidos junto, ou não, do titular dos dados, e em situações em que está prevista a comunicação dos seus dados a terceiros, este tem o direito a informações que lhe garantam um tratamento leal dos seus dados (Artigos 10.º e 11.º da Diretiva 95/46/CE (CE, 1995), Artigo 10.º da Lei 67/98 (AR, 1998)). O Artigo 14.º, da proposta de regulamento, descreve mais pormenorizadamente as obrigações de informação pelo responsável pelo tratamento para com o titular dos dados e acrescenta, em relação aos Artigos 10.º e 11.º da Diretiva 95/46/CE, informações suplementares, incluindo sobre o período de conservação, o direito de apresentar queixa, as transferências internacionais e a fonte de origem dos dados (GDPR, 2012).

Direito de acesso – o titular dos dados tem o direito de acesso a informação sobre as finalidades do tratamento sobre os seus dados pessoais, sobre que categorias de dados incidem, a origem dos dados, assim como os destinatários a quem são comunicados os dados. Para situações em que o tratamento não cumpra o disposto na lei, o titular dos dados nestas situações tem o direito à retificação, apagamento ou bloqueio dos seus dados (Artigo 12.º, alínea a), da Diretiva 95/46/CE (CE, 1995), Artigo 11.º da Lei 67/98 (AR, 1998)). O Artigo 15.º da proposta de regulamento prevê o direito de acesso do titular de dados aos seus dados pessoais, com base no Artigo 12.º,

alínea a), da Diretiva 95/46/CE, e acrescenta novos elementos, tais como prever a informação aos titulares dos dados sobre o período de conservação, os direitos de retificação, de apagamento e de apresentação de queixa (GDPR, 2012).

Direito de oposição e de definição de perfis – confere ao titular dos dados o direito de se "*opor em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de tratamento …*" (Artigo 14.º da Diretiva 95/46/CE (CE, 1995), Artigo 12.º da Lei 67/98 (AR, 1998)). A proposta de regulamento melhora o direito de oposição, ao contemplar no Artigo 20.º o direito de o titular dos dados não ser objeto de uma medida com base na definição de perfis ((GDPR, 2012)).

Direito de retificação – Apesar de já incluído no direito de acesso (Artigo 12.º, alínea b), da Diretiva 95/46/CE (CE, 1995)), o Artigo 16.º da proposta de regulamento estabelece definitivamente o direito do titular dos dados à retificação dos seus dados pessoais para todos os processos de tratamento de dados (GDPR, 2012).

Direito de eliminação dos dados – confere ao titular dos dados o direito a ser esquecido e ao apagamento dos seus dados pessoais. Desenvolve e especifica mais detalhadamente o direito de apagamento consagrado no direito de acesso, Artigo 12.º, alínea b), da Diretiva 95/46/CE (CE, 1995), e prevê as condições do direito a ser esquecido, incluindo a obrigação do responsável pelo tratamento, que tornou públicos os dados pessoais, de informar os terceiros sobre o pedido da pessoa em causa, de apagamento de quaisquer ligações para esses dados, ou cópias ou reproduções que tenham sido efetuadas. Este artigo integra igualmente o direito à limitação do tratamento em determinados casos, evitando o termo ambíguo de "bloqueio" (GDPR, 2012).

Direito de portabilidade dos dados – direito do titular dos dados à sua portabilidade, ou seja, de transferir os dados de um sistema de tratamento eletrónico para outro (num formato eletrónico estruturado e de utilização corrente), sem que o responsável pelo tratamento se possa opor (GDPR, 2012).

Obrigações do responsável pelo tratamento

O principal papel do conceito de responsável pelo tratamento é, antes de mais, determinar quem será o responsável pelo cumprimento das normas sobre proteção de dados e de que modo as pessoas em causa podem exercer na prática os seus direitos. Por outras palavras, atribuir a responsabilidade (Art. 29 WP, 2010a). Na opinião deste grupo de trabalho, é esta a essência da proposta de regulamento, dado que o seu principal objetivo é a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. Esse objetivo só pode ser concretizado, na prática, se os responsáveis pelo tratamento dos dados forem suficientemente incentivados, por meios jurídicos e outros meios, a tomar todas as medidas necessárias para assegurar que esta proteção é colocada em prática. Os meios para incentivar a responsabilidade podem ser pró-ativos e reativos. No primeiro caso, visam assegurar a aplicação efetiva de medidas de proteção dos dados e o estabelecimento de meios adequados de responsabilização dos responsáveis pelo tratamento. No segundo caso, podem envolver responsabilidade civil e sanções, a fim de garantir a reparação dos prejuízos relevantes e a adoção de medidas adequadas para corrigir irregularidades.

Verifica-se uma melhoria e uma atribuição de novas obrigações ao responsável pelo tratamento de dados pessoais na proposta de regulamento de proteção de dados. Enquanto na Diretiva 95/46/CE, o conjunto de obrigações se encontra disperso pelos sete capítulos do documento, na proposta de regulamento assistimos à concentração da maioria destas obrigações num capítulo específico. A Tabela 6 permite compreender a evolução prevista nas responsabilidades atribuídas a este ator.

Tabela 6 - Obrigações do responsável pelo tratamento dos dados

Obrigações	**Diretiva 95/46/CE**	**RGPD (2012)**
Obrigações gerais	●	○
Segurança do tratamento	●	○
Cooperação com a autoridade de controlo	●	○
Autorização prévia e consulta prévia	●	○
Avaliação de impacto sobre a proteção de dados	⊗	●
Proteção de dados desde a conceção e por defeito	⊗	●
Notificação da violação de dados pessoais à autoridade de controlo	⊗	●
Comunicação da violação de dados pessoais ao titular dos dados	⊗	●
Responsáveis conjuntos pelo tratamento	⊗	●

● - Existe
○ - Existe e foi melhorado
⊗ – Não existe

Obrigações gerais – são da responsabilidade do responsável pelo tratamento determinar as finalidades e os meios de tratamento dos dados pessoais (Artigo 2.º, alínea d), da Diretiva 95/46/CE (CE, 1995)), e assegurar os direitos de informação, acesso e oposição do titular dos dados (Artigos 10.º, 11.º, 12.º e 14.º da Diretiva 95/46/CE (CE, 1995)), assim como a sua proteção face a decisões que resultem de um tratamento automatizado (Artigo 15.º da Diretiva 95/46/CE (CE, 1995)). A proposta de regulamento reúne e descreve no Artigo 22.º as obrigações que incumbem ao responsável pelo tratamento para dar cumprimento ao regulamento e comprovar a sua observância, através da adoção de regras internas para este efeito (GDPR, 2012).

Segurança do tratamento – o responsável pelo tratamento deve colocar em prática medidas técnicas e organizacionais para implementar as exigências associadas ao princípio da *segurança do tratamento*, em casos de tratamento por sua conta ou em subcontratação (Artigo 17.º da Diretiva 95/46/CE (AR, 1998)). Estas medidas devem ser adotadas na sequência de uma avaliação de riscos, e devem assegurar um nível de segurança adaptado aos riscos que o tratamento representa e à natureza dos dados pessoais a proteger (Artigo 30.º da proposta de regulamento (GDPR, 2012)).

Cooperação com a autoridade de controlo – contempla a obrigatoriedade de notificar a autoridade de controlo da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente automatizados, destinados à prossecução de uma ou mais finalidades interligadas (Artigo 18.º da Diretiva 95/46/CE (CE, 1995)). A proposta de regulamento altera este procedimento, ao introduzir a obrigação, para os responsáveis pelo tratamento e os subcontratantes, de conservar a documentação das operações de tratamento sob a sua responsabilidade, em vez da notificação geral à autoridade de controlo (Artigo 28º da proposta de regulamento (GDPR, 2012)).

Autorização prévia e consulta prévia – o responsável pelo tratamento em casos que possam representar riscos para os direitos e liberdades das pessoas, deve solicitar um controlo prévio à autoridade de controlo (Artigo

20.º da Diretiva 95/46/CE (CE, 1995)). "*O responsável pelo tratamento ou o subcontratante, consoante o caso, deve obter uma autorização da autoridade de controlo antes de proceder ao tratamento de dados pessoais, a fim de assegurar a conformidade do tratamento previsto com o regulamento e, nomeadamente, atenuar os riscos para os titulares de dados* …" (Artigo 34.º da proposta de regulamento (GDPR, 2012)).

Avaliação de impacto sobre a proteção de dados – em situações de risco para os direitos e liberdades dos titulares dos dados, o responsável pelo tratamento deve efetuar uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais que permita: (1) uma descrição geral das operações de tratamento de dados previstas; (2) uma avaliação dos riscos; (3) apresentar as medidas previstas para fazer face aos riscos; e (4) conhecer as garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais (Artigo 33.º da proposta de regulamento (GDPR, 2012)).

Proteção de dados desde a conceção e por defeito – as medidas e os procedimentos técnicos e organizativos que garantam a proteção dos direitos do titular dos dados devem ser considerados no momento de definição dos meios de tratamento. Em simultâneo, o responsável pelo tratamento deve desenvolver mecanismos que garantam, por defeito, os princípios de minimização dos dados e limitação da finalidade (Artigo 23.º da proposta de regulamento (GDPR, 2012)).

Notificação da violação de dados pessoais à autoridade de controlo – o responsável pelo tratamento deve notificar à autoridade de controlo situações de violação de dados pessoais, o mais tardar 24 horas após ter tido conhecimento da situação. Deve ainda documentar a situação de violação para análise posterior pela autoridade de controlo (Artigo 31.º da proposta de regulamento (GDPR, 2012)).

Comunicação da violação de dados pessoais ao titular dos dados – se uma situação de violação de dados pessoais afetar negativamente a privacidade do titular dos dados, o responsável pelo tratamento deve comunicar este facto à pessoa em causa (Artigo 32.º da proposta de regulamento (GDPR, 2012)).

Responsáveis conjuntos pelo tratamento – introduz a exigência de definição e atribuição de obrigações, em situações de responsabilidade conjunta pelo tratamento de dados pessoais (Artigo 24º da proposta de regulamento (GDPR, 2012)).

Globalmente, a maioria dos países está a introduzir legislação de privacidade para proteger a privacidade pessoal. Infelizmente, estes regulamentos são, por vezes, demasiado amplos para terem qualquer impacto significativo, e estão quase sempre um ou mais passos atrás de cada nova inovação tecnológica que pode comprometer a nossa privacidade (Ernst & Young, 2012b). Ao invés de colocar a responsabilidade sobre a legislação, é tempo de as organizações e indivíduos serem responsáveis quanto à privacidade. Em particular, as organizações necessitam de ser responsabilizadas pelos dados que recolhem ou têm intenção de recolher sobre os indivíduos. É necessário que apresentem uma maior abertura e transparência sobre os dados que estão a recolher, e necessitam de assegurar a proteção dos dados recolhidos, nomeadamente através de medidas de segurança (Ernst & Young, 2013).

2.1.4 A privacidade em registos de saúde eletrónicos

Os ambientes de cuidados de saúde são frequentemente descritos como de grande intensidade no uso de informação, altamente paradoxais, e muito turbulentos. (Plummer, 2001). A adoção de TI nos sistemas de saúde tem, em geral, seguido o mesmo padrão das restantes indústrias. Apesar do relativo sucesso das primeiras vagas de adoção de TI, este foi insuficiente para o desenvolvimento de sistemas de saúde totalmente integrados (Biesdorf & Niedermann, 2014).

Atualmente, a informação de saúde dos cidadãos ainda está em grande parte residente e acessível apenas em cada uma das unidades de saúde a que o cidadão recorreu: o centro de saúde, o hospital, a clínica ou o consultório médico. No entanto, o acesso descentralizado a essa informação pode ser crucial (Patrício & Brito, 2012). A história tem demonstrado que a utilidade e o valor da informação multiplicam-se exponencialmente à medida que se torna mais acessível ao grande público. As TI aceleraram este fenómeno. Ter informação de qualidade sempre foi um fator primordial para melhorar o atendimento ao paciente (Berger, 2014). Os SI de saúde têm que ser desenvolvidos e explorados de forma a melhorar as oportunidades de acesso global aos serviços de saúde e conhecimento médico (Haux, 2006). Os dados

de saúde em si, estão a tornar-se num ativo organizacional extremamente valioso (Berger, 2014).

A privacidade é particularmente importante no contexto da saúde devido à sensibilidade potencial ou real dos dados de saúde. A sensibilidade de um indivíduo em relação aos seus dados de saúde é maior face: (1) ao seu potencial (percebido ou real) de discriminação, pela família, sociedade ou outros; (2) ao seu potencial em prejudicar através da divulgação de dados a terceiros, por exemplo a seguradoras, de dados sobre doenças geneticamente transmissíveis; e (3) o seu potencial de gerar uma atenção indesejada sobre aqueles que estão no centro das atenções públicas, por exemplo celebridades e políticos (NETHA, 2006).

Os pacientes não são a única parte interessada nos dados de saúde. Outras partes estão interessadas em beneficiar com estes dados, quer para benefício próprio, quer da sociedade, nomeadamente: (1) os profissionais de gestão dos hospitais, (2) os membros da família, (3) os médicos especialistas, técnicos de laboratório, instituições de saúde, e as farmácias, (4) os nutricionistas e fornecedores de serviços de medicina alternativa, (5) as seguradoras, (6) os cientistas, investigadores e agências de saúde pública, e (7) agentes comunitários, incluindo serviços de polícia e de ambulância (Peleg, Beimel, Dori, & Denekamp, 2008). Se nos anos de 1990 se considerava apenas a possibilidade de utilizar imagens, em especial de radiologia, em conjunto com os dados alfanuméricos, hoje, graças ao desenvolvimento de ferramentas de processamento de informação suportadas computacionalmente, estamos a considerar novos tipos de dados (Haux, 2006). Existem assim vários tipos de dados cuja confidencialidade, integridade e disponibilidade carecem de proteção: (1) dados pessoais de saúde; (2) dados apresentados sob pseudónimo, derivados dos dados pessoais de saúde; (3) dados estatísticos e de investigação, incluindo dados anonimizados derivados de dados pessoais de saúde através da eliminação de dados de identificação pessoal; (4) dados clínicos; (5) dados sobre os profissionais de saúde, funcionários e voluntários; (6) dados relacionados com a vigilância da saúde pública; e (7) dados de controlo, produzidos pelos sistemas, sobre as ações dos utilizadores em relação à utilização dos dados pessoais de saúde (ISO, 2008).

Até à década de 90, houve um uso quase exclusivo dos dados para a assistência ao paciente e fins administrativos, com algum uso na gestão e controlo da qualidade. Agora temos a capacidade de estender a possibilidade de utilização dos dados,

utilizados principalmente no atendimento ao paciente, também ao planeamento de cuidados de saúde e, acima de tudo, para a investigação clínica (Haux, 2006). Fazer com que o conteúdo dos registos de saúde seja utilizável para fins secundários, requer muito trabalho adicional para além do trabalho empregue no registo dos dados para utilização primária (Berg, Langenberg, Berg, & Kwakkernaat, 1998).

As pessoas dependem da privacidade por forma a controlarem ou limitarem a divulgação dos seus dados de saúde, que pode resultar em prejuízos tangíveis, materiais, como a perda de emprego, a perda do seguro, da posição na comunidade e a perda da intimidade. Proteger os dados de saúde através de políticas de privacidade, desempenha uma função importante de minimização de perdas materiais, num mundo em que crescem a discriminação e a rejeição (Allen, 2007). Na opinião desta autora, a privacidade contribui para aquilo que se pode denominar de "minimização do desconforto emocional". A exposição de problemas de saúde pode causar ansiedade e emoção. Infelizmente para alguns, a doença leva à vergonha, vergonha que diminui a autoestima e aumenta o sentimento de vulnerabilidade.

Enquanto a proteção e a segurança dos dados pessoais é importante para todos os indivíduos, instituições e governos, existem requisitos especiais na área da saúde que necessitam de ser cumpridos para garantir a confidencialidade, integridade, auditabilidade e disponibilidade dos dados pessoais de saúde (ISO, 2008), face a ameaças organizacionais que resultam do acesso inadequado aos dados do paciente, quer por profissionais internos, que abusam dos seus privilégios, quer por profissionais externos que exploram vulnerabilidades dos SI (Appari & Johnson, 2010).

O relatório anual da IBM (IBM, 2014), com base na monitorização da segurança dos seus clientes em 133 países, coloca o setor da saúde nas cinco indústrias mais atingidas pela maioria dos incidentes de segurança, onde ocupa a 5ª posição com 5.8% dos 16.900 eventos de segurança analisados (veja-se a Figura 1). Em 2013, segundo este relatório, atingiu-se um novo máximo com mais de 500 mil milhões de registos de informação pessoal – incluindo nomes, endereços de correio eletrónico, números de cartões de crédito e palavras-passe – a serem roubados.

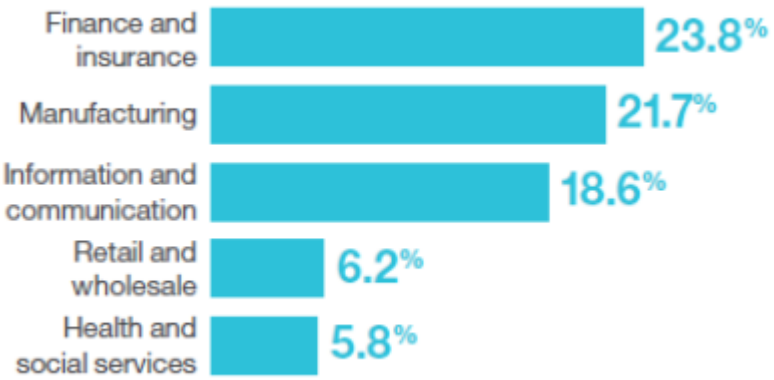

Figura 1 - Taxas de incidência de incidentes de segurança, por setor (IBM, 2014)

No domínio da saúde, um registo de dados digitais recolhidos sobre um paciente pode ser referido como um *Electronic Health Record* (EHR), *Electronic Medical Record* (EMR), ou *Computerized Patient Record* (CPR) (Peleg et al., 2008).

Um EMR é diferente de um EHR. Um EMR é um ambiente aplicacional composto por repositórios de dados clínicos, suporte à decisão clínica, vocabulário médico controlado, sistema computacional para o registo de entrada de pedidos, farmácia, e aplicações de documentação clínica. Este ambiente fornece o suporte necessário ao movimento do paciente em ambientes hospitalares e ambulatórios, e é usado por profissionais de saúde para documentar, monitorizar e gerir os cuidados de saúde, dentro de uma organização prestadora de cuidados de saúde. Os dados num EMR constituem um registo médico-legal dos episódios clínicos do paciente numa organização de cuidados de saúde, e são propriedade desta organização. (Kahn & Sheshadri, 2008). Os EMRs são cada vez mais a forma de armazenar informações sobre os pacientes, normalmente dentro de uma infraestrutura local, e só são acessíveis a partir desta infraestrutura. Para aumentar a eficiência dos serviços médicos e fornecer informações médicas completas e precisas, os EMR interinstitucionais são cada vez mais usados para registar e manter dados sobre os pacientes (Haas et al., 2011).

Um EHR é um subconjunto do EMR de assistência médica da organização, e é da propriedade do paciente. Apresenta dados registados pelo paciente, e permitem o acesso aos vários episódios de saúde realizados nas várias organizações prestadoras de cuidados de saúde dentro de uma comunidade, região ou estado, e em alguns casos no país inteiro (Kahn & Sheshadri, 2008). O utente tem agora responsabilidade

sobre estes dados e não apenas os serviços médicos, e os dados médicos sobre os utentes perdem a proteção implícita do domínio médico das instituições de saúde, devido à sua utilização por outras instituições (Haas et al., 2011). A tecnologia EHR[17] contribui para a criação de uma nova classe de ativos – a própria informação de saúde, sendo contudo evidente que nem todas as organizações de saúde veem a informação de saúde desta forma (Berger, 2014).

Face à complexidade do conceito de EHR, surgem duas organizações que procuram desenvolver um padrão para a troca de dados de saúde, nomeadamente a *Health Level 7* (HL 7) e o *European Committee for Standardization* (CEN). Ambas pretendem desenvolver um *standard* que permita, no imediato, a interoperabilidade entre os vários sistemas EHR existentes dentro das organizações de saúde, ou seja, a troca de dados interorganizacional a fim de aumentar a qualidade dos serviços para os pacientes (Peleg et al., 2008).

Independentemente do contexto de desenvolvimento de um EHR, a transferência de dados protegidos de saúde deve acontecer de forma segura, através de políticas e procedimentos que permitam identificar e tomar medidas contra violações, não desejadas para a privacidade e para a segurança (Kahn & Sheshadri, 2008). Tanto os pacientes, como os profissionais de saúde necessitam de ter a certeza de que interagem com os sistemas EHR num ambiente de confiança e em plena conformidade com a legislação relevante, nomeadamente sobre a privacidade e proteção de dados (de acordo com o princípio "*segurança e privacidade*" para o funcionamento da interoperabilidade no âmbito do projeto epSOS[18]). Isto significa que os serviços EHR devem garantir que a privacidade dos pacientes e a confidencialidade dos dados fornecidos pelas organizações de saúde, são respeitadas (epSOS, 2010).

---

[17] O documento de trabalho do Art. 29 WP (2007a) sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos, é importante para a compreensão do seu enquadramento jurídico, assim como dos requisitos de proteção de dados para a criação de um sistema EHR. As reflexões e recomendações indicadas no documento devem repercutir-se no desenvolvimento de medidas de segurança e de privacidade dos dados.

[18] O projeto epSOS (Smart Open Services for European Patients) tem por objetivo projetar, construir e avaliar uma infraestrutura de serviços que permita a interoperabilidade transfronteiriça entre sistemas de registos de saúde eletrónicos na Europa. Permite assim uma melhoria na qualidade nos cuidados de saúde para os cidadãos quando viajam para outro país europeu. Informação consultada em 23 de junho de 2015 no *URL*: http://www.epsos.eu/home/about-epsos.html.

2.2 Interoperabilidade

2.2.1 Definição de Interoperabilidade

O conceito de interoperabilidade está muito associado à especificidade do seu contexto de desenvolvimento, o que faz com que não exista uma definição de interoperabilidade globalmente aceite (Gasser & Palfrey, 2007). Apesar de existirem muitas definições de interoperabilidade, estas não permitem uma compreensão clara deste conceito, o que dificulta os esforços de desenvolvimento e investigação (Chen, 2008). A definição mais referenciada[19] sobre interoperabilidade tem origem no Departamento da Defesa dos EUA (DoD), publicada em 1977, definindo a "*interoperabilidade como a capacidade dos sistemas, unidades, ou forças de disponibilizarem serviços para, e aceitarem serviços de outros sistemas, unidades, ou forças e de utilizarem estes serviços no sentido de operarem eficazmente em conjunto"* (DoD JP1-02, 2010). Esta definição reflete a perceção da necessidade de diferentes elementos, sistemas e pessoas para trabalharem juntos (Moon, Fewell, & Reynolds, 2008).

O *IEEE Standard Computer Dictionary* define a interoperabilidade como "*a capacidade de dois ou mais sistemas ou componentes de trocarem dados e de serem capazes de utilizar os dados trocados*" (IEEE, 1990). Isto significa que existem duas partes na definição de interoperabilidade: (1) a capacidade de dois ou mais sistemas ou componentes de **trocarem** dados; e (2) a capacidade destes sistemas em **utilizar** os dados partilhados (Sensmeier, 2013). Desta forma a autora, para a área da saúde, refere-se à interoperabilidade como a capacidade dos SI da saúde em trabalharem em conjunto, tanto no interior como para lá das fronteiras organizacionais, com o objetivo de promover serviços eficazes de prestação de cuidados de saúde aos indivíduos e às comunidades.

De uma forma simples, interoperabilidade constitui a capacidade de pessoas, organizações e sistemas interagirem para que de uma forma eficiente e eficaz possam trocar e utilizar informação (Baird, 2007). Está relacionada com a capacidade de, sem esforço significativo, duas ou mais entidades independentes, e que operam de forma autónoma, conseguirem trocar informação e utilizar correta e convenientemente essa

[19] Tendo por base artigos científicos, relatórios, *standards* e outros documentos governamentais, o estudo de Ford et al. (2007) permitiu identificar 34 definições distintas de interoperabilidade e perceber quais as definições mais populares ou mais utilizadas.

informação, com vista a contribuir para o alcance de um propósito comum (Soares, 2009). O termo "interoperar" implica que um sistema realiza uma operação para outro sistema. Do ponto de vista computacional, é a capacidade de dois sistemas computacionais heterogéneos funcionarem em conjunto e darem acesso aos seus recursos de uma forma recíproca. No contexto de empresas em rede (colaboração), a interoperabilidade refere-se à capacidade de interação (partilha de dados e serviços) entre sistemas empresariais (Chen, 2008). Para o domínio do *E-Government*, a interoperabilidade ocorre sempre que SI independentes ou heterogéneos, ou os seus componentes controlados por diferentes jurisdições/administrações, ou por parceiros externos, trabalham em conjunto de forma coordenada e consensual (Scholl & Klischewski, 2007).

Tipos e categorias de Interoperabilidade

A perceção popular associa a interoperabilidade a conectividade. No entanto, a verdadeira interoperabilidade é muito mais do que apenas a conectividade entre sistemas (Kasunic & Anderson, 2004). De uma forma geral todos os tipos de interoperabilidade podem ser classificados em técnicos e não técnicos (Ford, Colombi, Graham, & Jacques, 2007). Exemplos de tipos de interoperabilidade técnicos incluem comunicações, eletrónica, aplicações informáticas e bases de dados. Exemplos de tipos de interoperabilidade não técnicos incluem organizacional, operacional, processos, culturas e coligações.

Chen et al., (2008) identificaram quatro categorias de interoperabilidade:

1. A *interoperabilidade de dados* - apresenta por objetivo a partilha e procura de informação a partir de fontes de dados heterogéneas, que podem residir em diferentes servidores, com sistemas operativos e sistemas de gestão de bases de dados diferentes. Ou seja, é necessário que diferentes modelos de dados e linguagens de pesquisa trabalhem em conjunto.
2. A *interoperabilidade de serviços* - relacionada com a identificação, composição e promoção de um funcionamento em conjunto de várias aplicações, as quais foram concebidas e implementadas de forma independente.
3. *A interoperabilidade de processos* - relacionada com a ligação de processos internos de duas organizações de forma a criarem um processo comum.

4. A *interoperabilidade de negócios* - apesar de diferentes modos de tomada de decisão, métodos de trabalho, legislação e culturas organizacionais, procura-se que um processo de negócio possa ser desenvolvido em conjunto.

Independentemente do seu tipo ou categoria, é unânime que a interoperabilidade abrange três dimensões diferentes: *técnica, organizacional e semântica* (Cechich, Gibbons, & Kesan, 2008; Vernadat, 2010; C4ISR, 1998; IDABC, 2004; Malhene, Trentini, Marques, & Burlat, 2012; epSOS, 2010):

Técnica – abrange as questões técnicas de ligação entre os sistemas, nomeadamente: interfaces, serviços de interligação, integração dos dados e serviços de segurança.

Organizacional – focada na definição de objetivos e na modelação de processos de negócio, proporcionando a integração de diferentes estruturas e processos internos. Contudo, há autores para os quais a interoperabilidade organizacional vai para além da vertente processual, envolvendo um conjunto de aspetos legais, políticos, culturais e estruturais que influenciam a colaboração entre entidades. Enquanto a interoperabilidade dos sistemas está relacionada com a capacidade dos sistemas ou dos seus componentes trocarem e utilizarem dados, a interoperabilidade organizacional está relacionada com a capacidade de várias unidades, fornecerem, aceitarem e usarem serviços, de modo a operarem eficazmente em conjunto (Gottschalk, 2009b).

Semântica – relacionada com a necessidade de garantir que a informação trocada entre sistemas mantém o seu significado e é compreensível mesmo que utilizada por outra aplicação que não foi inicialmente desenvolvida para esta finalidade. Permite que os sistemas possam combinar os dados recebidos com outras fontes de informação.

Interoperabilidade versus Integração

São várias as situações em que o conceito de interoperabilidade é confundido com os conceitos de integração, ou até mesmo compatibilidade e adaptabilidade. Tanto a integração como a interoperabilidade apresentam como objetivo principal facilitar a

continuidade das operações entre entidades organizacionais, sejam elas uma única organização, organizações em rede ou organizações virtuais.

A integração entre organizações ocorre quando há a necessidade de remover barreiras organizacionais e/ou melhorar a colaboração entre pessoas, sistemas, aplicações, serviços e até mesmo empresas (especialmente em termos de fluxos de materiais, informação/fluxos de decisão e controlo, ou fluxos de trabalho). O objetivo é criar sinergias dentro da organização ou na rede de organizações, ou seja, a criação de uma situação em que o sistema integrado oferece uma maior capacidade do que a soma dos seus componentes seria capaz de oferecer (Vernadat, 2010). A integração representa assim a fusão ou a unificação de vários SI - ou dos seus elementos – anteriormente separados, e que passam a funcionar como um todo (Stelzer, Fischer, & Nirsberger, 2006). Enquanto os sistemas interoperáveis podem funcionar de forma independente, um sistema integrado perde significativamente funcionalidade se o fluxo de serviços é interrompido (Kasunic & Anderson, 2004) [20].

A interoperabilidade permite que duas ou mais entidades (da mesma organização ou de organizações diferentes e, independentemente da sua localização) sejam capazes de trocar ou partilhar informação, e usar as funcionalidades da outra organização, num ambiente distribuído e heterogéneo (Vernadat, 2010). Ao constituir a capacidade de dois sistemas se entenderem e utilizarem funcionalidades um do outro, a interoperabilidade significa coexistência, autonomia e ambientes federativos, enquanto a integração significa coordenação, coerência, uniformização e unificação (Chen et al., 2008).

A norma ISO 14258 (1999) é essencial para compreender as diferenças entre estes dois conceitos, com base nas três formas distintas de relacionamento entre duas ou mais entidades, nomeadamente através da *integração*, *unificação* e *federação*.

---

[20] Autores como Jhingran, Mattos, & Pirahesh (2002) e Chen et al. (2008) identificaram várias formas de integração. Jhingran, Mattos, & Pirahesh, (2002) identificaram quatro formas distintas de integração: (1) *integração através de portais*, que cria um único ponto de entrada para aplicações díspares; (2) *integração de processos de negócio*; (3) *integração de aplicações*, em que aplicações que fazem tarefas similares ou complementares comunicam entre si, tipicamente focadas na transformação de dados e passagem de mensagens e (4) *integração de informações*, em que dados complementares, são reunidos física ou logicamente, possibilitando o acesso a dados relevantes mesmo que não estejam diretamente sob o controlo da empresa. A proposta de Chen et al. (2008), mais simples, apresenta apenas três formas de integração: (1) *integração física* - ligação de vários equipamentos através de uma rede de dados, (2) *integração de aplicações* - integração de aplicações informáticas e sistemas de bases de dados e (3) *integração de processos de negócio* - coordenação de funções para gerir, controlar e monitorizar processos de negócios.

Na opinião de Chen et al., (2008) a integração e interoperabilidade são conceitos interdependentes e não podem ser separados. Contudo, os sistemas interoperáveis não necessitam de estar integrados (Kasunic & Anderson, 2004). O termo "*co-operability*" é por vezes utilizado para se referir à interoperabilidade resultante de fatores não técnicos (Rohatgi & Friedman, 2010).

A compatibilidade é também confundida com a interoperabilidade. Se a interoperabilidade é definida pela capacidade de uma entidade servir outra, então compatibilidade é definida pelo grau em que um sistema eletrónico pode operar com outro – constitui um subconjunto da interoperabilidade (Clark & Jones, 1999). Ou seja, enquanto a compatibilidade é aplicada a níveis tecnológicos, mais baixos, a interoperabilidade é aplicada a níveis organizacionais, mais altos. Enquanto a compatibilidade é claramente um requisito mínimo, o grau de interoperabilidade/integração desejado entre sistemas ou unidades é impulsionado pelo conceito operacional subjacente (Kasunic & Anderson, 2004).

Em resumo, a interoperabilidade é uma condição necessária para garantir a longevidade de integração num ambiente de TI. A interoperabilidade cria um espaço para soluções de integração que se adaptem à mudança, em vez de contra a mudança (NETHA, 2007a). A Tabela 7 permite compreender as diferenças entre estes dois conceitos, indicando os aspetos chave para a sua distinção, quer do ponto de vista técnico, quer organizacional.

Tabela 7 - Interoperabilidade versus Integração

	Do ponto de vista técnico (sistemas, dados)	***Do ponto de vista organizacional***
Integração	• **Fusão** de sistemas, serviços, ou produtos, num único sistema, serviço, ou produto. • **Coordenação, coerência e unificação** de sistemas.	• **Interdependência** entre organizações. • **Integração** dos fluxos de informação.
Interoperabilidade	• Interconexão entre sistemas • **Coexistência, autonomia e federação** de sistemas heterogéneos. • Relacionada com os aspetos técnicos de comunicação, e partilha de serviços e dados entre as várias aplicações do sistema.	• Desenvolvimento de capacidades e mecanismos de **colaboração** entre as organizações, grupos e pessoas. • Relacionada com o **alinhamento** de processos de negócio, estruturas organizacionais, objetivos, bases legais, culturas e métodos de trabalho.

2.2.2 Abordagens à interoperabilidade

A investigação no domínio da interoperabilidade não consiste apenas na identificação de barreiras e soluções, mas também no estudo da forma como estas barreiras podem ser removidas (Chen, 2008; Chen et al., 2008).

A abstração e a separação de conceitos com base em vários pontos de vista são usadas para analisar ambientes complexos e em evolução, dando origem ao desenvolvimento de várias escolas de *frameworks*, modelos e arquiteturas de interoperabilidade, integração e desenho de soluções. Duas abordagens populares de interoperabilidade são as *frameworks* de interoperabilidade e as arquiteturas de interoperabilidade (NETHA, 2005). O termo "*framework*" refere-se a um mecanismo de organização para estruturar e categorizar "coisas" relacionadas com um domínio. Uma *framework* não fornece uma solução operacional para resolver um problema empresarial (Chen, 2008). Constitui uma abstração técnica (NETHA, 2005), um instrumento útil para posicionar, relacionar e comparar entre si, conceitos, princípios, métodos, padrões, modelos e ferramentas num determinado domínio de interoperabilidade (Vernadat, 2010).

Um modelo, por seu lado, identifica o espaço de um problema particular e define uma análise de requisitos, independente da tecnologia. O desenho ou arquitetura, mapeia os requisitos do modelo com uma determinada família de soluções, baseadas em *standards* e abordagens técnicas. Uma solução relaciona o projeto com o fornecedor da tecnologia, garantindo a adesão ao desenho, modelo e *framework* (NETHA, 2005).

Os modelos são descrições dos componentes essenciais e relevantes numa área de especial preocupação. Estes não duplicam a realidade, mas são aproximações limitadas do subconjunto da realidade em consideração. O nível apropriado de detalhe de um modelo é indicado pelo seu uso pretendido, isto é, o objetivo do modelo. Uma descrição completa de qualquer modelo inclui declarações do seu objetivo, premissas e restrições. Os modelos podem ter efeitos muito diferentes. Eles podem ser usados para estruturar uma área de preocupação para: ilustrar ou esclarecer o conhecimento sobre uma área; definir a estrutura, lógica e de comportamento de um sistema; apoiar o processo de resolução de problemas através da análise de diferentes opções ou soluções; ajudar a projetar, construir ou operar um sistema (ISO 14258, 1999).

Uma arquitetura de interoperabilidade define o desenho específico para a conectividade e partilha com base nos *standards*, políticas e especificações disponibilizadas pela *framework*, como são exemplo as arquiteturas orientadas a serviços, armazenamento e envio, ou fluxos de informação (NETHA, 2005).

De um modo geral, podemos classificar estas abordagens utilizando uma hierarquia, em que de uma forma progressiva cada nível apresenta medidas mais concretas para o desenho da solução, como apresentado na Figura 2.

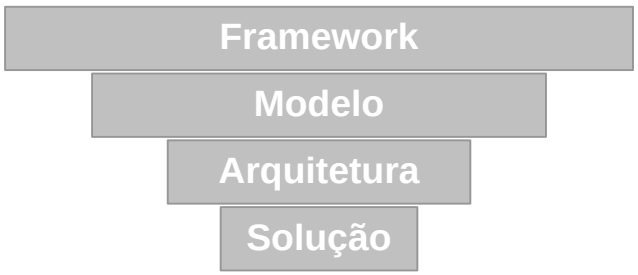

Figura 2 - Implementação com base numa *framework*
(Adaptado de NETHA, 2005)

A abordagem mais comum, utilizada pelos governos, para promover a resolução dos problemas de interoperabilidade consiste em estimular o uso de *standards* na atualização e no desenvolvimento de novas TI. Os governos, em geral publicam normas técnicas/*standards*, princípios e diretrizes de desenvolvimento na forma de *frameworks* de interoperabilidade (Ray, Gulla, & Dash, 2007).

A *Framework de Interoperabilidade Europeia* (EIF) é o projeto de maior relevância do programa IDABC[21], uma das iniciativas (Figura 3) mais importantes para o desenvolvimento da interoperabilidade, promovido pela Comissão Europeia, para apoiar a estratégia da UE para a prestação de serviços públicos eletrónicos centrados no cidadão (Vernadat, 2010).

A primeira versão da EIF (IDABC, 2004) pretendeu suportar o desenvolvimento de serviços de governação eletrónicos, através: (1) do suporte ao desenvolvimento no espaço europeu de serviços eletrónicos (*eServices*) centrados no cidadão, contribuindo para uma interoperabilidade entre serviços públicos; (2) do completar das *frameworks* de interoperabilidade nacionais em áreas que não podem ser

[21] Decisão 2004/387/EC "Decision of the European Parliament and of the Council on Interoperable Delivery of pan-European Services to Public Administrations, Businesses and Citizens (IDABC) (http://europa.eu.int/idabc/).

adequadamente tratadas através de uma abordagem puramente nacional, como é o caso da Saúde, através do projeto epSOS; e (3) da promoção da interoperabilidade, tanto dentro como entre diferentes áreas políticas, nomeadamente no âmbito do programa IDABC e quaisquer outros programas e iniciativas comunitárias. Contemplou 17 recomendações[22] estruturadas nas três dimensões de interoperabilidade: *organizacional, semântica e técnica*.

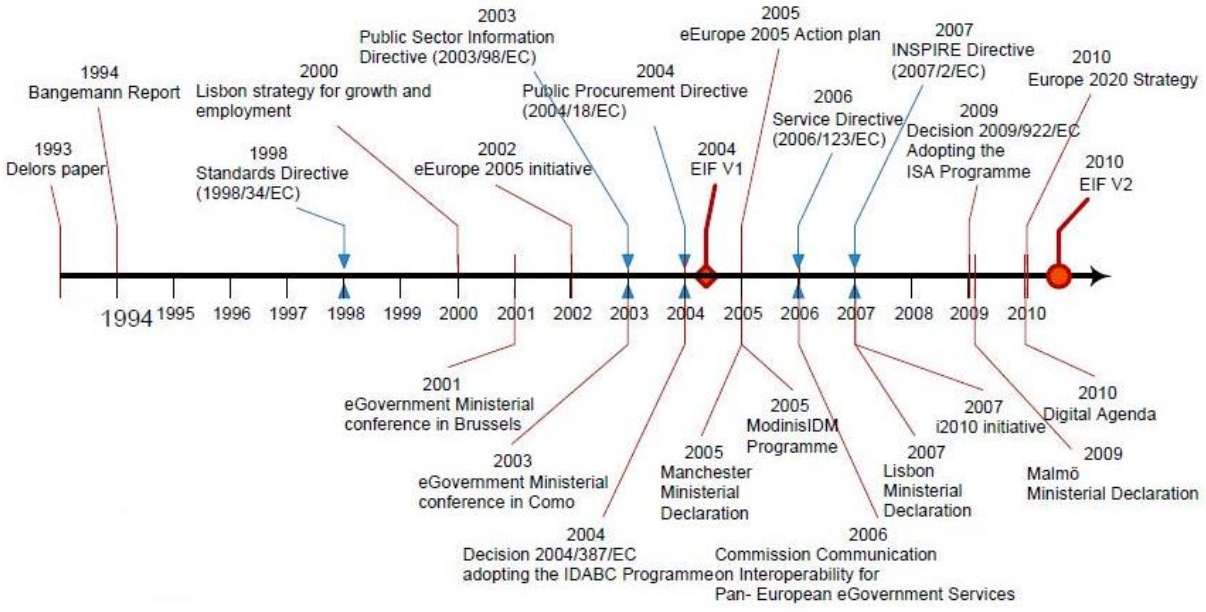

Figura 3 - Iniciativas na União Europeia no domínio da interoperabilidade
(IDABC, 2010)

A versão 2.0 da EIF (IDABC, 2010) manteve a linha de orientação do programa IDABC. Se numa fase inicial foi importante promover o desenvolvimento de plataformas de interoperabilidade para os vários serviços públicos em cada Estado-Membro da UE, o desafio seguinte consiste em promover a interoperabilidade transfronteiriça (*cross-border*). Ou seja, alinhar as plataformas existentes com a plataforma europeia. Esta segunda abordagem por parte do programa IDABC, sugere

[22] As recomendações foram construídas tendo por base os seguintes princípios: (a) a garantia de acessibilidade a todos os cidadãos sem qualquer discriminação; (b) a disponibilidade dos serviços em várias línguas; (c) a necessidade de segurança das comunicações e trocas de informação; (d) a necessidade de preservar a ***privacidade dos dados***; (e) a subsidiariedade, em que as decisões da UE são tomadas tão próximo quanto possível do cidadão, mas apenas em situações em que estas são mais eficazes que as decisões tomadas a nível nacional, regional ou local; (f) a utilização de *standards* abertos; e (g) a utilização de *software Open Source* (IDABC, 2004).

o desenvolvimento de serviços públicos assentes em "*Ecossistemas de Interoperabilidade*". Este termo engloba não só a interoperabilidade técnica, mas também a troca de informação e colaboração entre pessoas, organizações e sistemas, ou interoperabilidade organizacional (IDABC, 2010). Desta forma, a EIF adiciona mais duas dimensões de interoperabilidade às três já existentes, a dimensão legal e a política (epSOS, 2010).

Em Portugal, a Agência para a Modernização Administrativa (AMA) é responsável por vários projetos relacionados com o desenvolvimento da Administração Eletrónica. A "*Framework* de Serviços Comuns" foi concebida para garantir a máxima integração e interoperabilidade entre os diferentes sistemas das instituições públicas, contribuindo para que os cidadãos tenham uma perspetiva integrada dos serviços disponibilizados pela Administração Pública (AMA, 2008). A plataforma proposta pela *Framework* de Serviços Comuns fornece, entre outros aspetos, mecanismos robustos de autenticação e gestão de identidades, que facilitam a autenticação segura perante os organismos públicos, e mecanismos de controlo transacional, que garantem a qualidade dos dados durante o processo de utilização dos serviços eletrónicos, para além de um *gateway* central para os processos de pagamento eletrónico. Em conformidade com a EIF (IDABC, 2004), na conceção da plataforma, os *standards* abertos impuseram-se sempre como opção estratégica, no sentido de assegurar o maior nível de interoperabilidade. Esta plataforma constitui a base de funcionamento de projetos tutelados pela AMA, como o Cartão de Cidadão, o Portal do Cidadão, o Balcão Intermunicipal, o Balcão Multiserviços, o Balcão Perdi a Carteira, as Lojas do Cidadão, o Portal da Empresa, etc. (AMA, 2008).

Dado que o objetivo deste estudo não está relacionado com o desenvolvimento de soluções tecnológicas, nem a análise de requisitos que estas devem comportar, ficam desta forma descartadas a utilização de um arquitetura ou de uma solução de interoperabilidade, focadas nas questões técnicas. Este é um estudo que pretende abordar um contexto de interoperabilidade já implementado, e em que a partilha de dados e de serviços são já uma prática comum, com o objetivo de estudar a questão da privacidade dos dados. Ou seja, contemplar os diferentes níveis de requisitos e exigências que surgem da heterogeneidade e preparação organizacional em relação à interoperabilidade, que apenas pode ser conseguido com o apoio de um modelo de interoperabilidade em detrimento de uma *framework*.

2.2.3 Modelos de maturidade de interoperabilidade

A interoperabilidade não é um problema recente. O DoD em 1965 deparou-se com a incompatibilidade entre as comunicações de rádio entre o Exército e a Força Aérea, apelidando esta situação de "fiasco de comunicação" (Ford et al., 2007). Este facto deu origem a um conjunto de diretivas que no imediato resolveram os problemas existentes, problemas que surgiram novamente com a introdução de novas tecnologias, essencialmente de comunicações. Esta situação promoveu o surgimento de várias estruturas temporárias ou permanentes, vocacionadas para o estudo do problema da interoperabilidade no domínio do DoD.

Em 1991 é publicada a diretiva DoDD 8320.1, denominada "*DoD Data Administration*", com o objetivo de apoiar operações do DoD assim como a tomada de decisões com base em dados que estejam de acordo com as necessidades de disponibilidade, exatidão, qualidade e oportunidade, e por outro lado provocar a partilha tanto vertical como horizontal de dados entre o DoD e outras agências governamentais, organizações do setor privado e países aliados (Winters et al., 2006). De salientar que esta diretiva surge antes da publicação dos principais modelos de maturidade de interoperabilidade entre sistemas.

Os modelos de maturidade descrevem os estágios pelos quais os sistemas, processos ou organizações progridem ou evoluem (Clark & Jones, 1999). Visam ajudar uma organização, empresa ou um sistema a melhorar a forma de cooperar e interoperar com outras entidades (Guédria, Naudet, & Chen, 2008).

Nos últimos trinta anos, governos e indústria desenvolveram ativamente investigação em modelos de interoperabilidade, com o objetivo de criarem uma forma correta de analisar, documentar e melhorar a interoperabilidade entre redes de pessoas, equipamentos, processos e organizações (Ford et al., 2007). A constituição de vários grupos de investigação contribuiu com a apresentação de várias definições de interoperabilidade, distinção entre vários tipos de interoperabilidade, assim como atributos, modelos e metodologias de análise da interoperabilidade. De acordo com estes autores, é no período de 1997 a 2006 que se verifica uma maior publicação de definições distintas de interoperabilidade, assim como de modelos de maturidade de interoperabilidade, como ilustrado na Figura 4.

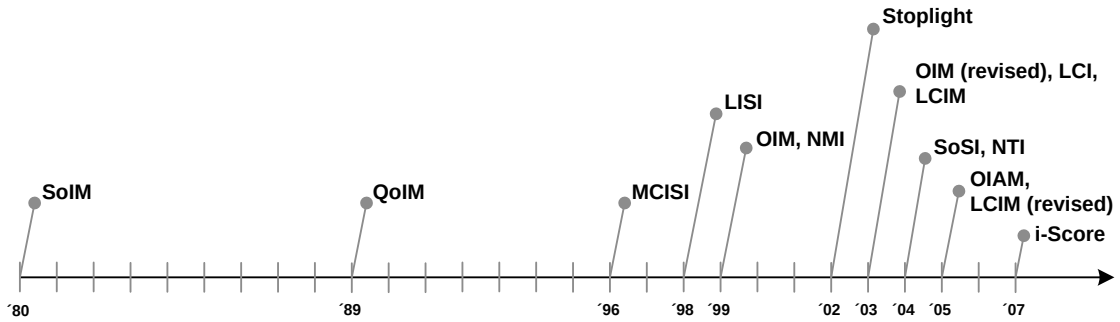

Figura 4 - Modelos de Interoperabilidade
(Ford et al., 2007)

Os vários modelos para análise e desenvolvimento de interoperabilidade entre sistemas, estruturam o processo em várias camadas ou níveis. A utilização de níveis ou camadas possibilita o desenho de um "sistema de sistemas" que apresente independência tecnológica, escalabilidade, funcionamento descentralizado, arquiteturas apropriadas, e suporta *standards*, segurança e flexibilidade (Kasunic & Anderson, 2004). Existem vários níveis de interoperabilidade entre dois sistemas, desde a não existência de interoperabilidade até uma interoperabilidade total (Tolk, 2003). Um modelo permite assim a construção de uma ponte entre o projeto conceptual e o projeto técnico para interoperabilidade, integração ou federação (Tolk & Muguira, 2003).

Winters et al., (2006) sugerem a categorização dos modelos existentes segundo três perspetivas de interoperabilidade, nomeadamente:

1. *Perspetiva organizacional* – focada em aspetos organizacionais da interoperabilidade, como objetivos e abordagens comuns, assim como mecanismos de interação;
2. *Perspetiva dos sistemas e tecnologias* – constitui a perspetiva mais utilizada, sendo que o seu principal objetivo está relacionado com a análise da ligação tecnológica dos sistemas;
3. *Perspetiva dos dados* – centrada na necessidade de os sistemas não se limitarem a partilhar dados, mas conseguirem partilhar como estes dados devem ser interpretados ou compreendidos pelos sistemas ou organizações.

Para este estudo é fundamental a utilização, podendo mesmo falar-se em adaptação, de um dos modelos de maturidade, como ferramenta de suporte ao estudo para a problemática da privacidade dos dados e o conhecimento do seu funcionamento em

contextos de interoperabilidade. O objetivo não é definir que nível de interoperabilidade deve ser atingido em matéria de proteção de dados, mas sim estudar este conceito em relação aos requisitos dos níveis de interoperabilidade de um dos modelos de maturidade. Ou seja, por um lado identificar os principais fatores essenciais à privacidade dos dados, e por outro estudar a sua relação e enquadramento com cada um dos níveis de maturidade da interoperabilidade, proposto por um dos modelos de referência.

Neste sentido, o sucesso deste estudo de investigação depende em grande parte da identificação do modelo de maturidade certo, que melhor suporte o estudo, com base nas suas características e objetivos de estudo. Com este propósito foi, numa primeira fase, recolhida informação sobre os modelos de maturidade publicados. Deste conjunto, foram excluídos alguns modelos[23] e selecionados os modelos *Levels of Information System Interoperability* (LISI), Organizational *Interoperability Maturity Model* (OIM), e *Levels of Conceptual Interoperability Model* (LCIM), como as potenciais opções de suporte ao estudo. Alguns dos modelos excluídos constituem versões destes três modelos, aplicáveis a domínios muito específicos e em alguns casos demasiado técnicos. Outros têm apenas por objetivo a avaliação da capacidade de interoperabilidade de uma organização.

Levels of Information System Interoperability (LISI)

O modelo LISI (Figura 5) considera cinco níveis crescentes de sofisticação em relação à partilha de informação e serviços. Os fatores que influenciam os cinco níveis de maturidade são classificados através de quatro atributos principais: **P**rocedimentos, **A**plicações, **I**nfraestruturas e **D**ados (PAID). Abrangem toda a gama de considerações de interoperabilidade, fornecendo uma metodologia para definir e identificar o conjunto de características necessárias para a troca de informações e serviços em cada nível de maturidade do LISI (C4ISR, 1998). Cada um dos atributos PAID tem

[23] Layers of Coalition Interoperability (LCI); System-of-Systems Interoperability (SoSI) Model (Morris, Levine, Meyers, Place, & Plakosh, 2004); NATO C3 Technical Architecture Reference Model for Interoperability (NMI); Organizational Interoperability Agility Model (OIAM) (Kingston et al., 2005) (Fewell et al., 2004); Organizational Interoperability Maturity Model for C2 (OIM) (Clark & Jones, 1999); The Layered Interoperability Score (*i-Score*) (Ford et al., 2007); NETHA Interoperability Maturity Model (NETHA, 2007b); Maturity levels for interoperability in digital government (Gottschalk, 2009b).

impacto na troca de informação, ou seja, existe um nível de interoperabilidade dentro de cada um dos atributos (Tolk, 2003).

Description	Computing Environment	Level	P	A	I	D
Enterprise	Universal	4	Enterprise Level	Interactive	Multi-Dimensional Topologies	Enterprise Model
Domain	Integrated	3	Domain Level	Groupware	World-wide Network	Domain Model
Funcional	Distributed	2	Program Level	Desktop Automation	Local Network	Program Model
Connected	Peer-to-peer	1	Local/Site Level	Standard System Drivers	Simple Connection	Local
Isolated	Manual	0	Access Control	N/A	Independent	Private

Figura 5 - Modelo LISI
(C4ISR, 1998)

Os 5 níveis de maturidade do processo de interoperabilidade são identificados por termos que descrevem tanto o nível de interoperabilidade como o ambiente em que esta ocorre (Clark & Jones, 1999). No nível 0 (Isolado), a informação é partilhada manualmente. Os sistemas necessitam de trocar dados mas não existe interoperabilidade física. No nível 1 (Ligado), a existência de uma ligação *peer-to-peer* entre os sistemas, permite que aplicações homogéneas partilhem informação, mas com aplicações e dados separados. No nível 2 (Funcional), sistemas distribuídos permitem que produtos heterogéneos partilhem conjuntos de dados heterogéneos, mas com aplicações e dados ainda separados. O nível 3 (Domínio), de integração dos sistemas, pois estes são capazes de partilhar dados de acordo com um modelo definido, assim como aplicações dentro de um domínio funcional específico. No nível 4 (Empresa), os sistemas são capazes de utilizar informação de múltiplos domínios, distribuída globalmente por vários espaços. Dados e aplicações são independentes e ambos podem ser partilhados (Winters, Gorman, & Tolk, 2006; Fewell & Clark, 2003).

Organizational Interoperability Maturity (OIM) Model

O *modelo* OIM desenvolvido por Clark & Jones (1999) em 1999 foi revisto em 2003 por Fewell & Clark (2003) e em 2004 por Fewell, Clark, Kingston, Richer, & Warne (2004). O seu desenvolvimento deveu-se à perspetiva demasiado técnica do modelo LISI (Ford et al., 2007), assim como à natureza cada vez mais técnico-social das organizações militares (Moon et al., 2008). Tecnicamente os SI podem ser

compatíveis e interoperáveis. No entanto, se as organizações participantes não apresentarem capacidades para interoperar, a sua eficácia numa determinada situação será substancialmente reduzida (Clark & Jones, 1999). O objetivo do OIM é ajudar a esclarecer as questões de, e facilitar o desenvolvimento de melhorias na, interoperabilidade (Clark & Moon, 2001).

O OIM (Figura 6) foi desenvolvido como um modelo de avaliação da interoperabilidade interorganizacional e não para avaliação de uma única organização face a um padrão. O seu foco principal constitui os fatores humanos que afetam a troca de informações (Fewell et al., 2004). Apenas a interoperabilidade organizacional está em causa (Guédria et al., 2008).

	Preparedness	**Understanding**	**Command and Coordination**	**Ethos**
4. Seamless	Complete – normal day-to-day working	Shared	Homogeneous	Uniform
3. Associative	Detailed doctrine and experience in using it	Shared communications and shared knowledge	One chain of command and interaction with home organization	Shared ethos but with influence from home organization
2. Collaborative	General doctrine in place and some experience	Shared communications and shared knowledge about specific topics	Separate reporting lines of responsibility overlaid with a single command chain	Shared purpose; goals, value system significantly influenced by home organization
1. Cooperative	General guidelines	Electronic communications and shared information	Separate reporting lines of responsability	Shared purpose
0. Independent	No preparedeness	Communication via phone etc.	No interaction	Limited shared purpose

Figura 6 - Modelo OIM
(Clark & Jones, 1999; Fewell & Clark, 2003; Fewell et al., 2004)

No nível 0 (Independente), existe apenas a interação entre organizações independentes, que não partilham objetivos nem uma plataforma comuns, mas com situações pontuais em que a interoperabilidade (não planeada) é necessária. No nível 1 (Cooperativo), apesar de ser possível poderem partilhar um objetivo global, as organizações continuam distintas, sendo que podem existir algumas linhas orientadoras que descrevem como deve decorrer a interoperabilidade, mas no essencial esta continua a acontecer de forma não planeada. No nível 2 (Colaborativo) existe uma *framework* comum de suporte à interoperabilidade e à partilha de objetivos, assim como à atribuição de funções e responsabilidades aos seus participantes, mantendo-se contudo as organizações distintas. No nível 3 (Associado), são partilhados sistemas de valor e objetivos, assim como uma

preparação e compreensão comuns de interoperabilidade. O nível 4 (Contínua), constitui o nível ideal de interoperabilidade organizacional, onde não existem impedimentos a uma interoperabilidade plena e completa, de uma forma continuada (Clark & Jones, 1999).

Os atributos capazes de influenciar a interoperabilidade focam-se nas questões organizacionais, onde se incluem a: (1) preparação – descreve e examina o grau de preparação da organização em interoperabilidade, onde se inclui as regras e práticas que serão aplicadas, bem como o nível de formação e experiências prévias em interoperabilidade; (2) compreensão – examina o nível e capacidades de partilha de informação e conhecimento, assim como o grau de entendimento comum desenvolvido entre as organizações participantes; (3) comando e coordenação – permite conhecer a partilha e delegação de responsabilidades entre as organizações que participam na colaboração, assim como a compatibilidade entre os estilos de gestão e de comando existentes; (4) ética – permite conhecer o impacto dos fatores socioculturais em cada um dos níveis de interoperabilidade. São o caso de restrições externas (legislação, ambientes político e económico, opinião pública e natureza da sociedade), estruturas organizativas, e níveis de confiança (risco, segurança, abertura e honestidade) entre as organizações (Clark & Jones, 1999; Kingston, Fewell, & Richer, 2005; Tolk & Muguira, 2003).

Levels of Conceptual Interoperability Model (LCIM)

A primeira versão do LCIM foi desenvolvida por Tolk & Muguira (2003), e à semelhança dos modelos LISI e OIM, apresentava cinco níveis de interoperabilidade. Foi posteriormente revisto por Turnitsa (2005) (Figura 7), justificando esta revisão pela necessidade de um maior conhecimento sobre os dados trocados entre sistemas, assim como na importância de conhecer qual a utilização (com compreensão) que os sistemas fazem com os dados.

Numa perspetiva centrada nos dados, permite aos sistemas interoperáveis uma compreensão do contexto dos dados, assim como os próprios conceitos que os dados representam (Winters et al., 2006).

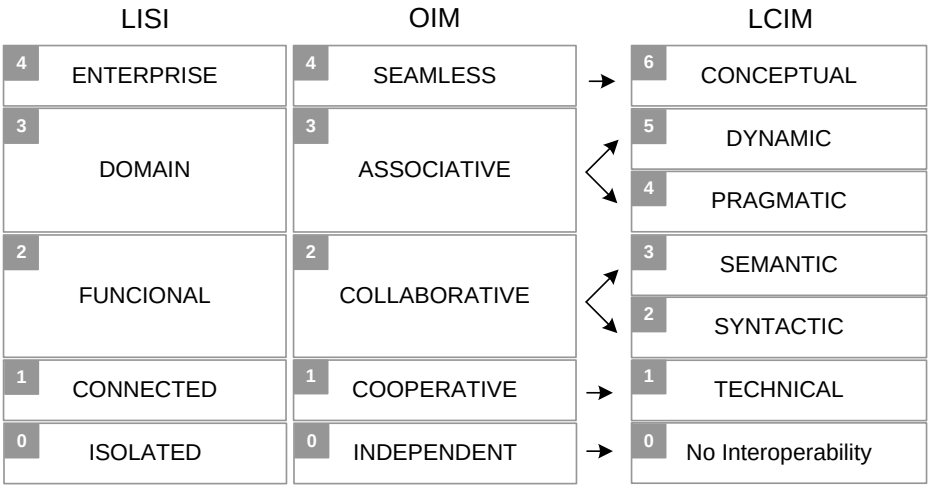

Figura 7 - Alinhamento entre modelos LISI, OIM e LCIM
(adaptada de (Winters et al., 2006; Tolk, 2006))

Na versão revista do LCIM, com sete níveis, no nível 0 – *não existe interoperabilidade* - os sistemas estão isolados. No nível 1 – *interoperabilidade técnica* - existe um protocolo para a troca de dados entre os sistemas, através de uma infraestrutura de comunicação comum, mas não existe um alinhamento entre os elementos de dados a enviar e receber. No nível 2 – *interoperabilidade sintática* - é introduzida uma estrutura comum para a troca de informação através da utilização de um protocolo comum para formato dos dados. No nível 3 – *interoperabilidade semântica* - é partilhado não apenas o mesmo protocolo para formato dos dados, como também o significado dos dados a partilhar, através de um modelo de referência para a troca de informação. No nível 4 – *interoperabilidade pragmática* – é atingida quando os sistemas conhecem mutuamente os métodos e procedimentos utilizados. Ou seja, a utilização de dados – ou o contexto da sua aplicação – foi entendida pelos sistemas participantes. No nível 5 – *interoperabilidade dinâmica* - os sistemas são capazes de se adaptar às alterações dos dados ao longo do tempo, nomeadamente às premissas e restrições que afetam o seu intercâmbio. No nível 6 – *interoperabilidade conceptual* - pressupõe-se a existência de modelos conceptuais que permitam modelar de forma abstrata a realidade (Wang et al., 2009; Tolk & Diallo, 2005; Rohatgi & Friedman, 2010).

Modelo de interoperabilidade selecionado para suporte do estudo

Os projetos que envolvem integração e interoperabilidade têm sido realizados com base em diferentes perspetivas. Alguns projetos centram-se principalmente nas vertentes administrativas e organizacionais sem enfatizar, por exemplo, as implicações tecnológicas. Outros projetos foram desenvolvidos numa perspetiva centrada unicamente no cidadão, minimizando os enormes obstáculos da interoperabilidade subjacente. No entanto, outros projetos tomam uma perspetiva centrada na tecnologia, desrespeitando inclusive numerosos desafios não-técnicos. A maioria dos projetos não consegue refletir a complexa rede de questões e restrições legais, organizacionais e técnicas envolvidas (Scholl & Klischewski, 2007).

São vários os modelos de maturidade, padrões, metodologias e diretrizes que podem auxiliar uma organização, empresa, ou um sistema, a melhorar as formas de cooperação ou interoperabilidade com outras entidades (Guédria et al., 2008). A sua utilização é essencial para lidar com a complexidade da problemática da privacidade dos dados em contextos de interoperabilidade. Podem, por um lado, facilitar a identificação e documentação dos vários de níveis de exigência e requisitos quanto à privacidade dos dados, e por outro permitem compreender a evolução necessária da interoperabilidade entre os vários sistemas, de forma a suportar os requisitos de proteção da privacidade dos dados. Ou seja, permitem definir linhas orientadoras e requisitos de proteção para a privacidade dos dados para cada um dos níveis de maturidade em interoperabilidade. Para este estudo foram apresentados os três modelos considerados nesta fase do estudo como os mais indicados para a abordagem pretendida da privacidade dos dados, nomeadamente os modelos LISI, LCIM e OIM.

A Tabela 8 permite compreender a área predominante de atuação destes três modelos quanto à interoperabilidade organizacional, entre processos, entre serviços concebidos e implementados de forma independente, e entre modelos de dados.

Tabela 8 - Áreas de preocupação da interoperabilidade para os modelos LISI, OIM e LCIM (Adaptada de (Guédria et al., 2008))

	LISI	**OIM**	**LCIM**
Organização	-	+++	-
Processos	-	-	-
Serviços	+++	-	-
Dados	+++	-	+++

O símbolo "+++" significa que existe uma preocupação forte do modelo em relação à área em que a interoperabilidade tem lugar, enquanto "+" denota uma preocupação fraca. O símbolo "-" significa que o modelo não cumpre.

Sendo o modelo LISI demasiado focado na complexidade da interoperabilidade técnica entre sistemas e na sua evolução tecnológica, este limitaria o estudo da privacidade dos dados às questões técnicas relacionadas com comunicações, *interfaces* e partilha de dados e serviços (aplicações). A avaliação de procedimentos, dados, infraestruturas e aplicações (atributos PAID) dentro de cada nível está muito orientada para os requisitos técnicos.

O LCIM por seu lado, está orientado para a interoperabilidade de dados e está focado nos aspetos da sua representação (sintática e semântica). Para Guédria et al. (2008) é o mais indicado para contextos de interoperabilidade de dados e serviços, uma vez que propõe soluções para resolver problemas de interoperabilidade, como o desenvolvimento de ontologias comuns, utilização e partilha de modelos conceptuais comuns e elementos de dados padronizados.

O modelo OIM, ao contrário dos modelos LISI e LCIM, está focado nas questões organizacionais relacionadas com as diferenças existentes nos métodos e processos de decisão, realidade e cultura organizacional. É um modelo de análise dos processos e trocas de informação entre organizações, assim como dos principais fatores, relacionados com a "*atitude humana*", mais influentes sobre estes (Fewell et al., 2004). Não propõe explicitamente uma abordagem específica para resolver problemas de interoperabilidade, mas sim a apresentação em cada nível de orientações e requisitos essenciais para se alcançar cada um dos níveis de maturidade.

Face ao exposto, em nossa opinião, o modelo OIM é o mais indicado para a abordagem pretendida à temática da privacidade de dados, uma vez que vai permitir abranger todos os requisitos essenciais à sua proteção de uma forma estruturada, do ponto de vista organizacional, com base nos atributos preparação, compreensão, coordenação e ética.

2.3. Desafios à problemática da privacidade dos dados em contextos de interoperabilidade

A privacidade é parte de um contexto social sujeito a uma série de fatores. A relação entre a privacidade e a sociedade sempre existiu. Contudo, os fatores (ou pressões) que afetam a privacidade nesta *era da informação* são variados e profundamente interligados. Fatores que individualmente e coletivamente, mudam e expandem-se a uma velocidade sem precedentes, com influência na nossa capacidade de compreender e lidar com as suas implicações para o mundo, em geral, e na nossa privacidade, em particular (Waldo, Lin, & Millett, 2010b). Estes autores identificaram um conjunto de fatores (apresentados na Tabela 9), capazes de provocarem grandes mudanças e que afetam as noções atuais, perceções e expetativas sobre a privacidade.

Tabela 9 - Fatores de larga escala que afetam a privacidade
(adaptada de Waldo, Lin, & Millett, 2010a)

Mudanças tecnológicas	Mudanças sociais	Descontinuidades na circunstância
• Ubiquidade • Conectividade • Recolha de dados • Armazenamento • Poder computacional • Usabilidade do *software* • Encriptação • Biotecnologia relevante para a privacidade • Portabilidade de dados e dispositivos de comunicação • Persistência dos dados • Acessibilidade dos dados e das comunicações • Avanços na tecnologia de sensores	• Globalização • Mobilidade • Virtualidade • Urbanização • Acessibilidade constante • Litigiosidade • Demografia/Envelhecimento • Novas formas de viver e comunicar • O crescimento das redes sociais • O aumento da interdependência social • O aumento da literacia em comunicações eletrónicas • O aumento da expectativa de disponibilidade de informação • Interligação dos sistemas monetários • Interligação dos sistemas de produção	• Ataques catastróficos em 2001 ao World Trade Center / Pentágono • Invenção em 1995 da World Wide Web[24] • Ameaças de saúde nacionais e internacionais (SARS[25] e a gripe das aves) • Audiências do Comité da Igreja de 1976 no Senado dos EUA • Escândalo de Watergate em 1972-1973 • Ataque a Pearl Harbor em 1941

Na opinião de Waldo, Lin, & Millett (2010a) estes múltiplos motores de mudança sugerem como as nossas atitudes em relação à privacidade estão dependentes do contexto. É difícil manter uma visão precisa do que a privacidade é, ausente de considerações sobre que tipo de informação é solicitada, quem a procura, e como esta

[24] A World Wide Web pode ser um produto dentro da categoria mudanças tecnológicas, mas também constitui a principal força motriz subjacente à explosão do uso da Internet que finalmente permitiu que enormes quantidades de dados – pessoais e outros – estejam acessíveis publicamente.

[25] SARS (do inglês *Severe Acute Respiratory Syndrome*) ou síndrome respiratória aguda grave.

deve ser obtida, protegida e utilizada. Segundo estes autores, determinar o que deve (1) ser deixado no âmbito da ética, (2) ser incentivado ou desencorajado, ou (3) ser formalizado em regulamentos ou leis, é cada vez mais uma questão de equilíbrio, no contexto da privacidade, e como o ambiente muda, é fácil verificar como entendimentos e o *status quo* desenvolvidos anteriormente podem ser abalados.

A maioria das TI afeta a privacidade, sendo que muitas constituem meios sofisticados e facilitadores de recolha "silenciosa" de informações. Permitem a recolha de dados pessoais muito detalhados, a construção de perfis que podem ser usados para identificar grupos específicos de pessoas, assim como localizar e acompanhar pessoas (Frissen et al., 2007). Para estes autores, o papel das tecnologias na salvaguarda do direito à privacidade é ambíguo e constituiu um paradigma[26]: as tecnologias são tanto um potencial protetor como um agressor de privacidade.

Para Waldo et al. (2010b) as TI promoveram de forma significativa uma alteração nas formas e conceitos associados à pesquisa, produção, manipulação, armazenamento[27], aquisição[28] e análise de informação. Estas alterações tiveram como consequência direta uma erosão da proteção da privacidade. Isto porque durante muito tempo os efeitos da recolha de dados não eram considerados como uma questão importante, uma vez que os dados importantes eram inacessíveis para outros fins práticos, e eram armazenados em locais diferentes, difíceis de agregar.

Tendo em conta o rápido desenvolvimento, crescimento e inovação tecnológica, é necessário questionar: qual a segurança numa perspetiva de privacidade destas inovações tecnológicas? A resposta a esta questão reside não só na tecnologia em si, mas também noutros fatores essenciais para o desenvolvimento de tecnologias mais "amigáveis" da privacidade (Aquilina, 2010).

---

[26] Tecnologias *Web*, redes sociais, RFID, tecnologias biométricas, sistemas de gestão do conhecimento, *Web* semântica, perfis inteligentes e sistemas de *workflow* – são algumas das tecnologias que mais afetam o paradigma da privacidade. Vão levar a um aumento na quantidade de dados pessoais reunidos e consequentemente no número de bases de dados.

[27] Os registos de informação já não são "deitados fora". Tornou-se menos dispendioso manter maiores quantidades de dados, face a dispositivos de armazenamento mais baratos, do que "abater" informações com precisão de modo a remover os dados. Como resultado, os dados que sobrevivem à sua utilização original são mantidos, tornando-se objeto de utilizações futuras imprevistas.

[28] Dispositivos como sensores, de recolha de imagem e vídeo, etiquetas de radiofrequência (RFID), telemóveis e cartões eletrónicos, entre outros, facilitam a aquisição de muitos tipos de informação sobre indivíduos.

Tal como as empresas em todo o mundo continuam a expandir os seus negócios e infraestruturas de TI, que agregam mais dispositivos e conectividade com outras empresas, também o volume de dados que requerem uma monitorização 24x7 continua a crescer. Este facto pode aumentar consideravelmente a vulnerabilidade de uma organização, ao ser cada vez mais difícil, por um lado desenvolver e implementar medidas efetivas de proteção destes dados, e ao mesmo tempo lidar com enormes quantidades de dados de eventos de segurança, que este crescimento origina (IBM, 2014).

A interoperabilidade e a cooperação podem ser consideradas como facilitadoras da integração de serviços. Um pré-requisito, ou mesmo o "objetivo final" para qualquer sistema integrado ou de colaboração, é a *partilha de informações ou dados*, a qual deve acontecer num ambiente seguro e de proteção da sua privacidade (Otjacques et al., 2007). A evolução da interoperabilidade entre sistemas pode apresentar como consequência direta uma erosão da proteção da privacidade (Waldo et al., 2007). Apesar da importância do desenvolvimento da interoperabilidade, esta não deve ser abordada apenas como uma questão puramente técnica, dados os riscos que podem surgir da interligação dos sistemas, que podem ter um impacto profundo sobre a privacidade e a proteção de dados (Art. 29 WP, 2009). A pressão para partilhar dados pessoais dentro e fora das organizações, pode levar a problemas relacionados com a privacidade, que surgem pelo facto de: (1) os dados de sistemas "que respeitam a privacidade" serem partilhados com outros sistemas, menos capazes de respeitar as necessidades de privacidade, fazendo com que os dados fiquem vulneráveis; (2) as cópias de dados pessoais em trânsito nem sempre são adequadamente protegidas; (3) as organizações muitas vezes agregam dados, em vez de os partilhar, duplicando assim dados pessoais e aumentando o risco de inconsistência e perda de controlo sobre estes dados; e (4) os identificadores – dados como nome, data de nascimento, número de segurança social que em muitos casos funcionam como credenciais de identificação primária – são muitas vezes usados como índices, o que dificulta que estes dados sejam anonimizados, e apesar de facilitarem a partilha de dados, faz com que estes sistemas fiquem vulneráveis a fraudes relacionadas com a identidade (ICO, 2008).

No âmbito do projeto NETHA (2005) foram identificadas uma série de restrições que permitem distinguir a implementação de interoperabilidade num ambiente alargado de colaboração, do de uma única organização, nomeadamente:

a. A comunidade colaborativa é diferente nas suas capacidades individuais e estruturas organizacionais, sendo que a diversidade oferece resistência, mas também destaca os desafios e potenciais fraquezas da colaboração.
b. Apesar da abertura da comunidade à mudança da sua constituição, esta necessita de suporte para uma série de eventos previsíveis e às vezes imprevisíveis.
c. As estruturas organizacionais são complexas, mas a comunidade é uma ordem de magnitude mais ampla e portanto, de evolução mais complexa.
d. Os membros têm obrigações na comunidade de colaboração, mas ao mesmo tempo esforçam-se por objetivos organizacionais que podem colocá-los em concorrência com outros membros da comunidade.
e. Muitos vão destacar a fraca capacidade de interoperabilidade dos ambientes de integração modernos. São precisamente estes que exigem a presença de peritos externos sempre que é necessário reconstruir a interoperabilidade, cada vez que é necessária uma mudança. Uma comunidade ou ambiente de colaboração não pode evoluir nem funcionar desta forma.
f. Num ambiente de colaboração, as questões técnicas podem ser ofuscadas por questões de jurisdição.
g. As fronteiras são uma consequência natural do desenho de múltiplos sistemas independentes, mas numa comunidade diversificada, o reconhecimento e a transição entre fronteiras são um alicerce central à colaboração.
h. A tecnologia muda mais rápido do que a informação. Uma abordagem orientada aos dados para a interoperabilidade é mais sustentável do que uma abordagem tecnológica, num ambiente em mudança.

Este aumento da partilha de dados faz com que seja necessário o desenvolvimento de tecnologias e padrões de proteção da privacidade inter-organizacionais (Moen et al., 2010). Este desenvolvimento depende da capacidade de partilha de dados e experiências, para lá das fronteiras departamentais, organizacionais, geográficas e institucionais, fundamental ao desempenho conjunto das organizações (Gottschalk, 2009b).

Os desafios de investigação, tanto em privacidade como em segurança, estão longe de ser resolvidos, especialmente os relacionados com a gestão da privacidade dos dados, sendo necessárias soluções de apoio à definição e aplicação de políticas de proteção, monitorização e negociação de políticas conjuntas entre as várias organizações. A Tabela 10 permite compreender os principais desafios identificados em relação à privacidade dos dados para o ambiente de interoperabilidade entre organizações.

Tabela 10 - Desafios em relação à privacidade dos dados, para os intervenientes num ambiente de interoperabilidade

• Disponibilizar ao titular de dados ferramentas de controlo e monitorização das questões da privacidade dos seus dados pessoais.
• Assegurar os direitos que assistem o titular dos dados.
• Assegurar nas organizações práticas de gestão da privacidade e proteção dos dados e garantir a sua conformidade com os requisitos regulamentares e da legislação em vigor.
• Analisar e gerir os riscos das várias situações normativas locais de privacidade.
• Assegurar a privacidade e a segurança dos dados quando estes são transferidos e/ou partilhados entre organizações.
• Desenvolver níveis de colaboração que ajustem as medidas de proteção da privacidade ao nível de interoperabilidade implementado.
• Promover a colaboração (interoperabilidade organizacional) por forma a integrar todos os aspetos da gestão da privacidade em todas as organizações.
• A operacionalização da privacidade através de uma rede distribuída, que inclua profissionais dedicados à gestão da privacidade.

A interoperabilidade entre SI, ao facilitar a partilha de dados e o desenvolvimento de serviços conjuntos, implica que tanto dados como serviços sejam da responsabilidade dos vários intervenientes. É, desta forma, essencial o desenvolvimento de um ambiente de colaboração, que consiga para o contexto de multiutilização expandido, de profissionais ou sistemas que apresentam na sua base conceitos e condições muito diferenciadas (ou mesmo inexistentes) no tratamento dos dados, compreender quais os fatores críticos à privacidade dos dados e que devem resultar da interoperabilidade numa perspetiva organizacional.

Capítulo III – Fatores críticos à privacidade dos dados em ambientes de interoperabilidade

No Capítulo anterior foram apresentados os conceitos relacionados com a privacidade no geral, a privacidade dos dados em particular, e a interoperabilidade entre sistemas, resultantes da primeira fase da revisão bibliográfica. O conhecimento destes dois conceitos, o estudo da sua interdependência, a sua importância e os principais desafios colocados ao desenvolvimento dos SI, foram fundamentais para definir um rumo para o estudo da dinâmica da privacidade dos dados, localmente ou em ambientes de interoperabilidade.

Este terceiro Capítulo, tendo como ponto de partida os principais desafios colocados para a privacidade dos dados para ambientes de interoperabilidade identificados no Capítulo anterior, procura identificar aquilo que é determinante à proteção da privacidade dados e que deve resultar da colaboração entre as organizações.

Indo assim de encontro ao objetivo principal deste estudo, o resultado final desta fase da investigação deve permitir identificar, compreender e fundamentar teoricamente um conjunto de fatores críticos que, pensamos, têm forte influência sobre a proteção da privacidade dos dados para um ambiente de interoperabilidade.

Ainda neste Capítulo, os fatores identificados serão alinhados com os atributos e um dos níveis de maturidade de interoperabilidade do modelo OIM.

3.1 Fatores considerados para a problemática em estudo

Este estudo só é viável se, com base nas várias fontes fidedignas de informação, for possível identificar fator a fator, se este é determinante para a privacidade dos dados, compreender exaustivamente o seu funcionamento, as suas características e posteriormente proceder à sua validação num cenário *natural* de utilização de dados, com recurso às ferramentas adequadas. Isto significa que o detalhe e conhecimento nesta fase do estudo vão repercutir-se nas fases posteriores, devendo para cada fator em causa diminuir-se a incerteza ao mínimo. Desta forma, procurou reunir-se para cada um dos fatores o máximo de informação, com qualidade científica, e criar uma estrutura de conhecimento e argumentos sólidos, essenciais à viabilidade do estudo.

Foram desta forma, consideradas como principais fontes de informação, documentos legislativos e regulamentares, relatórios e pareceres de instituições nacionais e internacionais, projetos relevantes no domínio da privacidade, fóruns especializados em privacidade e segurança e em tecnologias no domínio da saúde, teses de doutoramento, e variadíssimos artigos de investigação científica.

É muito importante que a lista dos fatores identificados seja representativa do fenómeno em estudo e suficientemente compreensível para uma futura aplicação prática. Contudo, tal não significa que a mesma se encontre fechada; deve manter-se a perspetiva de incluir novos conhecimentos, que possam surgir durante o processo de recolha de dados.

A decisão de um fator poder ser considerado para a problemática em estudo, depende da sua real influência sobre a privacidade dos dados partilhados entre as organizações, e de acordo com as suas características, pode resultar da interoperabilidade entre as partes envolvidas no processo de partilha de dados. Deve, assim, ser possível para cada fator compreender, a forma como este pode afetar a privacidade dos dados, assim como as medidas de proteção relacionadas com este fator que dependem do trabalho conjunto entre as organizações envolvidas.

3.1.1 Experiência

Apesar das dificuldades que se podem colocar ao desenvolvimento da interoperabilidade e da desadequação de algumas disposições, as questões da privacidade e proteção de dados devem ser impreterivelmente preservadas e salvaguardadas neste tipo de iniciativas. É importante que os profissionais responsáveis pela interconexão dos sistemas tenham sensibilidade e consciência da importância que esta questão assume, assim como os profissionais tenham as competências necessárias para utilizar devidamente as tecnologias, cada vez mais disponíveis no mercado, para garantir a privacidade e segurança dos dados (Soares, 2009). A complexidade crescente de tecnologias e sistemas, e o facto de estes serem cada vez mais críticos para o funcionamento das organizações, assim como na aplicação de características, padrões e práticas de desenho em privacidade, exige conhecimentos cada vez mais especializados (Cavoukian, 2009).

A delegação de autoridades e responsabilidades para a proteção de dados a unidades organizacionais apropriadas é apontada como uma solução eficaz em muitas organizações, assegurando-se nestes casos a disponibilização dos meios de formação necessários que lhes permita manterem-se atualizados quanto às necessidades atuais e emergentes em questões de privacidade e proteção de dados, e conscientes da importância da privacidade dos dados para os indivíduos e para o sucesso e reputação da organização (Hunton & Williams, 2010). A realização de fóruns, *workshops*, relatórios, e outros eventos de colaboração entre organizações, de partilha de experiências ou aprendizagem, podem apoiar a partilha de visões e conhecimentos dos vários setores em relação à privacidade. Através destes processos, a colaboração com outras organizações pode afetar a mudança, dado que "a organização incorpora aquilo que resultou da exploração conjunta com outras organizações" (Bamberger & Mulligan, 2011).

Neste mundo cada vez mais digital, é assim necessário que os profissionais compreendam o conceito de privacidade dos dados e saibam como devem ser geridas informações sigilosas. Consciencializar todos os profissionais sobre o que é esperado deles neste domínio, ajuda a construir uma cultura que valoriza a proteção de dados e consegue gerir, de uma forma segura, um ativo valioso para as organizações – os dados pessoais (Cavoukian, 2011). Se uma organização pretende levar a sério as questões da privacidade, então é necessário que haja uma maior responsabilidade na gestão da privacidade - por exemplo através de um *Chief Privacy Officer (CPO)* ou equivalente (ICO, 2008). A ambiguidade do ambiente externo em relação à privacidade promove cada vez mais a dependência das organizações em relação à análise profissional dos CPO (Bamberger & Mulligan, 2011).

Uma maior responsabilidade das organizações em relação à privacidade dos dados está dependente de pessoas com profundos conhecimentos e compreensão dos aspetos técnicos e jurídicos no domínio da proteção de dados, com aptidões para comunicar, dar formação a colaboradores, criar e aplicar políticas de proteção e realizar auditorias neste domínio (Art. 29 WP, 2010b). Apesar de reconhecerem a necessidade de trabalhar dentro das limitações económicas e de recursos, as organizações devem ter profissionais suficientes para garantir o sucesso do seu programa de privacidade, com uma formação adequada, que lhes permita, por um lado, assumirem um papel no programa de privacidade e, por outro, serem capazes

de lidar com os desafios resultantes da evolução do próprio programa (Hunton & Williams, 2010). É extremamente importante um padrão exigente de preparação destes profissionais em relação às questões da privacidade, assim como uma atenção especial em relação à qualidade dos materiais a disponibilizar, bem como ao acompanhamento da performance e participação de todos os outros profissionais (Cavoukian, 2011).

Esta evolução é vital para assegurar que os responsáveis pelo tratamento de dados consigam realizar as suas obrigações incluindo, se necessário, a realização de auditorias internas e externas. Simultaneamente, tal evolução é benéfica para as autoridades de proteção de dados pois, na medida em que o sistema contribuirá para uma maior conformidade geral, as autoridades terão ao seu dispor mais e melhor informação sobre as práticas internas das empresas, e a formação de profissionais em matéria de proteção de dados altamente qualificados facilitará certamente a sua interação com os responsáveis pelo tratamento de dados (Art. 29 WP, 2010a).

Um estudo[29] da *European Union Agency for Network and Information Security* (ENISA, 2010) a 18 organizações líderes na prestação de serviços *on-line,* concluiu que no domínio dos dados pessoais, mais de metade (54.5%) processa informações confidenciais dos seus utilizadores e que das 18 organizações apenas duas não têm um gabinete de privacidade ou alguém que cumpra esta função. Contudo, o relatório revela uma situação preocupante: apenas 29% dispõe de profissionais em tempo integral com esta responsabilidade.

A definição do profissional em privacidade está a mudar. A privacidade é um assunto multidisciplinar, que requer o conhecimento das diferentes funções da organização, bem como a compreensão e colaboração com outras partes interessadas na informação. Além dos profissionais para os quais a privacidade é a sua função principal, verifica-se uma tendência de aumento nas competências e conhecimentos em privacidade por parte de outros profissionais. São os casos de responsáveis por recursos humanos, segurança, TI, auditorias internas, marketing, gestão documental, gestão de projetos e outras funções. Todos eles necessitam de conhecer o suficiente

[29] Este estudo teve como objetivos identificar quais as práticas atualmente aplicadas pelas organizações para alcançarem uma conformidade em relação à regulamentação e expetativas de privacidade, e também apontar quais destas práticas podem ser amplamente vinculadas como boas práticas. Incluiu seis áreas principais: responsabilidade, confiança, consentimento, rastreamento, segurança e privacidade (ENISA, 2010).

sobre a proteção da privacidade e dos dados, para evitarem erros simples e serem capazes de identificar as questões da privacidade dentro da organização (Ernst & Young, 2012b). As funções do profissional em privacidade, com influência sobre a importância da privacidade na tomada de decisão corporativa, estão a contribuir para que a questão da privacidade seja integrada no processo de decisão estratégico da organização, e respondem à necessidade crescente de interação com intervenientes externos, incluindo reguladores e outras organizações (Bamberger & Mulligan, 2011).

Apesar de os profissionais de privacidade ainda não constituírem um forte centro de gravidade dentro das organizações, esta situação pode mudar nos próximos anos, essencialmente devido ao aumento crescente atribuído à sua *responsabilidade* para com a privacidade e proteção de dados pessoais, assim como ao papel operacional cada vez mais necessário destes profissionais face à insuficiência da legislação em resolver todos os problemas (Ernst & Young, 2012b). Os profissionais em privacidade operam, contudo, num ambiente desregulado, onde existem poucas qualificações reconhecidas ou organismos de acreditação, o que dificulta a compreensão por parte das organizações do nível de competências desejável para estes profissionais (ICO, 2008).

A maturidade de um gabinete de privacidade tem um efeito direto sobre a maturidade da gestão da privacidade como um todo. Com a presença de um profissional em privacidade dentro da organização, o seu conhecimento é passado a outros profissionais. Isto não só cria uma fluência da privacidade com outras partes da organização, como também faz com que a privacidade seja uma responsabilidade de todos (Ernst & Young, 2013). Em organizações que tratam a informação intensivamente, o papel do gabinete de privacidade evoluiu significativamente. Além de um aumento no número de profissionais em privacidade, na opinião de J. Trevor Hughes, CEO da *International Association of Privacy Professionals*[30] (IAPP), também se alterou o papel que os profissionais de privacidade desempenham dentro da organização, verificando por exemplo um maior crescimento por parte da gestão do risco nas questões da privacidade (Ernst & Young, 2012b). No entanto, em organizações de dimensão média, em que as responsabilidades de privacidade são de

[30] A IAPP é uma comunidade de profissionais de privacidade, atualmente com mais de 1300 membros em 78 países. Informação consultada em 14.setembro.2013 no *URL*: https://www.privacyassociation.org/about_iapp.

evolução lenta e que não tratam dados intensivamente, a gestão da privacidade é cada vez mais assegurada por gestores de nível médio, para os quais a privacidade é uma das muitas tarefas ao longo da sua carreira (Ernst & Young, 2013).

Para o espaço Europeu, a proposta de alteração do regulamento de proteção de dados (GDPR, 2012) não propõe diretamente que as organizações adotem a figura do profissional em privacidade dos dados, mas sim a criação de uma nova função especializada, denominada de *delegado para a proteção de dados*, profissional que deve ser associado a todas as matérias relacionadas com a proteção de dados pessoais. A introdução da figura de delegado de proteção de dados é indubitavelmente bem-vinda, pela função crucial de apoio ao cumprimento interno das regras de proteção de dados, além da vantagem de ser um interlocutor privilegiado da autoridade de controlo (CNPD, 2012b).

Em resumo, para a experiência:

- Uma interoperabilidade organizacional que promova o alinhamento de medidas de proteção de dados está muito dependente da experiência organizacional em questões de privacidade e em proteção de dados, assim como em projetos que envolvam partilha de dados ou serviços sob a forma de interoperabilidade.
- É essencial para o contexto da colaboração a existência de profissionais especializados e dedicados ao desenvolvimento conjunto de um projeto de proteção de dados.
- Uma experiência em projetos de interoperabilidade, quer técnicos, quer organizacionais, é fundamental para fazer face aos desafios que surgem das exigências da interoperabilidade organizacional.

3.1.2 Cultura de privacidade

Reconhecer que cada organização é única, e que as necessidades de privacidade são igualmente únicas, devem incentivar ao desenvolvimento de uma cultura de privacidade. Entenda-se por cultura de privacidade como o desenvolvimento de uma "mentalidade" – uma forma de pensar em toda a organização, que está comprometida em implementar as melhores práticas de gestão da informação que respeitem a privacidade. Mesmo as mais avançadas tecnologias, em conjunto com as políticas de privacidade mais rigorosas, não serão eficazes se a privacidade não for aceite como uma parte da cultura empresarial (IPC, 2009). É desejável um aumento no reconhecimento da importância da privacidade (consciencialização coletiva) e dos conceitos de segurança, dentro das organizações, a fim de fomentar um alto nível de segurança e confiança por parte dos cidadãos e da sociedade nas infraestruturas tecnológicas e nos serviços prestados dentro da UE (ENISA, 2010).

Para algumas organizações a privacidade constitui apenas uma função da segurança da informação, o que leva a falhas e lacunas no que diz respeito às necessidades de privacidade (ICO, 2008). São vários os argumentos apresentados pelos proponentes e responsáveis pelo desenvolvimento de tecnologias, fornecedores e integradores, executivos e gestores de projetos, no sentido de a privacidade dar prioridade aos objetivos operacionais e organizacionais. Por exemplo, é comum verificar-se uma análise privacidade versus segurança, privacidade versus funcionalidade do sistema de informação, privacidade versus eficiência operacional, privacidade versus controlo organizacional, e privacidade versus usabilidade (Cavoukian, 2009). Apesar do aumento de consciência da necessidade de considerar a privacidade em projetos tecnológicos, os seus engenheiros ainda reconhecem mal as suas questões e a sua importância (Al-Fedaghi, 2012). Quando questionados sobre questões de privacidade no âmbito do desenvolvimento aplicacional, estas questões são vistas tanto como "um problema abstrato, não é um problema imediato, não é de todo um problema (uma *firewall* e a encriptação dos dados conseguem resolver o problema), ou simplesmente não fazem parte dos requisitos do projeto" (Lahlou, Langheinrich, & Röcker, 2005).

Um relatório da *US Federal Trade Commission* (2010) recomenda que as organizações devem incorporar a privacidade e a segurança na sua rotina de práticas de negócio, com a segurança a ser um elemento de um programa de privacidade abrangente. De todas as perdas de dados comunicadas, acredita-se que apenas 5%

são devidas a questões tecnológicas, enquanto 95% se devem a fatores culturais ou ao comportamento das pessoas. A maioria das organizações está a passar por algum tipo de transformação, em que as culturas tradicionais estão a ser desmontadas e reconstruídas no sentido de incluir novas perceções e comportamentos em relação à segurança. No entanto, se esta mudança não for tratada de forma explícita, a mudança cultural, tão desejada, pode causar medo, incerteza e dúvidas, que podem ter um impacto sobre as atitudes dos profissionais em relação à segurança. A mudança deve ser gerida (Colwill, 2009).

Embora exista consenso sobre os princípios da privacidade, continuam a existir muitas questões e desafios relacionados com a aplicação generalizada destes princípios e como estes se relacionam com a utilização e reutilização da informação (Culnan, 2011). O facto de a segurança e a privacidade da informação constituírem um fenómeno relativamente novo, coloca desafios constantes às organizações. Ainda que só com aproximadamente 30 anos, a sociedade no seu todo, tenta entender o desgaste contínuo das fronteiras digitais. O excesso de partilha de dados pessoais, que constantemente empurram os limites da privacidade, é apenas uma das várias questões que o mundo digital gerou. Dentro das organizações, compreender e estabelecer estas fronteiras tornou-se extremamente importante. As organizações devem incorporar a privacidade dentro dos seus processos de negócio na mesma forma que incorporam outros valores fundamentais como a justiça, a transparência e a proporcionalidade. Para atingirem um sucesso estável e de alto nível, as organizações necessitam de adotar a proteção de dados pessoais como um imperativo de negócio (Ernst & Young, 2013).

Cavoukian (2009a) desenvolveu o conceito "*Privacy by Design*" (PbD), no qual a privacidade constitui um conceito de *design*/arquitetónico, com o objetivo de incorporar proativamente a privacidade nas especificações de desenho das várias tecnologias, práticas de negócios e projetos físicos. Para esta autora, o futuro da privacidade não pode ser assegurado apenas pela sua conformidade em relação aos quadros regulamentares, tem que ser também pelo seu enquadramento na forma regular de operação de uma organização. Os sete princípios orientadores de base ao conceito PbD, apresentados pela autora, são essenciais a este enquadramento e importantíssimos para o desenvolvimento de uma cultura de privacidade, nomeadamente: (1) tomar medidas proativas e não reativas, medidas preventivas e

não corretivas; (2) garantir uma proteção integrada no sistema, implicitamente; (3) integrar a privacidade no modelo e na arquitetura dos sistemas e nas práticas organizacionais; (4) garantir um funcionamento total com base no "todos ganham", e não "se alguém ganha, o outro perde"; (5) garantir a segurança de um extremo ao outro, durante todo o período de proteção da informação; (6) garantir a visibilidade e a transparência; e (7) respeitar a vida privada dos utilizadores — manter a atenção centrada no utilizador.

Para o conceito *PbD,* o maior desafio será alcançar um ambiente cultural, de gestão, tecnológico e regulamentar que consiga efetivamente resolver os problemas da privacidade (ICO, 2008), muito dependente, na prática: (1) do reconhecimento de que as preocupações e interesses de privacidade devem ser abordados através da compreensão do valor e dos benefícios da adoção de boas práticas de privacidade; (2) da aplicação, de forma sistemática, dos princípios básicos e universais de proteção da privacidade; (3) de contemplar atempadamente as questões da privacidade em todo o ciclo de vida dos dados; (4) da necessidade de profissionais e líderes qualificados em privacidade; e (5) da adoção e integração de tecnologias de proteção da privacidade (Cavoukian, 2009).

Muitas organizações já começaram a aplicar os princípios do PbD, como o *Information Commissioner's Office*[31] (ICO), que face ao facto de as organizações nem sempre considerarem ou tratarem as questões relacionadas com a privacidade durante todo o ciclo de vida dos seus sistemas, promoveu a utilização da abordagem PbD (ICO, 2011). Procurou-se, desta forma, incentivar as organizações a darem a devida atenção às questões da privacidade, antes do desenvolvimento de qualquer novo sistema ou processo, assim como promover o seu controlo durante todo o ciclo de vida do sistema (EPG, 2008). Esta abordagem vai garantir o desenho de controladores mais fortes sobre a privacidade, mais simples de implementar, difíceis de ultrapassar e totalmente incorporados nas funcionalidades principais do sistema (ICO, 2008).

[31] Autoridade independente do Reino Unido, criada para defender os direitos de informação de interesse público, e promover a abertura dos organismos públicos e da privacidade dos dados aos indivíduos. Mais informação sobre esta instituição pode ser consultada no *URL*: http://www.ico.gov.uk/.

No entanto, a evolução de uma nova abordagem para a gestão da informação pessoal que enraíze os princípios da privacidade em cada uma das partes de cada sistema e de cada organização, constitui um enorme desafio. O seu sucesso está condicionado pela eliminação de um conjunto de "barreiras", condicionantes de um ambiente de privacidade mais produtivo, nomeadamente a falta de consciência e compromisso das necessidades de privacidade ao nível executivo da gestão; a falta de planeamento da funcionalidade privacidade dentro do ciclo de vida dos sistemas; e o conflito existente entre as necessidades de privacidade e a pressão constante para partilhar dados pessoais dentro e fora das organizações (ICO, 2008).

O grupo de trabalho do Art. 29 WP (2009) recomendou mesmo que, para reforçar os direitos individuais de privacidade e proteção de dados, o conceito PbD seja reconhecido como um novo princípio de privacidade, e em caso de necessidade, seja utilizado para regulamentação de determinados contextos tecnológicos (Wong, 2011). Esta recomendação deve-se ao facto de apesar de a Diretiva 95/46/CE ser útil na promoção do conceito PbD, na prática não tem sido suficiente para garantir que a privacidade é incorporada nas TIC. Os utilizadores de serviços de TIC – empresas, setor público e certamente indivíduos – não estão em posição de por si mesmos tomarem medidas de segurança relevantes, a fim de protegerem a sua informação pessoal. Esta recomendação por parte do Art. 29 WP (2009) foi contemplada na proposta de regulamento para a proteção de dados (GDPR, 2012), através do Artigo 23º do Capitulo IV – Proteção de dados desde a conceção e por defeito.

Em resumo, em relação à cultura de privacidade:

- O desenvolvimento de uma cultura de privacidade é sinónimo de uma melhor preparação organizacional em questões de privacidade e de proteção de dados.
- A identificação, definição e gestão dos vários tipos de privacidade, assim como o seu alinhamento (interoperabilidade organizacional) com situações similares em outras organizações, está interligado com o desenvolvimento de uma cultura e conhecimento sobre privacidade.
- A compreensão das decisões e medidas desenhadas ao nível da privacidade, da proteção e da segurança dos dados, fica facilitada com uma maior cultura de privacidade por parte de todos os profissionais.

3.1.3 Segurança e infraestruturas

A segurança está normalmente associada à disponibilidade e resiliência dos sistemas e infraestruturas tecnológicas, e no domínio da informação à garantia da sua confidencialidade e integridade. Envolve a aplicação e gestão de medidas de segurança adequadas, tendo por base o conhecimento de uma ampla gama de ameaças, com o objetivo de minimizar os impactos e garantir o sucesso e a continuidade de um processo de negócio sustentado (ISO/IEC, 2009). É, sem qualquer dúvida, um componente crítico de qualquer sistema informático, devendo fornecer as garantias necessárias à proteção dos dados, sendo que numa situação ideal deve ser desenvolvido como um serviço quase invisível, mas forte. (Liberty Alliance, 2003). A necessidade de uma melhor segurança não é mais uma opção (Berger, 2014).

A *segurança* é consagrada como um dos princípios da proteção de dados, através do artigo 17º da Diretiva 95/46/CE (CE, 1995), que define que os dados pessoais devem ser tratados de uma forma que garanta um nível de segurança adequado aos riscos inerentes ao tratamento e à natureza dos dados. Ou seja, para qualquer processo de recolha de dados pessoais, a garantia da sua segurança, depende do conhecimento dos riscos associados, assim como do tipo de dados utilizados.

A segurança da informação é particularmente importante na prestação de serviços de saúde, uma vez que contribui para garantir que as obrigações de privacidade são cumpridas (NETHA, 2009). Mesmo que em algumas situações a segurança seja definida como um aspeto da privacidade (Solove, 2008), é consensual que a privacidade e a segurança são conceitos diferentes (Jericho Forum, 2007b), e não devem ser separados uma vez que estão interligados (Wuyts et al., 2009). Contudo, lidar com sucesso com estes dois conceitos depende do entendimento que se tenha sobre as diferenças importantes entre estes (NETHA, 2009). As organizações podem garantir com sucesso a segurança dos dados pessoais sob a sua custódia e tomarem péssimas decisões sobre a forma como estes dados pessoais foram recolhidos e posteriormente utilizados, com implicações diretas na sua privacidade. Assumir que uma segurança adequada de dados resolve as necessidades de privacidade pressupõe que o problema foi mal entendido (Jericho Forum, 2007b).

Não é possível ter privacidade sem segurança (Hamidovic, 2010; Culnan, 2011). Por um lado, a privacidade depende da segurança, por exemplo na necessidade de

assegurar o controlo do acesso aos dados sensíveis. Por outro lado, dependendo dos requisitos de segurança, é necessária a seleção de diferentes técnicas de privacidade - por exemplo, quando se impõe perfis de utilizadores, deve ser possível associar diferentes ações a um utilizador, o que significa que o utilizador não pode agir em anonimato (Wuyts et al., 2009). A segurança abrange assim as tecnologias, políticas, processos, medidas e ferramentas utilizadas para assegurar confidencialidade e privacidade. É o mecanismo de proteção da privacidade dos dados pessoais, com capacidade para controlar o acesso, a divulgação, alteração, perda ou destruição de dados (NETHA, 2009).

É cada vez mais importante que as organizações, independentemente da sua dimensão, estejam preparadas para reagir a incidentes de segurança dos dados (Cavoukian, 2011). Numa situação de violação de dados, a melhor defesa de uma organização é agir rapidamente (Ernst & Young, 2012b). As causas destes incidentes podem variar desde atividades maliciosas a lapsos involuntários em processos que envolvem dados pessoais (Cavoukian, 2011). Segundo esta autora, o conhecimento de quando e onde estes acontecem, e por que motivo, possibilitam uma resposta imediata, estruturada, a fim de resolver a situação, proteger indivíduos (atende às expectativas das entidades reguladoras) e preservar a reputação afetada da organização. Minimizar o dano potencial é extremamente importante. As organizações não podem evitar todas as situações, mas uma resposta rápida pode reduzir o risco (Ernst & Young, 2012b).

Contudo, como a maioria dos processos de proteção de dados são realizados por equipamentos de rede, sistemas operativos, aplicações informáticas ou sistemas gestores de bases de dados (SGBD), em que a segurança não é o seu principal objetivo, a sua inclusão como parte do mecanismo de proteção dos dados, potencialmente amplia significativamente a superfície de ataque e de vulnerabilidades. Muitos destes mecanismos, na maioria das vezes não têm qualquer proteção ajustável à sensibilidade da informação (Jericho Forum, 2012). A proteção é realizada por equipamentos com capacidade de encriptação do tráfego, e por sistemas de controlo de acesso. Contudo, é necessário considerar que (1) qualquer violação tende a expor a totalidade dos dados e recursos; e (2) a segurança baseada na camada de rede tende a ser controlada isoladamente por uma organização – o que faz com que não funcione tão bem com a ligação a outras organizações (Jericho Forum, 2012).

Enquanto na segurança da informação existem vários padrões detalhados disponíveis e reconhecidos, assim como metodologias de desenvolvimento, testes de segurança e mecanismos de auditoria, a gestão das questões da privacidade, face à falta de *standards* reconhecidos, depende (1) das políticas de privacidade e proteção de dados da organização (se houver); (2) da consciência e preparação dos responsáveis pelos SI; (3) da complexidade, agenda e orçamento para o desenvolvimento dos sistemas, que pode impedir a introdução de controlos de privacidade, muitas vezes vista como uma complexidade adicional; e (4) do ambiente regulatório em que a organização opera (por exemplo, às organizações de serviços financeiros é-lhes exigida a implementação de controlos) (ICO, 2008).

Uma organização pode identificar os seus requisitos de segurança com base: (1) numa avaliação dos riscos para a organização, que identifica e avalia as ameaças e vulnerabilidades, e estima a sua probabilidade de ocorrência e impacto potencial; (2) nos requisitos legais, regulamentares e contratuais; e (3) através de um conjunto particular de princípios, objetivos e requisitos do negócio para o processamento da informação, desenvolvido pela organização (ISO/IEC, 2005).

Identidade e gestão da identidade digital

A identidade é, em simultâneo, um conceito do "mundo real" e um artefacto digital. A identidade digital surgiu da necessidade de partilhar sistemas computacionais por vários utilizadores. Quando vários utilizadores partilham um sistema, é necessário atribuir a cada utilizador um espaço para os dados da sua autoria, para garantir que os utilizadores utilizam os recursos de forma justa, e para proteger os utilizadores contra a interferência de outros. O acesso a este espaço, e a utilização dos dados são controlados por um identificador, normalmente designado por "conta de utilizador" à qual é associada um "senha secreta" (OCDE, 2007). O conceito de *informação de identidade,* isto é dados relacionados com uma pessoa, surge regularmente como uma expressão de identidade digital (Lips, 2008), que para Bertino, Bhargav-Spantzel, & Squicciarini (2006) pode ser definida como a representação digital da informação conhecida sobre um determinado indivíduo ou organização. A identidade digital denota a atribuição de valores a atributos de um indivíduo, que são imediatamente acessíveis por meios técnicos (Pfitzmann & Hansen, 2010).

A privacidade dos dados torna-se num problema quando os dados processados podem ou devem estar relacionados com pessoas. Este facto faz com que a identidade

e a proteção de dados sejam temas fortemente interdependentes (Otjacques et al., 2007). No domínio da segurança, a identidade[32] está intrinsecamente relacionada com a privacidade (OCDE, 2007), ou por outras palavras, está intimamente entrelaçada com a privacidade (ICO, 2008). Certamente, a identidade digital é um componente importante da segurança, mas a sua utilidade vai para além da proteção da informação. Ao mesmo tempo, a segurança da informação é mais do que simplesmente executar a autorização e autenticação de um pedido (Windley, 2005). Para este autor, o objetivo da segurança da informação é o de proteger a informação contra acessos, alterações e eliminações não autorizadas. A privacidade diz respeito à proteção dos atributos, preferências e características associadas a uma identidade, de serem disseminados além das necessidades do sujeito numa qualquer transação particular. De forma circular, a privacidade é construída sobre uma boa base de segurança da informação, que, por sua vez, depende de uma boa infraestrutura de identidade digital, como representado na Figura 8.

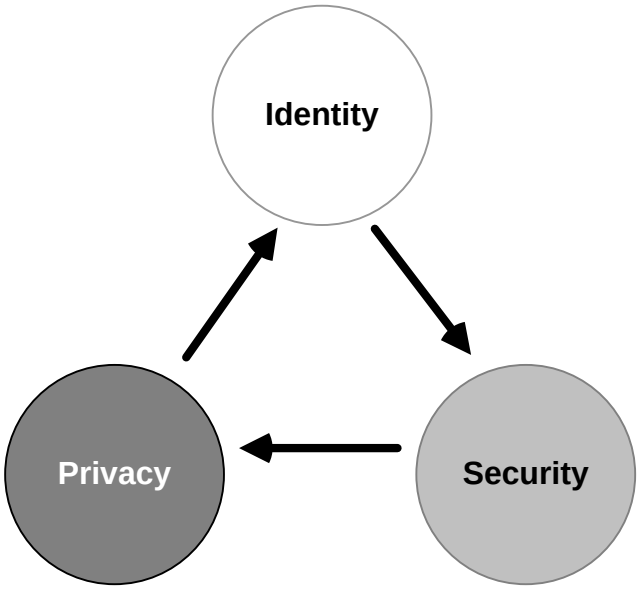

Figura 8 - O triângulo identidade, privacidade e segurança
(Windley, 2005)

A informação pessoal, seja ela biográfica, biológica, genealógica, histórica, transacional, de localização, relacional, computacional, profissional ou de reputação,

[32] Pode ser definida como "qualquer conjunto de atributos de um indivíduo que suficientemente identifica essa pessoa dentro de qualquer conjunto de indivíduos" (Pfitzmann & Hansen, 2010). Para ter acesso ao recurso, o sujeito reivindica uma identidade. Um sujeito ou entidade pode constituir uma pessoa, organização, aplicação ou equipamento, que realiza um pedido para aceder a um recurso. Um recurso pode ser uma página *Web*, um ficheiro de dados, um conjunto de dados numa base de dados, ou até mesmo uma transação num cartão de crédito.

é o material que compõe a nossa identidade moderna. Deve ser gerida de forma responsável. Quando não o é, a responsabilidade fica comprometida e a confiança na sociedade da informação em evolução é corroída. Pode muito bem ser necessário mudar e adaptar as ideias fundamentais sobre identidade e privacidade e as tecnologias, à rápida evolução de um mundo de conectividade (Cavoukian, 2009). Qualquer organização que mantém um registo extenso de dados de identidade digital sobre indivíduos apresenta um poder considerável, do qual não pretende abdicar. Este poder deve ser balanceado com uma responsabilidade adequada (OCDE, 2007).

A gestão da identidade significa a gestão das várias identidades parciais de um indivíduo, ou seja, a administração dos atributos de identidade, incluindo o desenvolvimento e escolha da entidade parcial e pseudónimo que deve ser (re)utilizado num contexto ou função específica (Pfitzmann & Hansen, 2010). Tem um impacto potencialmente significativo sobre a privacidade da pessoa, a privacidade do comportamento da pessoa, a privacidade das comunicações pessoais, bem como sobre a privacidade de dados pessoais (Clarke, 2004). As organizações que não reconhecem a ligação entre sistemas de gestão de identidade e privacidade tornam-se vulneráveis a incidentes de violação de dados (ICO, 2008).

A identidade é essencial à proteção de dados pessoais e ao direito de privacidade. Num SI, e em ambientes de colaboração com outros sistemas, a identidade é um conjunto de dados sobre uma entidade (indivíduo, grupo ou organização) que é usado para diferenciá-la de outras entidades no mesmo ambiente. Numa perspetiva de preservação da privacidade, a proteção da identidade está relacionada com o controlo da entidade na forma como esta interage com o sistema de informação e com outras entidades do sistema (Skinner, Han, & Chang, 2006).

Neste momento é exigível às organizações interações contínuas, de uma forma segura, com outras partes interessadas, internas e externas, no sentido de criarem relações de confiança e identidade eletrónica para acesso aos recursos críticos de informação (Gupta & Sharman, 2008). Inevitavelmente estas organizações são confrontadas com a necessidade de gerir um grande número de identidades, tanto internas como externas, sendo que não existe um sistema único que responda às necessidades de todos os contextos de identidade digital (Cavoukian, 2003).

Os sistemas de gestão de identidade – definidos como programas informáticos ou *frameworks* que gerem a obtenção, autenticação, ou a utilização da identidade e da

informação relacionada com a identidade – implementados tanto em setores públicos como privados, obrigam a que os utilizadores se identifiquem com muita frequência (Hansen, Schwartz, & Cooper, 2008). Cada vez mais as organizações procuram diminuir a carga imposta aos utilizadores na gestão de várias contas para diferentes organizações. Fazem-no recorrendo às tecnologias de *single sign-on* (SSO) e federação (OCDE, 2007).

O SSO constitui uma forma especializada de autenticação que permite que um utilizador se autentique apenas uma vez, e tenha acesso aos recursos de múltiplos sistemas. O sistema autentica o utilizador para todas as aplicações, para as quais tem direito, e elimina a necessidade de nova autenticação cada vez que muda de aplicação (Gupta & Sharman, 2008). A federação, por seu lado, reduz o número de contas a criar por utilizador, através da construção de relações de confiança entre os vários sistemas de autenticação, através da qual um prestador de serviços confia na autenticação de um utilizador, realizada por outro prestador de serviços (OCDE, 2007). Sem uma identidade federada, o utilizador é obrigado a gerir diferentes credenciais para o acesso a cada um dos recursos que utiliza (Gupta & Sharman, 2008). As federações devem neste sentido, fornecer aos seus utilizadores ambientes protegidos, através de uma gestão de identidades, assim como uma gestão dos atributos de identidade para a globalidade da federação (Bertino et al., 2006). A federação pode permitir às organizações a partilha de dados e aplicações de forma segura, sem a necessidade de manter registos completos de utilizadores de todas as organizações parceiras (uma boa e muito útil prática de privacidade) (IPC, 2009).

A identidade federada constitui uma identidade única do utilizador que pode ser usada para aceder a um conjunto de recursos dentro da federação. Resulta de uma computação distribuída que reconhece o facto de os utilizadores se moverem entre sistemas a um ritmo cada vez mais frequente (Bhargav-Spantzel, Squicciarini, & Bertino, 2005) (Gupta & Sharman, 2008). A diferença mais distinta entre a gestão de identidade numa federação e a gestão da identidade comum, está relacionada com a necessidade de uma identidade de um domínio de segurança aceder a recursos (aplicações ou sistemas operativos) num outro domínio de segurança (Liu & Gao, 2008). Ao não pertencerem ao mesmo círculo de confiança, existe um problema de confiança entre as entidades de domínios de segurança diferentes, fazendo com que uma não acredite que a outra vai sempre agir corretamente. A solução passa pela

existência de uma entidade de confiança entre os dois lados, que assegure o acesso aos recursos de outro domínio de uma forma segura. A federação de identidades implica assim a partilha de informação de identidade entre domínios, mas apenas quando existe uma relação de confiança ou acordo (Koshutanski, Ion, & Telesca, 2007).

A gestão da identidade federada surge como um requisito fundamental ao funcionamento da federação (Pham, Mccullagh, & Dawson, 2007). Este é o primeiro passo para que seja possível partilhar aplicações sem a necessidade de adotar as mesmas tecnologias para serviços de domínio, segurança e autenticação (Gupta & Sharman, 2008), sendo possível que todas as entidades interajam com sucesso através da autenticação segura de utilizadores e serviços (Ji, Chen, & Wu, 2011). Contudo, a gestão de perfis de utilizadores para todo o sistema federado, apresenta-se como uma tarefa complexa, sendo fundamental a utilização de tecnologias de gestão da identidade digital federada[33] (Bertino et al., 2006). Esta infraestrutura utiliza a identidade no processo de autenticação e mapeia os identificadores com a informação necessária para identificação e autorização (Poursalidis & Nikolaou, 2006), podendo funcionar de uma forma isolada[34], centralizada[35], e distribuída[36] da identidade federada (Shin, Ahn, & Shenoy, 2004; OCDE, 2007; Lips, 2008).

---

[33] Informação detalhada sobre o funcionamento, composição e *standards* dos sistemas de gestão da identidade digital federada pode ser encontrada nas publicações de (Lips, 2008), (Bertino et al., 2006), (Koshutanski et al., 2007), (IEEE, 2007), (Peyton, Hu, Doshi, & Seguin, 2007), (Poursalidis & Nikolaou, 2006) e (Ji et al., 2011).

[34] A gestão *isolada* de identidade constitui o modelo mais conservador, em que cada sistema membro da federação gere de forma isolada a sua *framework* de segurança, o seu domínio de gestão de identidade, assim como os atributos de identidade. Apesar de ter uma implementação simples, obriga os utilizadores a gerirem múltiplas identidades para acesso aos outros sistemas da federação (Shin et al., 2004).

[35] No modelo de identidade federada *centralizada*, todos os membros da federação têm que pertencer ao mesmo círculo de confiança. O facto de existir apenas um provedor de identidade, contribui para que este modelo seja mais adequado para grandes organizações sob a égide de uma única autoridade, normalmente membros de uma empresa multinacional ou agências do governo. Contudo, a existência de um único gestor da identidade constitui um ponto de enorme fraqueza para este modelo (Shin et al., 2004).

[36] O modelo de gestão *distribuída* da identidade federada apresenta-se como uma solução promissora para a gestão de identidade. Aumenta a flexibilidade e disponibilidade, superando assim o único ponto de falha identificado no modelo de gestão centralizada. Contudo, o cruzamento de aspetos de reconhecimento (políticas, perfil de risco ou atributos do utilizador) faz com que a implementação deste modelo seja complexa. Mesmo assim, é o modelo que apresenta um maior potencial, dada a sua flexibilidade, escalabilidade, usabilidade e baixos custos de gestão para o utilizador (Pham et al., 2007).

O funcionamento de uma federação requer que sejam devidamente definidas e atualizadas um conjunto de políticas de funcionamento. Em particular, políticas relevantes relacionadas com a segurança e privacidade, dado serem cruciais para garantir que a informação de identidade dentro da federação se encontra fortemente protegida, como são os casos de políticas de autorização de acesso aos recursos, políticas de disponibilização de serviços, políticas de privacidade do provedor de serviços, políticas de privacidade, e políticas de adesão à federação (Bertino et al., 2006).

Análise do risco e do impacto sobre a privacidade

Na medida em que a natureza da governação da privacidade requer uma abordagem dinâmica de "aprendizagem", contribui na opinião de Bamberger & Mulligan (2011) para que a privacidade seja cada vez mais enquadrada na prática em evolução da gestão do risco. Como a segurança é um elemento da privacidade, a experiência no desenvolvimento de regulamentos de segurança focados nas organizações, deve fornecer perceções para a regulação da privacidade, uma vez que tanto a privacidade como a segurança resultam de processos organizacionais para minimizar o risco (Culnan, 2011). Sem programas robustos de gestão da privacidade e da segurança, as organizações tendencialmente vão continuar a sofrer problemas de privacidade. Face a esta tendência, é necessário que uma nova legislação procure responsabilizar as organizações sobre as suas decisões. Aquilo a que vários autores (veja-se, por exemplo, (Art. 29 WP, 2010b) e (Hunton & Williams, 2010)) definem como uma nova abordagem baseada no princípio da responsabilidade, questão que será abordada no ponto 3.2.5.

Para muitas organizações, a privacidade atualmente apresenta riscos que necessitam de ser geridos profissionalmente, de forma semelhante a outras categorias de riscos (ICO, 2009). Uma análise do risco insuficiente pode contribuir fortemente para um histórico de violação de registos de saúde de pacientes (Berger, 2014). A natureza dinâmica da privacidade moveu os CPO, e as organizações, a abordarem a privacidade como um risco, a ser gerido, em vez de ser apenas o cumprimento de uma questão legal (Bamberger & Mulligan, 2011). As organizações devem assim analisar os riscos para a privacidade que surgem de produtos e práticas desde o seu desenvolvimento inicial, durante a sua implementação e posterior evolução, assim como quando os seus requisitos sobre os dados se alteram (Hunton & Williams,

2010). Ou seja, as organizações devem fomentar o desenvolvimento de políticas de gestão da privacidade ao mais alto nível, que lhes permitam: (1) incorporar em todo o ciclo de vida de um sistema, avaliações de impacto sobre a privacidade; (2) gerir os riscos relacionados com a privacidade de acordo com níveis pré-definidos; e (3) promover uma maior transparência, através da publicação dos estudos de impacto sobre a privacidade (ICO, 2008). As organizações devem assim tomar medidas para anular os riscos detetados, não de uma forma estática, mas num processo contínuo, que responda à dinâmica que envolve a natureza dos dados recolhidos, a sua utilização e processamento (Hunton & Williams, 2010).

De acordo com a norma ISO/IEC[37] 27000:2009 (ISO/IEC, 2009) um processo de gestão do risco, no domínio da gestão da informação, deve contribuir para: (1) a identificação e avaliação dos riscos, nomeadamente as suas consequências e a sua probabilidade de ocorrência; (2) a compreensão e comunicação da probabilidade e consequências destes riscos; (3) estabelecer uma ordem de prioridade para o tratamento do risco; (4) estabelecer prioridades nas ações para reduzir a ocorrência dos riscos; (5) envolver e manter informados os parceiros (*stakeholders*) sobre as decisões de gestão do risco; (6) a eficácia da monitorização do tratamento do risco; (7) a revisão regular dos riscos e do processo de gestão do risco que estão a ser monitorizados; (8) melhorar a informação recolhida de suporte à abordagem de gestão do risco; e (9) preparar os gestores e técnicos sobre os riscos e as medidas tomadas para mitigá-los.

Toda a orientação para a avaliação do risco está muito focada em cada sistema de informação de forma individual, e não na globalidade da organização, o que constitui para Gantz (2010) uma importante limitação, dada a necessidade de uma abordagem mais alargada que inclua todos os riscos potenciais para a informação da saúde. Desta forma, defende este autor, as organizações que pretendam, para a avaliação e gestão do risco uma perspetiva ao nível organizacional, podem encontrar um maior suporte nas *frameworks* de *IT Governance*.

---

[37] A série de padrões internacionais ISO/IEC 27000 abrange a avaliação do risco e a gestão do risco para os sistemas de informação, em especial a ISO/IEC 27002 (ISO/IEC, 2005) para análise do risco, e a ISO/IEC 27005 (ISO/IEC, 2005) no suporte à gestão do risco. A ISO 27799 (ISO, 2008) aborda as necessidades especiais na gestão da segurança da informação para o setor da saúde, e constitui um documento complementar à norma ISO/IEC 27002.

As metodologias tradicionais de avaliação e gestão de risco falham ao não considerarem devidamente o valor de informações pessoais, e ao não considerarem e gerirem de uma forma rigorosa as necessidades de privacidade durante todo o ciclo de vida de um sistema. Deste modo assiste-se ao desenvolvimento, modificação e reutilização de sistemas sem controlos de privacidade adequados e inovadores, e sem a consideração necessária das implicações sobre a privacidade (ICO, 2008). Incorporar a privacidade em outros processos de gestão do risco, permite por um lado aproveitar recursos existentes para o serviço da privacidade, e por outro colocar o tratamento da privacidade da informação ao nível de outras preocupações fundamentais de gestão (Bamberger & Mulligan, 2011).

O processo de gestão do risco da segurança da informação pode ser aplicado a uma organização como um todo, a qualquer parte discreta da organização (por exemplo, um departamento, um local físico, um serviço), ou apenas a um sistema de informação (ISO/IEC, 2008). A definição do contexto é importante, pois permite iniciar uma avaliação do risco, que caso forneça informação suficiente à definição das ações necessárias à diminuição do risco a um nível aceitável, permite iniciar a fase de tratamento do risco. A eficácia do tratamento do risco depende da qualidade dos resultados da avaliação do risco, o qual pode ter origem em várias fontes. Muitas considerações sobre o risco são baseadas em conceitos tradicionais de compromisso de um sistema – isto é, a violação por uma pessoa de fora. Existem também riscos, difíceis de identificar e controlar, decorrentes de ameaças internas. Outros riscos incluem a possibilidade de uma falha operacional na anonimização suficiente de dados que impeça a sua identificação (IPC, 2009). A escolha ou desenvolvimento da abordagem adequada para a gestão do risco, em conformidade com o âmbito e objetivos definidos para este processo, deve contemplar critérios básicos, tais como: critério de avaliação do risco, critérios de impacto (grau de danos ou custos para a organização causado por um evento), e critérios de aceitação do risco (definição de uma escala de níveis de aceitação do risco) (ISO/IEC, 2008).

Sempre que as operações de tratamento de dados apresentem riscos específicos para os direitos e liberdades dos seus titulares, em virtude da sua natureza, do seu âmbito ou da sua finalidade, deve ser efetuada uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais (GDPR, 2012). Um *privacy*

impact assessment (PIA)[38] é uma metodologia para avaliar os impactos sobre a privacidade de um projeto, política, programa, serviço, produto ou outra iniciativa, de modo a realizar ações corretivas quando necessárias, a fim de evitar ou minimizar os impactos negativos (Wright, 2012). É uma espécie de avaliação de risco, uma vez que tem por objetivo avaliar as possíveis consequências de uma atividade sobre a proteção de dados e sobre a privacidade (Costa & Poullet, 2012). Para estes autores, além da verificação da conformidade legal, um PIA "*tem que considerar os riscos para a privacidade num quadro mais amplo, que têm em conta o mais amplo conjunto de valores e expectativas da comunidade sobre a privacidade*". Neste sentido, um PIA só pode apresentar valor, se apresentar potencial em alterar iniciativas propostas, a fim de mitigar os riscos de privacidade. Quando é realizado de forma automática para satisfazer apenas um requisito legislativo ou burocrático, a avaliação do risco, como elemento-chave do PIA, é muitas vezes omisso (Hamidovic, 2010).

Para Wright (2012) um PIA é mais que uma ferramenta: constitui um processo que deve iniciar nas primeiras fases, quando ainda há oportunidades para influenciar o resultado do projeto, devendo continuar mesmo depois do projeto implementado. Deve constituir mais que uma lista de verificação de conformidade, no sentido de permitir a uma organização demonstrar a sua conformidade com a legislação de privacidade, por exemplo no contexto de uma auditoria, reclamação ou investigação. No caso de ocorrer uma rutura da privacidade, o relatório PIA pode fornecer evidência de que a organização agiu apropriadamente na tentativa de prevenir a ocorrência, anulando assim publicidade negativa ou perda de reputação.

Pode auxiliar organizações governamentais na antecipação da reação pública a qualquer implicação sobre a privacidade de uma proposta, e como resultado evitar serviços e programas dispendiosos ou a reengenharia de processos (Aquilina, 2010).

---

[38] O conceito emergiu e amadureceu no período 1995-2005. Na opinião de Clarke (2009), o seu crescimento pode ter duas interpretações: primeiro, a procura desta metodologia pode ser vista como uma reação tardia contra as ações cada vez mais invasivas da privacidade por parte de governos e outras organizações durante a segunda metade do século XX; segundo, a adoção de um PIA surge do desenvolvimento natural de técnicas de gestão racionais, face a ataques nocivos por parte dos meios de comunicação. Embora utilizada desde 1990 na Austrália, Canadá, Nova Zelândia e EUA, esta metodologia é um fenómeno relativamente recente na Europa. O *Information Commissioner's Office* do Reino Unido publicou o primeiro manual PIA em dezembro de 2007 e uma versão revista em junho de 2009 (Wright, 2012). Este manual pode ser consultado no endereço: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/0-advice.html.

Esta avaliação deve analisar soluções e alternativas menos intrusivas, e estabelecer se estas medidas podem ser limitadas a certos períodos e/ou locais.

O sucesso de um processo PIA é, contudo, facilitado em organizações que apresentem uma estratégia bem definida para a privacidade. Essencialmente porque os técnicos estão por dentro deste tipo de questões, e mais conscientes das preocupações do público e dos riscos que estas preocupações representam para a reputação da organização (Wright, 2012). Não se trata, para este autor, de preparar um relatório, mas sim de um processo que deve iniciar quando um projeto está na sua fase inicial de planeamento, e deve continuar durante toda a vida do projeto. Com o avançar do projeto podem surgir novos riscos.

A Comissão Europeia iniciou o projeto "*Privacy Impact Assessment Framework*" (PIAF[39]), com o objetivo de analisar as metodologias PIA da Austrália, Canadá, Hong Kong, Irlanda[40], Nova Zelândia, Reino Unido e EUA, e promover recomendações iniciais para um PIA otimizado para o espaço Europeu (EC, 2011). Já na Diretiva 95/46/CE o processo PIA tinha sido institucionalizado através do Artigo 20.º, denominado "controlo prévio" (Clarke, 2009), aplicável a "*tratamentos que possam representar riscos específicos … sejam controlados antes da sua aplicação*" (CE, 1995).

Utilização secundária dos dados

Os tipos mais conhecidos de utilização secundária dos dados na área da saúde, incluem: a saúde pública, a qualidade e segurança, e a investigação na melhoria dos tratamentos e na prevenção (NETHA, 2008). Por exemplo, muitas organizações copiam dados de produção para ambientes de desenvolvimento ou de testes para permitirem aos programadores a realização de testes sobre as novas aplicações. Organizações farmacêuticas ou de saúde partilham dados dos pacientes com médicos investigadores para avaliar a eficácia dos ensaios clínicos ou tratamentos médicos. Nestas situações as organizações não têm forma de saber se os dados foram ou não comprometidos (Athreya, 2010). O uso de cópias dos dados de produção para apoiar

[39] O projeto foi desenvolvido entre janeiro de 2011 e agosto de 2012 pelo consórcio composto pelos seguintes parceiros: Vrije Universiteit Brussel (Bélgica), Trilateral Research & Consulting (Reino Unido), Privacy International (Reino Unido).

[40] A Irlanda desenvolveu um guia específico para a realização de um PIA para a área da saúde (HIQA, 2010).

o desenvolvimento e testes das suas aplicações expõe dados privados a utilizadores privilegiados, como programadores e administradores, os quais não estão autorizados a visualizar estes dados. Só porque os dados estão armazenados num ambiente de testes ou de desenvolvimento, não retira responsabilidades à organização de cumprir com os regulamentos de privacidade (Yuhanna, 2009).

A utilização de dados identificados ou potencialmente identificáveis para fins secundários, é reconhecida como uma fonte valiosa de informação para a investigação na área da saúde. No entanto, é necessário que em tais casos sejam aplicadas proteções rigorosas da privacidade dos dados envolvidos (NETHA, 2008). A anonimização, também chamada de *de-identification*, é um dos instrumentos disponíveis, e fundamentais para a privacidade dos dados de saúde nestes casos (El Eman & Arbuckle, 2014).

Apesar do valor inquestionável dos dados, no caso da investigação ou saúde pública, se a proteção destes dados for comprometida, ou não atender à expetativa por parte dos seus titulares de um acesso limitado a estes dados "privilegiados" de saúde, a confiança nas organizações pode ser muito prejudicada (NETHA, 2008).

Em resumo, para a segurança e infraestruturas:

- A segurança dos SI, a sua interoperabilidade técnica e não-técnica, nomeadamente através de interoperabilidade organizativa, é preponderante ao desenvolvimento de um ambiente seguro de recolha, intercâmbio e utilização de dados pessoais para o domínio alargado de partilha de dados.
- A identidade digital e a interoperabilidade entre os sistemas de gestão da identidade são ferramentas essenciais à garantia de confidencialidade dos dados.
- O processo de análise de risco em segurança, em segurança da informação, assim como a análise do impacto sobre a privacidade de qualquer solução tecnológica, são dois instrumentos decisivos e de suporte ao desenvolvimento de medidas de proteção da privacidade dos dados.
- As situações de utilização secundária de dados pessoais devem ser comuns e do conhecimento de todas as organizações envolvidas, que exigem a adoção de medidas de segurança e privacidade específicas.
- No domínio da segurança, a existência de um plano de contingência para situações anómalas de utilização indevida, perda, destruição ou deterioração de dados pessoais, é fundamental para anular danos maiores sobre os dados pessoais ou sobre os titulares destes dados.

3.1.4 Linguagem de privacidade (taxonomia)

Tanto a nível nacional como internacional, os profissionais em segurança da informação conseguem colaborar de uma forma eficaz, com base em definições claras e no consenso crescente sobre o alcance da segurança da informação. No domínio da privacidade não existe uma definição amplamente aceite, nem uma descrição consensual da relação entre a privacidade, a identidade e a segurança da informação - o que constitui um problema quando diferentes partes estão envolvidas na gestão da privacidade. Existe uma necessidade urgente de definições claras e um acordo entre as partes envolvidas que facilite a colaboração para o domínio da privacidade (ICO, 2008).

À semelhança de outras temáticas no domínio dos SI, a existência de um vocabulário próprio é um facilitador para operacionalizar questões complexas. Uma linguagem ou taxonomia específica para a privacidade, integrada com outras taxonomias, apresenta-se como uma ferramenta indispensável aos profissionais, por um lado no suporte ao desenvolvimento integrado de políticas de proteção da privacidade, e por outro no suporte ao desenvolvimento interno de um programa de privacidade aplicado a todo o ciclo de vida da privacidade dos dados (Cavoukian, 2012).

Os profissionais que têm que agir de acordo com as políticas de privacidade em vigor, devem ser capazes de as compreender. A escrita de boas políticas requer caminhar numa linha ténue entre a linguagem formal e informal. Os utilizadores muitas vezes não percebem linguagem formal, e em muitas situações a linguagem informal não tem a precisão necessária para expor claramente o que se pretende expor (Windley, 2005). Continua a ser um desafio proporcionar políticas de privacidade que os utilizadores realmente entendam e que servem como normas para o processamento dentro da organização (Hansen et al., 2008). Uma linguagem de privacidade é complexa e de momento existe muita divergência entre os profissionais neste domínio, sobre como descrever os conceitos relacionados com a privacidade (ICO, 2008). Esta falta de um vocabulário partilhado para analisar ou para especificar os requisitos de privacidade de uma forma inequívoca e clara, agravada com a falta de consciência do que é necessário, provoca que tanto os administradores de sistemas como os gestores executivos, muitas vezes promovam especificações para o sistema que não conseguem lidar com a privacidade de forma satisfatória.

A capacidade de construir um sistema que está em conformidade com a legislação em privacidade, depende muito da capacidade de se compreender o significado da privacidade. Compreender a natureza da legislação de privacidade é uma dificuldade que os engenheiros de sistemas enfrentam na construção de soluções tecnológicas em áreas como finanças, saúde, ou em outros domínios de informação sensível. Se a existência de uma taxonomia conseguir garantir um vocabulário comum a todos os profissionais responsáveis pelo desenvolvimento do SI, então esta pode desempenhar um papel fundamental na sua conformidade legal (Massey & Antón, 2008).

O propósito de qualquer taxonomia é contribuir para um melhor estudo de um assunto, ajudando a tomar determinadas decisões, não substituindo contudo a necessidade de formular e responder a questões fundamentais (Dutch, 2010). Uma taxonomia de privacidade dos dados[41] constitui "*um conjunto documentado e ordenado de tipos, classificações, categorizações e/ou princípios que são frequentemente alcançados por meio de mecanismos, incluindo a nomeação, definição e/ou o agrupamento de atributos, e que por sua vez ajudarão a descrever, diferenciar, identificar, organizar e fornecer relações contextuais entre entidades, tipos e itens de privacidades dos dados*".

Na impossibilidade de identificar uma taxonomia globalmente aceite, foi possível, contudo, identificar na revisão bibliográfica, várias propostas de taxonomia aplicáveis à privacidade. São os casos da taxonomia de Solove (2006), a taxonomia da privacidade dos dados para ambientes colaborativos de Skinner et al. (2006), a qual contempla uma dimensão *computacional*, uma dimensão *estrutural* e uma dimensão de *dados* para abordar a privacidade dos dados num ambiente colaborativo. Existem ainda taxonomias muito específicas, como são os casos da taxonomia proposta na *framework* para desenvolvimento de políticas de privacidade para a *Web*, de Earp, Antón, & Jarvinen (2002), da taxonomia proposta por Antón & Earp (2003) para análise dos requisitos de privacidade de um sítio *Web*, e o esquema de classificação das tecnologias para a proteção da privacidade de Yeonjung, Hyangjin, Kilsoo, & Junghwan (2007).

[41] Termo consultado em 13 de janeiro de 2013 no sítio web da "The International Foundation for Information Technology (IF4IT)", no URL: http://www.if4it.com/SYNTHESIZED/GLOSSARY/D/Data_Privacy_Taxonomy.html

A taxonomia sobre a privacidade, representada na Figura 9, de Solove (2006), foca-se essencialmente nas atividades potencialmente perigosas ou problemáticas que podem criar danos ou problemas de privacidade, e não sobre o que constitui uma atividade ou assunto privado, muito dependentes de contextos e culturas variáveis. Foi desenvolvida para fornecer uma compreensão abrangente da pluralidade de problemas de privacidade globalmente reconhecidos, não tendo por objetivo a definição de metas a manter ou alcançar (Massey & Antón, 2008), e não tem em consideração os aspetos atuais dos SI (Wuyts et al., 2009). É para Culnan (2011) uma alternativa à perspetiva individual da privacidade, na qual Solove caracteriza a privacidade como consistindo num conjunto de problemas resultantes das diferentes formas organizacionais de processamento de informações pessoais.

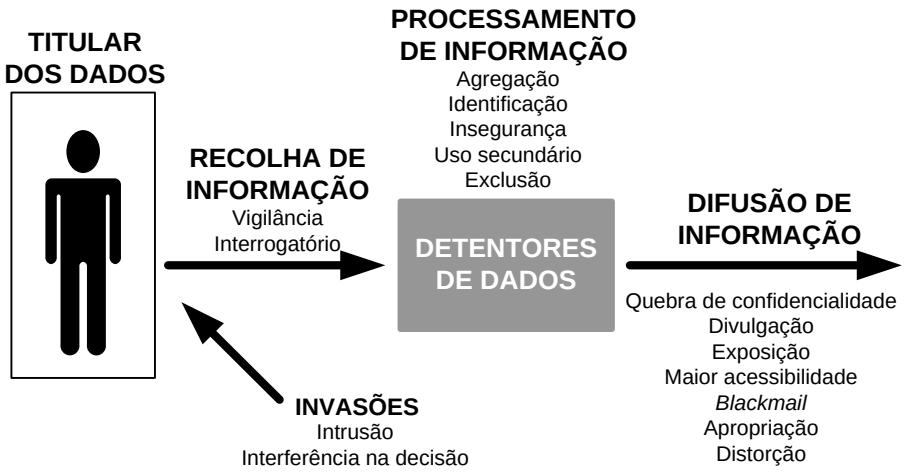

Figura 9 - Relação entre os vários grupos da taxonomia de Solove
(adaptada de (Solove, 2006))

Solove (2006) definiu 16 categorias distribuídas por quatro grandes grupos de atividades problemáticas: (1) *recolha de informação*[42], (2) *processamento de informação*[43], (3) *difusão de informação*[44], e (4) *invasões*[45]. A Figura 9 representa a

[42] Engloba a "*vigilância*" e o "*interrogatório*". Por *vigilância* entende-se a observação, escuta e gravação de atividades de um indivíduo. Constitui uma forma passiva de recolha de informação, e pode ser realizada em espaços públicos ou privados (Marsh et al., 2008). O *Interrogatório* consiste em várias formas de questionar ou investigar para obter informações.

[43] O segundo grupo de atividades envolve a forma como a informação é armazenada, manipulada e utilizada. Engloba os subgrupos "*agregação*", "*identificação*", "*insegurança*", "*uso secundário*" e "*exclusão*". *Agregação* envolve a combinação de vários conjuntos de dados, sobre uma pessoa. É o processo pelo qual diferentes itens de informação pessoal são reunidos para inferir "factos" novos (Marsh et al., 2008). *Identificação* constitui a vinculação de informações a indivíduos em particular. *Insegurança* envolve descuido, falhas na proteção de informações armazenadas, podendo ser causadas por processos de agregação, modificação, utilização e acessos ilícitos. *Utilização secundária* constitui o

relação entre os vários grupos da taxonomia proposta. Culnan (2011) reagrupa estes quatro grupos em duas categorias globais: a reutilização de informação e o acesso não autorizado a informações pessoais. A reutilização da informação envolve todas as decisões das organizações sobre novas utilizações para os dados pessoais recolhidos, incluindo a agregação de dados e a mineração de dados, e a reutilização ou partilha de dados inicialmente recolhidos para um outro fim. Os problemas de privacidade que resultam da reutilização de dados incluem inferências incorretas, decisões baseadas em dados errados, exclusões ou intrusões. O acesso não autorizado inclui dois tipos de atividades relacionadas com a segurança: a navegação (*browsing*) e a violação de dados. No caso da navegação, é possível visualizar dados pessoais para os quais não se tem autorização, e no caso de violações de dados, existe o acesso não autorizado a dados pessoais, resultante de uma variedade de incidentes de segurança.

De acordo com Marsh, Brown, & Khaki (2008) a taxonomia de Solove (2006) é uma base útil para o desenvolvimento de uma análise risco/benefício, isto porque, segundo estes autores, proteger a privacidade num sistema depende de como atingir um equilíbrio adequado entre riscos e benefícios. A taxonomia de Solove (2006), ao ser desenvolvida com o objetivo de influenciar a compreensão da privacidade no desenvolvimento de futura legislação, é uma ferramenta útil para a análise de requisitos na construção de um sistema que se pretende em conformidade com a legislação de privacidade (Massey & Antón, 2008)

---

uso de informação, não para a finalidade inicialmente definida, mas por uma outra diferente, e sem o consentimento do titular dos dados. *Exclusão* diz respeito à ausência de conhecimento por parte do titular dos dados, sobre que dados outros têm sobre si, e à impossibilidade de poder participar no seu manuseamento e utilização.

[44] O terceiro grupo de atividades envolve a difusão da informação, na qual dados pessoais são difundidos, transferidos, ou se ameaça fazê-lo. Engloba os subgrupos "*quebra de confidencialidade*"," *divulgação*", "*exposição*", "*maior acessibilidade*", "*blackmail*", "*apropriação*" e "*distorção*". *Quebra de confidencialidade* diz respeito à quebra da promessa de manter informações pessoais confidenciais. *Divulgação* envolve a revelação de informações verdadeiras sobre uma pessoa que pode ter impacto na forma como outros julgam o seu carácter. *Exposição* constitui a exposição a outros de certas características físicas e emocionais de uma pessoa. *Maior acessibilidade*, surge associada à disponibilização de informação através de médias de *broadcast* e da internet. As informações em questão já são públicas, em algum sentido, mas o modo de apresentação faz com que se torne disponível para uma gama maior de pessoas do que originalmente destinadas. *Blackmail* surge como uma ameaça de divulgar informações pessoais. *Apropriação* envolve o uso da identidade do titular dos dados para servir os objetivos e interesses de outro. *Distorção* consiste na divulgação de informações falsas ou enganosas sobre um indivíduo.

[45] O quarto grupo inclui atividades de invasão em assuntos privados ou particulares das pessoas, neste caso "*intrusão"* e "*interferência na decisão"*. *Intrusão* diz respeito a atos invasivos que perturbam a tranquilidade ou solidão de alguém. *Interferência na decisão* envolve a incursão de decisões governamentais nas decisões do titular dos dados quanto aos seus assuntos privados.

Para Wuyts et al. (2009) uma taxonomia de privacidade, semelhante às taxonomias desenvolvidas de segurança[46], é fundamental para a escolha de soluções de privacidade durante o processo de engenharia de *software*. A taxonomia desenvolvida por estes autores vai de encontro a esta pretensão, promovendo a divisão da privacidade em dois ramos (o ramo de *dissimulação*, que descreve todos os objetivos de restrição à formação de associações quando o utilizador comunica informação sensível com o sistema, e o ramo de *vigilância* que lida com as associações após a sua partilha), e a definição em cada um dos dois ramos de vários objetivos implementados por diferentes estratégias (por exemplo: estratégia de pseudónimos, de atributos, remoção, ocultação, substituição e generalização de dados, consentimento, transparência, controlo de acesso, atualização e expiração de dados).

O domínio da privacidade dos dados necessita de uma *framework* coerente que inclua os aspetos legais, tecnológicos e éticos, que permita aos defensores da privacidade um entendimento comum sobre este assunto. A criação de uma taxonomia é um passo essencial à construção desta *framework* (Dayarathna, 2011).

Em resumo, para a linguagem de privacidade (taxonomia):

- Uma taxonomia focada na privacidade e proteção de dados, integrada com outras taxonomias, é uma ferramenta facilitadora na gestão e controlo de conformidade das situações de privacidade, assim como o seu alinhamento com situações similares nas outras organizações.
- Deve constituir um meio que permita que os elementos de um programa de privacidade sejam expressos de forma compacta e flexível e que facilite a tomada de decisões relevantes quanto à privacidade.
- Uma taxonomia não se pode limitar à classificação de dados – deve abranger outros parâmetros em que a sua classificação é útil à gestão da privacidade.

3.1.5 *Accountability*: responsabilidade e conformidade

O termo "*accountability*" (responsabilidade) tem origem no mundo anglo-saxónico, onde o seu uso é comum e onde existe um consenso generalizado sobre o seu significado – apesar de ser complexo defini-lo na prática. Em termos gerais, porém, a ênfase recai na forma como a responsabilidade é assumida e na forma como torná-la verificável. Na maioria das outras línguas europeias, devido principalmente a

[46] Para estes autores, as taxonomias de segurança permitem classificar os objetivos de segurança e consequentemente a seleção orientada aos objetivos das melhores soluções de segurança.

diferenças nos sistemas jurídicos, a tradução do termo "*accountability*" não é fácil, pelo que existe um risco significativo de interpretações divergentes e consequentemente de falta de harmonização (Art. 29 WP, 2010b).

No domínio dos SI, encontramos regularmente a referência ao termo técnico *accountability*, e no domínio da proteção de dados ao princípio da responsabilidade – são conceitos diferentes. Para efeitos deste estudo, o termo *responsabilidade* centra-se na atitude da organização e nas medidas que devem ser tomadas ou previstas para garantir a conformidade no domínio da proteção de dados, com especial incidência no que se relaciona com a sua privacidade, assim como na demonstração desta conformidade.

Responsabilidade

No sentido técnico do termo, *accountability*, constitui uma das funcionalidades dos sistemas de processamento de dados, sendo que: (1) permite que utilizadores, operadores e outras partes verifiquem, *a posteriori*, se o sistema em causa realizou uma tarefa de processamento de dados como o esperado (validação); (2) em caso de um desvio do comportamento esperado (falhas), permite revelar qual o componente responsável (atribuição); e (3) produz provas utilizáveis para provar que ocorreu ou não uma falha (evidência) (ENISA, 2011). Constitui uma funcionalidade muito dependente do conhecimento da identidade da parte que falhou (Jericho Forum, 2006), e de formas de identidade digital suficientemente fortes, não permitindo que um indivíduo atue sob múltiplas identidades, ou altere a sua identidade livremente ao longo do tempo. Caso contrário, o indivíduo pode fugir à sua responsabilidade sobre uma falha, ou escapar de uma má reputação simplesmente através da mudança de identidade (ENISA, 2011).

Apesar de os vários regulamentos de segurança e de privacidade apresentarem como requisito fundamental a monitorização, na realidade poucas organizações implementam programas eficazes de *accountability*. Muitos sistemas mantêm os ficheiros de *logs*, mas o tratamento destes dados para monitorização da privacidade muitas vezes é demasiado dispendioso e ineficiente (Ernst & Young, 2012b). Ao tornarem possível verificar a integridade (se a tarefa produz o resultado correto) e a confidencialidade (se a tarefa não disponibilizou dados a pessoas não autorizadas -

também definida como *information accountability*[47]) de uma tarefa, um programa de *accountability* aumenta a transparência dos atos de utilização de informação (Weitzner et al., 2008). Para estes autores a *information accountability* significa que a utilização da informação deve ser transparente, sendo possível determinar se um determinado uso é apropriado com base num dado conjunto de regras e que o sistema permite que os indivíduos e as instituições sejam responsabilizados por utilizações indevidas. Se para verificar a integridade de uma tarefa, é suficiente verificar se a tarefa produz o resultado correto, a validação da sua confidencialidade (em oposição à garantia de confidencialidade) é mais complexa, uma vez que o sistema deve monitorizar o fluxo de informações de uma forma mais abrangente.

A antiga abordagem à política de proteção de dados, focada na prevenção da "fuga" de dados para lá das fronteiras estabelecidas, é inadequada num mundo em rede, onde a informação é facilmente copiada e agregada e onde inferências e correlações automáticas sobre várias bases de dados permitem descobrir novas informações, mesmo quando estas não são explicitamente relevantes. Como alternativa, o princípio da responsabilidade deve tornar-se o meio principal pelo qual a sociedade aborda o uso adequado de dados (Weitzner et al., 2008). Atualmente, as novas abordagens[48] para a proteção da privacidade dependem significativamente da *responsabilidade* como o meio para garantir a proteção de dados (Hunton & Williams, 2010).

Todas as organizações que "tocam" em dados devem ser responsáveis pela gestão da privacidade destes dados (Ernst & Young, 2013). A *responsabilidade* é reconhecida como um elemento crítico à eficácia da proteção de dados (Hunton & Williams, 2009) e tem recebido um destaque especial nas discussões nacionais e internacionais sobre os regimes de proteção de dados (Hunton & Williams, 2010). Contudo, e embora haja consenso de que a *responsabilidade* é fundamental para uma eficaz

---

[47] Existe relativamente pouco trabalho de investigação em *information accountability*, isto é, em meios técnicos de registo (*account*) que garantam que o uso da informação é confiável. Por outro lado, existe um trabalho considerável em controlar o acesso, fluxo e utilização de dados, que vão desde os mecanismos de controlo de acesso convencionais, sistemas operativos que controlam o fluxo de dados, a sistemas que controlam que informação pode ser inferida por consultas a bases de dados (ENISA, 2011).

[48] É o caso da opinião do Art. 29 WP (2009), em que é evidenciada a importância e utilidade do princípio da responsabilidade, e identificados os desafios para a proteção de dados que surgem da globalização e das novas tecnologias, que na opinião deste grupo de trabalho, constitui uma oportunidade para "*inovar o atual quadro legal através da introdução de princípios como o da responsabilidade*".

proteção de dados, o conceito não tem sido na prática claramente operacionalizado (Hunton & Williams, 2009).

A responsabilidade é um conceito que tem tanto uma dimensão de governação como de ética, aplicável a uma variedade de regimes jurídicos e culturas, e é implementado por processos contínuos de avaliação e mitigação do risco (Culnan, 2011). Engloba as expetativas de que as organizações irão demonstrar, explicar e responder pelas consequências das decisões sobre a proteção de dados. Promove a implementação de mecanismos práticos que se traduzem em proteção efetiva dos dados, com base nos requisitos e orientações legais existentes (Hunton & Williams, 2010). Culnan (2011) salienta contudo, que ao não existir uma solução única que sirva a todos as organizações, estas necessitam de uma flexibilidade suficiente para desenvolver programas de governação apropriados ao seu contexto particular.

Os programas baseados no princípio da responsabilidade devem ser sensíveis às normas culturais e sociais sobre o uso aceitável de dados, e sensíveis às mudanças de modelos de negócios e novas tecnologias, sem impor encargos desnecessários para as organizações (Art. 29 WP, 2010b). A *responsabilidade* não redefine a privacidade nem substitui a legislação ou regulamentação em vigor. A *responsabilidade* desloca o foco da gestão da privacidade para a capacidade da organização em demonstrar a sua preparação para alcançar os objetivos de privacidade especificados (Hunton & Williams, 2009). Isto significa que, apesar de o titular dos dados continuar a desempenhar um papel importante na proteção dos seus dados, uma abordagem baseada na responsabilidade desloca a responsabilidade primária pela proteção de dados do indivíduo para a organização. É exigido às organizações, uma utilização apropriada dos dados, mesmo quando o seu titular não tenha consentido a sua utilização. Esta alteração exige às organizações uma distinção e identificação perante que entidades[49] devem ter uma atitude de responsabilidade, assim como um conhecimento do que está na base do desenvolvimento de um programa de

[49] Os autores salientam a importância de três entidades: (1) o titular dos dados, que espera que os seus dados sejam utilizados e geridos de forma responsável e segura; exige que as organizações lidem com os seus dados de acordo com os requisitos da legislação, regulamentação e as políticas publicadas de privacidade da organização; (2) as entidades reguladoras de privacidade e proteção de dados, que exigem que as organizações cumpram com as leis e regulamentos aplicáveis, e que honrem com os compromissos acordados para com os titulares dos dados em relação à recolha, utilização e gestão dos seus dados pessoais; (3) os parceiros de negócios, que necessitam de informação adequada sobre a natureza dos dados, as suas obrigações em relação a estes dados e garantias que os responsáveis pelo tratamento dos dados cumpriram com todas as suas responsabilidades.

responsabilidade[50] (Hunton & Williams, 2010). Trata-se para estes autores de estabelecer metas para a proteção da privacidade, com base em critérios estabelecidos na legislação, regulamentos e boas práticas, e de preparar a organização na sua capacidade e responsabilidade de determinar quais as medidas adequadas e eficazes para atingir estas metas. Com base nesta interpretação de responsabilidade, definem um conjunto de elementos[51] essenciais que permitem articular entre as condições que devem existir para que uma organização estabeleça, demonstre e teste a sua responsabilidade.

Para se alcançar uma maior *responsabilidade*, as organizações terão assim de repensar a sua abordagem à privacidade no contexto da sua estratégia mais ampla para os SI. Tal como as organizações planeiam o desenvolvimento e atualização dos seus sistemas, redes e aplicações, a privacidade deve ser incorporada como um pilar fundamental no processo de desenvolvimento e não ser adicionada posteriormente (Ernst & Young, 2012b). É exigido que as organizações estejam preparadas para demonstrar, a pedido das autoridades competentes, que asseguram a segurança e proteção de dados em caso de falhas do sistema (Hunton & Williams, 2010). Para os autores, organizações que desejam ser consideradas responsáveis devem estar cientes dos requisitos que devem implementar, e preparadas para demonstrar o cumprimento de tais condições assim como da sua adequação à natureza dos dados recolhidos, ao seu modelo de negócio, e aos riscos que a sua utilização pode representar para os indivíduos.

---

[50] Os autores identificaram as seguintes situações que obrigam a uma atitude de responsabilidade: (1) a legislação e regulamentação em vigor; (2) a opção por programas de autorregulação de um setor específico, sendo a sua responsabilidade analisada em relação aos requisitos deste programa (3), para cumprir com as promessas estabelecidas nas políticas de privacidade; e (4) como resposta aos programas de avaliação e mitigação de riscos que a recolha, utilização, processamento e retenção de dados representam para os indivíduos, com o objetivo de se adaptar as políticas de proteção, às constantes mudanças tecnológicas, aos modelos de negócio e à legislação.

[51] Nomeadamente: (1) o compromisso da organização para a responsabilidade e a adoção de políticas internas coerentes com critérios externos (encontrados na lei, normalmente princípios aceites e melhores práticas no setor); (2) os mecanismos para colocar em vigor as políticas de privacidade, incluindo ferramentas de decisão sobre a utilização e proteção apropriadas aos dados, e formação sobre como utilizar estas ferramentas; (3) os sistemas para uma monitorização interna contínua; (4) os mecanismos transparentes de participação individual; e (5) os meios para reparação e aplicação externa com o objetivo de lidar com prejuízos causados por falhas na aplicação de práticas de privacidade (Hunton & Williams, 2010).

Conformidade

A recolha de dados pessoais implica o dever de cuidar da sua proteção. As obrigações que resultam das políticas e procedimentos relevantes no domínio da privacidade devem ser documentadas e comunicadas conforme o contexto, e atribuídas a um indivíduo específico dentro da organização (IPC, 2009). As organizações regularmente apresentam sérias dificuldades na implementação de sistemas que estejam em conformidade com a lei de proteção de dados, e vão gerindo a privacidade de acordo com o "melhor esforço", com cada sistema a abordar a questão numa base de caso-a-caso. As organizações deveriam estar a utilizar *standards* de privacidade consistentes e demonstráveis, tal como já o fazem com os *standards* em segurança da informação (ICO, 2008).

Conformidade é o estado de estar de acordo com uma norma, especificação, ou requisitos definidos de forma clara (Dutch, 2010). Representa um subsistema (Hamidovic, 2010), e um dos componentes mais importantes, embora complexo, de um sistema maior de proteção da privacidade (Dutch, 2010). Uma organização deve demonstrar a sua vontade e capacidade em ser tanto responsável como responsabilizada pelas suas práticas de gestão de dados (Hunton & Williams, 2009), e procurar garantir que todas as partes interessadas estão em conformidade com os requisitos de privacidade acordados (ICO, 2008). Esta atitude por parte da organização pode criar ou melhorar a confiança dos consumidores nos seus serviços (Hamidovic, 2010).

A análise da conformidade em relação à privacidade difere da avaliação de impacto sobre a privacidade (tema abordado na seção 3.2.3 Segurança e infraestruturas), uma vez que determina o nível atual de conformidade da organização com a lei e identifica medidas para evitar uma não conformidade futura (Hamidovic, 2010).

Nos termos da Diretiva 95/46/CE (CE, 1995), o *responsável pelo tratamento* dos dados é o ator chave para garantir a conformidade para com os princípios e as obrigações destinadas a garantir a proteção dos dados pessoais. Atendendo a que (1) o volume de dados existentes, processados e depois transferidos não cessa de crescer, (2) o volume crescente de dados pessoais é acompanhado por um aumento do seu valor em termos económicos, políticos e sociais e (3) a violação de dados pessoais poderá ter efeitos significativamente negativos para os responsáveis pelo tratamento de dados nos setores público e privado, os responsáveis pelo tratamento de dados têm

uma necessidade e um interesse crescente em garantir que tomam medidas efetivas para assegurar uma verdadeira proteção dos dados (Art. 29 WP, 2010b). Com as entidades reguladoras cada vez mais interessadas na demonstração da *responsabilidade* (conformidade) da organização, este não é o tempo para esperar que a legislação determine uma maior ação sobre a privacidade. As leis podem levar anos para ser implementadas, mas as consequências de uma quebra – ou a falta de responsabilidade – pode ser imediata, visível e dispendiosa (Ernst & Young, 2012b).

O estudo anual da Ernst & Young (2012b), no domínio da segurança, permite constatar que está em ascensão a consciência organizacional sobre a necessidade de monitorizar como a informação pessoal está a ser utilizada (monitorização da sua privacidade), resultado da necessidade das organizações em demonstrar uma maior *responsabilidade* através do acompanhamento dos dados de identificação pessoal recolhidos, e como forma de mitigar violações dos dados recolhidos que podem prejudicar a reputação da organização. As organizações terão assim de manter registos formais de documentação dos processos de tratamento de dados, a fim de demonstrar o seu compromisso com a responsabilidade e a sua conformidade com os novos regulamentos (Culnan, 2011). Apesar da dificuldade em desenvolver uma lista abrangente de conformidade, que seja apropriada a todas as situações, a autora apresenta uma amostra de elementos de um programa de privacidade (ver Tabela 11), essenciais ao suporte do processo de análise de conformidade.

A longo prazo, a disposição relativa à responsabilidade pode incentivar o desenvolvimento de programas ou selos de certificação. Esses programas contribuirão para comprovar que um responsável pelo tratamento de dados cumpriu a disposição e, por conseguinte, definiu e implementou medidas adequadas que foram periodicamente auditadas (Art. 29 WP, 2010b). Prevê-se que a avaliação de uma organização por uma autoridade de certificação seja conduzida numa base de caso-a-caso. Não existe uma solução que sirva a todas, sendo sempre necessário determinar que aspetos da *responsabilidade* devem ser demonstrados por uma organização (Hunton & Williams, 2010).

Tabela 11 - Amostra de elementos de um programa de privacidade abrangente (adaptada de Culnan (2011))

Elemento do programa	**Exemplo de atividade**	**Exemplo de evidência de conformidade**
Supervisão administrativa	Nomear a(s) pessoa(s) adequada(s)	• Descrição de funções • Organograma
Programa escrito de privacidade	Elementos da política incluem: • Regulamentação • Políticas e procedimentos • Processos de gestão do risco • Conformidade • Reparação e aplicação	• Cópia das políticas • Alterações ao documento de políticas
A avaliação dos riscos, atualmente em curso	• Equipa multidisciplinar para a privacidade • Análises de impacto sobre a privacidade para novos sistemas e novas utilizações de dados pessoais • Auditorias internas regulares ou outros processos de análise	• Duração e assuntos abordados nas reuniões da equipa multidisciplinar • Relatórios das análises de impacto sobre a privacidade • Relatórios das auditorias
Formação dos profissionais	• Programa de formação formal • Formação específica para novos funcionários • Reciclagem para os funcionários existentes	• Materiais de formação • Registos do local e dos participantes na formação
Implementar e monitorizar controlos de privacidade	• Inventário abrangente da utilização de dados pessoais • Diretrizes para a construção de controlos de privacidade em novos sistemas • Diretrizes para testar os controlos de privacidade • Política de retenção de dados	• Resultados do inventário • Cópias das diretrizes e políticas • Sistemas aprovados • Resultados dos testes de sistemas e monitorização contínua
Terceiros	• Contratos	• Cópias dos contratos • Registos de garantia de terceiros
Aplicação interna	• Políticas para garantir o cumprimento, a conformidade • Sanções para violações das políticas	• Cópias das políticas • Relatórios das violações e o procedimento adotado
Transparência para com os titulares dos dados	• Avisos de privacidade • Procedimentos para informar o titular de modificações relevantes nas políticas e forma de obter o consentimento para novas utilizações de dados pessoais • Procedimentos para tratamento de dados de reclamações ou de dados de inquéritos.	• Cópia do aviso • Documento de aviso sobre as alterações • Documento de consentimento para novas utilizações de dados pessoais • Registos de tratamento de reclamações

Para o Art. 29 WP (2009), a proposta de regulamento (GDPR, 2012), implícita e explicitamente, em muitos casos, vai exigir que o responsável pelo tratamento respeite os princípios de proteção de dados e o cumprimento de obrigações

específicas, através de medidas pró-ativas, como: (1) a utilização de políticas e processos internos para implementar os requisitos do regulamento para as operações de processamento de dados, aprovadas ao mais alto nível dentro da organização; (2) desenvolver uma consciencialização, formação e instrução dos profissionais em relação à proteção de dados; (3) a elaboração de relatórios de conformidade e de auditorias e a obtenção de certificação por terceiros, que permita avaliar se as medidas internas adotadas para gerir, proteger e tornar seguros os dados pessoais, são eficientes; (4) a realização de avaliações de impacto sobre a privacidade, especialmente para certas operações de processamento de dados, uma vez que apresentam riscos específicos para os direitos e liberdades da pessoa em causa, por exemplo, em virtude da sua natureza, âmbito ou finalidade; (5) a designação de pessoas com responsabilidade direta pelo cumprimento da conformidade organizacional com as leis de proteção de dados; (6) a certificação da conformidade, que confirme que foram implementadas as salvaguardas adequadas à proteção dos dados pessoais em causa; e (7) a transparência destas medidas quer para com o titular dos dados, quer para com o público em geral.

Em resumo, para a *accountability*:

- Para as questões da privacidade e proteção de dados é essencial uma atitude pró-ativa da organização, capaz de demonstrar o seu compromisso com a privacidade, implementar as políticas de privacidade dos dados de acordo com os critérios externos reconhecidos e implementar mecanismos para assegurar a responsabilidade na tomada de decisão na gestão e proteção de dados.
- Um programa de responsabilidade constitui o meio de demonstração da vontade e da capacidade da organização em ser responsável e responsabilizada pelas práticas de gestão de dados. É essencial à salvaguarda da privacidade de dados, assim como à confiança do titular dos dados na organização, e entre esta e outras organizações.
- Deve constituir-se como um programa sólido e transparente, que contemple medidas adequadas e eficazes para pôr em prática as obrigações e princípios da legislação em vigor sobre proteção de dados. Constitui a ferramenta operacional necessária para as questões da privacidade.
- A análise da conformidade dos contextos de utilização de dados pessoais permite aferir da preparação da organização e avaliar o sucesso das políticas de privacidade implementadas para os dados.

3.1.6 Dados e manipulação de dados

A interoperabilidade e a cooperação podem ser consideradas como facilitadoras da integração aplicacional no setor público. A partilha de dados é um pré-requisito a qualquer sistema ou organização integrada ou em colaboração. Esta partilha só é possível através de uma compreensão e identificação adequada das entidades e estruturas de dados (Otjacques et al., 2007). Com o avanço nas inter-relações/interoperabilidade entre os sistemas, as questões de propriedade, de controlo, de prerrogativa, e de privacidade dos dados tornam-se mais difíceis de gerir (Waldo et al., 2010b).

Os dados constituem assim a principal razão da construção de plataformas de interoperabilidade entre sistemas. São essenciais à construção de serviços partilhados. Sendo fáceis de reproduzir e distribuir, estes podem ser copiados um número infinito de vezes sem perder a fidelidade (Waldo et al., 2010b), o que faz com que proteger e promover a sua privacidade constitua, para Cavoukian (2003), um verdadeiro desafio numa época de criação exponencial de redes de duplicação de dados, na sua maioria identificáveis. É certo que muitas organizações recolhem sobre os seus clientes mais dados do que na realidade necessitam e não sabem como os usar (Ernst & Young, 2013).

O contexto atual de utilização de dados pessoais, não centrado no utilizador, é caracterizado por (a) o utilizador apresentar um controlo limitado sobre a gestão e utilização dos seus dados; (b) cada organização apresentar políticas de privacidade diferentes; (c) o utilizador apresentar pouca ou nenhuma capacidade para gerir as configurações de privacidade; (d) cada organização requer ao utilizador uma autenticação distinta, bem como a partilha de dados pessoais, aumentando o risco de exposição e duplicação de dados sensíveis; (e) cada serviço verifica de forma isolada a identidade do utilizador e (f) cada serviço acaba por ter uma visão parcial de cada utilizador (Cavoukian, 2012).

Os dados

Os dados desempenham um papel fundamental no domínio da privacidade, sendo que devem ser recolhidos, processados e divulgados de acordo com os princípios de privacidade em vigor (Guarda & Zannone, 2009). As medidas a adotar para a

proteção de dados devem ser adequadas à sua natureza, quer sejam dados pessoais, dados sensíveis, dados de identificação pessoal ou dados anónimos.

> *Dados pessoais* – são o conjunto de todos os dados que está associado a um indivíduo específico, por exemplo, o seu nome, a sua data de nascimento, sexo, endereço, escolaridade, localização geográfica às 13h:14m no dia 30.mar.2005, etc., (Waldo, Lin, & Millett, 2010a). "Qualquer informação relativa a uma pessoa singular identificada ou identificável[52] …" (CE, 1995; IPC, 2009). Estes dados, contudo, só têm sentido se permitem associar ou diferenciar um indivíduo de outros (Waldo et al., 2007). A classificação como dados pessoais, certamente tem implicações para a cadeia de prestação de serviços e para as suas partes interessadas, especialmente se estes dados são classificados de maneira diferente por cada organização. Neste tipo de situação, devem ser mediadas as opções e as configurações de privacidade, devendo ser cada exceção cuidadosamente considerada (ENISA, 2011). A divulgação de dados pessoais pode em algumas circunstâncias apresentar riscos particularmente graves para os seus titulares. São o caso de (i) dados que podem revelar a sua localização física, (ii) dados de cuidados de saúde ou (iii) dados financeiros, e que podem, por exemplo, contribuir para que o seu titular possa ficar numa situação de "pessoas em risco[53]" ou "populações vulneráveis[54]". (ICO 2009). A Diretiva relativa à proteção de dados da UE (CE, 1995) não permite o tratamento de todos os tipos de dados pessoais, sendo que para determinados tipos de dados é necessário uma base jurídica especifica que o permita

---

[52] Podem ser utilizados vários dados para determinar se uma pessoa é "identificável", sendo o conceito de "identificabilidade" fortemente debatido, existindo mesmo várias discussões se o endereço IP deve ser considerado um dado pessoal (ENISA, 2011).

[53] Categorias de pessoas cuja segurança física pode estar em risco incluem: (1) pessoas que estão sob a ameaça direta de violência (vítimas de violência doméstica, testemunhas protegidas, pessoas que tenham sido objeto de ameaças públicas ou privadas, pessoas que se pretendem esconder de anteriores associações criminosas); (2) celebridades e figuras públicas (políticos, artistas e desportistas, indivíduos que promovem publicamente pontos de vista controversos); (3) pessoas com funções de segurança sensível (agentes de segurança nacionais, polícias disfarçados, guardas prisionais, equipas de instituições psiquiátricas) (ICO, 2009).

[54] Mesmo quando a segurança física não está sob ameaça, são necessários cuidados especiais no que respeita a "populações vulneráveis", algumas das quais podem ter dificuldade para exercer um controlo sobre os seus dados pessoais, nomeadamente: crianças, pessoas com deficiência mental, pessoas com graves deficiências físicas, recluso em liberdade condicional, os sem-abrigo, refugiados, pessoas com determinado estado de saúde (ICO, 2009).

explicitamente ou quando os indivíduos envolvidos o consentem antes do processamento dos dados (Hansen et al., 2008).

Dados sensíveis - são um subconjunto dos dados pessoais, sobre o qual uma das partes acredita dever ser privado (Waldo et al., 2007), nomeadamente dados que divulgam informações sobre a origem racial ou étnica, religiosa, filosófica ou outra, opiniões políticas, filiação em partidos, sindicatos, associações ou organizações de carácter religioso, filosófico ou político-sindical, bem como dados pessoais de saúde e vida sexual (Guarda & Zannone, 2009). A definição sobre que dados devem ser considerados como "sensíveis" é na maioria das vezes uma questão controversa (Waldo et al., 2010b).

Dados de identificação pessoal – subconjunto[55] dos dados pessoais (Waldo et al., 2010b) que permitem uma identificação direta da pessoa em causa (Guarda & Zannone, 2009), ou qualquer informação que identifica ou pode ser usada para identificar, contactar, ou localizar a pessoa a quem se refere tal informação. Esta identificação pode depender dos dados específicos da informação de identificação pessoal em questão, como da capacidade de agregação de dados de forma a reduzir significativamente ou até mesmo eliminar o anonimato implícito (Waldo et al., 2007). A Diretiva 95/46/CE define que *"... é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social"* (CE, 1995, p.38).

Dados anónimos – dados que não podem ser associados a qualquer titular de dados identificado ou identificável. (Guarda & Zannone, 2009). Esta categoria de dados não é regida por regulamentos de proteção de dados.

Os dados têm valores diferentes para diferentes pessoas (Jericho Forum, 2009a). A exigência e a expetativa individual variam para diferentes tipos de dados, e para o mesmo elemento de dados em situações diferentes. Quer isto dizer que numa situação um indivíduo pode considerar um elemento específico de dados como

[55] Por convenção e para efeitos legais, este subconjunto geralmente inclui o nome da pessoa em causa. Contudo, as pessoas utilizam múltiplas identidades, e conciliar estas múltiplas identidades, com base na união de vários subconjuntos de dados, é muitas vezes controverso (Waldo et al., 2010b).

altamente privado, e numa outra situação considerar o mesmo elemento de dados tudo menos privado (Waldo et al., 2010a). Para este grupo de autores, fatores como (1) o valor específico do elemento de dados, e se este pode ou não estigmatizar ou prejudicar; (2) o objetivo para o qual um elemento de dados é solicitado; (3) a acessibilidade a um determinado elemento de dados; e (4) a transitoriedade de um elemento de dados, apresentam uma forte influência sobre a expectativa individual de privacidade, que é importante conhecer.

Ciclo de vida dos dados

Para se avaliar efetivamente um ecossistema de dados, deve-se estar familiarizado com o ciclo de vida dos dados. De acordo com uma variedade de propósitos, os dados são recolhidos, usados/partilhados, atualizados e eliminados. A natureza cíclica do ciclo de vida dos dados deve ser apoiada por políticas, práticas, procedimentos e ferramentas adequadas. Embora os princípios do ciclo de vida sejam relativamente constantes, o seu funcionamento, o seu propósito e a forma como são suportados varia de organização para organização. Estão dependentes das necessidades, tipos de informação, sensibilidade da informação, escolhas políticas e uma série de outras variáveis. A avaliação de todas estas considerações sobre o ciclo de vida dos dados pressupõe uma familiaridade não só com as necessidades das entidades envolvidas, mas também os riscos que estas enfrentam, geridos através de uma adequada análise do risco (IPC, 2009).

A proteção deve ser consistente ao longo do ciclo de vida dos dados (representado na Figura 10), independentemente da sua localização ou ambiente de utilização, e considerar os seguintes princípios na conceção de mecanismos de proteção de dados: (1) os dados devem ser ininteligíveis, exceto quando um utilizador autorizado realiza tarefas autorizadas sobre os dados; (2) as especificações de acesso aos dados devem ser definidas tão próximo quanto possível dos dados, devendo as especificações de proteção serem transportadas com os dados, mantendo-se constantes em qualquer ambiente em que os dados residam; (3) os dados devem ser protegidos em todas as fases do seu ciclo de vida, devendo existir mecanismos para alterar a proteção se a sensibilidade dos dados se alterar; (4) deve existir uma raiz de confiança baseada em *hardware* para controlar a identidade das organizações que acedem aos dados e que possa anular intenções comprometedoras para aplicações e sistemas operativos de base aos sistemas de proteção de dados; (5) padronizar as decisões de acesso aos

dados de forma a lidar com a heterogeneidade aplicacional das organizações, assim como com a evolução e substituição das soluções tecnológicas – *hardware* e *software* (Jericho Forum, 2012). Este processo pode ser muito complexo e tornar-se crítico e dispendioso em contextos não confiáveis e extremamente dinâmicos (Canfora, Costante, Pennino, & Visaggio, 2008).

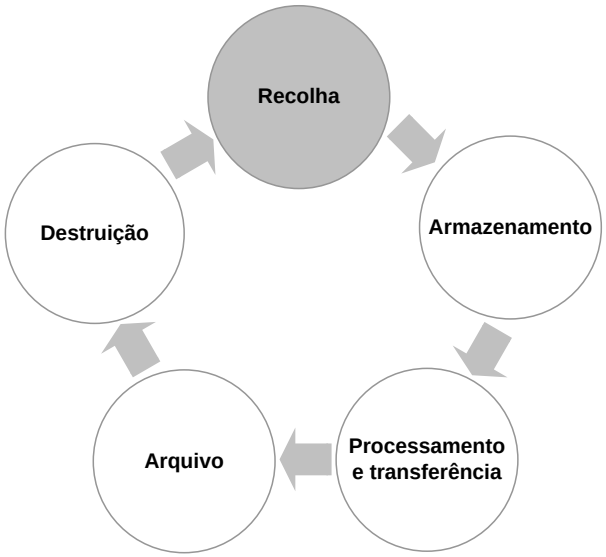

Figura 10 - Ciclo de vida dos dados
(adaptado de (Jericho Forum, 2012))

Quando os dados são gerados, partilhados e guardados por várias organizações, o controlo destes dados é uma questão ainda mais importante. As tecnologias atuais de proteção da informação foram desenhadas no pressuposto de que apenas uma organização irá controlar os mecanismos de execução e as políticas de acesso aos dados. A viabilidade dos mecanismos de proteção necessita de uma negociação entre as organizações envolvidas que lhes permita ajustar o seu risco ou nível de conforto de forma adequada (Jericho Forum, 2012). O problema da preservação da privacidade durante a disseminação de dados, consiste em assegurar a privacidade de dados confidenciais, confiados pelo seu proprietário a um guardião primário para toda a vida útil dos dados, que inclui a recolha dos dados, o processamento, o armazenamento e a disseminação a guardiões subsequentes, que por sua vez, recolhem, processam, armazenam e disseminam dados (Lilien & Bhargava, 2006).

Num processo de partilha de dados não podemos simplesmente partilhar todos os dados sem a atenção devida para com as questões da proteção destes dados, ou então, decidir não partilhar a totalidade dos dados, por falta de medidas de proteção. Está

em causa o princípio da "minimização dos dados", que define que os sistemas devem recolher, processar e reter, apenas os dados pessoais necessários para cumprir com o objetivo do sistema. No entanto, questões como a proporcionalidade ou a necessidade do processamento são igualmente importantes, e devem ser consideradas a fim de proporcionar uma abordagem de minimização (ICO, 2008).

A encriptação constitui a única tecnologia interoperável que pode ser aplicada aos dados independentemente da sua localização ou ambiente de utilização. Contudo, a encriptação não é persistente. Após a desencriptação dos dados, o seu proprietário perde o controlo sobre a distribuição, utilização e proteção futuras (Jericho Forum, 2012). Embora a encriptação tenha sido suficiente e continue a ter uma utilização intensiva, muitas das novas formas de utilização de dados necessitam de um modelo de proteção diferente da encriptação – um modelo de proteção centrado nos dados. Este deve contribuir para se captar as características dos dados que podem ser utilizadas para facilitar a sua utilização apropriada, em cenários onde existem múltiplos acessos válidos para fins diferentes (Barker et al., 2009). Por exemplo, um prestador de cuidados de saúde pode exigir informações muito específicas sobre uma determinada condição do paciente, enquanto uma companhia de seguros necessita apenas de uma declaração resumo dos custos dos cuidados do paciente.

Um sistema ideal de proteção centrado nos dados deve contemplar todos os tipos de documentos e ficheiros, vídeos e outros arquivos, sítios de colaboração baseados na *Web*, serviços de conferências, e até mesmo chamadas telefónicas (Jericho Forum, 2012). A necessidade de controlo sobre o acesso a dados sensíveis ou confidenciais e a sua proteção, justificam o desenvolvimento conjunto de um programa de classificação dos dados (Jericho Forum, 2009a). Os SGBD mais modernos não consideram a privacidade como um recurso dos seus sistemas de primeira ordem, nem a privacidade é uma característica explícita do modelo de dados subjacente, sob o qual estes sistemas são construídos. Mesmo quando um fornecedor de um SGBD disponibiliza recursos de gestão da privacidade, fazem-no usando o seu próprio entendimento do que constitui a proteção da privacidade (Barker et al., 2009). Para estes autores, quando se considera as questões da privacidade de qualquer ambiente de armazenamento de dados, devem ser considerados como intervenientes-chave o fornecedor dos dados, o responsável pela recolha de dados, os utilizadores de dados, e o sistema de armazenamento de dados em si.

Manipulação de dados

A manipulação dos dados está muito relacionada com o princípio da limitação da finalidade da Diretiva 95/46/CE (CE, 1995), que estipula que os dados pessoais devem ser "*recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com estas finalidades*". É, segundo a CNPD (2012a), um princípio insuficiente se não se verificar uma das seguintes condições: que a lei estabeleça o que são fins incompatíveis ou que a CNPD seja chamada a pronunciar-se quando houver alteração da finalidade inicialmente prevista. Este é um princípio crucial, na medida em que da explicitação da finalidade depende a aplicação de um conjunto de outros princípios, como o da qualidade dos dados ou o princípio do tratamento lícito e equitativo (CNPD, 2012b).

Ao abrigo da legislação europeia de proteção de dados (CE, 1995), e no âmbito do processamento de dados pessoais, são reconhecidas três categorias distintas de entidades: (1) o *titular dos dados* pessoais; (2) a pessoa *responsável pelo tratamento,* que individualmente ou em conjunto com outrem "determine as finalidades e os meios de tratamento dos dados pessoais" (Artigo 2º (d) da Diretiva 95/46/CE, (CE, 1995)); e (3) o *processador de dados* ou *subcontratante,* um terceiro que simplesmente trata os dados pessoais por conta do responsável pelo tratamento, sem controlar ou fazer uso dos dados (Artigo 2º (e) da Diretiva 95/46/CE, (CE, 1995)).

O papel principal do responsável pelo tratamento é, antes de mais, determinar quem será o responsável pelo cumprimento das normas sobre proteção de dados e de que modo as pessoas em causa podem exercer na prática os seus direitos. Por outras palavras: atribuir a responsabilidade. O conceito de subcontratante desempenha um papel importante no contexto da confidencialidade e da segurança do tratamento (artigos 16º e 17º da Diretiva 95/46/CE), na medida em que permite identificar as responsabilidades daqueles que apresentam um envolvimento mais direto no tratamento de dados pessoais, quer sob a autoridade direta do responsável pelo tratamento ou por sua conta (Art. 29 WP, 2010a).

No entanto, num cenário emergente de composição de serviços, a principal questão é identificar o local onde os dados são processados e o que realmente pode ser considerado como "processamento de dados" (ENISA, 2011). A diferenciação organizacional no setor público e no setor privado, a evolução das TIC, bem como a globalização do tratamento de dados, aumentam a complexidade dos mecanismos de

tratamento de dados, exigindo uma clarificação destes conceitos, a fim de assegurar uma aplicação efetiva e o cumprimento na prática (Art. 29 WP, 2010a). A aplicação concreta dos conceitos de responsável pelo tratamento e subcontratante está a tornar-se cada vez mais complexa, face ao facto de, tanto no setor privado como no público, apostar-se cada vez mais na criação de cadeias de prestação de serviços ou numa prestação de serviços que envolve várias organizações e no recurso à subcontratação ou externalização de serviços.

São cada vez mais os casos em que diferentes intervenientes agem na qualidade de responsáveis pelo tratamento, ou seja, situações em que existem vários corresponsáveis que conjuntamente determinam as finalidades do tratamento. A probabilidade de existirem vários intervenientes no tratamento de dados pessoais está naturalmente associada aos vários tipos de atividades que, de acordo com a diretiva, podem ser consideradas como "tratamento", que no fundo, é a atividade objeto de "controlo conjunto" (Art. 29 WP, 2010a). Neste cenário tão complexo, é ainda mais importante poder atribuir facilmente papéis e responsabilidades, a fim de evitar que as complexidades do controlo conjunto resultem numa distribuição inviável das responsabilidades, o que prejudicaria a eficácia da legislação sobre proteção de dados (ENISA, 2011). A compreensão do conceito e âmbito de responsável pelo tratamento, passa por dividir este conceito em três grandes grupos constituintes: o aspeto subjetivo («*a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo*»); a possibilidade de controlo coletivo («*que, individualmente ou em conjunto com outrem*»); e os elementos essenciais que distinguem o responsável pelo tratamento de outros intervenientes («*determine as finalidades e os meios de tratamento dos dados pessoais*») (Art. 29 WP, 2010a).

A recolha facilitada e rápida de dados, a sua agregação e partilha, a sua facilidade de recolha sem qualquer consentimento, a durabilidade de longo prazo do fácil acesso aos dados, e o espaço quase ilimitado e as tecnologias avançadas de análise, são preocupações e questões que emergem da contínua abertura dos SI, nomeadamente para a Internet, durante a última década (Otjacques et al., 2007). Normalmente, a reutilização de informação envolve uma decisão da organização com base legal, sobre novos usos para as informações pessoais recolhidas, incluindo a agregação de dados, a mineração de dados, o redireccionamento ou partilha de dados originalmente

recolhidos por um motivo deferente. Problemas de privacidade potencialmente resultantes da reutilização de informação incluem inferências incorretas, decisões baseadas em erros nos dados, exclusões ou invasões (Culnan, 2011).

As organizações têm feito um esforço para alcançar um equilíbrio entre a proteção da privacidade dos seus utilizadores e a valorização dos seus conjuntos de dados, nomeadamente no controlo da geração de perfis[56] comportamentais para fins de marketing e vendas. Contudo, como pode um utilizador ter a certeza de que o perfil gerado é suficientemente anónimo e está bem protegido por vários anos? Não está definido qual o nível de fiabilidade necessário e existe uma variação muito grande na demonstração dos níveis relatados de proteção (ENISA, 2010). Na origem deste problema está a diferença nas definições nos vários regulamentos, o que pode levar, por exemplo, a que muitas organizações tenham que desenvolver as suas definições internas de dados pessoais e proteção da privacidade.

Em resumo, para os dados e manipulação de dados:

- A compreensão do propósito principal da recolha, utilização e partilha de dados (através de interoperabilidade) com outras organizações deve constituir-se como o ponto de partida para a compreensão das necessidades de privacidade e proteção destes dados.
- À semelhança da segurança, e da proteção de dados, a privacidade deve ser preocupação constante durante todo o ciclo de vida dos dados.
- Uma classificação objetiva e dinâmica (durante todo o seu ciclo de vida) é condição fundamental à aplicação de medidas de privacidade e proteção.
- As medidas de proteção de dados dependem diretamente do âmbito ou contexto da utilização dos dados, das tecnologias aplicadas, dos *standards* utilizados, quer ao nível local do sistema de informação quer na interoperabilidade com outros sistemas.

[56] O conceito de perfil comportamental (*profiling*) consiste na recolha e análise de vários eventos, cada um atribuível a uma única entidade de origem, a fim de obter informação relacionada com a entidade de origem. Consiste, por outras palavras, na transformação de dados em conhecimento (ENISA, 2011). A geração de perfis envolve a recolha de dados (registo, armazenamento e rastreamento) e pesquisas sobre estes dados para identificar padrões (com a ajuda de algoritmos de mineração de dados). A criação de perfis cria sérias preocupações à privacidade, uma vez que, a informação pessoal está a ser (em silêncio) recolhida ou exposta sem o consentimento do cidadão, e não é conhecido o destino ou finalidade para o qual a informação pessoal vai ser utilizada.

3.1.7 Estratégia para a privacidade

No centro das preocupações de cada indivíduo, sobre o processamento de informações pessoais, está a perceção da não existência de processos rigorosos, da incapacidade das organizações reconhecerem a sua responsabilidade na gestão da privacidade, e da falta de responsabilidade nos quadros superiores das organizações em relação ao tratamento adequado de dados pessoais (ICO, 2008). O desenho de políticas de privacidade dos dados é um processo de adaptação constante, que vai desde a definição de estratégias para proteger adequadamente os dados, até ao *design* de uma tecnologia de suporte que implementa as medidas estabelecidas (Canfora et al., 2008). O respeito pela privacidade é um processo, em que o primeiro passo deve permitir identificar onde a organização está, e então determinar para onde deve ir, e por fim identificar o caminho para lá chegar (Hamidovic, 2010).

Apesar de as disposições da Diretiva 95/46/CE (CE, 1995) formarem uma base sólida para a proteção de dados pessoais, o cumprimento destas obrigações legais muitas vezes não é devidamente incorporado nas práticas internas das organizações. Os gestores executivos, em geral, não estão suficientemente conscientes dos problemas, nem têm conhecimento das práticas de processamento de dados nas suas organizações (Art. 29 WP, 2009) – mesmo (especialmente) os que afirmam ter uma política de segurança documentada (Jericho Forum, 2007a). A menos que a proteção de dados se torne parte dos valores e práticas de uma organização, e sejam expressamente atribuídas responsabilidades neste domínio, uma conformidade efetiva estará sempre em risco e vão continuar a existir percalços na proteção de dados. É necessário reconhecer que a privacidade é uma questão de gestão, tanto quanto é uma questão técnica (ICO, 2008).

A questão de como relacionar as políticas de acesso à informação com os imperativos de negócio que a justificam, está apenas a iniciar-se (Jericho Forum, 2007a). Para muitas organizações que dependem de dados pessoais, a privacidade tornou-se um fator estratégico. Uma abordagem abrangente é muitas vezes referida como uma estratégia para a privacidade. Entende-se por estratégia para a privacidade, uma abordagem sob orientação do nível executivo da organização, em que a privacidade é reconhecida como um fator de grande importância para a realização dos objetivos da organização. Envolve a inclusão de preocupações com a privacidade na estratégia organizativa, através do planeamento e implementação de medidas para lidar com as

questões da privacidade, e através do desenvolvimento de uma sensibilidade em privacidade na cultura organizacional e nos sistemas computacionais (ICO, 2009).

Como acontece com qualquer estratégia, uma estratégia para a privacidade necessita de ser pró-ativa, figurar explicitamente e não meramente implícita. Deve ser articulado um plano de desenvolvimento, afetados recursos e monitorizado o seu desempenho (ICO, 2009). Neste sentido, as organizações devem ser mais pró-ativas no desenvolvimento de estratégias de gestão da privacidade que permitam equilibrar entre aquilo que são os requisitos regulamentares e o desenvolvimento tecnológico. Isto requer um conhecimento sobre a natureza da sua arquitetura de TI, assim como do possível impacto de novas soluções tecnológicas que pretendam adotar (Ernst & Young, 2012b). É assim necessário capacitar e requerer profissionais para o desenvolvimento e implementação de programas, políticas e práticas organizacionais, considerando o alcance, natureza e sensibilidade da utilização de dados (Hunton & Williams, 2010).

De acordo com o ICO (2008), o âmbito de uma estratégia para a privacidade deve refletir a natureza e missão da organização, podendo ser adotadas três abordagens: (1) uma estratégia minimalista para a privacidade dos dados; (2) uma estratégia abrangente para a privacidade dos dados; e (3) uma estratégia abrangente para a privacidade.

> *Estratégia minimalista para a privacidade dos dados* – deve dar resposta às exigências da legislação de privacidade, incluindo (mas não se limitando a) os princípios de proteção de dados estabelecidos pela diretiva de proteção de dados (CE, 1995) e pela Lei n.º 67/98 (AR, 1998). No mínimo, uma organização que lida com dados pessoais deve: (1) desenvolver uma compreensão organizacional da privacidade e das principais questões de privacidade que surgem nas relações da organização com indivíduos, (2) conduzir uma revisão e avaliação de todos os processos que lidam com dados pessoais, e (3) reconhecer a necessidade de considerar as questões da privacidade na fase inicial do desenho de novos projetos, e em todas as fases do seu ciclo de vida.
>
> *Estratégia abrangente para a privacidade dos dados* – geralmente implementada por organizações que reconhecem a privacidade como um fator estratégico na relação de confiança para com o titular dos dados e como uma

questão de responsabilidade organizacional, pressupõe o compromisso do nível executivo da organização para com um programa de privacidade e a nomeação de um diretor responsável pela privacidade (*Chief Privacy Officer*), que em conjunto vão permitir: (1) realizar um processo de formação de uma estratégia, que antecipe problemas, e é baseado na apreciação dos dados na posse da organização, práticas, tecnologias e legislação de utilização de dados; (2) garantir que a engenharia de processos de negócios e atividades de reengenharia têm embutida uma sensibilidade para as questões da privacidade dos dados; (3) fomentar o respeito pela privacidade na filosofia e mentalidade organizacional - cultura de privacidade; (4) estabelecer e manter um programa de comunicação interna e externa.

Estratégia abrangente para a privacidade – as pessoas estão preocupadas com outras dimensões da vida privada, bem como, as organizações podem achar vantajoso definir um âmbito mais amplo da sua estratégia de privacidade de modo a contemplar estas preocupações, nomeadamente as relacionadas com a privacidade da pessoa, a privacidade do comportamento da pessoa e a privacidade das comunicações pessoais.

A natureza dinâmica e multifacetada da privacidade dificulta o desenvolvimento de soluções claras por parte dos gestores de topo, porque "as regras mudam", porque "as expetativas dos clientes mudam", porque "os regulamentos ou mesmo a perceção pública mudam" (Bamberger & Mulligan, 2011).

Em resumo, em relação à estratégia para a privacidade:

- *A privacidade dos dados em contextos de interoperabilidade não se apresenta como um problema interno e isolado em cada organização, mas sim um problema comum a todas as organizações.* O desenvolvimento de um plano integrado de proteção e controlo da privacidade dos dados deve apresentar na sua base uma estratégia conjunta de todas as organizações.
- O conhecimento e consciência da importância da privacidade como fator estratégico, do risco associado à ausência de políticas de proteção, podem desencadear nos responsáveis executivos a necessidade de uma visão estratégica para este domínio.
- Um ambiente de interoperabilidade confiável para a recolha, partilha e utilização de dados pessoais, está dependente da colaboração organizacional no desenho de uma estratégia conjunta.

3.1.8 Confiança e gestão da confiança

O direito à privacidade dos dados visa salvaguardar a autonomia individual contra o poder que instituições ou indivíduos ganham sobre outros através da utilização de dados pessoais. Sensíveis, e possivelmente imprecisos, os dados podem ser usados contra as pessoas em ambientes financeiros, políticos, de emprego e de saúde. Nas sociedades democráticas, o comportamento dos cidadãos retrai-se quando estes se apercebem que estão a ser observados continuamente (Weitzner et al., 2008). A mera perceção de uma ameaça à sua privacidade face a um determinado serviço ou situação, pode levar a uma redução substancial da confiança do utilizador. Pode, inclusive, dificultar a partilha de dados sensíveis entre as entidades, e pode resultar numa rejeição completa de colaboração entre possíveis parceiros (Lilien & Bhargava, 2006). São necessárias garantias de privacidade para a divulgação de dados privados. Sem estas, podemos perder muitas oportunidades de interação.

Para o Jericho Forum (2006), a confiança é uma condição essencial à cooperação entre pessoas e organizações. Uma das partes escolhe cooperar com outra com base na confiança, porque acredita que é possível (1) a parte confiável estar disposta a confiar na outra; (2) é do interesse de ambas as partes confiarem; (3) a parte confiável cumpre com as competências, capacidades e recursos necessários; e (4) existe um mecanismo de responsabilidade que pode obrigar a parte confiável a cumprir. A divulgação cuidadosa de dados sensíveis, e proteger o direito à privacidade da parte mais fraca, são fundamentais não só para as partes envolvidas, mas também para a sociedade em geral. Ainda assim, a proteção da privacidade dos dados e a disponibilização de mecanismos adequados é principalmente uma responsabilidade da parte mais forte (Lilien & Bhargava, 2006). A confiança depende da negociação da privacidade em diversas áreas de aplicação – incluindo a prestação de cuidados de saúde, *e-commerce*, e serviços de localização baseados em rede.

Francis Fukuyama, citado por Windley (2005), argumenta que os valores públicos, especialmente a confiança, moldam a direção das economias nacionais. A confiança é assim um tema importante mas complexo - apesar de ser um conceito que os seres humanos entendem implicitamente, existe uma grande dificuldade na sua captura digitalmente através de algoritmos. Em certo sentido, privacidade e confiança são valores concorrentes: a privacidade implica sigilo, enquanto a confiança prospera na abertura e na transparência (Wright et al., 2009). O processo de atribuir confiança é

mais simples quando o processo é físico e de proximidade – quando podemos ver, sentir e tocar no que se está prestes a confiar. O surgimento das redes de comunicação que nos afastam daquilo em que queremos confiar introduz uma série de novas dificuldades (Jericho Forum, 2009b). Qualquer interação, seja uma simples operação ou uma operação complexa, apenas pode ter início depois de existir um nível adequado de confiança entre as entidades em colaboração (Lilien & Bhargava, 2006). A gestão da confiança é uma função essencial a todo o trabalho colaborativo, nomeadamente à confiabilidade, comportamento e comprometimento de todas as partes (Vernadat, 2010).

A confiança constitui uma crença firme na veracidade, boa-fé e honestidade de outra parte, o que envolve algum risco. Não há dúvida que quando consideramos em quem e sobre o quê estamos dispostos a confiar, a confiança está ligada ao risco (Windley, 2005). O uso da confiança é muitas vezes implícito. A privacidade e a confiança são dois conceitos intimamente relacionados em ambientes de computação, tal como acontece em sistemas sociais (Lilien & Bhargava, 2006).

A confiança é um fenómeno social. Com cada vez mais negócios e interações sociais a serem realizados eletronicamente, os processos de autenticação e autorização são fundamentais à gestão da confiança. Enquanto a autenticação liga o agente eletrónico a uma identidade do mundo real, a qual constitui a base de um mecanismo de responsabilidade, a autorização representa o grau de confiança ou competência que foi atribuído à identidade. A autorização representa um contrato – um conjunto de regras acordado sobre o comportamento esperado para a autorização (Jericho Forum, 2006). No mundo da identidade digital, a confiança está assim associada a um determinado conjunto de credenciais de identidade e os atributos que lhe estão associados (Windley, 2005). Situações em que um sistema de autenticação/autorização permite determinar a identidade do utilizador, e com base nesta identidade atribui-lhe certos privilégios de acesso aos dados e aplicações, é manifestamente insuficiente para o nível de confiança necessário. Num ambiente de interoperabilidade, as estruturas organizativas podem ser muito diferentes, o que pode significar privilégios diferentes para o acesso a um processo ou a determinado tipo de dados desse processo. É desta forma imperativo que dentro de um ambiente de interoperabilidade a proteção dos dados mantenha um nível de confiança semelhante ao praticado dentro do sistema de informação (CALLIOPE, 2010).

O primeiro passo para gerar confiança neste novo modelo de organizações em rede ou "federado", é desenvolver formas seguras de recolher e armazenar dados pessoais. Existe uma série alargada de meios técnicos para garantir que a informação está segura quando é transferida entre organizações. No entanto, a tecnologia é apenas parte da solução. Atua em prol das pessoas, políticas e procedimentos (IPC, 2009). Mesmo quando surge uma nova tecnologia e parece inspirar riscos para a privacidade, na sua essência, a tecnologia é essencialmente neutra para a privacidade. O que é geralmente questionável é a forma como é aplicada (Cavoukian, 2011). Para Wright et al. (2009) é assim necessário: (1) conciliar ou pelo menos lidar com as diferentes interpretações da privacidade entre os diferentes atores; (2) desenvolver e fortalecer mecanismos de reforço da confiança, e analisar a sua aplicabilidade a diferentes domínios, circunstâncias e grupos de interessados; (3) compreender as perceções das partes interessadas sobre *confiabilidade* e como tais perceções podem ser acomodadas; e (4) estabelecer compromissos (equilibrar interesses em conflito) entre a privacidade (e confiança quando necessário) e outros valores e exigências da sociedade (por exemplo, entre a privacidade individual e a segurança coletiva).

Uma série de capacidades e recursos devem ser desenvolvidas, a fim de evitar a perda, potencialmente catastrófica, de confiança, nomeadamente: (1) gerir a identidade e os acessos entre as organizações em que podemos confiar, e não apenas dentro de cada organização; (2) desenvolver mecanismos de gestão da confiança em que podemos estar confiantes; (3) ter um conhecimento comum do impacto sobre os níveis de negócio para desenvolver decisões de risco eficazes; (4) acordo comum sobre uma classificação da sensibilidade da informação; e (5) gestão do relacionamento entre organizações (especialmente no que se refere à confiança) (Jericho Forum, 2009b).

Em resumo, para a confiança e gestão da confiança

- O contexto de interoperabilidade pode gradualmente influenciar a confiança das organizações sobre os dados e serviços partilhados, com implicação sobre as pretensões de privacidade dos dados.
- A análise prévia do impacto sobre a privacidade, sempre que novas soluções tecnológicas ou de tecnologias de informação processam dados pessoais, influencia positivamente a confiança sobre o futuro funcionamento destas soluções.
- O alinhamento (interoperabilidade) e uniformização da gestão da privacidade para todas as organizações participantes no ambiente de colaboração são determinantes à confiança na partilha de dados.

3.1.9 Ética e cooperação humana

Na nossa vida privada pretendemos controlar a informação sobre nós mesmos, que nos pode embaraçar ou prejudicar, assim como controlar a informação que pode aumentar as nossas oportunidades de sucesso. Existe assim uma tradição, no que diz respeito à privacidade dos dados, para definir a privacidade com base no controlo (Tavani & Moor, 2001). De acordo com a teoria de controlo da privacidade, a obtenção de privacidade está diretamente ligada à capacidade de controlo individual sobre a sua informação pessoal (Tavani, 2008), e à autodeterminação sobre informações e assuntos pessoais (Amicelle, 2012). Uma das principais ideias subjacentes a esta teoria está no reconhecimento do papel que a *escolha* individual desempenha na teoria da privacidade (Tavani, 2008), separando assim o conceito de privacidade dos conceitos de liberdade e solidão (Tavani, 2007). Contudo, para Amicelle (2012) as teorias de controlo da privacidade são teorias subjetivas, dada a sua dependência em relação à subjetividade humana e à escolha e atitude individual. Apresentam como falha principal o facto de não especificarem de forma clara o grau de controlo necessário à proteção dos dados pessoais, e sobre que tipo de dados pessoais se espera ter controlo, para se desfrutar de privacidade (Tavani, 2008). Ou seja, pode-se questionar se alguém pode razoavelmente esperar ter o controlo sobre todos os seus dados pessoais (Tavani, 2007). Na opinião deste autor, este controlo limita-se ao que classifica como "informação pessoal não pública", a qual inclui dados sensíveis e confidenciais.

Contudo, e atendendo a que privacidade é fundamentalmente proteção contra invasões e recolha de dados por terceiros, e que o controlo individual de informação pessoal constitui parte da justificação da privacidade com influência sobre a sua gestão, fazem, na opinião de Moor (1997), com que o conceito de privacidade em si, seja melhor definido pelas teorias de restrição do acesso. Se a definição de privacidade depender unicamente do nosso controlo individual, simplesmente não teremos privacidade, face à necessidade de controlar uma vasta quantidade de informações que circulam entre redes de computadores e bases de dados (Tavani & Moor, 2001). É o caso da necessidade de manter privados dados pessoais sensíveis, mesmo que o seu titular não esteja em condições de controlar a sua utilização – um paciente não deve perder o direito a ter os seus registos médicos protegidos, mesmo quando não está em condições de os controlar.

Com base na teoria de restrição do acesso, existe privacidade se a pessoa em causa é capaz de limitar e restringir outros de acederem à sua informação ou assuntos pessoais. A privacidade é vista como um direito normativo objetivo ou um valor moral que existe mesmo que políticas ou práticas humanas escolham implementar mecanismos que revelam factos particulares em público ou permitem o acesso público à esfera privada de um ou mais indivíduos (Amicelle, 2012). A restrição ou limitação do acesso, expressa o direito à proteção. Proíbe que alguém ou qualquer outra coisa aceda e processe informações (Tavani & Moor, 2001). Quando um acesso não autorizado é realizado numa situação de privacidade normativa, a privacidade não só se perdeu, foi violada ou invadida (Moor, 1997). Alguns críticos argumentam que esta teoria não consegue estabelecer uma distinção adequada entre os contextos "privado" e "público", ou zonas em que o acesso à informação pessoal é restrito, assim como tende a ignorar, ou, pelo menos, subestimar, o papel do controlo ou de escolha, necessários à obtenção de privacidade no que se refere à informação pessoal (Tavani, 2008).

Apesar de tanto as teorias de controlo como as de restrição da privacidade terem algo de importante a dizer no domínio da proteção da privacidade de dados pessoais, não conseguem, segundo Tavani (2008), fornecer uma explicação adequada de privacidade informacional. A solução passa por uma teoria de privacidade que apresente pelo menos três componentes, uma estrutura tripartida em que cada componente desempenha uma função diferente: uma definição de privacidade, uma justificação para a privacidade e um processo para a gestão da privacidade (Tavani & Moor, 2001).

Moor (1997) concilia as perspetivas destas duas teorias, numa teoria mais abrangente, denominada *teoria da restrição do acesso/controlo limitado* (RALC[57]) da privacidade, e persegue o pressuposto de que uma teoria adequada de privacidade deve diferenciar o conceito de privacidade dos conceitos de justificação e gestão da privacidade (Tavani, 2007). Na base desta teoria, está a distinção entre o "conceito de privacidade", definido através de termos de restrição do acesso, e da "gestão da privacidade", conseguida através de um sistema de controlos limitados (Tavani, 2008). À semelhança das teorias da restrição de acesso, a teoria RALC salienta a

[57] Do inglês *Restricted Access/Limited Control.*

importância da criação de zonas, essenciais à limitação ou restrição do acesso aos dados pessoais.

Ao analisar o conceito de privacidade, a teoria RALC distingue entre a *condição* de privacidade (ou seja, o que é necessário para ter privacidade num sentido descritivo) e o *direito* à privacidade (Tavani, 2007). Uma pessoa tem privacidade "numa situação em relação a outros", se, nessa situação está "protegida contra invasões, interferências e acessos à sua informação pessoal por parte de outros" (Moor, 1997). O autor distingue, assim, situações de privacidade natural e situações de privacidade normativa. Uma situação de privacidade normativa constitui uma situação protegida por normas éticas, legais, ou convencionais. Virtualmente todas as sociedades estabelecem *situações*[58] normativas de privacidade, *zonas* de privacidade, as quais definem e limitam para determinadas condições o acesso a pessoas ou aspetos sobre estas. Apesar de uma situação variar de cultura para cultura, de local para local, tem como objetivo a proteção de indivíduos e o fomentar das relações sociais (Tavani & Moor, 2001). Contudo, assistimos ao surgimento de situações com políticas diferentes e justificáveis de proteção de dados pessoais. É evidente que num contexto de dados pessoais muito sensíveis, não podem existir duas situações com políticas diferentes de proteção. Nestes casos é necessário criar *zonas* de privacidade, uma variedade de situações particulares, com tipos e níveis de acesso diferenciados para diferentes indivíduos (Moor, 1997). É necessária a criação de novas zonas de privacidade para a proteção de indivíduos, especialmente quando estes não têm controlo sobre os seus dados pessoais e não se podem proteger (Tavani & Moor, 2001). É de salientar a opinião de Moor (1997), para o qual a noção de privacidade na realidade está mais ligada a uma situação ou uma zona do que à própria informação.

Quanto às situações de privacidade natural, os indivíduos são protegidos contra a observação, interferência e intrusão por meios naturais. Por exemplo, os limites físicos em ambientes naturais. Numa situação de privacidade natural, falamos em *perda* da privacidade, e não em *violação* ou *invasão*, dado que não existem normas

[58] Normalmente o conceito de *situação normativa* de privacidade está associado à localização física. Uma habitação é uma situação normativa privada em que o acesso ao seu interior carece de permissão. Contudo, situações, que não localizações físicas, que envolvem relacionamentos, atividades, e informação, são também situações normativas. O ato de votar é uma atividade privada, quer em suporte papel ou através de máquinas de voto ou Internet. Informação e registos médicos são privados. Todos estes exemplos são situações privadas – contextos em que se espera que exista uma proteção normativa adequada da privacidade (Tavani & Moor, 2001).

legais ou éticas segundo as quais o direito à privacidade deve ser protegido (Tavani, 2007). Em situações de privacidade normativa, a privacidade pode ser violada ou invadida, além de perdida, por causa das leis e normas que foram estabelecidas para proteger essas situações

O controlo individual, por sua vez, ajuda-nos a gerir a nossa privacidade. O controlo individual com influência sobre a gestão da privacidade tipicamente acontece de três formas distintas: a escolha, o consentimento e correção (Tavani & Moor, 2001). Sem a capacidade de se controlar o acesso e a distribuição de dados pessoais, a sua privacidade não pode estar protegida (Cleff, 2007).

Grande parte das pesquisas anteriores sobre a privacidade tem, tipicamente, definido a privacidade dos dados a partir das perspetivas dos indivíduos serem capazes de controlar ou limitar o acesso às suas informações pessoais (Xu et al., 2008). A abordagem "aviso e escolha" é uma operacionalização deste ponto de vista da privacidade, em que o objetivo é proporcionar aos indivíduos medidas de controlo. O elemento "aviso", é suposto ajudar as pessoas a decidirem, inicialmente, se devem ou não disponibilizar dados pessoais, e o elemento "escolha" é uma oportunidade para que as pessoas possam colocar alguns limites sobre como os seus dados pessoais são posteriormente reutilizados. Ou seja, pretende-se desta forma aumentar a disposição dos consumidores a revelar dados pessoais, minimizando os riscos de divulgação (Culnan, 2011). Contudo, para esta autora esta abordagem tem falhado devido essencialmente à vulnerabilidade da relação entre consumidores e as organizações, nomeadamente o défice de informação e controlo por parte do consumidor, no acesso contínuo a todas as informações sobre as práticas de gestão da informação de uma organização e no facto de estar limitado na sua capacidade de exercer controlo sobre as formas como as organizações usam os seus dados pessoais. Como resultado, os consumidores dependem da forma de agir das organizações, em prol do seu melhor interesse e que não lhes provoque danos.

Com o objetivo de proteger a privacidade, o titular dos dados deve ter a capacidade de controlar o acesso e a distribuição dos seus dados pessoais. Em situações em que os dados são utilizados sem o seu conhecimento ou consentimento, a sua privacidade é claramente comprometida (ENISA, 2011). Como argumentado por Cleff (2007), o titular dos dados, ao recear pela sua privacidade, pode reagir restringindo os dados que fornece, ou dando dados falsos, comprometendo assim a validade das bases de

dados. Uma organização deve assim implementar processos bem elaborados e de confiança para resolver os problemas que possam surgir com a proteção de dados, nomeadamente através de procedimentos formais de apresentação de reclamação (adequados ao tipo de organização, à natureza do conjunto de dados em utilização, e à forma como os dados estão a ser utilizados num determinado contexto), de forma a responder às preocupações dos indivíduos sobre as práticas de proteção de dados e falhas potenciais ou reais, e para garantir que os direitos dos indivíduos no que diz respeito aos seus dados são respeitados (Hunton & Williams, 2010).

Na maioria dos sistemas jurídicos que abordam a privacidade, o livre consentimento do titular dos dados é necessário para a recolha, utilização e divulgação de dados pessoais (ou sensíveis), exceto quando é permitido por lei. A "qualidade" deste consentimento depende do contexto em que obrigatoriamente necessita de ser expresso; um consentimento mais específico e mais claro será provavelmente necessário sempre que a sensibilidade dos dados aumenta. O consentimento também não é permanente, e pode ser retirado ou revogado em data posterior (IPC, 2009).

A transparência é um elemento essencial. Deve ser disponibilizada informação clara ao titular dos dados sobre a utilização dos seus dados e da lógica subjacente ao tratamento, e esta informação só deve ser limitada se necessário, em casos individuais para não comprometer investigações e por um período limitado de tempo (Art. 29 WP, 2009). Uma organização deve desenvolver, implementar e comunicar aos indivíduos as políticas de privacidade de dados desenhadas para lhe proporcionar uma proteção eficaz da sua privacidade (Hunton & Williams, 2010). O direito do titular dos dados de acesso e retificação aos dados deve ser permitido mesmo em contextos transfronteiriços, sendo de evitar que o titular dos dados perca este controlo (Art. 29 WP, 2009). Um problema persistente, na gestão da privacidade, é dar a possibilidade aos indivíduos de revogar o consentimento já dado para tratamento de dados pessoais (ICO, 2008).

A privacidade envolve o fornecimento aos indivíduos de um controlo adequado sobre os seus dados pessoais, determinado pelo contexto de utilização, e deve garantir a aplicação de salvaguardas adequadas para proteger estes dados (IPC, 2009). O titular dos dados deveria ter o direito de decidir o que acontece com os seus dados, quem pode vê-los, quando podem vê-los, e idealmente deveria ser capaz de rastrear quem acedeu aos dados. O facto de o titular dos dados não ter a possibilidade (ou ser capaz)

de controlar o acesso, a utilização e a modificação dos seus dados, contribui para uma perda de integridade dos mesmos. Esta falta de controlo leva a que os dados não sejam atualizados e podem ficar obsoletos. No limite, se o titular não gerir adequadamente os riscos da utilização dos seus dados pessoais, perde quaisquer direitos que possa ter tido sobre os seus dados (Jericho Forum, 2007a). Não devem existir situações, mesmo que exista um consentimento formal do utilizador, geralmente aprovadas por defeito ou através de termos e condições padrão, em que o utilizador ou não entendeu completamente as consequências do seu consentimento, ou não tem outra alternativa a não utilizar o serviço em causa (Otjacques et al., 2007).

Para Haas et al. (2011) a preservação da privacidade num EHR depende dos seguintes requisitos: (1) um utente deve ser capaz de expressar as políticas de privacidade obrigatórias relativas aos fluxos de dados relacionados com ele; (2) um utente deve ser capaz de verificar se as políticas de privacidade acordadas foram cumpridas, e em casos de fluxos de dados não autorizados este deve ser capaz de identificar a sua origem; (3) o utente não deve ser forçado a confiar em ninguém, a não ser as partes diretamente envolvidas no tratamento, porque a interligação de várias fontes públicas de dados podem expor os seus dados pessoais; e (4) os dados obtidos a partir da interligação de diferentes fluxos de dados médicos devem ser insuficientes para estabelecer perfis ou para adquirir novos conhecimentos sobre os pacientes.

Em resumo, para a ética e cooperação humana:

- A transparência para com o titular dos dados deve evoluir no sentido de se adaptar às exigências do contexto de partilha de dados, e permitir ao titular dos dados uma compreensão sobre as medidas de proteção específicas para o ambiente de colaboração.
- A ética e atitude dos profissionais face ao requisito de partilha de dados entre organizações, que em algumas situações pode questionar a sua privacidade profissional, podem condicionar o funcionamento pretendido para o ambiente de colaboração.

3.1.10 Estrutura organizativa

Uma rede (ou ambiente) de colaboração representa uma união de entidades organizacionais, infraestruturas, processos de negócio, recursos e relações, que suportam o esforço comum para desenvolver um benefício coletivo, quer seja um programa, serviço, ou um produto (Gottschalk, 2009a). As redes de colaboração são criadas quando as organizações concordam em partilhar informação numa base contínua, reguladas de maneira informal, ou pode apresentar mecanismos formais de gestão e uma estrutura organizacional explícita (Fedorowicz, Gogan, & Williams, 2007). Apresentam assim, uma forma alternativa de organização, distinta da hierárquica tradicional, uma vez que são baseadas em colaboração, conhecimento distribuído, dependência mútua e normas de reciprocidade (Navarrete, Gil-Garcia, Mellouli, Pardo, & Scholl, 2010). A capacidade operacional para a colaboração é um fator chave de sucesso para as organizações em rede, e a interoperabilidade é o resultado a atingir para as organizações envolvidas, de uma forma continuada, bem como formas ocasionais de colaboração (ATHENA, 2010). A solução passa pela colaboração entre vários níveis governativos, organizações privadas e organizações não lucrativas. É necessário, contudo, entender como criar redes de organizações públicas ou privadas destinadas a partilhar informação dentro de um domínio específico, e como trabalhar em conjunto de forma a responder eficazmente aos novos problemas (Navarrete et al., 2010).

Gerida formal ou informalmente, uma rede de colaboração tem a sua própria estratégia, estrutura de gestão, sistemas inter-organizacionais, e outros sistemas, processos e recursos, para além das estratégias, estruturas de gestão, sistemas, processos e recursos de cada uma das organizações participantes (Gottschalk, 2009a). O setor público que durante anos tinha como formato padrão as hierarquias, ao depender cada vez mais da colaboração e partilha de informação, criou condições para o desenvolvimento de organizações em rede, dada a sua eficiência (Navarrete et al., 2010). Na base desta mudança está a evolução de normas e tecnologias que contribuíram para que as instituições dessem início à utilização de serviços externos de uma forma mais eficiente (Suess & Morooney, 2009).

Em termos de gestão, uma organização em rede pode ser definida como uma federação constituída informalmente, com autogestão, muitas vezes temporária, em

que o trabalho é dividido dentro das equipas ou unidades de trabalho e que são coordenadas através de um mercado interno (Navarrete et al., 2010).

Os aspetos organizacionais da interoperabilidade estão relacionados com a definição dos objetivos do negócio, o alinhamento e coordenação de processos de negócio e a atribuição de recursos de colaboração às organizações que pretendem trocar informações, as quais podem apresentar diferentes processos e estruturas internas (Vernadat, 2010). Sem dúvida que quando o objetivo é aumentar a interoperabilidade entre sistemas, o desafio é bastante complexo (Brownsword et al., 2004). Vários fatores, na opinião destes autores, podem contribuir para que a interoperabilidade não funcione como o esperado: (1) a interoperabilidade planeada para novos sistemas sofre frequentemente adaptações por forma a ser compatível com sistemas antigos que não podem ser atualizados; (2) a especificação dos *standards* utilizados revela-se insuficiente; (3) as políticas de promoção de um único ponto de vista em detrimento de outros, onde as políticas que aumentem os níveis de interoperabilidade num domínio são generalizadas para outros domínios; e (4) os testes construídos para verificar regularmente a interoperabilidade, não conseguem identificar deficiências de interoperabilidade.

Chen et al., (2008) sugerem três categorias de problemas ou barreiras que podem influenciar o funcionamento e desempenho da interoperabilidade: (1) *problemas conceptuais* devido à diferença sintática e semântica da informação a trocar entre os sistemas; (2) *problemas tecnológicos* relacionados com a incompatibilidade entre as tecnologias de informação dos dois sistemas; (3) *problemas organizacionais*, relacionados com a definição de responsabilidades (quem é responsável por quê?) e autoridade (quem está autorizado a fazer o quê?), assim como a incompatibilidade entre as estruturas organizativas. A estas três categorias, Scholl & Klischewski (2007), para o domínio da governação eletrónica (eGov), adicionam outras restrições como: (1) as restrições legais/constitucionais, (2) as restrições jurisdicionais, (3) restrições de colaboração, (4) restrições informativas, (5) restrições de gestão/coordenação, (6) restrições de custo, e (7) restrições de desempenho. Embora algumas destas restrições ou limitações sejam de fácil resolução, outras devem ser consideradas na sua plena complexidade em relação ao nível ideal de interoperabilidade que se pretende atingir (Gottschalk, 2009b).

Dadas as características deste fator em estudo, é importante a descrição de (Scholl & Klischewski, 2007), para as restrições relacionadas com a dependência da interoperabilidade face à estrutura organizativa, ou seja, as restrições de colaboração e restrições organizacionais.

> *Restrições de colaboração*: as organizações são distintas em termos da sua disponibilidade e prontidão para a colaboração e interação (interoperabilidade) com outras organizações. Estilos de liderança compatíveis, organização sociopolítica adequada, e experiências passadas, influenciam o grau de vontade e proficiência do potencial de interoperação.
>
> *Restrições organizacionais*: os processos e os recursos organizacionais podem variar entre as organizações, de tal forma que a integração e a interoperabilidade podem revelar-se extremamente difíceis de conseguir sem a padronização de processos, sistemas e políticas. No entanto, quando as organizações alinham o seu contexto organizacional, permitem um aumento nos níveis de integração e interoperabilidade.

Em resumo, para a estrutura organizativa:

- A disponibilidade e prontidão no desenvolvimento de soluções de interoperabilidade ao nível organizacional, é fundamental ao desenvolvimento integrado de um projeto para a privacidade e proteção de dados.
- A agilidade organizativa, entendida como a capacidade das interfaces não técnicas da organização em se adaptarem às alterações constantes no seu ambiente, é preponderante para o desenvolvimento e adaptação contínua de medidas de proteção da privacidade dos dados aplicáveis ao ambiente de interoperabilidade.

3.2. Alinhamento dos subdomínios identificados com o modelo OIM

Independentemente da sua dimensão *técnica, organizacional ou semântica* (Cechich et al., 2008; Vernadat, 2010; C4ISR, 1998; IDABC, 2004), os modelos de maturidade de interoperabilidade, ao descreverem os estágios pelos quais os sistemas, processos ou organizações progridem ou evoluem (Clark & Jones, 1999), ajudam uma organização, ou um sistema, a melhorar a forma de cooperar e interoperar com outras entidades (Guédria et al., 2008), numa perspetiva organizacional, dos sistemas e tecnologias, ou dos dados (Winters et al., 2006).

As iniciativas de interoperabilidade apresentam vários níveis de maturidade. E, à semelhança dos requisitos técnicos, a complexidade da privacidade dos dados também aumenta com a evolução do nível de maturidade da interoperabilidade, a implementar entre organizações. É, assim, necessário que a preparação das organizações, a sua capacidade de colaboração e partilha de conhecimento, a sua compreensão dos objetivos da colaboração e dos requisitos de proteção da privacidade dos dados, evoluam no sentindo de retirar a privacidade dos dados da lista das barreiras impeditivas ao desenvolvimento da interoperabilidade. Neste sentido, a utilização de um modelo de interoperabilidade de suporte ao estudo é essencial para compreender a evolução das questões da privacidade dos dados sempre que evolui o nível de interoperabilidade, e desta forma apresentar as melhores soluções que permitam lidar corretamente com a proteção da privacidade dos dados. Desta forma, as organizações ao acordarem, entre si, o nível de interoperabilidade que pretendem implementar, dispõem de informação suficiente que lhes permite implementar a colaboração necessária para as questões da privacidade dos dados.

O modelo de maturidade OIM, apresentado no ponto 2.2.3 do Capítulo II, para uma perspetiva mais organizacional da interoperabilidade, contempla 5 níveis de maturidade, e em simultâneo, 4 atributos focados nas questões organizacionais, a preparação, a compreensão, a coordenação e a ética. Cada atributo é importante para averiguar a capacidade das organizações para interoperar (Clark & Moon, 2001). Tendo por base o entendimento de Clark & Jones (1999) em relação à utilização destes atributos, é necessário compreender como podemos associar cada um dos dez subdomínios de fatores identificados neste capítulo, com cada um dos atributos. Esta relação pode ser conseguida compreendendo aquilo que cada atributo pode representar para a privacidade dos dados:

a. *Preparação* – se tivermos em conta o grau de prontidão (agilidade) e preparação das organizações necessários à interoperabilidade a vários níveis entre sistemas heterogéneos, é necessário estudar quais os fatores que podem condicionar esta preparação em matérias de privacidade dos dados;
b. *Compreensão* – dada a necessidade de compreensão das questões associadas à privacidade dos dados (podem incluir-se neste grupo questões técnicas) para todo o ambiente de interoperabilidade, é desta forma essencial identificar as

principais influências que neste domínio podem condicionar o nível de desenvolvimento de um entendimento partilhado, assim como a abrangência e capacidade de partilha de informação e conhecimento;

c. *Coordenação* – tendo em conta a importância da compatibilidade entre as várias organizações, nomeadamente estruturas de coordenação e estilos de liderança, pretende-se conhecer os fatores determinantes neste nível para a privacidade dos dados;
d. *Ética* – atendendo a que os maiores problemas de interoperabilidade não são de cariz técnico, é essencial compreender se existem fatores relacionados com a natureza das organizações, as estruturas organizativas, os meios e cultura organizacional, a confiança e confiabilidade de cada organização participante, que podem comprometer os objetivos da colaboração ao nível da privacidade dos dados.

Atendendo à essência de cada um dos dez subdomínios apresentados, assim como à sua relação com os atributos de interoperabilidade, cada subdomínio foi alinhado com o modelo OIM como se apresenta na Figura 11.

OIM	Preparedness	Understanding	Command and Coordination	Ethos
4. Seamless				
3. Associative				
2. Collaborative				
1. Cooperative	"Experiência" "Cultura de privacidade"	"Segurança e infraestruturas" "Linguagem de privacidade (taxonomia)" "*Accountability*: responsabilidade e conformidade" "Dados e manipulação de dados"	"Estratégia para a privacidade" "Estrutura organizativa"	"Confiança e gestão da confiança" "Ética e cooperação humana"
0. Independent				

Figura 11 - Enquadramento dos fatores identificados com os atributos do OIM

Capítulo IV - Abordagem metodológica e conceção do *estudo de caso*

Em qualquer investigação é fundamental a adoção de uma perspetiva filosófica para compreender a posição ontológica e epistemológica do investigador e deste modo justificar a escolha da estratégia e método(s) de investigação (Caldeira & Romão, 2002).

Neste estudo estão em causa fatores com influência sobre o sucesso da interoperabilidade organizacional, *a privacidade e a proteção de dados*. O foco principal é constituído por questões organizacionais, nomeadamente a atividade humana e a partilha de dados e informação, a colaboração, e não as questões técnicas ou tecnológicas. Constitui-se como um estudo enquadrado no domínio científico dos SI. Para Parker et al., (1994) um SI constitui um sistema de atividade humana (social), que pode ou não envolver a utilização de sistemas computacionais. Os SI constituem uma disciplina aplicada (Clarke, 2000) e multi-perspetiva, ao envolver uma pluralidade de métodos de investigação (Villiers, 2005), e por outro lado constituem uma disciplina ampla e aplicada, que usa, redefine e reestrutura teorias desenvolvidas noutras disciplinas, para um maior conhecimento sobre os seus próprios problemas (Vessey, Ramesh, & Glass, 2002; Ramesh, Glass, & Vessey, 2004). O desenvolvimento da investigação foca-se em simultâneo no desenvolvimento de formas práticas e inovadoras de resolução de problemas reais, e propõe princípios gerais de desenho, essenciais para decisões futuras (Villiers, 2005).

Num primeiro momento é importante o enquadramento deste estudo face às perspetivas filosóficas e às metodologias de investigação existentes no domínio dos SI, e num segundo momento a escolha do método de investigação. As questões de investigação necessitam assim de estar ligadas a uma das perspetivas filosóficas (Iqbal, 2007), a qual fornece a base ideológica à metodologia a utilizar (Gonzalez & Dahanayake, 2007).

4.1 Enquadramento filosófico

Um paradigma fornece um quadro conceptual para visualizar e dar sentido ao mundo social – "o principal ponto de partida filosófico" - ou seja, a filosofia e pressupostos subjacentes que formam a base de uma abordagem ou metodologia (Villiers, 2005). É

um conjunto de convicções básicas sobre a natureza da realidade social, a natureza do "mundo" e neste, o lugar de cada indivíduo (Guba & Lincoln, 1994). Os modelos e paradigmas de investigação são baseados em diferentes fundamentos filosóficos e conceções da realidade (Villiers, 2005). Guba & Lincoln (1994) argumentam que as crenças básicas que definem paradigmas, podem ser resumidas pelas respostas dadas pelos seus proponentes de qualquer paradigma a três questões fundamentais: (1) Qual é a forma e a natureza da realidade (a questão ontológica)? (2) Qual é a relação entre o investigador e o que pode ser conhecido (a questão epistemológica)? (3) Como é que o investigador valida que aquilo em que acredita pode ser conhecido (a questão metodológica)?

A ontologia preocupa-se com a natureza da realidade (Cavaye, 1996), com a nossa visão da realidade (Villiers, 2005). Constitui a ciência que estuda o ser, as suas propriedades e o modo como se manifesta. A ontologia inclui o conjunto de princípios assumidos como verdadeiros, numa determinada abordagem de investigação em ciências sociais, relativamente à natureza da realidade social (Caldeira & Romão, 2002). Por sua vez, a epistemologia é a teoria ou ciência do conhecimento, corresponde às diferentes formas assumidas como válidas de obter conhecimento da realidade social (Caldeira & Romão, 2002), procurando responder a questões do tipo: Como é construída a teoria? Como pode o conhecimento científico ser adquirido? Como testar a teoria? Que métodos de investigação podem ser utilizados? (Gregor, 2006). Os diferentes paradigmas de investigação são assim baseados em diferentes fundamentos filosóficos e conceções da realidade, e têm associados várias estratégias e abordagens metodológicas (Villiers, 2005).

São várias as perspetivas filosóficas nas áreas das ciências sociais, tendo-se destacado três na investigação no domínio dos SI: o positivismo, o interpretativismo e a teoria crítica (Myers, 1997; Bolan & Mende, 2004).

De entre estas três perspetivas filosóficas, o positivismo é provavelmente a mais conhecida, com um papel dominante ao longo dos séculos (Caldeira & Romão, 2002). Com o intuito de testar uma teoria e melhorar o conhecimento preditivo de fenómenos (Myers, 1997), o positivismo enfatiza o papel da ciência como o único método que conduz à verdade (Gonzalez & Dahanayake, 2007). Uma das características fundamentais da doutrina positivista é exatamente a unidade do método científico, isto é, o princípio de que existe apenas um método científico,

lógico-dedutivo, válido para qualquer área do conhecimento (Caldeira & Romão, 2002). O paradigma positivista sustenta que o conhecimento é absoluto e objetivo, descoberto por meios empíricos controlados, e tem por objetivo uma representação exata e imparcial da realidade (Villiers, 2005). Baseia-se principalmente em métodos quantitativos, onde os dados compreendem principalmente números e medições, e a análise é realizada com recurso a métodos estatísticos.

Enquanto o positivismo testa hipóteses, o interpretativismo estuda questões de investigação, focadas na compreensão dos fenómenos que ocorrem em ambientes naturais (Villiers, 2005). Radicalmente diferente da perspetiva positivista, assume que a realidade social é intelectualmente construída e deve ser entendida através da interpretação das atividades sociais que são objeto de estudo no processo de investigação (Caldeira & Romão, 2002). Recolhe dados qualitativos e a análise destes produz resultados relacionados com detalhes intrincados, onde são relevantes valores e experiências humanas (Villiers, 2005). Em vez da generalização visa a compreensão em profundidade. Apesar de recente, a abordagem interpretativa é cada vez mais utilizada na área dos SI (Caldeira & Romão, 2002), visando a compreensão do contexto do SI e a forma como os atores interpretam e desenham os elementos do contexto (Gonzalez & Dahanayake, 2007). Ou seja, a abordagem interpretativa destina-se a produzir uma compreensão do contexto do SI, e o processo através do qual o SI influencia e é influenciado pelo contexto (Myers, 1997).

A teoria crítica é uma perspetiva filosófica antipositivista e que deve ser claramente distinguida da abordagem interpretativista. Procura a emancipação do indivíduo, tentando remover as barreiras sociais e organizacionais que inibem a discussão de valores e normas (Caldeira & Romão, 2002). Procura revelar como os SI estão incorporados nos processos organizacionais e são utilizados por indivíduos e grupos, através do desenvolvimento de uma compreensão das posições e experiências das pessoas afetadas pelos sistemas, e ligando estes conhecimentos com condições mais amplas, relações de poder e estruturas sociais. A investigação crítica cria conhecimento com intenção transformadora e emancipadora (Cecez-kecmanovic, 2001), ou seja, pretende ajudar a eliminar as causas de alienação e dominação (Myers, 1997). É caracterizada pela reflexividade (autocrítica) e na crença de que ninguém tem o monopólio da verdade (Gonzalez & Dahanayake, 2007).

A privacidade dos dados é um conceito (de aplicação) complexo, de entendimento subjetivo, circunstancial, e pouco desenvolvido nas organizações. A experiência dos vários profissionais em privacidade dos dados ainda é insuficiente, o que dificulta a preparação de um programa de proteção aplicável localmente e ao conjunto heterógeno de SI. É necessário desenvolver uma compreensão profunda da problemática da privacidade dos dados e das questões da interoperabilidade, capturar as perspetivas possíveis num contexto específico, e desenvolver ferramentas para validar cientificamente o conhecimento recolhido. O resultado do estudo está dependente da visão individual dos profissionais e da experiência das organizações em contextos de partilha de dados, e sobre todas as questões com influência sobre a sua privacidade. Neste sentido, consideramos adequada a opção por uma abordagem interpretativa para este estudo.

4.2 Estratégia de investigação

A adoção de uma estratégia particular de investigação, e respetivos métodos associados, está condicionada pela perspetiva filosófica adotada pelo investigador, pelo objeto de estudo e, principalmente, pelos objetivos da investigação (Caldeira & Romão, 2002). Contudo, para estes autores, a escolha da abordagem metodológica a utilizar não depende, de uma forma rígida, da perspetiva filosófica adotada.

A conclusão de um projeto de investigação está assim dependente do contributo do método de investigação, o qual é fundamental para se gerar conhecimento, através da pesquisa (Iqbal, 2007). É contudo importante, a compreensão destes métodos com base na distinção mais comum entre os métodos de investigação: qualitativos e quantitativos (Myers, 1997; Bolan & Mende, 2004).

Os métodos qualitativos realçam a descrição de eventos naturais ou sociais, onde o investigador tenta desenvolver a compreensão relativa a uma situação social, o papel e a interação de um grupo (Iqbal, 2007). O investigador concentra-se numa análise indutiva, em vez de uma análise dedutiva, e explora o que as pessoas fazem ou dizem, formando assim a sua opinião. Os métodos de investigação qualitativos foram desenvolvidos para as ciências sociais, para permitir o estudo de tendências/fenómenos culturais e sociais (Myers, 1997). Incluem métodos como a *action research*, o *estudo de caso*, a *etnografia* e a *grounded theory* (Bolan & Mende, 2004), e podem ter um contributo muito importante na investigação em SI (Caldeira

& Romão, 2002). Os investigadores qualitativos normalmente trabalham com pequenas amostragens de pessoas, inseridas no seu contexto e estudadas em profundidade – ao contrário de pesquisas quantitativas, que visam um grande número de casos descontextualizados, com o objetivo de obter significância estatística. Ou seja, as amostras qualitativas tendem a ser dirigidas, focadas, em vez de ao acaso (Miles & Huberman, 1994).

Ao contrário, as pesquisas quantitativas lidam com fenómenos naturais, análises objetivas e com resultados numéricos (Iqbal, 2007; Myers, 1997). A replicação é fácil de obter, podendo o investigador colocar restrições desejadas ao resultado da atividade de investigação. O alcance destes métodos expandiu-se, sendo agora aceites nas ciências sociais através de inquéritos, experiências de laboratório, métodos formais (por exemplo, econometria) e modelação matemática (Bolan & Mende, 2004).

Nem sempre a pura utilização de métodos quantitativos se traduz num contributo relevante para as ciências sociais, em geral, e para os SI em particular (Caldeira & Romão, 2002). Os autores justificam esta afirmação pelo facto de, em determinado tipo de objetos de estudo, ser bem mais interessante conhecer exatamente e com profundidade como funcionam algumas, poucas, organizações e respetivos SI que têm um comportamento diferente da generalidade, do que estimar o comportamento médio da generalidade das organizações.

A motivação para uma investigação qualitativa, em oposição à investigação quantitativa, vem da observação que, se existe uma coisa que distingue os seres humanos do mundo natural, é a nossa capacidade de falar (Myers, 1997). Contudo, este autor realça que a palavra "*qualitativo*" não é sinónimo de "*interpretativo*" – uma investigação qualitativa pode ou não pode ser interpretativa, dependendo dos pressupostos filosóficos do investigador. A investigação qualitativa pode ser positivista, interpretativa ou crítica. Daqui resulta que a escolha de um método específico de investigação qualitativa é independente da posição filosófica subjacente adotada. É o caso do método *estudo de caso*, que pode ser positivista, interpretativo ou crítico (Yin, 2009; Myers, 1997). Pode utilizar uma abordagem indutiva ou dedutiva, utilizar métodos qualitativos e quantitativos, investigar um ou múltiplos casos (Cavaye, 1996). Existem assim estratégias e métodos de investigação naturalmente mais coerentes com determinada perspetiva filosófica, mas também é

possível alguma flexibilidade na seleção de métodos de investigação a adotar dentro de uma determinada perspetiva filosófica (Caldeira & Romão, 2002).

Pelas características e objetivos deste trabalho de investigação, em que o fenómeno em estudo está mal compreendido, não existem conceitos teóricos para a sua compreensão em ambientes de interoperabilidade, em que existe um interesse particular por parte das organizações em entender a dinâmica do fenómeno e onde a compreensão do contexto de ação e as experiências individuais são relevantes, podemos concluir que estamos perante uma realidade complexa, subjetiva e que obriga ao seu estudo em contexto real. Estamos perante fatores relacionados com a "atividade humana" que podem condicionar a privacidade dos dados em processos de colaboração entre organizações. Neste sentido, a opinião, a experiência e o conhecimento dos vários atores num fenómeno com estas características constituem a principal, senão única, fonte primária de informação.

Estando o estudo já anteriormente identificado com a perspetiva filosófica interpretativista, e tendo em consideração que (1) as características do estudo exigem que se investigue a problemática num local específico (em contexto real), e (2) neste constituem como fonte primária de informação a opinião e perspetivas individuais dos profissionais das várias organizações, uma abordagem qualitativa é, em nossa opinião, a abordagem indicada para um projeto de investigação desta natureza. Isto não exclui a possibilidade de se utilizar dados quantitativos, desde que o objeto de estudo o justifique.

4.3 A opção pelo método de investigação *estudo de caso*

Existem áreas de pesquisa dentro dos SI onde a teoria e a compreensão não se encontram muito desenvolvidas. Áreas onde os fenómenos são dinâmicos e sem maturidade, em que as terminologias, as definições e a linguagem comum, não são claras ou amplamente aceites (Darke, Shanks, & Broadbent, 1998). A investigação em SI tem sido essencialmente dominada por três estratégias – experiências laboratoriais, inquéritos e respetiva análise estatística, e estudos de casos – embora existam muitas outras formas de investigação: *action research*, estudos longitudinais, *grounded theory*, etc. (Caldeira & Romão, 2002). Um grande número de teorias de gestão nasceu da observação e interpretação de casos empresariais particularmente

interessantes, sem uma evidente comprovação estatística dos fenómenos identificados (Caldeira & Romão, 2002).

A estratégia de investigação de *estudos de caso* é uma estratégia particularmente bem adaptada à investigação em SI, desde que o objeto seja o SI nas organizações, e o interesse sejam questões organizacionais em vez de questões técnicas (Myers, 1997), em que é necessária uma compreensão das interações entre as TI e o contexto organizacional (Darke et al., 1998). É uma estratégia de investigação que se concentra na compreensão da dinâmica presente no interior de contextos únicos (Eisenhardt, 1989). Constitui um meio muito útil para investigar o desenvolvimento, implementação e utilização dos SI nas organizações, apesar das dificuldades em se generalizar os resultados (Darke et al., 1998). O facto de este conhecimento não poder ser formalmente generalizado, não significa que ele não possa entrar no processo coletivo de acumulação de conhecimento num determinado domínio (Flyvbjerg, 2006). Um *estudo de caso* puramente descritivo, fenomenológico, sem qualquer intenção de generalizar pode certamente ser de valor neste processo, e ajudar a abrir caminho rumo à inovação científica. A ideia que um *estudo de caso* é uma simples descrição de uma situação ocorrida, desprovida de contexto teórico e de possibilidade de generalização (analítica), não corresponde à realidade (Caldeira & Romão, 2002).

O método *estudo de caso* é uma característica integrante da estratégia de investigação de estudos de caso[59]. Constitui um termo que descreve "uma forma de sistematizar a observação", o qual (1) não controla ou manipula explicitamente as variáveis em estudo, (2) estuda o fenómeno no seu contexto natural e (3) faz uso de técnicas e ferramentas qualitativas para recolha e análise de dados (Cavaye, 1996). Tipicamente combina técnicas de recolha de dados, tais como entrevistas, observação, questionários e análise de documentos e textos, podendo desta forma ser utilizados

[59] Várias estratégias de investigação utilizam o método estudo de caso, assim como partilham várias características deste método. São os casos: (1) *estudo de campo* – realizado no ambiente natural do fenómeno, em que o investigador é um observador, utiliza técnicas sistemáticas (questionários e realização de entrevistas) para a recolha de dados, e não tem nenhuma intenção de controlar ou manipular as variáveis; (2) *action research* – combina a investigação pura (observação) com ação (participação), na qual o investigador não define um problema de investigação à priori, permitindo que o problema seja definido pelo local, tendo por objetivo, observar, registar e participar ativamente na tentativa de resolver o problema no local; (3) *descrições de aplicação* – constituem relatos de eventos reais em torno de um fenómeno, no qual o investigador não entra no local para investigar uma questão de investigação específica, mas usa a descrição do caso para informar os leitores de aplicações bem-sucedidas; (4) *pesquisa etnográfica* – em vez de interpretar os dados do ponto de vista teórico ou do ponto de vista do investigador, este procura entender o significado de fenómenos através do que os participantes no local lhe atribuem (Cavaye, 1996).

tanto métodos qualitativos de recolha e análise de dados (mais relacionados com palavras e significados), como métodos quantitativos (mais relacionados com números e medições) (Darke et al., 1998). O método *estudo de caso* não é nem uma tática para a recolha de dados, nem meramente uma característica do planeamento em si, mas uma estratégia de investigação abrangente (Yin, 2009).

Um *estudo de caso* pode ser usado para atingir vários objetivos da investigação: para descrever um fenómeno, para construir uma teoria (indutivo), ou para testar conceitos teóricos existentes (dedutivo) (Darke et al., 1998; Cavaye, 1996; Eisenhardt, 1989). O método *estudo de caso* pode ser usado para estas três finalidades, apesar da forte tradição na descrição e construção de teorias (Cavaye, 1996), em que é utilizado para fornecer evidências para a gestão de hipóteses e para a exploração de áreas onde o conhecimento existente é limitado (Darke et al., 1998). Yin (2009) é um forte defensor do uso dedutivo do *estudo de caso*, para o qual a teoria suporta o caso de estudo. Este ou desenvolve ou testa uma teoria.

Independentemente do objetivo da investigação, a abordagem metodológica com base no *estudo de caso* pode ser tanto numa perspetiva filosófica interpretativista como positivista (Darke et al., 1998). Por exemplo, numa perspetiva interpretativista, o *estudo de caso* é desenhado para compreender e explicar um fenómeno social específico, procurando capturar as diferentes perspetivas dos elementos envolvidos no contexto e processo em análise. A interpretação dos dados deve ser realizada utilizando modelos teóricos anteriormente estabelecidos, que poderão ter um contributo significativo para explicar a realidade (Caldeira & Romão, 2002).

Para Yin (2009), a definição técnica de um *estudo de caso* pode ser apresentada em duas partes:

1. Quanto ao seu âmbito, um *estudo de caso* é uma investigação empírica que (a) investiga um fenómeno contemporâneo dentro do seu contexto de vida real, especialmente quando (b) as fronteiras entre fenómeno e contexto não são claramente evidentes.
2. Uma vez que fenómeno e contexto nem sempre são discerníveis em situações de vida real, um conjunto de outras características técnicas, como a recolha de dados e as estratégias de análise de dados, tornam-se a segunda parte da definição, em que a investigação de um estudo de caso (a) enfrenta uma situação tecnicamente única em que haverá muito mais variáveis de interesse

do que pontos de dados, e, como resultado, (b) baseia-se em várias fontes de evidências, e (c) beneficia-se do desenvolvimento prévio de proposições teóricas para conduzir a recolha e análise de dados.

Yin (2009) descreveu as várias fases de desenho que um *estudo de caso* deve apresentar, como representado na Figura 12. Definiu o *estudo de caso* como estratégia de investigação, desenvolveu uma tipologia para desenho de estudos de caso, descreveu a lógica de replicação, que é essencial para a análise de múltiplos casos, e salientou a necessidade de validade e confiabilidade em projetos de pesquisa de estudo de caso (Eisenhardt, 1989).

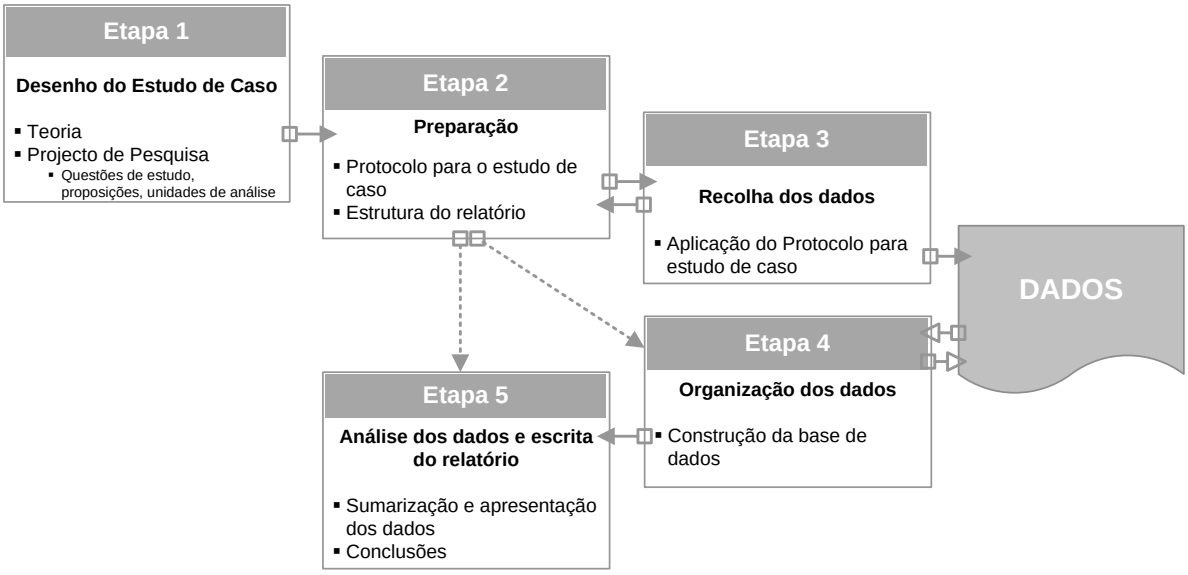

Figura 12 - Etapas de um projeto de *estudo de caso*
(adaptado de (Yin, 2009))

Um *estudo de caso* pode ser exploratório (compreender um fenómeno ainda pouco estudado ou aspetos específicos de uma teoria ampla), descritivo (descrever determinada população ou fenómeno) ou explicativo (identificar os fatores que determinam ou contribuem para a ocorrência dos fenómenos, explicando as suas causas). Podemos identificar algumas situações em que todas as estratégias de pesquisa podem ser relevantes, e outras situações em que se pode considerar duas estratégias de forma igualmente útil. Três condições permitem contudo diferenciar estas três estratégias de pesquisa: (1) o tipo de questão, (2) a abrangência do controlo sobre eventos comportamentais e (3) o grau de enfoque em acontecimentos históricos versus acontecimentos contemporâneos (Yin, 2009).

Um esquema básico de categorização para os tipos de questão pode ser representado pela conhecida série: "quem", "o que", "onde", "como" e "porquê". Questões do tipo "o que" são mais exploratórias, em que o tipo de questão apresenta um fundamento lógico justificável para conduzirem a um estudo exploratório. Contudo, quando o tipo de questão "o que" é, na verdade, uma forma de investigação na linha do "quanto" ou "quantos", um *estudo de caso* não será uma estratégia vantajosa. Em contraste, questões do tipo "como" e "porque", mais ambivalentes e que necessitam de ser bem esclarecidas, são normalmente mais explicativas, pelo facto de lidarem com ligações operacionais que necessitam de ser traçadas ao longo do tempo (Yin, 2009).

Considerando as características deste estudo, e dado que este pretende conhecer com detalhe um fenómeno dinâmico (privacidade dos dados) em contextos de interoperabilidade (contexto real), tendo por base pressupostos teóricos a testar (com base na perspetiva dos envolvidos), decidiu-se adaptar, no domínio das ciências sociais e da estratégia de investigação de estudos de caso, o método de investigação *estudo de caso*, de cariz exploratório, de acordo com as linhas orientadoras de Yin (2009), para o desenho de um *estudo de caso*.

4.4 Conceção e implementação do *Estudo de Caso*

O *estudo de caso* é uma ferramenta poderosa para investigação em SI, com validade científica, desde que corretamente entendida e utilizada, e quando teoricamente bem sustentado e desenhado o projeto de investigação (Caldeira & Romão, 2002). Existem várias questões práticas que têm impacto sobre o desenho e âmbito de um projeto de *estudo de caso*, nomeadamente o propósito de realização do estudo, os recursos disponíveis, e os resultados necessários ou esperados (Darke et al., 1998). Os autores distinguem a realização de um *estudo de caso* no âmbito dos requisitos de pesquisa de um doutoramento ou mestrado, com recursos e tempo limitados, de outras situações, realizadas à medida dos interesses específicos de organizações que patrocinam o estudo, em que o número de investigadores, o financiamento disponível e as expetativas das organizações financiadoras e outras partes interessadas, vão afetar o alcance das questões a serem abordadas, a profundidade e a extensão das atividades de recolha de dados, bem como a natureza do produto final.

De acordo com a opinião de Darke et al. (1998) a conceção, definição e âmbito de um projeto de *estudo de caso* exige uma análise exaustiva da literatura a fim de

compreender o estado atual da investigação na área de pesquisa, e para posicionar a questão de estudo dentro do contexto da literatura existente. Isto fornece uma base importante ao desenvolvimento cuidadoso da estrutura e âmbito do projeto de pesquisa, de modo a que possa ser determinada a unidade de estudo e o número de casos apropriados.

A informação recolhida e processada através da revisão bibliográfica confirmou a intenção inicial de utilizar o método *estudo de caso*. Essencialmente por duas razões:

a. Esta evidenciou a falta de conhecimento científico sobre as questões da privacidade dos dados, tanto em contextos em que os SI estão limitados às fronteiras da organização, como em contextos de partilha de dados com outros SI, nomeadamente através de processos estruturados para os quais a interoperabilidade é um requisito essencial.
b. Resultado da consulta dos vários relatórios de instituições nacionais e internacionais reguladoras com responsabilidade sobre o desenvolvimento a nível global da privacidade e da proteção de dados (veja-se, por exemplo, (ICO, 2008), (ENISA, 2011) e (CNPD, 2004)), verificou-se que a realidade no interior das organizações é muito preocupante, caracterizada em primeiro lugar pela ausência de profissionais especializados em privacidade dos dados, e em segundo pelo facto de esta questão não assumir a prioridade necessária. Estas duas situações contribuem ambas, na maioria das situações, a uma atitude puramente reativa por parte dos seus responsáveis em relação aos problemas associados à privacidade e à proteção de dados. A par da questão em estudo, é também importante compreender o porquê desta situação.

Da revisão bibliográfica, neste caso direcionada para a privacidade dos dados, surge um modelo inicial, teoricamente fundamentado e descrito no capítulo III, e que foi decisivo no alinhamento daquilo que se pretende estudar, aquilo que se pretende validar. Em simultâneo, foi necessário melhorar o conhecimento inicial sobre o método *estudo de caso* (suficiente na fase inicial do processo de investigação), conhecer com detalhe a sua estrutura e requisitos de sucesso, os seus maiores problemas, assim como projetos de investigação, artigos de opinião e científicos sobre a operacionalização de um *estudo de caso*.

Ao invés de vários estudos que consideram o método *estudo de caso* apenas na fase exploratória, no suporte a outra estratégia de pesquisa, o método *estudo de caso* não

foi apenas utilizado como uma tática para a recolha de dados, nem meramente uma característica do planeamento em si, mas sim como uma estratégia de pesquisa abrangente, no suporte à globalidade do estudo. Tendo presente aquilo que deve ser um *estudo de caso*, os seus principais instrumentos, as etapas que deve compreender, aquilo que é o propósito deste estudo e os recursos disponíveis, a conceção e desenvolvimento do *estudo de caso* decorreu de acordo com o processo de investigação representado na Figura 13.

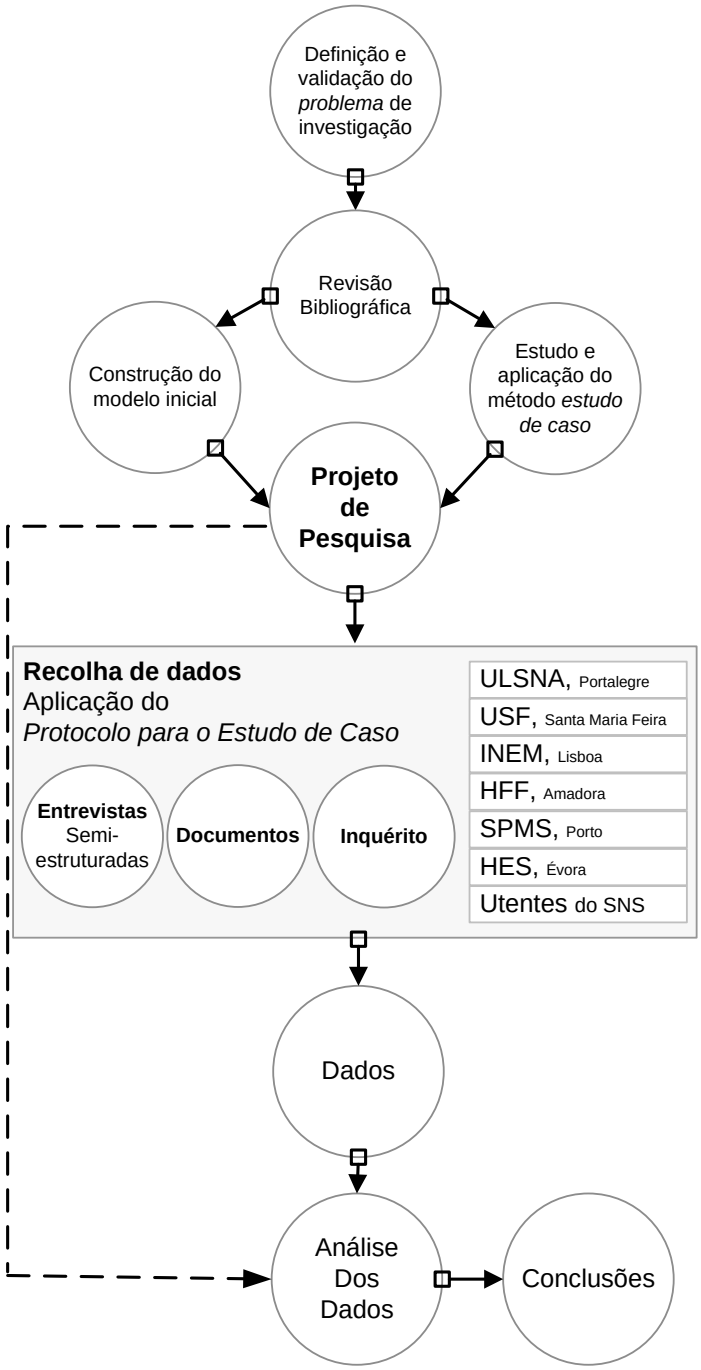

Figura 13 - Processo de investigação

O projeto de pesquisa constitui o instrumento principal, que transporta todos os conceitos teóricos desenvolvidos para a aplicação prática através do *estudo de casos*. Trata-se de um instrumento exigente, para o qual foi necessária uma grande dedicação, com o objetivo de se obter um instrumento credível, integrado e otimizado. Os componentes do projeto de pesquisa são apresentados no ponto seguinte, e sempre que necessário fundamentadas as opções tomadas no seu desenvolvimento.

A consulta de Yin (2009) foi fundamental na conceção do *estudo de caso*, naquilo que diz respeito à definição e implementação da estratégia do *estudo de caso*.

4.4.1 Projeto de pesquisa

A decisão de utilizar o método *estudo de caso* como uma estratégia de pesquisa abrangente, no suporte à globalidade do estudo, é conseguida através do desenvolvimento de um dos componentes mais importantes deste método – o *projeto de pesquisa* – o qual deve ser desenvolvido na etapa 1 de um projeto de *estudo de caso* (veja-se a Figura 12, na página 133). Este orienta o investigador durante o processo de desenho, recolha, análise e interpretação dos dados (Yin, 2009). É na opinião deste autor um modelo lógico de provas que permitem ao investigador fazer inferências relativas às relações causais entre as variáveis sob investigação. É um plano de ação, um esquema de pesquisa, em que são especialmente importantes a definição dos seguintes componentes: (1) a questão de estudo; (2) as suas proposições; (3) a(s) unidade(s) de estudo; (4) a lógica que une os dados às proposições; e (5) os critérios de interpretação dos dados recolhidos.

Projetar e desenhar um projeto de pesquisa de um *estudo de caso*, a fim de garantir para a questão de estudo (ou questões) uma resposta apropriada e adequada, pode ser difícil, em que a recolha de dados para o estudo pode ser demorada e tediosa, e muitas vezes resulta na acumulação de grandes quantidades de dados (Yin, 2009; Cavaye, 1996; Darke et al., 1998). Um *estudo de caso*, desde que devidamente desenhado e executado, é uma estratégia de investigação que permite captar de uma forma poderosa os mais diferentes aspetos inerentes à complexa realidade social que envolve as organizações e os respetivos SI (Caldeira & Romão, 2002).

Antes de se iniciar o trabalho de campo numa unidade de análise, é essencial que se chegue a um acordo com a organização participante sobre: (1) os requisitos de confidencialidade relativos aos dados e aos resultados do estudo de caso, (2) as limitações sobre a divulgação da identidade dos participantes; e (3) as restrições e direitos de publicação da investigação em causa (Darke et al., 1998).

4.4.1.1 Questão de estudo

Na identificação da questão de estudo a ser abordada através da utilização do método de *estudo de caso*, é importante assegurar que a questão é adequada em termos do seu interesse, importância e valor, tanto para o investigador como para a comunidade de profissionais de SI (Darke et al., 1998).

A questão de estudo deve apresentar de forma clara e precisa a questão ou problema a ser resolvido, de forma a não poder haver ambiguidade sobre o que está a ser realizado (Iqbal, 2007). É fundamental para se estabelecer a estratégia de pesquisa mais relevante a ser utilizada, devendo ser formulada e validada antes da escolha da unidade de estudo, ou seja, não deve ser associada nem estar dependente da unidade de estudo (Yin, 2009). Se a área de pesquisa for particularmente relevante para uma organização e se a questão de estudo for aquela que a organização precisa ou quer dirigir, então é mais provável que esta ceda o acesso aos seus recursos e às suas pessoas (Darke et al., 1998). De acordo com estes autores, é importante que os resultados da investigação sejam claros para a organização, assim como os benefícios que vai ter.

Definir a questão de estudo é para Yin (2009), provavelmente, o passo mais importante no desenvolvimento de um projeto de pesquisa, sendo necessário paciência e tempo suficiente para a realização desta tarefa. A forma de uma questão fornece uma chave importante para se traçar uma estratégia de pesquisa que será utilizada, afirma o autor.

Neste sentido a questão de estudo deve permitir identificar e compreender:

> "*Quais os fatores críticos à privacidade dos dados em ambientes heterogéneos de interoperabilidade entre sistemas sociotécnicos e como estes fatores podem ser alinhados com os vários níveis e atributos de interoperabilidade do modelo OIM?*".

Apesar de extensa, a compreensão da questão de estudo fica facilitada com a sua apresentação em duas partes:

a. A primeira parte centrada na identificação de "*quais os fatores críticos à privacidade dos dados em ambientes heterogéneos de interoperabilidade entre sistemas sociotécnicos [...]*", destina-se a identificar quais os subdomínios dentro dos SI que é necessário considerar no desenho de uma solução de proteção da privacidade dos dados, quando estes são partilhados entre organizações. O tipo de questão "*quais os ...*", é na realidade mais uma questão do tipo "*o que ...*", para melhor entendermos a estratégia de investigação a seguir.
b. A segunda parte da questão de estudo *"[...] e como estes fatores podem ser alinhados com os vários níveis e atributos de interoperabilidade do modelo OIM?"*, tem por objetivo compreender as características dos fatores identificados por forma a que possam ser alinhados com os atributos e os níveis de interoperabilidade. Ou seja, compreender quais os requisitos de proteção da privacidade dos dados em cada nível de interoperabilidade, e desta forma permitir às organizações uma maior agilidade na implementação dos meios de colaboração necessários ao seu desenvolvimento.

4.4.1.2 Proposições do estudo

A questão de estudo pressupõe a existência de vários fatores críticos à privacidade dos dados, com grande influência sobre o sucesso das medidas de proteção da privacidade dos dados em contextos de partilha de dados. O resultado do segundo momento de revisão bibliográfica, que deu origem ao Capítulo III, permitiu a definição dos dez subdomínios que entendemos serem decisivos para o desenvolvimento de um ambiente de partilha de dados entre organizações, capaz de assegurar ao máximo a privacidade dos dados (ver modelo inicial, representado na Figura 13, na página 136).

Yin (2009) sugere a formulação de proposições, através das quais o investigador consegue focar-se nos aspetos a serem estudados dentro da questão de estudo. Estas vão permitir refletir sobre as questões teóricas e identificar onde devemos procurar evidências relevantes. Constituem conclusões que podem ser deduzidas da teoria

(Shanks & Parr, 2001). Permitem que o investigador, ao formular proposições, siga na direção certa. Sem as proposições o investigador pode ficar tentado a recolher "tudo", algo absolutamente impossível de fazer, afirma Yin (2009). É opinião deste autor que quanto mais proposições específicas apresentar um estudo, mais ele vai permanecer dentro dos limites exequíveis.

Neste sentido, a base teórica de cada um dos dez subdomínios, apresentados no Capítulo III, deu origem à formulação de uma proposição, ou seja, cada proposição representa um dos subdomínios, uma área de influência sobre a privacidade dos dados em contextos de interoperabilidade que é necessário estudar. De salientar que uma proposição não constitui em si um fator crítico. Apresenta sim, vários fatores críticos. Por forma a facilitar a identificação e o enquadramento individual de cada proposição, decidiu-se atribuir a cada proposição uma identificação (ID), que permite identificar e enquadrar cada proposição, e constitui apenas um termo unificador, capaz de representar os fatores identificados dentro de um subdomínio em estudo. No ponto 3.2 do capítulo III foi apresentado o processo desenvolvido que levou a encontrar a terminologia atribuída a cada proposição. As dez proposições (P1, P2, …, P10) apresentadas na Tabela 12 representam assim a especificidade dos subdomínios que se pretende estudar. Os dados a recolher vão permitir validar ou não estas proposições, e permitir compreender se são determinantes para a privacidade dos dados, assim como, qual a sua potencialidade em termos de interoperabilidade.

Na definição e fundamentação das proposições, constatou-se que cada proposição atua de uma forma nitidamente diferente sobre a privacidade dos dados, assim como sobre as outras proposições. Surgiu assim necessidade de dispor de uma ferramenta capaz de representar esta realidade, e que complementasse a compreensão das proposições em estudo. A opção passou pelo desenvolvimento de uma *framework* conceptual. O seu desenvolvimento, em conjunto com a questão de investigação, é a melhor defesa contra sobrecargas no processo de investigação, defendem Miles & Huberman (1994).

Tabela 12 - Proposições do *estudo de caso*

Proposições
ID e descrição da proposição
P1. "Experiência" Num contexto de interoperabilidade, a experiência e a compreensão coletiva das questões da interoperabilidade e da proteção e privacidade são essenciais ao planeamento conjunto de medidas transversais e eficazes para a proteção da privacidade.
P2. *"Cultura de privacidade"* A implementação eficaz das soluções tecnológicas e das políticas de privacidade está dependente do compromisso das organizações no desenvolvimento das melhores práticas de gestão da informação que respeitem a privacidade. Este contexto só é alcançável quando a privacidade constituir uma parte integrante da cultura organizacional.
P3. "Segurança e infraestruturas" A colaboração e a interoperabilidade técnica entre as várias soluções de segurança e infraestruturas de armazenamento de dados são essenciais ao suporte e à viabilidade das medidas adotadas nos níveis superiores de proteção e privacidade dos dados.
P4. *"Linguagem de privacidade* (*taxonomia*) " A existência de uma linguagem comum nos domínios da proteção e da privacidade é essencial à definição clara e inequívoca das questões associadas à privacidade dos dados, e ao esforço comum no compromisso para a sua preservação.
P5. *"Accountability - responsabilidade e conformidade"* Um programa continuado de análise de conformidade, de monitorização dos controlos de proteção e privacidade, assim como a disponibilização de provas de evidência sobre quebras detetadas, são ferramentas essenciais à proteção da privacidade num ambiente de colaboração.
P6. "Dados e manipulação de dados" A privacidade dos dados está dependente do conhecimento desenvolvido pelas instituições sobre os dados que utiliza e da transparência e qualidade dos processos de tratamento em todo o seu ciclo de vida num ambiente de interoperabilidade.
P7. "Estratégia para a privacidade" Num ambiente de colaboração com outras organizações, impõe-se a existência de estratégias individuais, e a sua harmonização, para a privacidade como um todo e em particular para a proteção e privacidade dos dados.
P8. "Confiança e gestão da confiança" É essencial à privacidade dos dados a confiança entre as organizações participantes, como pilar fundamental à colaboração num ambiente de interoperabilidade.
P9. *"Ética e cooperação humana"* No domínio da ética, a iniciativa (atitude), confiança e conhecimento por parte do titular dos dados do novo contexto de utilização dos seus dados pessoais, assim como a atitude face à mudança por parte dos profissionais, podem comprometer os objetivos para a colaboração, e consequentemente o sucesso das medidas para proteção da privacidade dos dados.
P10. "Estrutura organizativa" O compromisso para com os valores e objetivos subjacentes à colaboração sob a forma de interoperabilidade organizacional é essencial para minimizar possíveis impactos sobre a privacidade que derivam de culturas e estruturas organizativas diferentes.

A *framework* conceptual apresentada na Figura 14 representa a conceção inicial, que resulta da revisão bibliográfica, sobre a importância e a relação de influência das dez proposições formuladas sobre a privacidade dos dados em contextos de interoperabilidade, assim como a relação entre estas. A análise dos dados permitirá adaptar a importância atribuída a cada proposição (expressa no tamanho do quadrado), a sua relação de influência direta ou indireta sobre a privacidade dos dados (expressa na maior ou menor distância do centro da *framework* conceptual), ou apenas a sua relação com as outras proposições. Com base nos resultados finais do *estudo de caso*, a *framework* terá de ser adaptada posteriormente.

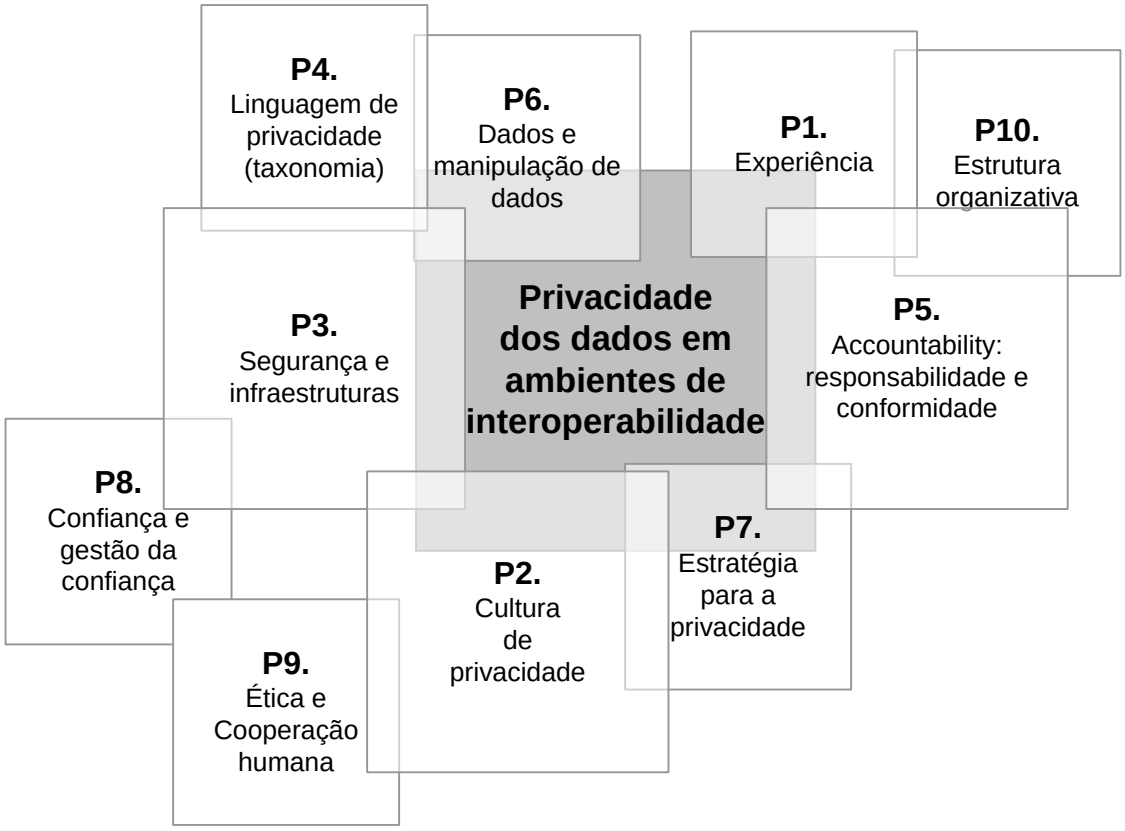

Figura 14 - *Framework* conceptual, versão inicial

4.4.1.3 Estratégia e método utilizado para a análise dos dados

A análise dos dados de um *estudo de caso* é um dos aspetos menos explorados e mais complicados na realização de estudos de caso, pois as estratégias e as técnicas não foram muito bem definidas no passado (Yin, 2009). Este problema agrava-se quando o investigador inicia a recolha de dados, sem ter uma ideia clara de como as evidências recolhidas vão e devem ser analisadas. O investigador deve no início da definição do *estudo de caso*, optar por uma estratégia analítica geral, que lhe permita

estabelecer prioridades sobre o que deve ser analisado e o porquê, e desta forma escolher entre as diferentes técnicas e concluir, com sucesso, a fase analítica da pesquisa. O objetivo é proceder ao tratamento dos dados de forma correta e justa, produzir conclusões analíticas irrefutáveis e eliminar interpretações alternativas.

Neste sentido, Yin (2009) propõe que o investigador siga uma de duas estratégias gerais: (1) seguir as proposições teóricas que levaram ao estudo de caso, ou (2) na ausência destas, desenvolver uma estrutura descritiva do caso a fim de organizar o *estudo de caso*. Após esta decisão é possível optar por uma das quatro técnicas analíticas específicas, também definidas por este autor como *métodos principais de análise*, aplicáveis a estudos de caso único: adequação ao padrão, construção de explanação, análise de séries temporais, e modelos lógicos de programa.

A *construção de uma explanação* (ideal para explicar um fenómeno), a *análise de séries temporais* (ideal para a analise de questões do tipo "como" e "porquê" sobre a relação de um evento ao longo do tempo), e os *modelos lógicos de programa* (estabelece um encadeamento complexo de eventos (padrão) ao longo do tempo (série temporal)), foram opções descartadas uma vez que não viabilizavam os objetivos deste estudo.

A interpretação dos dados recolhidos será assim realizada tendo em vista as proposições iniciais, com base na adequação ao padrão como método de análise principal, como representado na Figura 15. Se os *valores* inicialmente previstos para cada resultado forem encontrados e, ao mesmo tempo, não se encontrarem padrões alternativos, podem-se fazer fortes inferências causais (Yin, 2009).

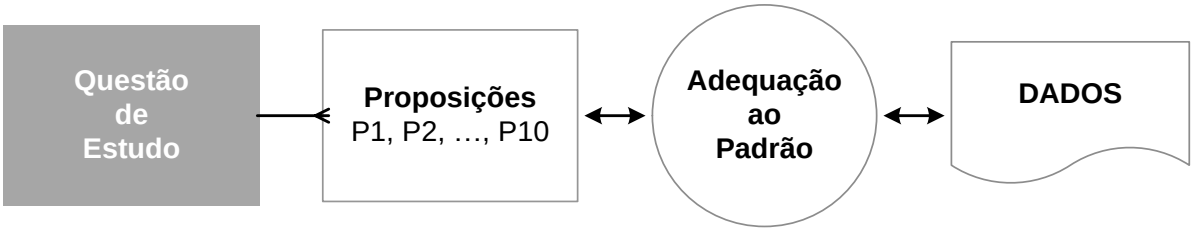

Figura 15 - Lógica que une os dados às proposições

4.4.1.4 Proposições e variáveis dependentes do estudo

Ao contrário de *estudos de caso* de cariz descritivo, em que o padrão previsto de variáveis específicas é obrigatoriamente definido antes da recolha dos dados, para *estudos de caso* exploratórios, como é este caso, os padrões podem estar relacionados

com as variáveis dependentes ou independentes do estudo (Yin, 2009). De acordo com este autor, para a estratégia geral baseada em proposições, e a adequação ao padrão como técnica de análise específica, o investigador pode estruturar o estudo utilizando: (1) variáveis dependentes não equivalentes tidas como padrão, (2) explanações concorrentes como padrão – variáveis independentes; e (3) padrões mais simples.

Através do tipo de adequação ao padrão - *variáveis dependentes não equivalentes tidas como padrão* - uma experiência, ou uma pesquisa quase-experimental pode apresentar inúmeras variáveis dependentes – ou seja, uma variedade de resultados. Para cada proposição do estudo, podem assim existir um conjunto de variáveis dependentes diferentes, podendo cada uma ser avaliada com base em valores e instrumentos diferentes. Para cada variável dependente é previsto um padrão geral de resultados. Se a análise dos dados recolhidos confirmar o padrão previsto, podem-se inferir conclusões sólidas para a variável em causa, e por influência para a proposição. Por outro lado, se os resultados não atingirem o padrão previamente estabelecido – basta uma variável do conjunto de variáveis não apresentar os valores padrão previstos – a proposição inicial terá de ser questionada (Yin, 2009).

Tanto as *explanações concorrentes como padrão*, como a *construção de padrões mais simples* não foram consideradas como opção para o tipo de estudo em desenvolvimento. No primeiro caso, porque é exigível o desenvolvimento de proposições teóricas concorrentes, em que cada proposição teórica concorrente envolve um padrão de variáveis independentes que é mutuamente excluída: se uma explanação for válida a outra não o pode ser. No segundo caso, pressupõe a existência de padrões com um número mínimo de variáveis dependentes ou independentes, o que limitaria as conclusões do estudo.

Independentemente da estratégia analítica específica escolhida, Yin (2009) salienta como fundamental a existência de uma análise qualitativa de qualidade, em que o investigador deve basear a sua análise em todas as evidências relevantes, abranger todas as principais interpretações concorrentes, dedicar-se aos aspetos mais significativos do *estudo de caso*, e desenvolver um conhecimento prévio especializado sobre as questões de estudo.

Atendendo à opção da técnica específica de adequação ao padrão para análise dos dados obtidos, optámos neste estudo por analisar este padrão recorrendo à

decomposição de cada proposição em proposições mais específicas, denominadas de *variáveis dependentes não equivalentes tidas como padrão* (Yin, 2009). Esta decomposição da proposição em proposições mais específicas, permite clarificar "o que se pretende conhecer" e o "motivo da recolha de informação". Tal como as proposições, as variáveis dependentes refletem a pesquisa realizada e que resultou na apresentação dos dez subdomínios a estudar. Se a proposição constitui um pressuposto que procura abranger todo um subdomínio, as variáveis dependentes surgem como pressupostos mais específicos, mais focados. O resumo que consta no final da apresentação teórica de cada um dos dez subdomínios, apresentados no Capitulo III, apresenta algumas afirmações que posteriormente dão origem às variáveis dependentes associadas a cada proposição.

A definição e associação de uma variável dependente a uma proposição, impunha que fossem definidos um ou mais itens de ligação com o processo de recolha de dados, neste caso, também definidas como fontes de evidências. Assim, cada variável dependente pode apresentar várias fontes de informação ou de evidências. Deste modo, os dados ficam ligados às proposições através das variáveis dependentes, como demonstrado na Figura 16. Se os dados recolhidos, em todos os itens de uma variável dependente estiverem de acordo com o planeado, pode-se inferir uma conclusão sólida sobre esta variável dependente, caso contrário, a variável dependente terá de ser questionada. A análise do conjunto das variáveis dependentes, por seu lado, valida ou não a proposição.

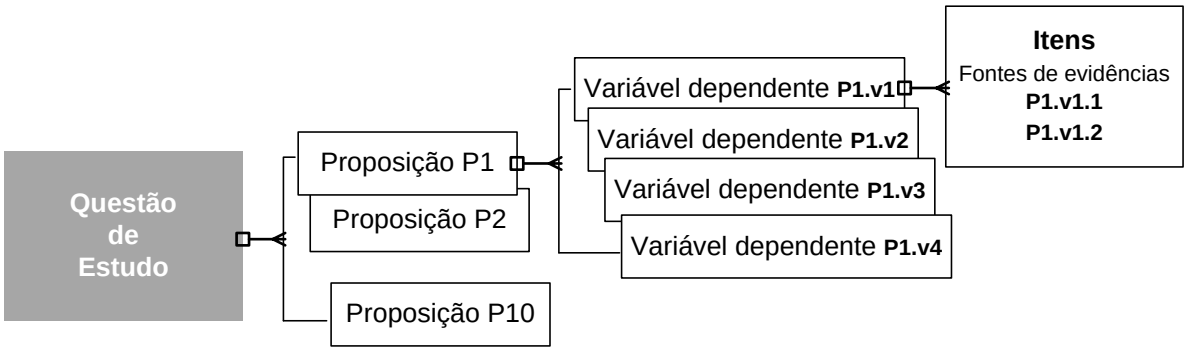

Figura 16 - Ligação entre a questão de estudo, as suas proposições e as fontes de informação

Como fontes de informação ou evidências, foram considerados tanto dados qualitativos como quantitativos, recolhidos através dos seguintes meios:

1. Realização de entrevistas semiestruturadas aos vários profissionais ligados às questões da privacidade dos dados;

2. Recolha de diferentes tipos de documentos, como por exemplo: (a) documentos que descrevam o objetivo da recolha de dados nos vários processos; (b) políticas de privacidade; (b) políticas de segurança; (d) *newsletter*, *espaços web*, jornais, e outros meios de comunicação, onde o tema privacidade tenha sido abordado e promovido; (e) documentos de análise do risco no domínio da segurança; e (f) qualquer outro documento relacionado com a proteção de dados que seja relevante para o estudo desta temática;
3. Recolha de dados quantitativos através da realização de um inquérito.

A estrutura de cada proposição, nomeadamente as suas variáveis dependentes, a sua caracterização e justificação, assim como os itens de ligação com as fontes de evidência, são apresentados nas tabelas seguintes. Com base nestas tabelas será posteriormente elaborado o *protocolo para o estudo de caso*, que entre outros elementos contem o guião para as entrevistas semiestruturadas.

A Tabela 13 apresenta a estrutura da proposição *P1. Experiência*, constituída por quatro variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.1, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 13 - Estrutura e ligação da proposição P1 com as fontes de evidência

P1. "Experiência"	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P1.v1. É fundamental uma experiência em partilha de dados, em interoperabilidade, em projetos internos do próprio sistema de informação e em projetos de colaboração com outras organizações. *[1] Identificar situações/projetos de partilha de dados, de interoperabilidade (locais ou com outras organizações) em que a organização em estudo participou. Perceber qual a importância atribuída às questões da interoperabilidade, e se estrategicamente é uma aposta de futuro. Identificar projetos futuros de interoperabilidade.* [2] Perceber se o fator "experiência em interoperabilidade" é importante à privacidade dos dados, e se a ausência de experiência constitui uma barreira à sua proteção.	**P1.v1.1** Podemos afirmar que o sucesso do planeamento de políticas de proteção e privacidade de dados está muito dependente da experiência em projetos de partilha de dados e em interoperabilidade? Pode indicar alguns exemplos de projetos na sua organização?
P1.v2. A experiência em questões de privacidade, em proteção de dados, no seu enquadramento legislativo (nacional e internacional), em avaliações do impacto sobre a privacidade, ao nível dos	**P1.v2.1** Se nos focarmos no objetivo de desenvolver um ambiente seguro e confiável para a partilha de dados, que experiência é exigível aos responsáveis pelo desenvolvimento dos sistemas de informação?

P1. "Experiência"	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
sistemas locais, permitem uma colaboração mais produtiva com outras organizações no desenvolvimento de um ambiente seguro de partilha de dados. *[1] Compreender se o conhecimento nos domínios da privacidade, da proteção de dados, é um facilitador para a abordagem da privacidade dos dados num contexto de colaboração com outros sistemas. Identificar práticas de proteção de dados, tanto em projetos locais como em projetos de partilha de informação com outras organizações, mesmo que com total ausência de interoperabilidade.* [2] Perceber se a experiência em privacidade e proteção de dados é importante quando a organização implementa interfaces para partilha de informação ou serviços com outras organizações.	**P1.v2.2** Qual o resultado expectável de uma melhoria do conhecimento da legislação de proteção e privacidade dos dados? **P1.v2.3** [docs] – recolher documentos focados na proteção de dados de um processo ou de um sistema. **P1.v2.4** [docs] – verificar se a legislação é referida nas políticas de privacidade publicadas. Confirma a importância atribuída à legislação.
P1.v3. É essencial a existência de profissionais especializados em proteção e privacidade, a cooperação entre estes, e de um órgão de supervisão para o contexto da colaboração, para garantir que as políticas de privacidade são atendidas por todos. *[1] Analisar se é essencial à experiência global da organização, a existência de profissionais permanentes especializados em proteção e privacidade dos dados, e neste sentido, mais bem preparados para os desafios que surgem das exigências da interoperabilidade organizacional* [2] Verificar se a existência de profissionais com competências em proteção e privacidade de dados é importante ao desenvolvimento de programas integrados de proteção e privacidade dos dados. Compreender que profissionais devem incorporar competências em proteção e privacidade dos dados.	**P1.v3.1.**Quais os recursos humanos que considera fundamentais ao suporte das questões da privacidade dos dados para o âmbito alargado do contexto de colaboração com outras organizações? Justifica-se uma estrutura organizativa de suporte às questões da privacidade dos dados para o âmbito alargado do contexto de colaboração?
P1.v4. Eventos como programas periódicos de educação, formação e sensibilização entre os profissionais da organização, participação em *workshops*, seminários nacionais ou internacionais, no domínio da privacidade e proteção de dados, são importantes para uma melhor experiência e preparação coletiva. *[1] Analisar a formação disponibilizada nas organizações que melhore a sua preparação em questões associadas à proteção e privacidade de dados. Qual a regularidade destas ações. Qual o grau de adesão.* [2] É importante perceber qual o contributo de ações de formação ou sensibilização para a formação de uma consciência coletiva da problemática da privacidade de dados.	**P1.v4.1** Que tipo(s) de eventos pode(m) contribuir para uma melhoria da preparação da globalidade dos profissionais em relação à privacidade dos dados? **P1.v4.2** [docs] Podem ser analisadas *newsletters*, espaços *web*, jornais, e outros meios de comunicação, onde este tema tenha sido abordado.

A Tabela 14 apresenta a estrutura da proposição *P2. Cultura de privacidade*, constituída por três variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.2, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 14 - Estrutura e ligação da proposição P2 com as fontes de evidência

P2.*"Cultura de privacidade"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P2.v1. A existência de uma cultura de privacidade é sinónimo de uma melhor preparação organizacional para agir em situações/contextos de privacidade. A privacidade dos dados ao ser reconhecida como um *valor*, é integrada nas práticas de uma organização e considerada durante todo o ciclo de vida de um sistema. *[1] Analisar a relação e dependência da privacidade dos dados com uma cultura de privacidade em toda a organização, assim como a necessidade de esta ser reconhecida como um valor para que seja considerada no desenvolvimento de um sistema (privacy by design).* [2] Validar a proposição P2 em relação à necessidade de que as questões da privacidade dos dados sejam parte integrante de uma cultura de privacidade em toda a organização.	**P2.v1.1** Muitas organizações utilizam o termo "cultura", quando de alguma forma querem evidenciar *valores* importantes para o seu sucesso. Por exemplo: "cultura da qualidade", "cultura de segurança", "cultura empreendedora". De que forma o sucesso da partilha de dados pode ser influenciado pelo desenvolvimento de uma cultura de privacidade transversal a todas as organizações?
P2.v2. Uma cultura de privacidade é fundamental (1) à identificação e definição de *situações* de privacidade dentro de uma *zona* maior de privacidade, (2) à sua justificação e (3) à sua posterior implementação e gestão, assim como à previsão de exceções às políticas de privacidade desenvolvidas. *[1] Compreender se uma cultura em privacidade é fundamental para que os profissionais saibam identificar e planear o funcionamento de uma situação de privacidade, assim como serem capazes de interligar[60] (interoperabilidade organizacional) uma situação com uma similar em outras organizações.* [2] Validar a relação dos vários profissionais em relação à proposição P2, como condição para lidarem com contextos de informação sensível.	**P2.v2.1** *Existem nas organizações várias situações (contextos) de privacidade, justificadas e geridas muitas vezes de formas diferenciadas.* Qual a importância de uma cultura de privacidade para que uma organização consiga lidar com as várias situações de privacidade que identificou?
P2.v3. Uma cultura de privacidade é essencial à	**P2.v3.1** A maioria dos profissionais consegue

[60] Podem existir situações similares de privacidade em várias organizações, já identificadas (ou não), mas a funcionar com políticas de privacidade díspares (ou sem qualquer política de privacidade). O desafio passa por integrar estas regras de funcionamento para o contexto de interoperabilidade. Aqui tem um papel decisivo o órgão de supervisão para o contexto da colaboração em questões de privacidade dos dados.

P2.*"Cultura de privacidade"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
distinção dos vários tipos de privacidade, e no domínio da privacidade dos dados compreender as diferenças e dependências em relação à proteção de dados e à segurança dos dados. *[1] Normalmente a privacidade dos dados é confundida com segurança e proteção de dados. Importa perceber se organizações com uma cultura forte em privacidade distinguem e identificam com facilidade estes três contextos e a sua interdependência.* [2] Validar a proposição P2 em relação à definição e distinção do conceito de privacidade dos dados, dos conceitos proteção de dados e segurança de dados.	distinguir os vários tipos de privacidade com que é confrontado diariamente? De que forma a compreensão e distinção da privacidade dos dados, face aos outros tipos de privacidade, dependem de uma maior cultura de privacidade? **P2.v3.2** Por outro lado, a distinção entre privacidade, proteção e segurança dos dados está também dependente de uma cultura de privacidade, ou apenas do conhecimento das questões técnicas associadas?

A Tabela 15 apresenta a estrutura da proposição *P3. Segurança e infraestruturas*, constituída por cinco variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.3, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 15 - Estrutura e ligação da proposição P3 com as fontes de evidência

P3.*"Segurança e infraestruturas"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P3.v1. A segurança de infraestruturas locais e de comunicação, a sua interoperabilidade técnica e não-técnica (*a "padronização das melhores práticas de segurança" específicas de cada sistema são essenciais ao desenvolvimento de uma plataforma segura e de confiança*), são preponderantes para camadas superiores de segurança, nomeadamente a privacidade dos dados. *[1] Compreender se os profissionais identificam a relação de dependência da privacidade dos dados em relação às questões da segurança para o contexto de colaboração. Analisar qual o contributo e importância da interoperabilidade organizacional a este nível.* [2] Validar a proposição P3 em relação à interoperabilidade técnica e não técnica entre infraestruturas.	**P3.v1.1** Quais as maiores preocupações enfrentadas pelas organizações pelo facto de que, cada vez mais, as organizações funcionam e dependem do funcionamento em rede (integradas ou em colaboração com outras organizações)? **P3.v1.2** É possível e desejável uma interoperabilidade organizacional que suporte a partilha de experiência ao nível da segurança de infraestruturas e promova uma padronização das melhores práticas de segurança? Que efeitos práticos pode apresentar esta partilha de experiência? **P3.v1.3** [docs] – recolha e análise de documentos com as políticas de segurança existentes com o objetivo de compreender as medidas relacionadas com a privacidade de dados. **P3.v1.4** [docs] – recolha e análise de documentos com as políticas de segurança existentes com o objetivo de identificar pontos comuns interoperáveis.
P3.v2. Uma análise de risco em segurança e uma	**P3.v2.1** Os procedimentos ou políticas de

P3.*"Segurança e infraestruturas"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
análise do impacto sobre a privacidade, que englobem todos os equipamentos e situações de recolha, armazenamento, utilização e partilha de dados, são dois instrumentos decisivos para o enquadramento e conhecimento das situações problemáticas para a privacidade dos dados. *[1] Compreender se para os responsáveis pelos sistemas de informação a existência de análise de risco é uma ferramenta imprescindível e ponto de partida para o desenvolvimento de medidas que permitam corrigir os riscos identificados.* [2] Validar a proposição P3 em relação à dependência de um programa de segurança que tenha na sua origem uma análise de risco.	segurança existentes têm por base uma análise prévia do risco em segurança, dos sistemas e das tecnologias de informação? *Se sim*, quais as vantagens ou contributos para a definição das políticas de segurança? *Se não*, qual foi a base para a definição das políticas de segurança implementadas? **P3.v2.2** [docs] – recolha e análise de documentos relacionados com a análise de risco no domínio da segurança, caso esta análise tenha sido realizada.
P3.v3. No domínio da segurança e infraestruturas, a identidade digital, os sistemas de gestão de identidade, e a confiança (federação) e interoperabilidade entre estes sistemas, são um componente essencial à gestão e monitorização da confidencialidade e privacidade dos dados. *[1] É unânime que a identidade digital é fundamental ao controlo da exposição de dados pessoais e é um fator decisivo para a privacidade de dados em contextos de interoperabilidade. É contudo necessário verificar como estes sistemas devem evoluir para cumprir eficientemente com este requisito.* [2] Validar a proposição P3 em relação aos conceitos de gestão da identidade e federação de sistemas, assim como a sua influência sobre a proposição P5.	**P3.v3.1** A identidade digital e os sistemas tecnológicos para a sua gestão constituem um dos elementos de suporte ao funcionamento e à evolução do ambiente de colaboração e partilha de dados. Qual a evolução desejável para estes sistemas tecnológicos face aos desafios do ambiente de colaboração com outras organizações?
P3.v4. A segurança em cenários de exposição de dados a ambientes vulneráveis de "não-produção"[61] é essencial para a preservação da sua privacidade. Os requisitos de privacidade dos dados nestes contextos devem cumprir com os requisitos legais. *[1] Determinar se ambientes de não-produção, ou seja, processos ou tarefas que estão fora do âmbito e objetivo principal para a recolha de dados, não constituem lacunas no que diz respeito à privacidade dos dados.* [2] Validar a proposição P3 em relação à necessidade de medidas de segurança de preservação da privacidade dos dados quando utilizados para outros objetivos que não os	**P3.v4.1** Os problemas de privacidade dos dados que surgem na sua utilização primária[62] são diferentes da sua utilização secundária[63]? Qual a melhor forma de lidar com a exigência de privacidade nas situações de utilização secundária?

[61] São o caso das equipas de desenvolvimento tecnológico e das equipas de investigação.

[62] Interfaces ou aplicações que colaboram na manutenção de um conjunto de dados sobre um titular dos dados.

[63] Cruzamento com outros dados, utilização dos dados para objetivos secundários, retenção e destruição dos dados.

P3.*"Segurança e infraestruturas"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
inicialmente propostos (principio relativo à qualidade dos dados).	
P3.v5. A existência de um plano de contingência para lidar com os efeitos de eventos não previstos como a perda acidental, destruição ou deterioração de dados pessoais, e tratamentos ilegais e não autorizados, contribui para anular possíveis quebras de privacidades destes dados. *[1] Verificar se a privacidade dos dados é uma das preocupações na base do desenvolvimento de planos de contingência.* [2] Validar a proposição P3 em relação à inclusão da privacidade dos dados no plano de contingência desenhado para o sistema.	**P3.v5.1** É possível elaborar planos de contingência para situações em que há uma violação da proteção de dados pessoais? Que tipo de medidas devem ser definidas?

A Tabela 16 apresenta a estrutura da proposição *P4. Linguagem de privacidade (taxonomia)*, constituída por duas variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.4, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 16 - Estrutura e ligação da proposição P4 com as fontes de evidência

P4.*"Linguagem de privacidade (taxonomia) "*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P4.v1. Uma linguagem ou taxonomia comum de suporte à definição, justificação e gestão de zonas e situações de privacidade constitui um auxiliar importante para analisar de uma forma clara e inequívoca as questões da privacidade, tanto no interior de uma organização como na sua integração com outras organizações. *[1] Sendo a privacidade dos dados de difícil definição, uma taxonomia comum facilitaria o seu desenvolvimento em todas as organizações. Importa perceber qual a sensibilidade dos responsáveis pelas questões da privacidade dentro das organizações em relação à existência desta ferramenta de trabalho – uma framework de suporte ao desenvolvimento de políticas de privacidade.* [2] Validar o contributo da proposição P4 para o desenvolvimento comum de políticas de privacidade dos dados.	**P4.v1.1** *A falta de um vocabulário partilhado para discutir as questões da privacidade faz com que tanto responsáveis de sistemas como gestores executivos, muitas vezes, concordem com especificações para os sistemas que não conseguem lidar com a privacidade de forma satisfatória.* Quais as maiores dificuldades que poderiam ser resolvidas com a existência de uma linguagem de privacidade, uma taxonomia, neste caso focada na privacidade dos dados?

P4.*"Linguagem de privacidade (taxonomia) "*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P4.v2. Uma linguagem comum de privacidade promove uma maior agilidade na definição de políticas de privacidade, no desenvolvimento de mecanismos de controlo de conformidade (P5), e na sua integração com situações similares em outras organizações. *[1] Analisar qual o contributo de uma linguagem comum sobre privacidade para a agilidade organizacional que se pretende para as questões da proteção e privacidade dos dados.* [2] Validar o contributo da proposição P4 para o desenvolvimento comum de políticas de privacidade dos dados.	**P4.v2.1** Para o contexto da colaboração e partilha de dados entre organizações, que benefícios práticos pode apresentar uma taxonomia orientada para as questões da privacidade, utilizada por todos os responsáveis dos sistemas de informação?

A Tabela 17 apresenta a estrutura da proposição *P5. Accountability – responsabilidade e conformidade*, constituída por quatro variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.5, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 17 - Estrutura e ligação da proposição P5 com as fontes de evidência

P5.*"Accountability – responsabilidade e conformidade"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P5.v1. Um programa de responsabilidade sólido e transparente, que contemple medidas adequadas e eficazes para pôr em prática as obrigações e princípios da legislação em vigor sobre proteção de dados, constitui a ferramenta operacional necessária para as questões da privacidade. *[1] Compreender qual a importância atribuída aos programas de responsabilidade. Verificar se estes já se encontram institucionalizados, e nestas situações compreender o seu efeito prático.* [2] Analisar a relação e dependência da proposição P5 em relação ao princípio da responsabilidade e na consequente necessidade de um programa de responsabilidade da organização.	**P5.v1.1** *É cada vez mais exigido às organizações que estas apresentem um programa de responsabilidade em relação à proteção de dados pessoais. Permite identificar perante que entidades devem ter uma atitude de responsabilidade, bem como, o que deve estar na base do desenvolvimento de um programa de responsabilidade.* A elaboração de um programa de responsabilidade, que contemple medidas para pôr em prática as obrigações e princípios da legislação, pode contribuir para a passagem da teoria à prática no domínio da privacidade dos dados? Se sim, quais as partes que devem promover o seu enquadramento e desenvolvimento?
P5.v2. Um programa de conformidade constitui o meio de demonstração da vontade e da capacidade da organização em ser responsável e responsabilizada pelas práticas de gestão de dados. É	**P5.v2.1** *Na segurança informática, é prática regular a análise regular da sua conformidade face às políticas de segurança desenhadas, como garantia da sua eficácia e melhoria contínua.*

P5.*"Accountability – responsabilidade e conformidade"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
essencial à salvaguarda da privacidade de dados, assim como à confiança do titular dos dados na organização, e entre esta e outras organizações. A eficácia e exigência das tarefas de conformidade dependem da sensibilidade dos dados, do volume dos dados processados e dos riscos específicos identificados. *[1] Compreender qual a importância atribuída à necessidade de programas (cultura) de conformidade e verificar se estes já se encontram institucionalizados. Verificar se é possível existir partilha de conhecimento e experiências que permitam o desenvolvimento de um programa de conformidade global para todas as organizações que partilham dados.* [2] Analisar a relação e dependência da proposição P5 em relação ao desenvolvimento de uma cultura de conformidade.	Que ferramenta é necessária para que se possa avaliar, de uma forma contínua, se um determinado contexto de utilização dos dados está de acordo com os requisitos legais e políticas de privacidade existentes? **P5.v2.2** Quais os fatores determinantes para a definição do nível de exigência e periodicidade das tarefas de análise da conformidade em relação à privacidade e proteção dos dados? **P5.v2.3** Considera importante a publicação do resultado destes processos de análise de conformidade? Se sim, porquê e qual na sua opinião pode ser o resultado esperado com a publicação destes resultados?
P5.v3. Os sistemas de *accountability* são essenciais à confidencialidade dos dados, ao disponibilizarem provas de evidência que permitem atribuir responsabilidade a comportamentos não esperados no domínio da privacidade dos dados. *[1] Verificar se os sistemas de registo das tarefas realizadas sobre os dados, quer por utilizadores quer por outros sistemas, e que permitem monitorizar se estas estão de acordo com o perfil de comportamento definido, são uma ferramenta indispensável à privacidade dos dados.* [2] Validar a proposição P5 em relação aos sistemas de *accountability*. Esta proposição permite cruzar resultados com a proposição P3.v3 sobre identidade.	**P5.v3.1** *O registo de todas as tarefas e a sua origem local ou remota são uma das garantias da correta utilização destes dados face às políticas e legislação aplicáveis.* Qual o desempenho ou funções esperadas de um sistema de *accountability* para o contexto de partilha de dados entre sistemas e como se espera que estes evoluam no futuro?
P5.v4. O desenvolvimento de rótulos de qualidade (esquema de certificação) para as medidas adotadas para uma gestão eficiente da conformidade legal, proteção e segurança dos dados, são no futuro uma ferramenta essencial ao desenvolvimento de um ambiente de interoperabilidade confiável e seguro em matérias de privacidade dos dados. *[1] A certificação ou selo de qualidade é vital para o funcionamento dos sistemas de informação, como é o caso da segurança. Importa pois perceber qual a opinião sobre a criação de um selo de qualidade para o domínio global da privacidade e para o domínio específico da privacidade dos dados.* [2] Validar se é importante para a proposição P5 o desenvolvimento de selos de qualidade ou certificação.	**P5.v4.1** *No domínio da segurança de infraestruturas tecnológicas é muito comum os seus responsáveis recorrerem a esquemas de certificação reconhecidos publicamente, como forma de melhoria contínua das soluções implementadas e como garantia de qualidade tecnológica para os seus colaboradores.* Que benefícios pode apresentar a certificação de uma organização em matérias de proteção de dados? A certificação das organizações a este nível aumentaria a confiança entre as organizações participantes no ambiente de partilha de dados como a PDS?

A Tabela 18 apresenta a estrutura da proposição *P6. Dados e manipulação de dados*, constituída por quatro variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.6, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 18 - Estrutura e ligação da proposição P6 com as fontes de evidência

P6.*"Dados e manipulação de dados"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P6.v1. À semelhança da proteção de dados, a privacidade de dados deve ser preocupação constante durante todo o ciclo de vida dos dados em ambientes de interoperabilidade. *[1] A informação recolhida vai permitir esclarecer se a privacidade dos dados deve ser uma preocupação constante em todas as fases do ciclo de vida dos dados, ou se ao contrário, apenas algumas fases são problemáticas e necessitam de atenção especial.* [2] Validar a proposição P6 em relação à necessidade de a privacidade dos dados se apresentar como parte integrante do planeamento do ciclo de vida dos dados (principio *Privacy by Design*).	**P6.v1.1** Estão todas as organizações cientes das limitações relacionadas com a recolha, utilização, partilha e retenção de informação no ambiente de colaboração? **P6.v1.2** Quais são as fases do ciclo de vida dos dados - criação, utilização, *transferência [entre sistemas]*, armazenamento, arquivo e destruição - mais preocupantes em matérias de privacidade que justifiquem medidas adicionais de proteção?
P6.v2. A existência de procedimentos para analisar o tipo e quantidade de dados pessoais recolhidos (a sua adequação e relevância) em relação ao(s) objetivo(s) definido(s), o seu período de retenção (não mais que o necessário), assim como a transparência, clarificação e publicação destes procedimentos são essenciais à compreensão e definição de medidas de proteção da privacidade dos dados. *[1] Confirmar se existem procedimentos institucionalizados focados no estudo dos dados e qual a importância atribuída às questões da privacidade nesta fase.* [2] Validar a proposição P6 em relação à necessidade de procedimentos de análise dos dados, nomeadamente se são adequados, pertinentes e não excessivos face às finalidades para que são recolhidos e para que serão posteriormente tratados (princípio da *qualidade dos dados*).	**P6.v2.1** Concorda que o conhecimento generalizado do objetivo da recolha e tratamento dos dados é o ponto de partida para uma compreensão da necessidade de privacidade dos dados pessoais? **P6.v2.2** [docs] – procurar documentos e analisar a forma de apresentação do objetivo da recolha de dados.
P6.v3. A classificação[64], dinâmica (durante todo o seu ciclo de vida), dos dados é essencial à definição dos níveis de proteção e privacidade pretendidos,	**P6.v3.1** *A identidade digital dos profissionais permite-nos controlar quem, como e de onde se acede aos dados. Contudo, os dados apresentam*

[64] Exemplo - classificação da informação em quatro níveis: pública, atividade normal, sensível, altamente sensível (Jericho Forum, 2009a).

P6.*"Dados e manipulação de dados"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
assim como os domínios onde pode circular, isto é, dentro da organização e entre organizações. Esta *classificação dos dados vai permitir definir os requisitos de proteção associados à informação de forma a restringir a circulação da informação com base nas componentes identidade e legalidade* (Jericho Forum, 2009c). *[1] Analisar se é condição fundamental as políticas de proteção de dados e consequentes políticas de privacidade terem por base uma classificação objetiva de dados.* [2] Validar se a proposição P6 depende de uma classificação dos dados quando relacionada com privacidade dos dados.	*diferentes níveis de exigência quanto à situação de privacidade.* Uma nomenclatura de classificação dos dados permite adaptar melhor as políticas de privacidade dos dados? Quais os principais desafios, no domínio da classificação dos dados, que é necessário considerar quando os dados são partilhados com outras organizações?
P6.v4. A privacidade dos dados depende diretamente (1) do âmbito, (2) das tecnologias aplicadas e (3) dos *standards* usados da/na proteção de dados, implementados localmente e em ambientes de interoperabilidade. Quanto mais granular melhor. Quanto mais interoperáveis melhor. *[1] Compreender se a privacidade dos dados depende do âmbito desenhado e implementado para a proteção de dados, ou seja, a privacidade fica facilitada quando a proteção de dados é especificada individualmente para cada elemento de dados em vez de ser especificada para um conjunto de dados ou uma classe de dados.* [2] Validar a associação e dependência da proposição P6 em relação à proteção de dados, ao seu âmbito e às tecnologias aplicadas a este nível.	**P6.v4.1** *Não faz sentido pensar em políticas de privacidade se estas não tiverem por suporte medidas de proteção dos dados. A privacidade dos dados depende em parte das decisões implementadas ao nível da proteção dos dados.* Para um ambiente de interoperabilidade e colaboração, desenvolvido sobre sistemas heterogéneos, o que é preponderante para otimizar esta dependência (*da privacidade dos dados em relação à proteção dos dados*)?

A Tabela 19 apresenta a estrutura da proposição *P7. Estratégia para a privacidade*, constituída por cinco variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.7, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 19 - Estrutura e ligação da proposição P7 com as fontes de evidência

P7.*"Estratégia para a privacidade"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P7.v1. Uma estratégia para a privacidade está associada ao reconhecimento da privacidade como fator estratégico para a organização, e da sua	**P7.v1.1** Numa linguagem de gestão, qual o fator determinante para que os gestores executivos assumam a necessidade de uma estratégia para a

P7.*"Estratégia para a privacidade"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
responsabilidade sobre este assunto. *[1] O ponto de partida para a existência de uma estratégia para a privacidade está dependente da importância da privacidade para a organização em causa. Neste sentido é importante compreender se o desenvolvimento de uma estratégia para a organização está diretamente associada ao reconhecimento da privacidade como fator estratégico.* [2] Validar a dependência da proposição P7 em relação ao reconhecimento por parte dos gestores executivos da privacidade como fator estratégico e qual o seu papel neste domínio.	privacidade, não isolada, e integrada com a estratégia desenvolvida para o sistema de informação? **P7.v1.2** Qual a importância do reconhecimento por parte dos gestores executivos da responsabilidade da sua organização, ou a sua própria responsabilidade, em relação à proteção da privacidade dos dados e das pessoas?
P7.v2. Uma estratégia para a privacidade constitui uma ferramenta essencial ao planeamento e integração de mecanismos de proteção e controlo da privacidade. *[1] Compreender se a estratégia para a privacidade deve posicionar-se como a base de um programa integrado de proteção e controlo da privacidade, com outros existentes ao nível da segurança e da proteção de dados.* [2] Validar a influência da proposição P7 no desenvolvimento de um programa integrado de proteção, para toda a organização.	**P7.v2.1** De que forma ou qual será a ferramenta indicada para que todas as decisões relativas à privacidade dos dados possam ser integradas, proporcionando uma proteção mais eficiente?
P7.v3. O conhecimento e consciência das práticas existentes de processamento de dados e a identificação do risco associado à ausência de políticas de proteção da privacidade e proteção de dados são impulsionadores de uma visão estratégica para a privacidade. *[1] Conhecer a experiência das organizações em análises do risco em assuntos de privacidade e qual a sua relação com o desenvolvimento de uma estratégia para o controlo deste risco.* [2] Validar a relação da proposição P7 com o reconhecimento e conhecimento do risco associado a possíveis quebras de privacidade.	**P7.v3.1** Qual a influência que o risco, o seu conhecimento, a previsão do seu impacto pode ter sobre a necessidade de as organizações desenvolverem uma visão estratégica para a privacidade?
P7.v4. Uma estratégia para a privacidade é promotora de uma cultura de privacidade. Uma cultura de privacidade emerge em cenários em que as questões associadas à privacidade e proteção dos dados têm por base uma estratégia de desenvolvimento em detrimento de auditorias pontuais de conformidade. *[1] Determinar se em ambientes de colaboração o primeiro passo para a existência de uma cultura de privacidade (P2) generalizada em todas as organizações passa pela existência de uma estratégia para a privacidade* [2] Validar a relação da proposição P7 com a proposição P2.	**P7.v4.1** Considera que existe uma influência considerável entre a existência de uma estratégia de privacidade e uma cultura organizacional em privacidade? Qual a dependência entre estes dois conceitos (o que é que depende do quê)?

P7.*"Estratégia para a privacidade"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P7.v5. Em ambientes de interoperabilidade, a colaboração para o desenvolvimento de uma estratégia conjunta para a privacidade potenciaria o desenvolvimento de uma plataforma confiável para a recolha, partilha e utilização de dados pessoais. *[1] Compreender se a harmonização das estratégias de privacidade é preponderante ao desenvolvimento de uma plataforma confiável para a recolha, partilha e utilização de dados pessoais, ou se esta pode ser criada com a ausência de linhas orientadoras de desenvolvimento.* [2] Validar a relação da proposição P7 com a necessidade de unificar as várias estratégias de privacidade numa estratégia conjunta.	**P7.v5.1** Sendo que o âmbito de uma estratégia organizativa para a privacidade deve refletir a natureza e missão da organização, qual a colaboração possível a este nível entre as organizações participantes no ambiente de colaboração?

A Tabela 20 apresenta a estrutura da proposição *P8. Confiança e gestão da confiança*, constituída por três variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.8, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 20 - Estrutura e ligação da proposição P8 com as fontes de evidência

P8.*"Confiança e gestão da confiança"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P8.v1. A confiança constitui um dos pilares fundamentais aos processos de colaboração entre as organizações num ambiente de interoperabilidade. *[1] Compreender se a existência de relações de confiança entre os vários organismos da organização são fundamentais à interoperabilidade organizacional projetada.* [2] Validar a proposição P8 em relação aos contextos de interoperabilidade organizacional, e à necessidade de experiência nestes contextos (P1.v1).	**P8.v1.1** *Existem vários fatores com influência sobre a colaboração e a interoperabilidade organizacional entre organizações, nomeadamente questões de cultura, estrutura e práticas organizacionais.* De que forma o desenvolvimento de iniciativas de interoperabilidade organizacional, por exemplo nos domínios da segurança e proteção de dados, depende da confiança estabelecida entre as organizações?
P8.v2. O contexto de interoperabilidade influencia a atitude e a confiança de uma organização em relação às restantes, com implicação sobre a privacidade dos dados partilhados. *[1] Verificar se o nível de confiança dos utilizadores do sistema, num contexto de colaboração com outra ou outras organizações, é afetado em relação à privacidade dos dados.*	**P8.v2.1** O facto de uma organização operar em múltiplos sistemas, concebidos de forma isolada e com práticas de privacidade e proteção de dados diferentes, pode influenciar ou condicionar a confiança dos seus utilizadores nestes sistemas?

P8. *"Confiança e gestão da confiança"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
[2] Validar a proposição P8 em relação aos contextos de interoperabilidade organizacional e ao funcionamento da privacidade dos dados nestes.	
P8.v3. A utilização de tecnologias inerentemente invasivas da privacidade, tecnologias novas que apresentam ameaças e que provocam demasiado interesse público representam um risco à confiança sobre o sistema. *[1] Verificar se o nível de confiança pode ser afetado com o contínuo recurso a tecnologias de informação que podem afetar a privacidade tanto de profissionais como do titular dos dados.* [2] Validar a proposição P8 em relação à cada vez maior utilização de tecnologias de informação, que podem ser invasivas da privacidade.	**P8.v3.1** Uma análise atempada dos impactos (riscos) sobre a privacidade que podem surgir com o desenvolvimento ou aquisição de uma nova solução tecnológica ou serviço de informação, que utiliza dados pessoais, pode influenciar a confiança dos profissionais utilizadores destas soluções? Na sua opinião, de que forma?

A Tabela 21 apresenta a estrutura da proposição *P9. Ética e cooperação humana*, constituída por três variáveis dependentes, formuladas com base no conhecimento reunido na seção 3.2.9, e que entendemos como necessárias para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 21 - Estrutura e ligação da proposição P9 com as fontes de evidência

P9. *"Ética e cooperação humana"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P9.v1. A iniciativa (atitude) e falta de confiança do titular dos dados ao condicionar ou limitar o acesso e utilização dos seus dados têm influência direta sobre a sua disponibilidade entre sistemas. *[1] Analisar se a iniciativa do titular dos dados pode comprometer os objetivos que estão na base da colaboração entre organizações.* [2] Validar a proposição P9 em relação à iniciativa do titular dos dados.	**P9.v1.1** Qual a situação que mais o(a) preocupa quanto à sua privacidade? a. A violação da privacidade das suas comunicações pessoais. b. A perda de privacidade em espaços públicos (face às tecnologias de vigilância e localização). a. A violação da privacidade dos seus dados pessoais. **P9.v1.2** Qual a situação de utilização e partilha dos seus dados que lhe suscita mais preocupações quanto à sua proteção e privacidade? a. No apoio aos tratamentos de saúde, em que os seus dados de saúde podem ser partilhados entre profissionais de saúde. b. No funcionamento da organização, em que os seus dados podem ser utilizados e partilhados dentro da organização, para melhorar o apoio médico, melhorar o atendimento e se necessário contactá-lo pessoalmente. c. No contacto com outras instituições do setor da saúde,

P9.*"Ética e cooperação humana"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
	em que os seus dados podem ser partilhados para faturação dos serviços de saúde a outras entidades. **P9.v1.3** Considera que a sua atitude/ação pode ter uma influência significativa na gestão da privacidade dos seus dados (s/n)? **P9.v1.4** Que funcionalidades são fundamentais à sua participação na gestão e controlo da privacidade dos seus dados pessoais (pode escolher várias opções)? a. O consentimento – no sentido de limitar a utilização dos seus dados. b. O controlo e a monitorização da utilização dos seus dados – indicação clara sobre quais os utilizadores e porque utilizaram os seus dados. c. A atualização e correção dos seus dados. d. A possibilidade de portabilidade dos seus dados num formato digital comum. **P9.v1.5** Determinadas situações de partilha de dados exigem um **consentimento** por parte do seu titular, permitindo-lhe restringir o acesso aos seus dados a determinadas pessoas ou serviços. Em sua opinião (escolha uma opção): a. As situações que exigem consentimento não são claras nem compreensíveis. b. As situações que exigem consentimento são claras e compreensíveis. b. Este direito é um direito bem compreendido, mas de difícil gestão e controlo. **P9.v1.6** A **confiança** do titular dos dados (utente) na organização a quem facultou os seus dados pessoais é determinante para a gestão da privacidade. Atribua um grau de importância (1-5) aos seguintes conjuntos de informação, que sendo públicos, podem influenciar a confiança do titular dos dados na organização: a. A publicação das políticas de privacidade e proteção de dados. b. A publicação dos **direitos** que o titular dos dados (utente) tem sobre os seus dados pessoais. c. A demonstração da conformidade da globalidade da organização para com os requisitos legais no domínio da proteção e privacidade dos dados. d. A demonstração do compromisso de responsabilidade da organização na proteção de dados e. A publicação dos contextos e finalidades de utilização dos dados.
P9.v2. A *transparência* para com o titular dos dados, sendo necessário assegurar que este está suficientemente informado sobre o ambiente de colaboração entre as organizações, devendo ter acesso à informação sobre como estão a ser usados os seus dados, quem acedeu, de onde, para que fins e quais os meios técnicos utilizados para o seu processamento. *[1] Compreender se é necessário fazer evoluir o conceito de transparência face ao ambiente de colaboração e partilha de*	**P9.v2.1** A legislação sobre proteção de dados exige às organizações que utilizam os seus dados pessoais, determinadas **obrigações** (responsabilidades). Qual a sua opinião sobre estas obrigações: a. Não são do conhecimento generalizado dos utentes. b. Existem mas não são claras para a maioria dos utentes. c. Existem e são compreensíveis. d. Existem, são compreensíveis, mas a organização em causa não apresenta provas quanto ao seu cumprimento. **P9.v2.2** Como classifica a informação que lhe é disponibilizada sobre os seus **direitos** em termos de privacidade e proteção dos seus dados:

P9.*"Ética e cooperação humana"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
dados pessoais entre as organizações. Analisar se devem ser disponibilizadas soluções alternativas que permitam ao titular dos dados uma maior compreensão sobre o funcionamento e a proteção de dados em ambientes colaborativos, melhorando assim o princípio da transparência. [2] Validar a proposição P9 em relação à transparência do objetivo para o qual os dados pessoais estão a ser recolhidos e à partilha de dados entre vários sistemas.	a. Não é disponibilizada qualquer informação. b. A informação existente é mínima, e não permite compreender quais os **direitos** que assistem o titular dos dados. c. A informação existente é suficiente, é de fácil acesso e compreensão, formulada numa linguagem clara e simples, para um conhecimento detalhado dos **direitos** do titular dos dados. **P9.v2.3** Confrontado com uma situação que lhe suscite preocupações em relação à utilização dos seus dados pessoais, consegue com base na informação que lhe é disponibilizada: a. Identificar com facilidade os meios disponíveis para apresentar as dúvidas existentes (s/n)? b. Identificar a pessoa responsável pela utilização dos seus dados dentro da organização (s/n)? c. Contactar com facilidade o responsável na organização pela utilização dos seus dados (s/n)? **P9.v2.4** Com base na informação disponível, consegue **distinguir** entre situações (a) em que existe uma base legal que permite que os seus dados sejam partilhados e (b) situações em que os seus dados nunca serão partilhados (s/n)? **P9.v2.5** Sempre que os seus dados forem suscetíveis de serem legitimamente partilhados com outros destinatários, que informação considera importante que lhe seja enviada (atribua um grau de importância (1-5)). a. Os tipos de dados partilhados. b. A sensibilidade dos dados. c. O(s) destinatário(s) dos dados. d. O propósito da partilha dos dados. e. As medidas adotadas para a proteção dos dados. **P9.v2.6** Considera a PDS como uma oportunidade para melhor compreender as questões da privacidade dos dados pessoais no domínio dos sistemas de gestão de saúde? a. Sim b. Não
P9.v3. A atitude dos profissionais face à mudança que decorre dos novos requisitos do ambiente de colaboração, assim como a sua atitude face à deterioração da sua privacidade profissional, podem apresentar efeitos negativos para o sucesso das políticas de privacidade para o contexto da colaboração. *[1] Compreender se as mudanças tecnológicas associadas à interoperabilidade condicionam a atitude dos profissionais e se esta pode contribuir para o sucesso do projeto no global e a privacidade dos dados em particular.* [2] Validar a proposição P9 em relação	**P9.v3.1** A que níveis se pode manifestar a atitude dos vários profissionais face às mudanças e requisitos organizacionais decorrentes das iniciativas de colaboração entre organizações? **P9.v3.2** Existe a consciência de um aumento de práticas que degradam o direito e expectativas da privacidade profissional face ao crescimento de um "controlo tecnológico invisível"? **P9.v3.3** Qual a influência que este "controlo tecnológico invisível" do trabalho dos profissionais, que afeta a sua privacidade profissional, pode ter sobre a sua atitude face à sua participação num ambiente de colaboração? **P9.v3.4** Enquanto profissional de saúde, concorda que a sua própria ação ou omissão[65] pode prejudicar outros profissionais (ética)?

[65] Neste caso a confidencialidade do médico – proteção do paciente.

P9.*"Ética e cooperação humana"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
à resistência às mudanças tecnológicas inerentes a um ambiente de colaboração.	

A Tabela 22 apresenta a estrutura da proposição *P10. Estrutura organizativa*, constituída por uma variável dependente, formulada com base no conhecimento reunido na seção 3.2.10, e que entendemos como necessária para a validação desta proposição e compreensão de como este subdomínio de fatores pode afetar a privacidade dos dados em ambientes de interoperabilidade.

Tabela 22 - Estrutura e ligação da proposição P10 com as fontes de evidência

P10.*"Estrutura organizativa"*	
Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação	**Itens →Fontes de evidências**
P10.v1. A resolução das dificuldades em ambientes de colaboração em matéria de privacidade dos dados resultantes da heterogeneidade organizacional, depende da compreensão comum da importância da interoperabilidade organizacional e de uma estratégia e acordos comuns para o seu desenvolvimento. *[1] Analisar se uma cultura em interoperabilidade, neste caso organizacional, é importante ao desenvolvimento de práticas de privacidade dos dados.* [2] Validar a proposição P10 em relação à necessidade de desenvolvimento de uma cultura em interoperabilidade organizacional.	**P10.v1.1** Na sua opinião, e tendo em conta a complexidade da questão da privacidade dos dados no contexto de colaboração entre várias organizações, qual a abordagem que melhor se adapta a esta complexidade: uma abordagem conjunta e integrada, ou uma abordagem individual e isolada? O que é necessário para operacionalizar uma abordagem conjunta deste assunto? **P10.v1.2** *As organizações são diferentes em termos de disponibilidade e prontidão para a colaboração e interoperabilidade, nomeadamente devido à sua heterogeneidade tecnológica e organizativa.* Para a privacidade e proteção dos dados, o que é necessário para promover nas organizações uma maior capacidade de colaboração?

4.4.1.5 Unidade de estudo

A unidade de estudo identifica o que constitui um "caso", podendo ser um indivíduo, um grupo, uma organização, ou pode ser um evento ou outro fenómeno. Deve permitir a necessária amplitude e profundidade na recolha dos dados, para que a resposta à questão de estudo seja suficiente e a mais adequada (Darke et al., 1998). A questão de estudo determina assim a escolha do nível e âmbito da unidade de estudo, sugerindo "onde se vai obter respostas, com quem se vai falar, e o que se vai

observar" (Miles & Huberman, 1994). São as organizações e os SI que apresentam características particularmente interessantes, que necessitam de ser profundamente estudadas, pois poderão trazer um contributo muito significativo para a criação, extensão ou validação de teorias emergentes na área dos SI (Caldeira & Romão, 2002).

Para o investigador, a proximidade do *estudo de caso* de um cenário real e a sua multiplicidade de detalhes é muito importante, e influencia a qualidade do processo de aprendizagem do investigador e o desenvolvimento das competências necessárias à execução de uma boa pesquisa (Flyvbjerg, 2006). Uma grande distância do objeto de estudo e a falta de *feedback*, com facilidade conduzem a um processo de aprendizagem onde o efeito e a utilidade da pesquisa é incerto e não testado. Como método de investigação, o *estudo de caso* pode ser um "remédio" eficaz contra esta tendência, na opinião deste autor. Contudo, a disponibilidade de locais de estudo adequados pode ser limitada, as organizações nem sempre estão dispostas a participar, assim como pode ser difícil a apresentação dos resultados da pesquisa (Yin, 2009). As organizações só têm vontade de participar, se for claro para elas que os resultados da investigação serão pertinentes para as suas decisões, e que estes estarão disponíveis num prazo útil (Darke et al., 1998).

O número de casos a serem estudados depende do foco da questão de estudo (Benbasat, David, & Mead, 1987). Não há um número de casos ideal. Yin (2009) sugere que um maior número de casos dá uma maior segurança, mas que em algumas situações, por exemplo quando se estudam teorias rivais muito diferentes, pode ser necessário menos repetições. Eisenhardt (1989) sugere que entre quatro e dez casos são desejáveis para a construção de uma teoria. Para Darke et al. (1998) um *estudo de caso* exploratório tanto pode ser adaptado a situações de casos únicos como a múltiplos casos. Projetos de múltiplos casos são desejáveis quando o *estudo de caso* é descritivo, e se pretende desenvolver ou testar uma teoria (Benbasat et al., 1987).

Encontra-se um fundamento lógico para um caso único quando ele representa o caso decisivo ao testar uma teoria bem formulada. A teoria especificou um conjunto claro de proposições, assim como as circunstâncias nas quais se acredita que as proposições sejam verdadeiras. Para confirmar, contestar ou estender a teoria, deve existir um caso único, que satisfaça todas as condições para testar a teoria. O caso único pode, então, ser utilizado para se determinar se as proposições de uma teoria

são corretas ou se algum outro conjunto alternativo de explicações pode ser mais relevante (Yin, 2009).

A amostragem é crucial para a análise posterior. Por mais que se queira, não se consegue abranger tudo nem todos num estudo. A escolha – quem abordar ou com quem falar, onde, quando, sobre o quê e porquê – vai influenciar as conclusões finais, assim como a confiança sobre estas (Miles & Huberman, 1994). Na opinião destes autores, é necessário definir *limites,* definir os aspetos do caso que podemos estudar dentro dos limites de tempo e meios disponíveis, que estão diretamente relacionados com as questões de estudo e que provavelmente irá incluir vários exemplos do que se quer estudar.

O "caso" de estudo

A opção pelo domínio da saúde para a fase da recolha de dados resultou de um levantamento a nível nacional dos contextos de interoperabilidade entre SI, nos quais a privacidade e proteção dos dados fossem um requisito essencial. De um conjunto de possibilidades identificadas no domínio da justiça, finanças e também no domínio da educação, o domínio da saúde, dada a intensidade crescente na utilização de dados e a preocupação crescente com a sua privacidade, afirmou-se como o melhor contexto para a validação da questão e proposições do estudo.

Neste setor, encontrava-se na fase de desenho o projeto Registo de Saúde Eletrónico (RSE), que à semelhança de outras iniciativas a nível europeu previa a partilha de dados entre instituições na área da saúde. A reunião tida com o responsável deste projeto, e que nesta fase viabilizou a proposta de investigação, acabou comprometida face à interrupção e consequente abandono deste projeto.

Com o início de um novo, e distinto, projeto de partilha de dados no domínio da saúde – a Plataforma de Dados da Saúde (PDS) – foi possível voltar a considerar o contexto da saúde como o caso preferencial para a realização do *estudo de caso*. Os objetivos mantinham-se, mas agora com um contexto real de partilha de dados.

A PDS[66], projeto desenvolvido e coordenado pela Comissão para a Informatização Clínica (CIC) e pelos Serviços Partilhados do Ministério da Saúde (SPMS), com a

[66] Mais informação sobre este projeto disponível no URL: http://www.portaldasaude.pt/portal/conteudos/a+saude+em+portugal/informatizacao/PDSenglishm.htm

colaboração[67] da Faculdade de Engenharia do Porto (FEUP), constitui assim a unidade de estudo ou o "caso de estudo". Apresenta-se como um ecossistema tecnológico heterogéneo, onde participam vários SI com um objetivo comum – a construção de um sistema de colaboração e partilha de dados/serviços de saúde. Esta heterogeneidade dos SI, a natureza dos dados partilhados e a necessidade da sua proteção, assim como o facto de a interoperabilidade entre os vários sistemas se encontrar em franca expansão, com perspetiva futura de interoperabilidade com sistemas similares no espaço europeu, justificou a escolha da PDS para caso de estudo.

O objetivo da PDS é integrar e interligar todas as instituições entre si, de forma rápida, ágil e segura. Contudo, a complexidade da rede, e os agentes e sistemas a interagir impõe uma abordagem cuidadosa (Reis, 2012). O seu desenvolvimento envolveu a integração de múltiplas competências de gestão e engenharia para um desenvolvimento bem-sucedido deste serviço de base tecnológica (Patrício & Brito, 2012). Os processos de integração já se encontram perfeitamente alinhados através do *standard* internacionalmente aceite para a interoperabilidade clínica, o HL7 (Reis, 2012).

O desenvolvimento da PDS implicou interligar informação de múltiplos sistemas tecnológicos usados pelas diferentes instituições, e integrar procedimentos dos diferentes utentes e profissionais de saúde. A prestação de cuidados de saúde é complexa, e a diversidade de sistemas e de práticas é um grande desafio ao acesso integrado à informação preconizada pela PDS (Patrício & Brito, 2012).

O tratamento de dados pessoais, no domínio da PDS, para partilha de informação entre as instituições prestadoras de cuidados de saúde do Serviço Nacional de Saúde (SNS), foi autorizado pela CNPD através da AUTORIZAÇÃO nº 3742/2012 (CNPD, 2012a), tendo sido neste mesmo documento colocadas por parte da CNPD algumas reservas e considerações em relação às questões da proteção da privacidade dos dados, perfeitamente enquadradas com os objetivos deste estudo, nomeadamente:

[67] O projeto de colaboração da FEUP com o Ministério da Saúde envolveu o trabalho de dois investigadores e de três estudantes de doutoramento, que desenvolveram a sua investigação nas três áreas de apoio ao projeto. O projeto contou ainda com a colaboração de investigadores da *Carnegie Mellon University*, da *Texas State University* e da *University of Hawaii* (Patrício & Brito, 2012).

a. A CNPD, confrontada com a decisão do responsável pela PDS de não disponibilizar toda a informação de saúde existente devido à necessidade de inclusão de filtros de privacidade para a proteção de "áreas sensíveis", salientou a necessidade de o percurso ter que ser o oposto, ou seja, "*de implementar mecanismos de salvaguarda da privacidade, nomeadamente através de filtros de privacidade em relação a áreas sensíveis, e só após a sua adoção, a disponibilização da informação com os respetivos filtros*".
b. A fragilidade existente na questão da identidade e autenticação dos profissionais de saúde (que não surge com a PDS), que coloca problemas de confidencialidade e segurança da informação, derivado aos factos de (1) as instituições de saúde adotarem inúmeras aplicações informáticas com mecanismos de autenticação muito distintos, (2) a falta de planeamento da sua integração e compatibilidade com os sistemas de autenticação já existentes, (3) a compatibilidade agrava-se quando passamos de âmbito local para regional ou nacional, das aplicações, e (4) o comportamento pouco cauteloso dos utilizadores no uso da sua identidade digital. Sendo a "*PDS uma plataforma de interoperabilidade que irá permitir o acesso a um universo muito amplo de informação, a existência de mecanismos fortes de gestão de identidade é mais premente*".
c. Sendo que a filosofia do projeto assenta no acesso à informação de um utente específico, é *necessário garantir que quando um utilizador invoca o acesso, por referência a um utente, não tem acesso a toda a informação, de todos os utentes, …, mas tão só à síntese dos registos do utente em causa*.
d. No domínio da segurança, é questionada a ausência de uma análise prévia do risco, e de todas as medidas de segurança enunciadas serem fundamentadas nos riscos identificados, assim como evidenciada a necessidade de utilização de algoritmos e chaves seguras de encriptação, e a necessidade de um sistema de auditoria fiável, primordial e essencial para a proteção de dados pessoais, que permita uma rastreabilidade eficiente dos acessos e identificar utilizações indevidas do sistema.
e. A necessidade de os sistemas contemplarem desde a sua conceção, a questão da privacidade, ou seja, a aplicação do conceito *Privacy by Design*.
f. Quanto aos processos de tratamento de dados, não foi questionada a sua legitimidade (de acordo com o nº 4 do Artigo 7º da Lei nº 67/98). A

informação é lícita, para a finalidade determinada e não excessiva (Artigo nº 5 da Lei nº 67/98). É contudo salientada a necessidade de medidas adequadas que assegurem que os dados são exatos e atualizados. A qualidade da informação disponível pode com facilidade ser comprometida, dado que é do conhecimento geral que a informação em saúde, existente nas instituições de saúde, está muitas vezes, desatualizada e inexata, o que potencia erros na sua utilização.

A PDS constitui assim o contexto ideal para a realização do *estudo de caso*, uma vez que existem todas as condições para verificar se as proposições estão corretas, e os resultados finais podem contribuir para alterar as questões da privacidade dos dados. Decidiu-se assim pela realização de *um projeto de estudo de caso único incorporado (tipo 2)*, que envolve várias unidades de análise, como representado na Figura 17.

Ou seja, dentro de um caso único, constituído pela PDS, é dada atenção a sete subunidades, com experiência e maturidade diferentes na sua implementação e utilização, uma amostra do universo de instituições da área da saúde, tendo sido selecionadas as seguintes unidades de análise:

a. Unidade Local de Saúde do Norte Alentejano, Portalegre (ULSNA) - Projeto-piloto;
b. Hospital do Espírito Santo E.P.E, Évora (HES);
c. USF Saúde Mais, Santa Maria da Feira (USF);
d. Hospital Professor Doutor Fernando Fonseca E.P.E., Amadora (HFF);
e. Instituto Nacional de Emergência Médica, Lisboa (INEM);
f. Serviços Partilhados do Ministério da Saúde E.P.E. (SPMS);
g. Grupo de *beta-tester* de Utentes.

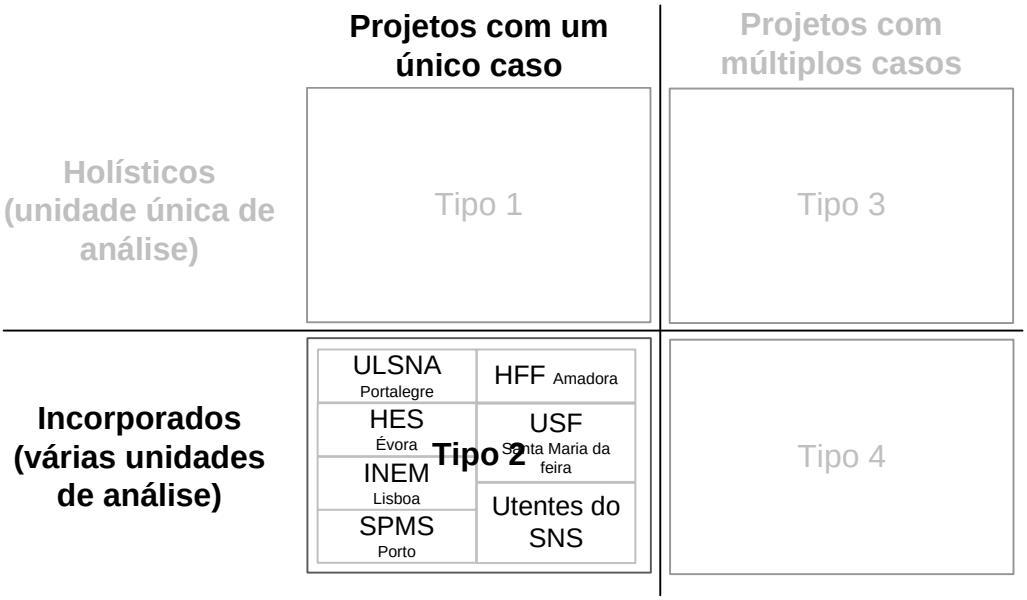

Figura 17 - Tipo de *estudo de caso*

Perfis dos participantes nas unidades de análise

Quando falamos de privacidade dos dados, de imediato o tema é associado à segurança de SI ou de infraestruturas, pelo que com alguma lógica os responsáveis pelos SI ou pelos serviços de informática, são identificados como os principais responsáveis, senão mesmo os únicos, pelo desenvolvimento de todas as medidas associadas à proteção de dados, e se possível assegurar em parte a sua privacidade. Seria um erro para este estudo seguir esta consideração. No desenvolvimento do *projeto de pesquisa*, verificou-se assim que a recolha de dados não se poderia limitar aos responsáveis locais pelos SI, deveria abranger outros profissionais, com outras experiências na utilização de dados, e com interesse e influência sobre o desenvolvimento das questões da privacidade. Foram desta forma definidos quatro perfis distintos de colaboradores para a recolha de dados através de entrevistas semiestruturadas, nomeadamente: (1) responsáveis locais pela implementação e coordenação da PDS, (2) técnicos e responsáveis pelos SI, (3) profissionais de saúde, e (4) gestores e administradores. Foi definido ainda mais um perfil - (5) utentes utilizadores da PDS, a inquirir através do *Portal do Utente*[68] - com um inquérito a disponibilizar *online*. Nas tabelas seguintes, Tabela 23 e Tabela 24, é apresentada

[68] https://servicos.min-saude.pt/utente/portal/paginas/default.aspx

uma descrição sucinta de cada um dos perfis de participantes, assim como a previsão inicial do número de participantes por perfil e por unidade de análise.

Tabela 23 - Perfis de participantes nas unidades de análise

Perfis de participantes nas unidades de análise	
Tipo de perfil	Descrição
Perfil 1 Responsáveis locais pela implementação e coordenação da PDS	Perfil que inclui os responsáveis, em cada organização, pela implementação e coordenação da PDS. *Estão-lhe destinadas questões relacionadas com a exigência que resulta da colaboração e partilha de dados entre as várias organizações (P1, P2, P3, P4, P5, P6, P8, P10).*
Perfil 2 Técnicos e responsáveis pelos sistemas de informação	Incluem-se neste perfil os responsáveis, em cada unidade de análise, pela coordenação global de todos os serviços informáticos, assim como os técnicos fundamentais à operacionalização do sistema como um todo e à PDS em particular. São os casos de técnicos especializados em segurança e técnicos especializados em questões de proteção de dados. Inclui-se neste perfil o responsável local pelo tratamento de dados (artigo 2º, alínea d, da Diretiva 95/46/CE) quando identificável. *Estão-lhe destinadas questões relacionadas com o funcionamento dos sistemas de informação no domínio da segurança, proteção e privacidade dos dados (P1, P3, P4, P5, P6).*
Perfil 3 Profissionais de saúde	Perfil que inclui médicos, enfermeiros e outros profissionais da área da saúde. Constituem os utilizadores principais da PDS e para os quais os dados são essenciais à realização da sua atividade profissional. *Estão-lhe destinadas questões relacionadas com a ética e atitude humana em relação às alterações resultantes do ambiente de colaboração e partilha de dados (P1, P2, P6, P8, P9).*
Perfil 4 Gestores e administradores	Perfil destinado aos administradores executivos das organizações que constituem uma unidade de análise. *Estão-lhe destinadas questões organizativas e de estratégia em relação à privacidade no geral e à privacidade dos dados em particular (P2, P4, P5, P7, P8, P9, P10).*
Perfil 5 Titular dos dados	Grupo de "*beta tester*" existente para a validação/avaliação dos serviços disponibilizados pela PDS, através do *Portal do Utente (*https://servicos.min-saude.pt/utente/portal/paginas/default.aspx). *Estão-lhe destinadas questões para analisar a sua confiança e atitude em relação à partilha de dados entre organizações, assim como a necessidade ou não de mais informação (transparência) sobre este novo contexto (P9).*

Tabela 24 – Número estimado de processos de recolha de dados por perfil/unidade de análise

Número de processos de recolha de dados							
Previsão inicial do número de processos de recolha de dados a realizar.							
Tipo de perfil	**Unidades de análise**						
	ULSNA	**HES**	**USF**	**HFF**	**INEM**	**SPMS**	**Utentes**
Perfil 1 Responsáveis locais pela implementação e coordenação da PDS	1	1-2	1-2	1-2	1-2	1-2	n/a
Perfil 2 Técnicos e responsáveis pelos sistemas de informação	2	3-5	3-5	3-5	3-5	1-2	n/a
Perfil 3 Profissionais de saúde	3	3-5	3-5	3-5	3-5	n/a	n/a
Perfil 4 Gestores e administradores	1	1-2	1-2	1-2	1-2	1-2	n/a
Perfil 5 Titular dos dados	n/a	n/a	n/a	n/a	n/a	n/a	1-300

4.4.2. Protocolo para o *estudo de caso*

Todo o trabalho conceptual e estruturante do *projeto de pesquisa* é numa fase posterior reunido no *protocolo para o estudo de caso*. É um ponto central de documentação do estudo e tem, segundo Yin (2009), um enorme peso sobre a sua confiabilidade. A experiência tida permitiu constatar que o sucesso da recolha dos dados esteve muito dependente deste documento. É sem dúvida um componente essencial, pois suporta o trabalho do investigador ao nível de procedimentos e regras, e define significativamente a rotina dos processos de recolha de dados. Estabelece a ponte que liga o *estudo de caso* às unidades de análise e aos participantes.

Foram incluídos neste documento os seguintes componentes: (1) uma descrição sucinta do estudo, os seus objetivos e a apresentação das organizações participantes; (2) os procedimentos necessários ao trabalho de campo; (3) a apresentação detalhada das questões do estudo; e (4) o elenco de questões para as entrevistas a realizar.

O protocolo para o estudo de caso, constitui assim o único documento deste estudo onde consta o elenco e a ordem de itens a incluir nas entrevistas semiestruturadas e no inquérito. A forma como cada item das variáveis dependentes foi atribuído a cada um dos quatro elencos distintos de entrevistas e no inquérito, de acordo com os cinco perfis profissionais, está apresentado na Tabela 25. No sentido de otimizar a

realização das entrevistas, a ordem pela qual as proposições surgem no elenco de questões das entrevistas, é a seguinte:

Perfil 1: P2 → P5 → P8 → P6 → P3 → P4 → P10 → P1 (25 questões),

Perfil 2: P3 → P4 → P6 → P5 → P1 (24 questões),

Perfil 3: P2 → P9 → P6 → P8 → P1 (13 questões),

Perfil 4: P2 → P5 → P4 → P7 → P8 → P9 → P1 → P10 (24 questões).

Foram desenvolvidos dois tipos de protocolo: o primeiro destinado aos responsáveis da organização (Anexo I), o qual reúne toda a informação necessária para a análise e aprovação da realização do *estudo de caso*, e o segundo enviado individualmente a cada profissional de acordo com o seu perfil de participante (Anexos II, III, IV e V), no sentido de lhe apresentar o estudo assim como o elenco de questões para a entrevista.

Tabela 25 - Ligação entre as variáveis dependentes com os perfis de participantes

Ligação entre variáveis dependentes com os perfis de participantes							
Identificação dos perfis destinatários dos itens identificados em cada variável dependente							
Proposição	Variável dependente	Item	**Perfil 1**	**Perfil 2**	**Perfil 3**	**Perfil 4**	**Perfil 5**
P1	P1.v1	1	✖	✖			
	P1.v2	1	✖	✖			
		2	✖	✖			
	P1.v3	1	✖	✖		✖	
	P1.v4	1	✖	✖	✖	✖	
P2	P2.v1	1	✖			✖	
	P2.v2	1	✖		✖	✖	
	P2.v3	1	✖		✖		
		2	✖		✖		
P3	P3.v1	1	✖	✖			
		2	✖	✖			
	P3.v2	1		✖			
	P3.v3	1		✖			
	P3.v4	1		✖			
	P3.v5	1		✖			
P4	P4.v1	1	✖	✖		✖	
	P4.v2	1	✖	✖			
P5	P5.v1	1	✖	✖		✖	
	P5.v2	1		✖		✖	
		2		✖			
		3		✖			
	P5.v3	1		✖			
	P5.v4	1	✖	✖		✖	
P6	P6.v1	1	✖	✖	✖		
		2	✖	✖	✖		
	P6.v2	1	✖	✖	✖		
	P6.v3	1	✖	✖			
	P6.v4	1		✖			
P7	P7.v1	1				✖	
		2				✖	
	P7.v2	1				✖	
	P7.v3	1				✖	
	P7.v4	1				✖	
	P7.v5	1				✖	
P8	P8.v1	1	✖			✖	
	P8.v2	1	✖			✖	
	P8.v3	1	✖		✖	✖	
P9	P9.v1	1					✖
		2					✖
		3					✖
		4					✖
		5					✖
		6					✖
	P9.v2	1					✖
		2					✖
		3					✖
		4					✖
		5					✖
		6					✖
	P9.v3	1			✖	✖	
		2			✖	✖	
		3			✖	✖	
		4			✖		
P10	P10.v1	1	✖			✖	
		2	✖			✖	

4.4.3. Operacionalização do *estudo de caso* - conceção e realização da recolha de dados

Uma recolha de dados eficaz e eficiente para o *estudo de caso* requer um planeamento cuidadoso, e uma utilização criteriosa do tempo disponível dos participantes e do investigador. A recolha de dados para um *estudo de caso* pode ser difícil e demorada (Cavaye, 1996).

Formalmente o projeto de investigação iniciou-se com sua apresentação ao presidente do Conselho de Administração da SPMS, em reunião tida nas instalações da Administração Central do Sistema de Saúde (ACSS) em Lisboa. Foi evidenciada a oportunidade do estudo, e a mais-valia do estudo para o contexto de partilha de dados em ritmo acelerado de implementação. O *estudo de caso* pôde assim iniciar com a colaboração da SPMS, a qual foi fundamental no suporte à operacionalização das fases seguintes do estudo. Sem este apoio o acesso às organizações e aos seus profissionais dificilmente teria sucesso.

Numa primeira fase dos trabalhos, foram identificadas, em colaboração com a SPMS, as unidades de análise (organizações) para a recolha de dados, assim como o profissional dentro de cada organização que poderia atuar como *interlocutor* para a realização do estudo. De uma forma ainda informal, foi realizado um primeiro contacto com estes profissionais, com o objetivo de apresentar o estudo, e perceber qual a sua recetividade em relação à sua realização (veja-se o esquema de trabalho representado na Figura 18). Só após este primeiro contacto, que em alguns casos obrigou a uma reunião presencial, o estudo pôde iniciar formalmente, com a sua apresentação oficial, através do envio da proposta de colaboração aos responsáveis de cada uma das organizações (Anexo VI), acompanhado do *protocolo para o estudo de caso* (Anexo I).

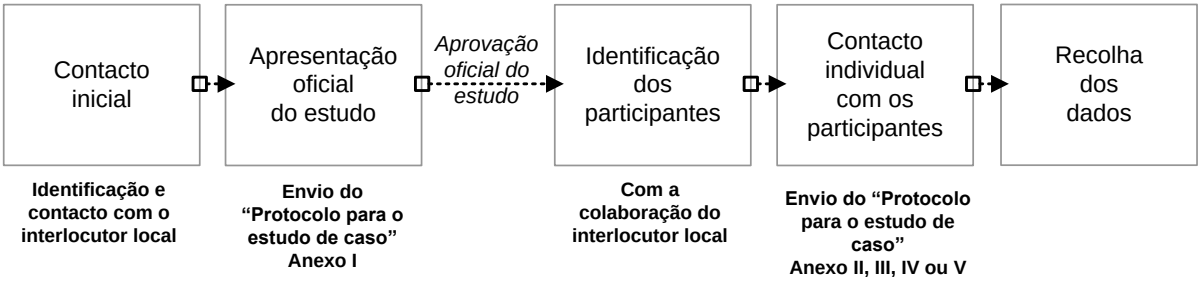

Figura 18 - Processo de trabalho com cada unidade de análise

O facto de o tema em estudo incluir o termo "privacidade", não facilitou em alguns casos a sua aprovação, tendo sido necessário o parecer adicional das comissões de ética ou mesmo jurídicas, face a preocupações relacionadas com os riscos associados à realização do estudo. Após a aprovação oficial, foi possível para cada uma das unidades de análise, e com a colaboração do interlocutor local, identificar os participantes de acordo com os requisitos dos perfis pré-definidos, e elaborar uma agenda consensual para a realização dos trabalhos de recolha de dados (Anexo VII). Foi sempre prioridade o horário e disponibilidade de cada profissional, procurando perturbar-se ao mínimo a atividade regular de cada organização. Neste sentido, reservaram-se sempre dois dias a cada unidade de análise, facilitando assim a elaboração da agenda. De salientar a excelente disponibilidade de todos os 34 profissionais envolvidos no estudo.

Para cada unidade de análise, e com a antecedência necessária em relação aos dias acordados para a recolha dos dados localmente, procedeu-se ao contacto individual com cada participante, através de correio eletrónico, com o envio de um *e-mail* (Anexo VIII) com o convite para a sua participação individual no estudo e em anexo foi enviado o *protocolo para o estudo de caso* de acordo, com o respetivo perfil de participante (Anexos II, III, IV ou V), com uma descrição sucinta do estudo, assim como o elenco de questões a abordar na entrevista. Houve nesta fase uma preocupação em incluir neste documento informação adicional de modo a facilitar a compreensão de alguns termos e conceitos em estudo. Pretendia-se assim que o participante pudesse ter um contacto prévio com as questões em estudo, dando-lhe condições para otimizar o seu contributo face à complexidade dos temas abordados. Verificou-se que muitos dos participantes leram atempadamente o documento, anotaram inclusivamente a sua opinião, o que permitiu encurtar o tempo de resposta em cada questão, e o mais importante, uma maior clareza e fluidez na opinião apresentada. Nos restantes participantes foi necessário uma exposição mais cuidadosa de cada questão, e a utilização de fundamentos adicionais durante a exposição ao participante. As entrevistas foram sempre conduzidas como um diálogo em que se foi evoluindo nos temas previstos. Foi sempre um diálogo a dois e nunca num único sentido, do tipo pergunta-resposta.

Todas as entrevistas foram gravadas em suporte digital, com a autorização do participante, e posteriormente transcritas. No total foram transcritas 34h 37m de suporte áudio, resultado das 34 entrevistas realizadas.

Projeto-piloto

O estudo iniciou com a aplicação do *protocolo para o estudo de caso* ao projeto-piloto, realizado na ULSNA. O objetivo principal do projeto-piloto foi averiguar da objetividade das questões em estudo, da forma de operacionalização do estudo, das principais dificuldades na interpretação e clareza do elenco de questões por entrevista e, muito importante também, conseguir uma experiência inicial na tarefa de conduzir uma entrevista. No global o resultado obtido foi bastante positivo para a continuidade dos trabalhos de recolha de dados nas restantes unidades de análise. Destacam-se como principais contributos da realização do projeto-piloto: (1) a validação da importância do estudo; (2) a constatação de que algumas questões eram muito extensas e de difícil compreensão; (3) algumas questões não se enquadravam com determinados perfis, nomeadamente no perfil 3 onde foram retiradas algumas questões; (4) verificou-se da necessidade de reorganizar o elenco de questões em alguns perfis, de forma a otimizar a fluidez dos temas a abordar.

Foram promovidas as alterações necessárias ao protocolo para o estudo de caso, e prosseguiu-se com a sua aplicação nas restantes unidades de análise.

4.4.4 Processo de análise dos dados

Os dados recolhidos nas várias unidades de análise através de entrevistas e documentos variados, foram numa primeira fase processados por forma a ficarem disponíveis para análise. Este processamento incluiu a transcrição cuidadosa das entrevistas em suporte áudio, a edição dos textos, a eliminação dos dados desnecessários, e a catalogação da informação recolhida dos documentos relacionada com a questão de estudo.

Após o processamento dos dados recolhidos em cada unidade de análise, os dados foram reunidos por proposição e por variável dependente[69]. Nesta fase todos os dados foram codificados, tendo-lhe sido retirada qualquer informação que identificasse o participante. Cada item de dados foi codificado de acordo com a sintaxe apresentada na Figura 19. Esta codificação permite manter o encadeamento dos dados ou evidências, permitindo perceber a qualquer momento a fonte de qualquer dado, assim como a sua relação com os resultados finais, tanto ao nível das variáveis dependentes como das proposições. Concluído este trabalho de processamento e preparação dos dados, estes consideram-se preparados para análise.

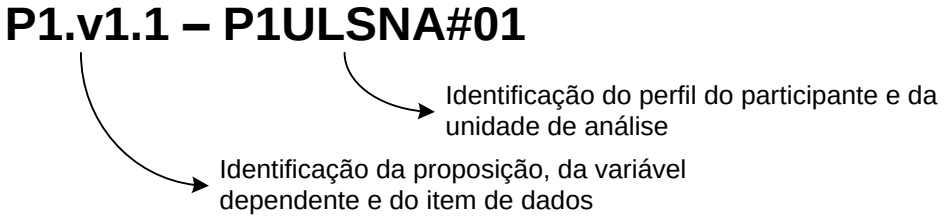

Figura 19 - Sintaxe de codificação de um item de dados

A recolha de dados qualitativos são a melhor estratégia para descobrir, explorar uma nova área, e desenvolver ou testar hipóteses (Miles & Huberman, 1994). No entanto, aquilo que se obtém dos dados qualitativos depende do processo de análise aplicado aos dados. Para Yin (2009) deve ser claro que a análise se baseou em todas as evidências relevantes e se dedicou aos aspetos mais significativos do *estudo de caso*.

A utilização da adequação ao padrão como técnica primária de análise dos dados requer alguma prudência interpretativa por parte do investigador, o qual pode apresentar uma restrição excessiva em afirmar que um determinado padrão foi violado, ou uma tolerância demasiada para decidir que um padrão foi igualado (Yin, 2009). Isto requer por parte do investigador a utilização de técnicas precisas e rigorosas na análise do padrão, neste caso de uma proposição.

Neste sentido, o instrumento para análise dos dados qualitativos foi desenvolvido com base nos componentes do modelo interativo representado na Figura 20. A análise qualitativa foi conseguida através de fluxos concorrentes das atividades: de

[69] Isto não significa que os dados tenham sido retirados do seu contexto e deixem de fazer sentido. A análise de uma proposição e das suas variáveis dependentes depende da reunião de todos os dados, mesmo que recolhidos com diferentes instrumentos.

redução de dados (*data reduction*), de exposição dos dados (*data display*), e de elaboração e verificação das conclusões (*conclusions: drawing/verification*).

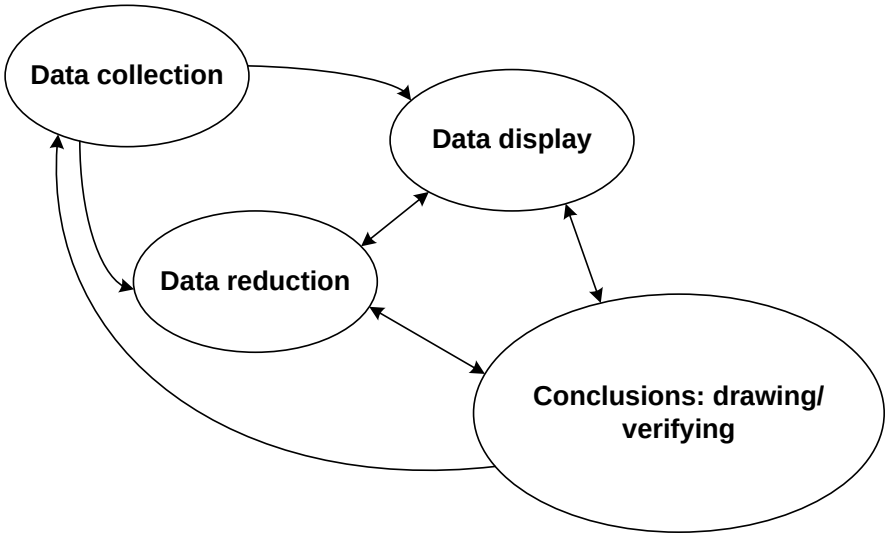

Figura 20 - Componentes da análise de dados: modelo interativo

(Miles & Huberman, 1994)

Sobre o conjunto de dados preparados para análise, a atividade de *redução de dados* permitiu retirar deste conjunto, apenas os dados com interesse para o estudo. Esta foi uma atividade de seleção, simplificação e transformação dos dados (não quer dizer quantificação dos dados). Foi assim desenvolvida para cada variável dependente uma tabela com os dados significativos, úteis, e relacionados com os resultados inicialmente previstos para a variável dependente. Com base nesta atividade de seleção foi observado para cada variável dependente o seu padrão[70]. Ou seja, identificados os termos representativos dos dados recolhidos. Para Miles & Huberman (1994) a atividade de redução de dados não é uma atividade separada do processo de análise, mas sim uma parte do processo de análise. As decisões do investigador – que dados codificar e relegar, quais os padrões que melhor resumem um conjunto de dados, e como organizar os dados – são todas escolhas analíticas.

A atividade de *exposição dos dados* incide sobre o resultado da atividade de *redução dos dados*. Permite organizar, comprimir e resumir a informação recolhida para simplificar a elaboração e verificação das conclusões. Os instrumentos desenvolvidos

[70] Esta atividade foi realizada pelo autor do estudo, manualmente, sem o recurso a qualquer aplicação informática para a análise de dados qualitativos, nomeadamente a aplicação NVivo.

nesta atividade devem permitir que a informação anteriormente organizada fique acessível de uma forma compacta, de modo a que o investigador possa verificar o que está a acontecer, e com base neste conhecimento tirar conclusões sólidas (Miles & Huberman, 1994).

Havia que desenvolver um instrumento de análise capaz de representar a riqueza dos dados recolhidos e que se adaptasse ao cariz exploratório das proposições em estudo. Das várias opções disponíveis (matrizes, diagramas, gráficos, e redes causais), decidiu-se pelo desenvolvimento de uma matriz de análise aplicável a todas as proposições, denominada de *matriz de análise da opinião*. O objetivo passou por condensar as várias tabelas que resultaram da atividade de *redução de dados*, numa única tabela, limitada a uma página A4. Esta matriz apresenta os resultados mais significativos, que reuniram uma forte convergência de opiniões, agregados em dois temas que emergem da análise dos dados, temas estes relacionados com todas as variáveis dependentes da proposição.

As proposições representam em si uma conclusão. Desde o início do processo de recolha de dados que as conclusões estão presentes, incipientes e vagas numa fase inicial, vão melhorando com o desenrolar da atividade de recolha de dados. Neste sentido, a elaboração das conclusões finais é apenas metade da atividade de apresentação das conclusões do estudo. No entanto, é necessário verificar e provar a validade das conclusões que emergem dos dados. Sempre que necessário, volta-se aos dados iniciais, e otimiza-se a atividade de redução de dados, assim como o transporte de resultados para a matriz de opinião, e finalmente verificar se a conclusão redigida é a correta. As conclusões, tanto ao nível das variáveis dependentes, como ao nível das proposições, resultam assim da análise dos dados obtidos, e não da opinião ou pensamento dos investigadores. A intervenção do investigador limita-se à aplicação do instrumento de análise dos dados desenvolvido no estudo, e ao alinhamento dos resultados, facilitando assim a sua leitura e compreensão.

No capítulo seguinte, serão apresentados os resultados obtidos com o processo de análise dos dados, num primeiro momento ao nível das variáveis dependentes, e num segundo momento ao nível das proposições.

Capítulo V – Relatório do *estudo de caso* – contributo da investigação

No capítulo anterior foi apresentado o *estudo de caso*, o seu objetivo, a sua estrutura, o seu enquadramento metodológico, assim como a sua operacionalização. As ferramentas de suporte à recolha de dados, que sabíamos de elevada exigência, foram desenhadas nesta fase, as quais permitiram posteriormente colocar o estudo em prática, e recolher os dados necessários à sua continuidade. Os dados foram recolhidos nas unidades de análise entre 11.dez.2013 e 17.dez.2014, e em simultâneo procedeu-se ao seu tratamento, organização e catalogação, com o objetivo de realçar e classificar os padrões encontrados, e simplificar a leitura destes dados.

Na continuidade do processo de investigação, este capítulo vai concentrar-se, para cada um das dez proposições em estudo, na apresentação (1) da análise dos dados obtidos ao nível de cada uma das suas variáveis dependentes associadas (resultado do processo de análise aplicado aos dados com base na estratégia e método apresentado na seção 4.4.1.3) e (2) dos resultados finais para cada uma das proposições. A análise dos dados obtidos para cada proposição, e após uma nota introdutória e de contexto, será apresentada[71] através da sua matriz de análise de opinião e dos resultados obtidos para cada uma das variáveis dependentes associadas. A proposição P9 é uma exceção a esta estrutura de apresentação de resultados, uma vez que inclui uma variável dependente estudada com recurso a dados quantitativos, pelo que serão utilizados outros componentes para a sua apresentação.

O capítulo será concluído com a apresentação dos resultados finais para as dez proposições formuladas. Os resultados finais permitirão compreender: (1) se o foco individual de cada proposição foi o correto, e se os dados recolhidos reuniram a qualidade esperada para validar os aspetos estudados no âmbito de cada proposição; e (2) se a importância e a influência de cada proposição sobre a privacidade dos dados, representada na *framework* conceptual da Figura 14, foi a correta ou se é necessário realizar adaptações.

[71] No Anexo XI, estão disponíveis os ficheiros que contêm os dados, assim como o processo de análise aplicado individualmente a cada proposição.

5.1 Análise dos dados obtidos

5.1.1 Proposição P1. Experiência

O âmbito da primeira proposição em estudo são os meios e a experiência necessários ao desenvolvimento das questões relacionadas com a privacidade dos dados em situações de interoperabilidade. É fundamental compreender a influência de fatores como a experiência em interoperabilidade e em proteção de dados, a especialização dos profissionais em privacidade dos dados, e os meios necessários para melhorar o conhecimento e preparação global das organizações.

Na seção 3.2.1 foi apresentada a abordagem inicial que deu origem à introdução no estudo de uma proposição com a denominação de *P1. Experiência*. Este estudo detalhado permitiu identificar aquilo que consideramos ser importante ao desenvolvimento de ambientes de partilha de dados, no que diz respeito à experiência e compreensão coletiva das questões da interoperabilidade e da privacidade dos dados. Na seção 4.4.1.4 (Tabela 13) foi apresentada a estrutura para o estudo da proposição P1, em que foram formuladas quatro variáveis dependentes e oito itens como fonte de evidências.

Em termos de interoperabilidade, a proposição P1 está relacionada com o atributo *preparação* do modelo OIM (ver Figura 6, na página 53), e deste modo muito centrada naquilo que deve ser a preparação necessária, individual e coletiva, no suporte à interoperabilidade. Contudo, é necessário compreender a sua maior ou menor influência sobre a privacidade dos dados, assim como a sua ligação a outras proposições. Neste sentido, e de acordo com a *framework* conceptual apresentada na Figura 14 (na página 142), a proposição P1 apresenta uma influência direta sobre a privacidade dos dados, mas inferior em relação a outras proposições. A ideia inicial é que esta proposição está muito associada aos conceitos abordados nas proposições P5 e P10.

A análise dos dados relativos a esta proposição consta no Anexo XI. Do processo de análise sobre todos os itens de dados recolhidos no âmbito da proposição P1, resultou a matriz de opinião apresentada na Tabela 26, assim com os seguintes resultados para cada uma das variáveis dependentes:

P1.v1 – A experiência em projetos de partilha de dados através de soluções de interoperabilidade é sinónima de uma melhor preparação dos profissionais para o

desenvolvimento de medidas de proteção de dados. Uma instituição que não tenha experiência em projetos de partilha de dados e de interoperabilidade, dificilmente consegue desenvolver políticas conjuntas de proteção de dados. Uma maior experiência a este nível significa uma diminuição dos riscos para a privacidade e uma maior probabilidade de as organizações atuarem de uma forma pró-ativa. A colaboração é um requisito fundamental à definição conjunta das questões técnicas de interoperabilidade, assim como à partilha de experiências em questões relacionadas com a segurança, a proteção e a privacidade dos dados.

A tendência aponta para um crescimento na participação em contextos de partilha de dados, o que garantidamente vai despertar uma maior atenção para os dados, para a sua estrutura e para a sua privacidade. As dificuldades iniciais associadas às soluções de partilha de dados, podem ser eliminadas com a perceção dos benefícios que a organização pode obter. Contudo, é necessário uma maior experiência em gestão da informação, que consiga adaptar medidas de proteção de acordo com o tipo e criticidade da informação partilhada. A PDS, atendendo à mudança de atitude que está a provocar, é um contexto privilegiado para este desenvolvimento.

Foram identificadas algumas iniciativas de interoperabilidade, nomeadamente entre a ULSNA e o HES, entre aplicações ao nível local no HFF, entre o HFF e outras instituições na área da saúde, e soluções desenvolvidas pela SPMS para aplicação a nível nacional onde a interoperabilidade é já requisito primário. A maior frente de interoperabilidade técnica está a acontecer ao nível dos sistemas de autenticação, que partilham alguns dados de identidade digital, com o objetivo de o profissional se identificar perante os sistemas o menor número de vezes possível.

P1.v2 – O desenvolvimento de um ambiente seguro e confiável para a partilha de dados, está sem dúvida dependente da experiência dos responsáveis pelo desenvolvimento dos SI em proteção de dados. Ou seja, para uma participação mais produtiva na colaboração com outras organizações, os responsáveis pelos SI devem apresentar um conhecimento e compreensão dos princípios de proteção de dados e da sua necessidade, e um conhecimento ao nível dos dados envolvidos, da sua estrutura, importância e da sua criticidade. Este conhecimento é fundamental na aplicação de medidas de proteção dos dados de acordo com o nível de interoperabilidade implementado para o domínio alargado de partilha de dados.

Tabela 26 - Matriz de análise da opinião sobre P1. Experiência

P1	**Matriz de análise da opinião sobre P1. Experiência**		
Variáveis dependentes	*Padrão encontrado*	*Compreensão individual e coletiva* (Qual a influência/relação sobre a *preparação individual e coletiva* para o desenvolvimento conjunto de medidas de proteção - colaboração)	*Planeamento e suporte* (Requisitos fundamentais ao planeamento e ao suporte de uma maior preparação coletiva ou da organização)
P1.v1. É fundamental uma experiência em partilha de dados, em interoperabilidade, em projetos internos do próprio sistema de informação e em projetos de colaboração com outras organizações.	Conhecimento dependente da experiência	Existe uma dependência direta entre a experiência em projetos de partilha de dados e a proteção destes dados.	Necessária uma maior disponibilidade por parte dos profissionais para iniciativas de partilha de dados.
	Experiência é fundamental ao sucesso da partilha de dados e na redução do risco	A interoperabilidade está a mover a atenção e a preocupação das pessoas para a proteção de dados.	Partilha de experiências como forma de diminuir o risco para a privacidade dos dados.
	Tendência para uma maior atenção para com a proteção de dados	Melhor conhecimento sobre a informação.	Experiência em projetos de partilha de dados essencial ao desenvolvimento de políticas conjuntas de proteção de dados.
	A interoperabilidade é um desafio recente.	Numa fase inicial as pessoas são muito céticas [...], mas depois começam a aperceber-se dos benefícios.	A experiência diminui o risco de haver problemas de privacidade [...] maior a probabilidade de sermos proativos e não reativos.
		Necessária experiência em gestão da informação, que saiba com que tipo de informação se trata e a sua criticidade.	
		A PDS está a contribuir para uma mudança de atitude, e é o contexto propício para o desenvolvimento destas questões.	
P1.v2. Experiência em questões de privacidade, em proteção de dados, no seu enquadramento legislativo (nacional e internacional), em avaliações do impacto sobre a privacidade (PIA), ao nível dos sistemas locais permitem uma colaboração mais produtiva com outras organizações no desenvolvimento de um ambiente seguro de partilha de dados.	Segurança e proteção de dados	É importante e exigível que no futuro os responsáveis pelos SI ou outro tipo de técnicos venham a ganhar experiência em matéria de proteção de dados.	Os responsáveis pelos SI devem ser os indutores da mudança e dinamizadores da colaboração.
	Conhecimento dos dados	Compreensão de forma clara dos conceitos e dos princípios de proteção de dados, assim como a sua necessidade.	É necessária uma cultura de segurança orientada para os dados.
	O conhecimento da legislação é fundamental	Classificar e conhecer a criticidade dos dados.	Constituição do *privacy information officer*.
		Capacidade de transposição da legislação para os SI.	Deveríamos apostar em profissionais especializados.
		Fundamental ao conhecimento do nível de exigência a desenvolver quanto à segurança e proteção dos dados.	Fomentar a prática do conhecimento especializado da legislação de uma forma permanente.
P1.v3. É essencial a existência de profissionais especializados em proteção e privacidade, a cooperação entre estes, e de um órgão de supervisão para o contexto da colaboração, para garantir que as políticas de privacidade são atendidas por todos.	Recursos humanos dedicados	Facilita a colaboração com outras organizações.	Justifica-se a existência a nível local de profissionais especializados e dedicados às questões da privacidade dos dados.
	Especialistas focados nos dados	Suporte à realização de análises de impacto sobre a privacidade.	
	Responsabilidade de vários decisores	Suporte à evolução e à implementação.	Para o contexto de colaboração justifica-se a criação de uma equipa permanente, para uniformizar medidas transversais e harmonizar soluções, com possível evolução para a certificação dos sistemas.
	Equipa pluridisciplinar	São necessários profissionais com maturidade suficiente para dialogar com todos os profissionais.	
	Equipa permanente.	Transporta para a prática os requisitos da legislação.	
P1.v4. Eventos como programas periódicos de educação, formação e sensibilização entre os profissionais da organização, participação em workshops, seminários nacionais ou internacionais, no domínio da privacidade e proteção de dados, são importantes para uma melhor experiência e preparação coletiva.	Formação específica	Envolver as pessoas, sensibilizá-las para a privacidade de dados.	Promover o debate sobre privacidade dos dados.
	Colóquios e congressos	Informar e alertar as pessoas.	Promover ações de formação, colóquios, congressos.
	Ações de sensibilização	Partilha de conhecimento e experiências.	Utilizar a Internet e o portal do utente e do profissional para difundir informação.
	Disponibilidade de informação	Uniformizar a informação sobre privacidade em todas as organizações.	Depende de um grupo de trabalho dedicado.
	Debate, partilha de conhecimentos/experiências		

A experiência atual em proteção de dados está, no geral, muito limitada a competências em TI, essencialmente em tecnologias de segurança. É evidente a necessidade urgente de esta experiência evoluir para uma cultura de segurança orientada para os dados, ou seja, uma preparação em privacidade dos dados. Os responsáveis pelos SI devem ser os principais indutores desta mudança.

A prática regular de análise e transposição da legislação aplicável sobre proteção de dados, é fundamental na adaptação do nível de exigência a desenvolver quanto à segurança e proteção dos dados. Pode apresentar um efeito e impacto positivos sobre a sensibilidade coletiva para com as várias situações de privacidade dos dados. A preparação insuficiente a este nível é uma preocupação de todos os responsáveis.

A constituição do *privacy information officer* pode promover e gerir a mudança necessária no interior de cada organização.

P1.v3 – À semelhança da existência de profissionais especializados em segurança, justifica-se para o perímetro local das organizações e para a sua colaboração com organizações do mesmo setor, a existência de profissionais especializados e totalmente dedicados à privacidade dos dados. É convicção que estes profissionais vão surgir de uma forma natural, dada a preocupação crescente em relação aos dados. São essenciais no suporte à mudança, liderando o desenho e implementação de soluções de proteção da privacidade. A preparação global das organizações em matérias de proteção de dados está dependente da maturidade e experiência destes profissionais. Podem atuar como um facilitador, na colaboração com outras organizações, e na definição conjunta de um programa alargado de privacidade.

Para o ambiente alargado de colaboração, a uniformização de medidas transversais a todas as organizações, assim como a harmonização de soluções conjuntas, depende da criação de uma equipa permanente que coordene para o contexto global da colaboração, as questões da proteção e da privacidade dos dados.

P1.v4 – Uma melhoria da preparação coletiva para as questões da privacidade dos dados pode acontecer se a organização considerar aspetos tão fundamentais como a qualidade da informação ao dispor dos profissionais, e realização de ações de formação e sensibilização, colóquios e congressos, que quando utilizadas no contexto de colaboração de uma forma estruturada, podem promover o debate e a partilha de conhecimentos e experiências. São recursos exigíveis para uma melhor preparação individual e coletiva, devendo o esforço de operacionalização a nível nacional ser

realizado por um grupo de trabalho dedicado, e a definição da sua incidência e prioridade resultar da colaboração deste grupo de trabalho com as organizações. Podem ter um contributo decisivo no desenvolvimento de uma cultura de privacidade, ao influenciarem a forma como as pessoas interpretam e atuam perante situações com requisitos quanto à privacidade [dos dados]. A Internet e o portal do utente e do profissional são dois meios privilegiados para difundir informação e chegar a públicos específicos.

5.1.2 Proposição P2. Cultura de Privacidade

A proposição, *P2. Cultura de Privacidade* tem por objetivo estudar a relação entre o compromisso das organizações no desenvolvimento das melhores práticas de gestão e utilização da informação, e uma cultura em privacidade como parte integrante da cultura organizacional. Ou seja, compreender de que forma a cultura de privacidade influencia a preparação necessária e exigível às organizações para o domínio da privacidade dos dados.

A abordagem inicial e os argumentos apresentados na seção 3.2.2 permitiram perceber que a "*forma de pensar*" de uma organização é determinante para se incorporar a privacidade dos dados em todas as fases do ciclo de vida de um sistema de informação. Foi com base neste conceito que se definiu esta proposição, no sentido de clarificar e distinguir o conceito de cultura de privacidade dos conceitos de segurança e da proteção dos dados, e indicar o seu contributo real para o desenvolvimento das questões da privacidade, quer para o interior do sistema de informação, quer na sua interoperabilidade com outros sistemas.

Na seção 4.4.1.4 (Tabela 14) foi apresentada a estrutura para o estudo da proposição P2, em que foram formuladas três variáveis dependentes e quatro itens como fonte de evidências.

Em termos de interoperabilidade, a proposição P2 está relacionada com o atributo *preparação* do modelo OIM, ou seja, com a preparação individual e coletiva que são necessárias nas questões da privacidade dos dados, capazes de suportar o seu desenvolvimento em ambientes de interoperabilidade. Constitui uma proposição que pensamos de elevada influência sobre a privacidade dos dados. De acordo com a *framework* conceptual apresentada na Figura 14 (página 142), a proposição P2

apresenta uma influência direta e elevada sobre a privacidade dos dados, e está muito associada aos conceitos abordados nas proposições P3, P7 e P9.

Do processo de análise sobre todos os itens de dados recolhidos no âmbito da proposição P2, resultou a matriz de análise da opinião apresentada na Tabela 27, assim como os seguintes resultados para cada uma das variáveis dependentes:

P2.v1 – Uma cultura em privacidade transversal a todas as organizações é sinónimo de uma melhor preparação organizacional na atuação em ambientes de partilha de dados pessoais e de dados clínicos. Uma cultura em privacidade dos dados pode assim influenciar o sucesso pretendido para as iniciativas de partilha de dados, uma vez que: (1) vai contribuir para uma melhor compreensão do objetivo e do contexto de utilização dos dados; (2) gera um maior conhecimento e controlo sobre a informação e sobre o contexto de utilização, diminuindo desta forma os riscos de desproteção da informação; (3) melhora a noção e perceção sobre as questões associadas à privacidade; (4) promove uma cultura de responsabilização sobre a partilha de dados; e (5) leva a uma maior abertura para a implementação de medidas de proteção da privacidade.

A partilha de dados de uma forma regular entre organizações está a despertar preocupações e a criar novos desafios que resultam de uma maior exposição dos dados pessoais. A aptidão para a partilha de dados num ambiente alargado pode ser positivamente influenciada por uma cultura generalizada em privacidade dos dados. Ou seja, o crescimento de uma cultura de privacidade vai promover melhorias no funcionamento dos cenários de partilha de dados.

É, desta forma, necessária uma atitude de responsabilidade e de compromisso das organizações para com a privacidade destes dados. Uma cultura de privacidade que inclua a privacidade dos dados como um valor organizacional vai promover uma sensibilização, conhecimento e compreensão do objetivo destes novos contextos de utilização de dados.

Uma cultura em privacidade é desta forma decisiva ao desenvolvimento de um contexto seguro e confiável de partilha de dados, assim como à abertura necessária das organizações, na colaboração com outras organizações no desenvolvimento e implementação de medidas de proteção da privacidade.

Tabela 27 - Matriz de análise da opinião sobre P2. Cultura de Privacidade

P2	**Matriz de análise da opinião sobre P2. Cultura de Privacidade**		
Variáveis dependentes	*Padrão encontrado*	*Privacidade como **parte integrante** da cultura organizacional* *(De que forma o compromisso das organizações no desenvolvimento de melhores práticas de gestão e utilização da informação que respeitem a privacidade depende de uma cultura em privacidade)*	*Fator com influência na **preparação** organizacional* *(Qual o contributo que pode resultar de uma cultura generalizada (tanto ao nível local como para o contexto alargado de partilha de dados) sobre a preparação organizacional)*
P2.v1. A existência de uma cultura de privacidade é sinónimo de uma melhor preparação organizacional para agir em situações/contextos de privacidade. A privacidade dos dados ao ser reconhecida como um valor, integrada nas práticas de uma organização e considerada durante todo o ciclo de vida de um sistema.	Impacto e contributo positivos	O aumento na exposição, utilização e partilha de dados está a originar uma maior preocupação e atenção em relação aos dados.	Uma cultura de privacidade é importante à compreensão do objetivo e do contexto da utilização da informação.
	Sensibilidade	Na base de uma partilha de dados mais segura e confiável deve estar o desenvolvimento de um maior conhecimento em privacidade e em proteção de dados.	Gera um maior conhecimento e controlo sobre a informação e sobre o contexto de utilização. Diminui os riscos de desproteção da informação.
	Responsabilidade	É necessária uma cultura forte em privacidade na base de um ambiente alargado de partilha de dados.	É preponderante para a partilha de dados pois melhora a noção e perceção sobre as questões associadas à privacidade.
	Confiança	É necessário regulamentação de suporte que promova um maior conhecimento sobre segurança e sobre privacidade dos dados.	Promove uma cultura de responsabilização sobre a partilha de dados.
			Vai existir uma maior abertura à implementação de medidas de proteção da privacidade.
P2.v2. Uma cultura de privacidade é fundamental (1) à identificação e definição de situações de privacidade dentro de uma zona maior de privacidade, (2) à sua justificação e (3) à sua posterior implementação e gestão, assim como à previsão de exceções às políticas de privacidade desenvolvidas.	Sim	Localmente permitiria saber agir ou atuar perante as várias situações de privacidade.	Homogeneidade na definição e tratamento das situações de privacidade com base nas experiências positivas.
	É importante, mas carece de desenvolvimento	Existe uma dependência entre cultura de privacidade e o sucesso da privacidade.	Alinhamento daquilo que são as situações similares de privacidade entre organizações.
	Maior exigência	Atualmente a cultura existente assenta num conhecimento pouco especializado.	Fomenta uma consciência e um conhecimento sobre os riscos associados à privacidade.
	Saber agir	A privacidade deve estar no DNA das organizações e ser padronizada.	Padronização de níveis de proteção da privacidade.
	Melhor conhecimento	Deve ser promovida para a globalidade das organizações de saúde.	Conduz a uma maior exigência quanto à privacidade, evitando situações problemáticas.
		A privacidade é fundamental, é muito importante em várias fases da atividade no domínio da saúde.	São necessários sistemas de controlo que garantam a privacidade dos dados.
P2.v3. Uma cultura de privacidade é essencial à distinção dos vários tipos de privacidade, e no domínio da privacidade dos dados compreender as diferenças e dependências em relação à proteção de dados e à segurança dos dados.	Noção e perceção básicas sobre privacidade	Existe uma noção básica do que é privacidade. Normalmente muito associada à segurança.	Permite distinguir com facilidade entre os vários tipos de privacidade.
	Privacidade vista mais como segurança	A maioria dos profissionais não consegue distinguir as várias situações de privacidade.	Uniformizar a forma como as instituições lidam com situações de privacidade.
	Maior concentração de medidas ao nível da segurança	Os profissionais de saúde têm uma melhor preparação em cultura de privacidade.	Melhor preparação no sentido de as pessoas saberem como atuar em contextos de partilha de dados – padronização.
		Profissionais em gestão da informação podem facilitar este desenvolvimento.	Saberem como atuar perante contextos de privacidade, proteção e segurança, com base nas melhores práticas.
		Merece uma atenção concertada da organização.	Facilita a compreensão das medidas de segurança, do seu contexto e da sua especificação.
		Não é clara a distinção entre privacidade, proteção e segurança.	Encontrado o padrão de proteção da privacidade, facilita o conhecimento da responsabilidade individual dos profissionais e do contexto onde se movem.
		As organizações evoluíram do ponto de vista informático e não evoluíram paralelamente com a proteção de dados.	

P2.v2 – Uma cultura de privacidade é fundamental para saber agir ou atuar perante situações com requisitos distintos de privacidade. Existe uma dependência direta entre cultura de privacidade e o sucesso pretendido para a privacidade. Para o domínio da saúde, a privacidade é fundamental e importante em várias fases da atividade dos profissionais. Podem ser apontados vários aspetos que reforçam a importância de uma cultura em privacidade, nomeadamente: (1) esta conduz a uma maior exigência quanto à privacidade, evitando situações problemáticas; (2) facilita a homogeneidade na definição e tratamento das situações de privacidade com base nas experiências positivas; (3) facilita o alinhamento de situações similares de privacidade entre organizações; e (4) fomenta uma consciência e um conhecimento sobre os riscos associados à privacidade.

A privacidade deve estar no ADN das organizações e ser padronizada. A mudança de atitude, o saber agir ou atuar, o desenvolvimento de medidas de proteção ao nível local, assim como o seu alinhamento com outras organizações, dependem deste processo de mudança. A padronização dos níveis e medidas de proteção, o conhecimento das situações de privacidade e do risco envolvido, conduzem a uma maior exigência quanto à privacidade.

Contudo não chega a existência de uma cultura de privacidade. São necessários sistemas de controlo, instrumentos que garantam a privacidade dos dados.

P2.v3 – É necessário inverter o cenário atual em que a maioria dos profissionais apresenta um conhecimento insuficiente sobre privacidade, que não lhes permite com facilidade, identificar, distinguir e saber atuar perante diferentes tipos e situações de privacidade, onde se incluem os dados. Uma cultura de privacidade é, assim, fundamental à identificação e conhecimento dos diferentes tipos de privacidade, e à distinção clara do conceito de privacidade dos dados.

Apesar de existir uma preparação mínima sobre privacidade ao nível dos profissionais de saúde, na globalidade os profissionais manifestam uma dificuldade no entendimento e distinção do conceito de privacidade dos dados, em relação aos conceitos de proteção e de segurança dos dados. Normalmente a privacidade está muito associada à segurança. Mais do que a existência de um conhecimento técnico, é necessário que a cultura existente em privacidade dos dados permita aos profissionais a distinção clara destes três conceitos, e o reconhecimento da sua responsabilidade individual em relação a cada um destes níveis de proteção, tanto ao

nível local, como na sua relação com outras instituições. Desta forma, fica facilitada a otimização do compromisso organizacional no desenvolvimento das melhores práticas de gestão e utilização dos dados.

O facto de (1) o domínio da proteção de dados não ter evoluído tão significativamente como aconteceu com as TI, e (2) ao não existirem profissionais especializados em proteção e em privacidade dos dados, fez com que estas questões fossem, quando muito, contempladas no desenvolvimento dos sistemas informáticos na componente de segurança. Este facto limitou o âmbito da proteção da privacidade a medidas de natureza técnica.

5.1.3 Proposição P3. Segurança e infraestruturas

A legislação de proteção de dados em vigor (Artigos 14.º e 15.º da Lei 67/98) consagra a *segurança do tratamento* como um dos princípios mais importantes na proteção de dados, com base no qual, as organizações devem adotar medidas técnicas e organizativas adequadas aos riscos inerentes ao tratamento e à natureza dos dados. As questões da segurança são assim um assunto incontornável quando abordamos a temática da privacidade dos dados. A atual dependência tecnológica faz com que não seja possível ter privacidade na utilização dos dados sem a segurança. No entanto, este é um domínio do conhecimento muito vasto. É necessário compreender qual a colaboração necessária para que as organizações possam desenvolver e adotar medidas técnicas e organizativas de acordo com o nível de interoperabilidade implementado. Neste sentido, a terceira proposição em estudo, com a denominação *P3. Segurança e infraestruturas,* considerou elementos como a análise do risco, a identidade digital, a utilização secundária dos dados, e os planos de contingência.

Na seção 4.4.1.4 (Tabela 15) foi apresentada a estrutura para o estudo da proposição P3, constituída por cinco variáveis dependentes e nove itens como fonte de evidências.

Em termos de interoperabilidade a segurança está ligada ao atributo *compreensão* do modelo OIM, e desta forma relacionada com a capacidade de partilha de informação e conhecimento, e com o desenvolvimento de um nível de entendimento nestas questões, capazes de influenciar a capacidade de interoperabilidade. Constitui uma proposição que pensamos de elevada influência sobre a privacidade dos dados. De

acordo com a *framework* conceptual apresentada na Figura 14 (página 142), a proposição P3 apresenta uma influência direta e elevada sobre a privacidade dos dados, e encontra-se muito associada aos conceitos abordados nas proposições P2, P4, P6 e P8.

Do processo de análise sobre todos os itens de dados recolhidos no âmbito da proposição P3, resultou a matriz de análise de opinião apresentada na Tabela 28, assim como os seguintes resultados para cada uma das variáveis dependentes:

P3.v1 – A segurança física e a disponibilidade dos sistemas constituem as preocupações dominantes e que mais recursos consomem, pelo facto de as organizações dependerem cada vez mais do funcionamento em rede, na partilha de dados e serviços com outras organizações. Atendendo à criticidade dos dados partilhados no domínio da saúde, é importante que as preocupações com a segurança evoluam e incluam também a privacidade destes dados. O conhecimento dos riscos associados ao contexto da partilha de dados no domínio da segurança é, assim, um primeiro passo para que se evolua posteriormente para a proteção de dados.

A proteção da privacidade dos dados para o ambiente de colaboração e consequente partilha de serviços, depende em grande parte da colaboração entre as organizações participantes no domínio da segurança, que conduza a uma maior padronização de medidas e práticas de segurança, capaz de suportar a partilha de dados. O desenvolvimento de um domínio alargado de confiança para a partilha de dados depende desta colaboração, com efeitos práticos sobre a agilidade e eficiência da segurança, e sobre a possibilidade de rastreabilidade dos dados. A este nível, a evolução do ambiente de partilha de dados depende mais de uma interoperabilidade não técnica, do que propriamente de uma interoperabilidade técnica, já conseguida com sucesso.

É necessário dar continuidade às iniciativas estruturadas de colaboração direcionadas apenas ao domínio da segurança de infraestruturas de comunicação e armazenamento de dados, que resultaram na implementação da Rede Informática da Saúde (RIS), e na promoção de uma maior consideração das questões da segurança ao nível local.

Tabela 28 - Matriz de análise da opinião sobre P3. Segurança e infraestruturas

P3	**Matriz de análise da opinião sobre P3. Segurança e infraestruturas**		
Variáveis dependentes	*Padrão*	*Contexto/desempenho e evolução necessária*	*Relação com a privacidade dos dados*
P3.v1. A segurança de infraestruturas locais e de comunicação, a sua interoperabilidade técnica e não-técnica (a "estandardização/padronização das melhores práticas de segurança" específicas de cada sistema são essenciais ao desenvolvimento de uma plataforma segura e de confiança), são preponderantes para camadas superiores de segurança, nomeadamente a privacidade dos dados.	Colaboração/partilha Padrão/padronização Confiança Disponibilidade dos sistemas	A segurança ainda é uma lacuna. Atualmente focada apenas na disponibilidade dos sistemas.	Rastreabilidade dos dados.
		Maior interoperabilidade [não técnica] ao nível da segurança.	Controlo do acesso e segurança da informação.
		Alinhamento de medidas de segurança. Evolução da segurança para a proteção de dados.	Domínio de confiança mais alargado entre organizações.
		Maior sensibilidade em relação à privacidade dos dados.	Partilha de experiências, padronização das melhores práticas.
		Estabelecer regras de interoperabilidade.	Garantia de confidencialidade.
		Identificar os riscos existentes.	A partilha de dados entre instituições depende de uma interoperabilidade não-técnica aos níveis da segurança, da proteção de dados, protocolos de entendimento.
		Um bom plano de interoperabilidade interna, ajuda na interoperabilidade com outras instituições.	
		Uniformização dos SI.	
P3.v2. Uma análise de risco em segurança e uma análise do impacto sobre a privacidade (PIA), que englobem todos os equipamentos e situações de recolha, armazenamento, utilização e partilha de dados, são dois instrumentos decisivos para o enquadramento e conhecimento das situações problemáticas à privacidade dos dados.	Risco Infraestruturas Segurança Disponibilidade	É necessário uma análise prévia do risco para a segurança.	Os dados hoje em dia são um risco muito grande.
		É necessário promover colaboração no conhecimento do risco.	Privacidade dos dados como uma questão de risco.
		As medidas de segurança surgem de alguns *standards* e da experiência acumulada.	Uma análise de impacto sobre a privacidade minimiza o risco - reconhecimento das vulnerabilidades e do impacto do risco.
		A disponibilidade dos sistemas ainda é uma prioridade o que contribui para que a análise do risco se limite às infraestruturas.	Análise do risco no suporte à proteção dos dados.
		A análise do risco não é ainda uma prática ao nível dos SI - evolução da análise do risco para o nível da privacidade dos dados.	Suporte ao desenvolvimento integrado da segurança.
			Análise do risco como ferramenta integradora de medidas de proteção e segurança.
P3.v3. No domínio da segurança e infraestruturas, a identidade digital, os sistemas de gestão de identidade, e a confiança (federação) e interoperabilidade entre estes sistemas, são um componente essencial à gestão e monitorização da confidencialidade e privacidade dos dados.	Autenticação Sistema único Interoperabilidade	Uniformização de processos ou sistemas.	Uniformização do conceito de identidade digital.
		Partilha da identidade digital, dos mecanismos de autenticação.	Responsabilização.
		Forma única de autenticação.	Mais segurança na partilha de dados.
		Confiança entre sistemas de identidade digital no suporte à mobilidade de profissionais.	
		Uniformização das regras de autenticação.	
		Federação dos sistemas de identidade digital.	
P3.v4. A segurança em cenários de exposição de dados a ambientes vulneráveis de "não-produção" é essencial a preservação da sua privacidade. Os requisitos de privacidade dos dados nestes contextos devem cumprir com os requisitos legais.	Garantias Medidas específicas Regras específicas Risco Pouco conhecimento e experiência	A utilização secundária no geral é mais preocupante.	Contextos propícios à utilização indevida dos dados, por falta de conhecimento. Dever de confidencialidade
		Situações funcionam sem o suporte de proteção exigível.	Necessidade de preservar a identidade dos dados.
		Necessidade de repensar situações, tipos e contextos de utilização dos dados. É necessário conhecer o risco associado.	Necessidade de ajustar o nível de proteção com aquilo que é o objetivo da utilização dos dados, e a natureza dos dados.
		Definição de regras e medidas específicas e transversais – em colaboração com outras organizações.	
P3.v5. A existência de um plano de contingência para lidar com os efeitos de eventos não previstos como a perda acidental, destruição ou deterioração de dados pessoais, e tratamentos ilegais e não autorizados, contribui para anular possíveis quebras de privacidades destes dados.	Necessário Incluir os dados	Desenhados apenas ao nível da disponibilidade dos sistemas.	Reposição da confidencialidade dos dados.
		Incluir infraestruturas físicas (disponibilidade dos sistemas) e evoluir de forma a incluir os dados.	Minimização dos impactos sobre a privacidade dos dados e sobre as pessoas afetadas (visadas).
		Medidas adaptáveis ao contexto.	O risco aumenta com o valor e a qualidade dos dados.
		Devem estar associados à identificação do risco.	
		Necessário desenvolver mecanismos de identificação da utilização indevida dos dados.	

P3.v2 – A existência e o conhecimento do risco ainda está muito associado à segurança física e à disponibilidade das infraestruturas, e apesar de reconhecida a sua importância, a análise do risco ainda não é uma prática regular e estruturada nas organizações.

Falta experiência e preparação a este nível, assim como na análise de impacto sobre a privacidade. As medidas de segurança são desenvolvidas com base na utilização de alguns *standards* e na experiência acumulada pelos técnicos.

Quando abordado o tema da análise do risco, as opiniões convergem ao considerarem necessário, que a análise do risco para a segurança dos SI evolua por forma a incluir a privacidade dos dados, e que seja realizada uma análise prévia do impacto sobre a privacidade de novas soluções para os SI, como instrumentos fundamentais ao conhecimento do risco associado às várias situações de privacidade dos dados. Desta forma, a privacidade dos dados seria vista como uma questão de risco, que exige que as organizações promovam a colaboração necessária para a identificação e alinhamento de medidas de proteção face aos riscos conhecidos. Pode constituir o ponto de partida para o desenvolvimento conjunto de um programa de proteção da privacidade dos dados.

P3.v3 – A identidade digital é um componente necessário e preponderante para o desenvolvimento de um ambiente seguro de partilha de dados e para a disponibilização de informação que permita responsabilizar os utilizadores em situações de quebras de privacidade. No sentido de suportar os desafios que o ambiente de colaboração coloca ao nível da privacidade dos dados recolhidos, e também a outros níveis, surgem os seguintes requisitos para o domínio da identidade digital:

a. É importante alterar o cenário atual no qual um profissional utiliza credenciais e métodos de autenticação distintos entre aplicações, quer ao nível local, quer na sua colaboração com outras organizações. Existem já algumas experiências positivas de interoperabilidade entre aplicações ao nível da autenticação dos utilizadores. Contudo, alguns dos sistemas em funcionamento nem sequer permitem esta interoperabilidade.
b. É fundamental uma maior colaboração (quer técnica, quer organizacional) que suporte a evolução dos sistemas de controlo da identidade digital. Pode ser implementado um sistema único alargado a várias organizações, que suporte

todos os processos de autenticação, ou pode fazer-se evoluir os sistemas atuais para uma federação, mantendo-se a independência dos sistemas locais de autenticação, mas promovendo-se uma maior confiança (através de interoperabilidade) entre os sistemas instalados.

c. É muito importante que se consiga obter uma visão agregada da atividade de utilização de dados por parte de um utilizador no interior da organização, assim como conhecer a utilização dos dados quando estes são partilhados com outras organizações (rastreabilidade dos dados). A partilha de dados da identidade digital do utilizador deve estar na base do desenvolvimento deste requisito.

A identidade digital é um conceito complexo, mas essencial ao futuro da proteção de dados, tanto a nível local como em contextos de partilha de dados entre organizações, apesar de normalmente limitada às questões técnicas de autenticação e acesso à informação e aos sistemas. Contudo, a mobilidade de profissionais e de dados coloca grandes desafios a este nível, nomeadamente quanto à uniformização do conceito de identidade digital (aquilo que carateriza um utilizador) e dos sistemas e tecnologias de suporte (formas e políticas de autenticação).

P3.v4 – As situações de utilização secundária dos dados, também denominadas de reutilização dos dados, são mais propícias à utilização indevida dos dados do que as situações de utilização primária. Esta situação é explicada pela falta de conhecimentos em proteção de dados, pela falta de regulamentação e de princípios, e consequentemente sem o suporte de proteção exigível. A atenção dada a estes cenários de utilização de dados ainda é residual, comparada com a atenção dada à utilização primária.

Face à exigência de privacidade destes cenários de utilização dos dados, é necessário repensar estas situações e contextos de utilização, conhecer o seu risco, e promover a definição de regras e medidas específicas para a utilização e para a proteção dos dados, transversais a todas as organizações. As organizações devem desenvolver soluções que permitam ajustar o nível de proteção com aquilo que é o objetivo da utilização secundária dos dados, e a natureza destes dados. A proteção em situações de reutilização dos dados deve adaptar-se (1) às situações de utilização secundária que podem apresentar benefícios para o utente em causa, sobre as quais deve ter conhecimento, e nas quais os seus dados não podem ser anonimizados, e (2) às

situações em que a identificação do utente obrigatoriamente tem que ser retirada dos dados, dado que não existe um benefício direto para o utente.

Existe uma forte convicção de que a legislação tem que acompanhar aquilo que são as necessidades de reutilização dos dados e que resultam muito dos benefícios da evolução tecnológica, e promover a sua utilização de uma forma responsável.

P3.v5 – É possível e importante que o desenvolvimento de planos de contingência, atualmente mais focados na disponibilidade dos sistemas informáticos, inclua também as situações de utilização dos dados, com o objetivo de atuar perante situações comprometedoras para a sua privacidade.

É necessário que estes planos sejam desenhados de acordo com o contexto de utilização, a criticidade dos dados, e com os riscos identificados. Por outro lado, a existência de mecanismos de controlo para a privacidade dos dados, para situações de quebras de confidencialidade ou outras situações de utilização indevida dos dados, são determinantes à ativação de um plano de continência. Estes planos devem assim contemplar medidas que permitam a reposição da confidencialidade dos dados afetados, e a minimização de possíveis impactos negativos sobre as pessoas afetadas.

5.1.4 Proposição P4. Linguagem de privacidade (taxonomia)

Quando se pretende abordar questões relacionadas com a privacidade, seja numa vertente técnica ou organizacional, a terminologia existente é ainda muito limitada e não contribui para a objetividade necessária para estas questões. Provavelmente o termo "*consentimento*" constitui o termo mais conhecido e mais utilizado, e mesmo este levanta muitas dúvidas quanto à sua implementação. O facto de não existirem padrões globalmente aceites em privacidade, pode estar a condicionar a atenção necessária das organizações para com estas questões. Os benefícios para a privacidade dos dados com o desenvolvimento de uma taxonomia serão semelhantes aos obtidos com a utilização de *standards* nos domínios da segurança, das bases de dados, das redes de comunicação, entre outros.

É neste sentido que se pretende, com base na proposição *P4. Linguagem de privacidade (taxonomia)*, compreender quais os benefícios que se podem obter e quais as dificuldades que se podem eliminar, com a utilização de uma taxonomia para

a privacidade dos dados no suporte à colaboração entre organizações, a par de outras taxonomias no domínio dos SI.

Na seção 4.4.1.4 (Tabela 16) foram apresentadas as duas variáveis dependentes e os dois itens como fonte de evidências, que constituem a estrutura para o estudo da proposição P4.

Em termos de interoperabilidade, a proposição P4 está ligada ao atributo *compreensão* do modelo OIM, e desta forma relacionada com a capacidade das organizações na partilha de informação e conhecimento, e com o desenvolvimento de um nível de entendimento nestas questões, capazes de influenciar a capacidade de interoperabilidade. É uma proposição que apresenta uma influência indireta e tem um menor peso sobre a privacidade dos dados, muito relacionada com as proposições P3 e P6, como representado na *framework* conceptual apresentada na Figura 14 (página 142).

Do processo de análise sobre todos os itens de dados recolhidos no âmbito da proposição P4, resultou a matriz de análise de opinião apresentada na Tabela 29, assim como os seguintes resultados para cada uma das variáveis dependentes:

P4.v1 – A existência de uma taxonomia para o domínio da privacidade dos dados, vista como um conjunto de termos unificadores, um glossário, um vocabulário em privacidade, permitiria resolver muitas das dificuldades na abordagem das questões da privacidade dos dados. Dada a imaturidade no desenvolvimento destas questões (da privacidade dos dados) em todas as organizações, permitiria num primeiro momento diminuir a dificuldade na definição e compreensão das questões da privacidade, atendendo àquilo que são os requisitos da legislação. Teríamos desta forma, uma maior facilidade no processo de diálogo entre profissionais, no desenho e execução de políticas de proteção e na sensibilização de toda a organização. Funcionaria como um padrão, um modelo, uma orientação para as organizações.

Por outro lado, uma taxonomia ajudaria os profissionais a distinguir os diferentes tipos de privacidade, a identificar e caracterizar as situações de privacidade para as quais é necessário o desenho ágil, integrado e objetivo de medidas de proteção.

Na prática pode contribuir para a objetividade e compreensão necessárias das questões da privacidade, e facilitaria o desenvolvimento de processos de monitorização, planos de contingência ou de segurança orientados aos dados.

Tabela 29 - Matriz de análise da opinião sobre P4. Linguagem de privacidade (taxonomia)

P4	**Matriz de análise da opinião sobre P4. Linguagem de privacidade (taxonomia)**		
Variáveis dependentes	*Padrão encontrado*	*Uma taxonomia partilhada como ferramenta de suporte* *(É necessário desenvolver uma taxonomia de suporte ao desenvolvimento de medidas de proteção da privacidade dos dados)*	Benefícios para a privacidade dos dados *(Aspetos que podem ser beneficiados na gestão da privacidade dos dados dentro da organização e para o contexto da colaboração)*
P4.v1. Uma linguagem ou taxonomia comum de suporte à definição, justificação e gestão de zonas e situações de privacidade constitui um auxiliar importante para analisar de uma forma clara e inequívoca as questões da privacidade tanto no interior de uma organização como na sua integração com outras organizações.	Terminologia Facilitava/facilitador Noção de privacidade Segurança Dados Agilidade	Taxonomia vista como um conjunto de termos unificadores, um glossário, um vocabulário em privacidade. Reconhecida a importância, utilidade e urgência do seu desenvolvimento. Facilitava a definição e compreensão do problema que é a privacidade dos dados. À semelhança das taxonomias em segurança, seria vantajoso a sua aplicação à privacidade dos dados. Uma linguagem comum, partilhada, de tradução das exigências da legislação. Mais fácil de caracterizar as situações de privacidade. Deve abranger os dados, e a sua classificação.	Facilita o processo de diálogo entre profissionais. Facilitava o desenho de políticas de privacidade e a execução de medidas de proteção. Funcionaria como um padrão, um modelo, uma orientação para as organizações. Maior facilidade na distinção dos diferentes tipos de privacidade. Maior agilidade na identificação e resolução de problemas. Maior objetividade e compreensão das questões da privacidade. Facilitador na caracterização do contexto, de um método de proteção, de um plano de contingência ou de segurança.
P4.v2. Uma linguagem comum de privacidade promove uma maior agilidade na definição de políticas de privacidade, no desenvolvimento de mecanismos de controlo de conformidade (P5), e na sua integração com situações similares em outras organizações.	Suporte na definição Facilitar a colaboração Agilizar	Deve ser uma terminologia global, partilhada e conhecida por todas as partes e entre as organizações. Facilita o trabalho dos profissionais de segurança. Facilita o trabalho conjunto de colaboração, de interoperabilidade.	Facilita a implementação e o alinhamento de medidas para as situações de partilha de dados. Permite uma padronização das melhores medidas e das melhores práticas. Permite agilizar as medidas de proteção para as situações de partilha de dados. Facilita o desenho de regras de utilização dos dados. Melhora a segurança dos dados partilhados.

P4.v2 – Podemos obter benefícios práticos muito importantes, com a existência de uma taxonomia comum e conhecida por todas as partes participantes, na implementação da interoperabilidade necessária ao desenvolvimento de um ambiente de partilha de dados. A facilidade e agilidade conseguidas na colaboração entre profissionais e uma melhoria na segurança dos dados partilhados são os benefícios mais evidentes.

Uma terminologia é desta forma fundamental no suporte à definição e distinção dos aspetos da privacidade dos dados, e estando integrada com uma nomenclatura de classificação dos dados, pode facilitar a definição de regras de utilização dos dados, quer localmente quer em situações de partilha de dados. Pode desta forma, contribuir para uma maior agilidade na definição, no alinhamento, na implementação e no controlo de medidas de proteção da privacidade dos dados entre todas as organizações. Podem, com base nesta taxonomia ser padronizadas com maior facilidade as melhores práticas ao nível da privacidade dos dados.

Uma taxonomia pode contribuir de uma forma significativa para se alterar, por um lado, o fraco desenvolvimento tanto de medidas de proteção como de mecanismos de controlo da privacidade, e por outro, a ideia errada que os aspetos da privacidade dos dados são do âmbito da segurança.

5.1.5 Proposição P5. *Accountability* – responsabilidade e conformidade

A sociedade exige cada vez mais às organizações um compromisso e uma maior responsabilidade na utilização correta e segura dos dados pessoais. Perante sistemas tão complexos como os da área da saúde, tanto os responsáveis pelos SI, como pela gestão executiva da organização, reconhecem a dificuldade que têm na definição do ponto de partida que lhes permita iniciar os trabalhos adequados à problemática da privacidade dos dados. Um programa de responsabilidade pode constituir este ponto de partida. Este não redefine o conceito de privacidade nem substitui a legislação em vigor, mas desloca o foco da gestão da privacidade para a organização e para a sua capacidade em definir e implementar objetivos para a utilização correta dos dados.

Esta quinta proposição, com a designação *P5. Accountability – responsabilidade e conformidade*, pretende assim analisar qual a importância atribuída pelos vários responsáveis da organização à ativação desta ferramenta operacional, no suporte à

implementação de um ciclo contínuo de desenvolvimento das questões da privacidade dos dados, e no suporte à colaboração com outras organizações.

Na seção 4.4.1.4 (Tabela 17) foram apresentadas as quatro variáveis dependentes e os seis itens como fonte de evidências, que constituem a estrutura para o estudo da proposição P5.

Em termos de interoperabilidade, a proposição P5 está ligada ao atributo *compreensão* do modelo OIM, e desta forma relacionada com a capacidade de partilha de informação e conhecimento, e com o desenvolvimento de um nível de entendimento nestas questões, capazes de influenciar a capacidade de interoperabilidade. Constitui uma proposição que pensamos de elevada e direta influência sobre a privacidade dos dados, e de acordo com a *framework* conceptual apresentada da Figura 14 (página 142), com influência sobre as questões abordadas nas proposições P1, P6 e P10.

Do processo de análise sobre todos os itens de dados recolhidos no âmbito da proposição P5, resultou a matriz de análise de opinião apresentada na Tabela 30, assim como os seguintes resultados para cada uma das variáveis dependentes:

P5.v1 – A elaboração de um programa de responsabilidade que contemple medidas que ponham em prática as obrigações e princípios da legislação em proteção de dados, pode contribuir para que se passe da teoria à prática no domínio da privacidade dos dados. A atitude das organizações em relação à proteção de dados não é proativa, mas reativa perante situações comprometedoras que suscitem dúvidas quanto à forma de recolha e utilização dos dados. A mudança de atitude da organização pode ser iniciada através do desenvolvimento de um programa de responsabilidade, e apresentar as principais diretrizes para o desenvolvimento de um programa de proteção de dados. Ou seja, este princípio da responsabilidade pode funcionar como um catalisador para as questões da privacidade dos dados.

Não existe nas organizações uma noção clara do que é a proteção de dados, nem da importância da privacidade dos dados recolhidos. A preparação das organizações [P1] é insuficiente. É necessário alterar a consciência interna do problema, por forma a fomentar ou agilizar medidas concretas de uma maior responsabilidade.

Tabela 30 - Matriz de análise da opinião sobre P5. *Accountability* – responsabilidade e conformidade

P5	**Matriz de análise da opinião sobre P5. *Accountability* – responsabilidade e conformidade**		
Variáveis dependentes	*Padrão encontrado*	*Atitude proativa da instituição* *(Que ferramentas podem influenciar a atitude e o compromisso da organização em relação à privacidade dos dados)*	*Influência sobre a privacidade* *(Que aspetos da privacidade dos dados são influenciados por uma atitude proativa e são interoperáveis)*
P5.v1. Um programa de responsabilidade sólido e transparente, que contemple medidas adequadas e eficazes para pôr em prática as obrigações e princípios da legislação em vigor sobre proteção de dados, constitui a ferramenta operacional necessária para as questões da privacidade.	Utilidade/útil/confiança Diretrizes Proativa Nível executivo/tutela Equipa multidisciplinar Iniciativa conjunta	Não existe esta atitude de responsabilidade. Deveria haver uma atitude proativa em matérias de proteção de dados. Um programa destes poderia apresentar as principais diretrizes, que podem ser materializadas em medidas e políticas de privacidade. Este princípio da responsabilidade pode funcionar como um catalisador para estas matérias.	A privacidade é uma questão tão técnica como de gestão. Poderá haver um alinhamento dos grandes princípios de privacidade entre instituições. Pode ser uma iniciativa individual ou conjunta de todas as organizações para dar resultado. Promover mais a colaboração entre as instituições com base nas suas experiências - a elaboração de políticas de privacidade com base na experiência de múltiplos locais.
P5.v2. Um programa de conformidade constitui o meio de demonstração da vontade e da capacidade da organização em ser responsável e responsabilizada pelas práticas de gestão de dados. É essencial à salvaguarda da privacidade de dados, assim como à confiança do titular dos dados na organização, e entre esta e outras organizações. A eficácia e exigência das tarefas de conformidade dependem da sensibilidade dos dados, do volume dos dados processados e dos riscos específicos identificados.	Ferramenta [aplicável à privacidade dos dados] Análise contínua Auditoria/auditar Criticidade dos dados Exposição dos dados Risco Impacto Confiança Garantias	É possível, e desejável, fazer esta análise contínua de conformidade - perceber se as nossas ferramentas, processos estão de acordo com a legislação. Deveria ser uma prática comum para a proteção de dados - seria uma ferramenta fundamental. Auditar-se regularmente aquilo que é a utilização dos dados, à semelhança da segurança seria vantajoso. Dados mais sensíveis, mais críticos obrigam a uma maior preocupação. É importante a publicação deste tipo de análises e resultados em relação à proteção de dados.	À semelhança do que já se faz com os testes de robustez para as infraestruturas, deveria pensar-se em algo semelhante para os dados, para a sua proteção. O conhecimento de todos os processos de recolha e tratamento de dados é uma boa base de atuação. Se percebermos quais são os riscos em termos de informação, podemos depois verificar regularmente se estamos a conseguir eliminar o risco. Cenários de partilha de dados também deveriam ser auditados com mais frequência. A transparência da proteção de dados gera confiança no titular dos dados e entre organizações.
P5.v3. Os sistemas de *accountability* são essenciais à confidencialidade dos dados, ao disponibilizarem provas de evidência que permitem atribuir responsabilidade a comportamentos não esperados no domínio da privacidade dos dados.	Prova de evidência Prova de utilização	O *accountability* é quase sempre realizado de uma forma isolada. Estes sistemas são importantes para o contexto de partilha de dados, ao produzirem prova da utilização de dados. São uma garantia de que os dados estão a ser utilizados de forma correta.	Estes sistemas têm que de uma forma transversal acompanhar os dados, rastrear os dados, mesmo para lá do nosso sistema. Saber quem é que no outro sistema acedeu e alterou os dados. Se queremos ter partilha de dados, estes sistemas têm que funcionar integrados - tem que haver uma interoperabilidade técnica ao nível destes sistemas.
P5.v4. O desenvolvimento de rótulos de qualidade (esquema de certificação) para as medidas adotadas para uma gestão eficiente da conformidade legal, proteção e segurança dos dados, são no futuro uma ferramenta essencial ao desenvolvimento de um ambiente de interoperabilidade confiável e seguro em matérias de privacidade dos dados.	Garantia/mais-valia Confiança Complexo de implementar	Esta certificação seria uma mais-valia, uma garantia à existência de menos falhas na segurança dos dados. Tem que ser mais transversal e focada nos dados. Para garantir a certificação vou ter que garantir conformidade com todas as normas existentes. Devemos apontar para a certificação mas de uma forma discreta. A certificação deve ser vista mais como a garantia do funcionamento correto da proteção de dados. O custo e a complexidade dos sistemas podem condicionar o âmbito pretendido para este processo.	Estes processos têm a vantagem de colocar todas as estruturas de uma organização, a conversar, a definir processos comuns, procedimentos comuns. Ao nível do Ministério da Saúde, havendo um conjunto de regras, é fácil a este Ministério proceder a esta certificação. A certificação aumentaria a confiança entre as organizações, ao nível da partilha de informação. Tem que se circunscrever muito bem o âmbito para a certificação.

Não existe um padrão quanto ao sucesso de um programa de responsabilidade. Por um lado acredita-se que uma instituição de forma isolada consegue implementar um programa desta natureza e obter sucesso nas medidas adotadas, por outro este sucesso está condicionado ao desenvolvimento simultâneo de um programa de responsabilidade em todas as instituições que trabalhem para o mesmo propósito – os cuidados de saúde.

Quanto à forma de implementação, a opinião é convergente no sentido em que esta deve surgir da iniciativa e compromisso no nível executivo, ao nível do conselho de administração. A privacidade é uma questão tão técnica como de gestão. A sua operacionalização depende da formação de uma equipa multidisciplinar, que inclua profissionais de SI, profissionais de saúde e conhecedores da legislação (juristas).

A colaboração entre organizações deve contribuir para o alinhamento de diretrizes, assim como dos principais princípios de proteção de dados, que devem suportar o âmbito alargado de partilha de dados e estar na base de um programa de responsabilidade – é sem dúvida um domínio com elevada potencialidade de interoperabilidade.

P5.v2 – A análise de conformidade, atualmente já aplicada aos SI (muito baseada na norma ISO/EIC 27001) e muito limitada às questões técnicas de segurança física, é apontada como a ferramenta correta para que se possa avaliar, de uma forma contínua, a conformidade das situações de utilização de dados em relação aos requisitos de proteção aplicados. Verificar se tanto aplicações como processos estão de acordo com os requisitos da legislação. É opinião firme que esta análise deve evoluir e contemplar os dados, de modo a avaliar as medidas de proteção e de privacidade em vigor. Ainda não se olha para os dados com a atenção e rigor que estes merecem. A análise da conformidade das políticas de proteção dos dados e consequente privacidade deverá ser uma prática regular, contínua, adaptada ao nível de proteção exigível, assim como aos contextos de utilização e de partilha de dados.

Com base num processo de avaliação contínua é possível verificar a conformidade das medidas ativadas face aos requisitos da legislação, avaliar o cumprimento destas medidas, avaliar os riscos identificados, e conhecer as situações regulares de exposição dos dados, quer internamente quer para o exterior da organização. Na base deste processo deve estar um conhecimento de todos os processos de recolha, utilização e exposição dos dados [tratamento].

A sensibilidade e a criticidade dos dados são o fator primordial na definição do nível de exigência, prioridade e periodicidade para um processo de análise de conformidade. Áreas críticas em relação à informação, neste caso em suporte digital, em que o impacto causado pela violação da privacidade dos dados é maior, devem ser prioritárias. Uma análise do risco deve estar na base do conhecimento do impacto sobre a privacidade dos dados, e na definição do ciclo de proteção.

As situações de partilha de dados estão a gerar preocupação, podendo mesmo falar-se em desconfiança, mais acentuada quando os dados são partilhados com outras organizações. As garantias existentes de proteção são insuficientes. Havendo resultados concretos sobre os processos de análise de conformidade, a sua publicação ou conhecimento público (o qual deve acontecer de uma forma cautelosa), pode ter um impacto bastante positivo sobre a confiança dos profissionais, do titular dos dados para com determinada organização, e não menos importante na confiança entre organizações.

P5.v3 – É necessário uma evolução nos sistemas de *accountability*, por forma a não condicionarem os desafios que resultam do ambiente em crescimento de partilha de dados. As situações de partilha de dados, obrigatoriamente, devem ser suportadas por sistemas de *accountability* capazes de monitorizar e registar (de acordo com o nível de detalhe acordado) todas as ações realizadas sobre os dados, e em simultâneo interoperar tecnicamente com sistemas similares, para que seja viável o controlo sobre os dados quando estes são enviados para um outro sistema, ou seja, rastrear os dados.

O registo atual da atividade dos utilizadores está mais direcionado para a monitorização do acesso aos serviços (aplicações) e às infraestruturas, e apenas as aplicações mais recentes incluem a utilização dos dados, permitindo saber quem acedeu, de onde acedeu e/ou que ações realizou sobre os dados. Contudo, este controlo acontece apenas de uma forma isolada, limitado ao âmbito de funcionamento das aplicações, e com um nível de detalhe diferente de aplicação para aplicação. Aplicações mais antigas não registam sequer a atividade dos seus utilizadores. Esta é uma atividade para a qual é necessária uma visão integrada de todo o sistema de informação.

P5.v4 – A preparação global em proteção de dados é insuficiente, quando comparada com a preparação em segurança, fruto de uma maior experiência acumulada a este

nível, mas ainda longe da ideal. É necessário um processo de mudança, uma mudança na atitude e compromisso das organizações para com a proteção e a privacidade dos dados. Um programa de responsabilidade pode gerar esta mudança, ao apresentar as principais diretrizes que permitam um posicionamento responsável nas práticas de gestão de dados. Posteriormente, um programa de conformidade pode avaliar a eficácia e o cumprimento das medidas de proteção aplicadas e promover as melhorias de correção necessárias.

A certificação é o passo seguinte, contribuindo para a adoção de rótulos de qualidade. Auditar a proteção de dados, significa caminhar para a normalização das medidas e políticas de proteção, e neste sentido é uma mais-valia, uma garantia de um maior rigor para com a gestão dos dados. Processos desta natureza têm a vantagem de colocar todas as estruturas de uma organização a dialogar, a definir processos e procedimentos comuns.

A confiança entre organizações (P8), fundamental ao desenvolvimento de um ambiente confiável de partilha de dados, aumenta, fruto do impacto positivo que a certificação apresenta. No entanto, o custo e a complexidade deste processo, aliados com a insuficiente preparação técnica dos profissionais, apontam para a necessidade de circunscrever bem o âmbito para a certificação. Deve-se apontar para a certificação mas de uma forma discreta, não devendo ser vista como garantia do funcionamento correto da proteção de dados.

5.1.6 Proposição P6. Dados e manipulação de dados

As organizações estão cada vez mais conscientes que o estado dos seus ativos na forma de dados, apesar dos elevados investimentos em TI, se tem deteriorado. O facto de não se gerirem os dados como um bem da organização, e ao não existirem profissionais dedicados a estas funções, explica em parte a situação problemática que se está a instalar nas organizações. Os dados são cada vez mais um recurso crítico, tal como o são as infraestruturas tecnológicas, os recursos financeiros, os edifícios e as pessoas, mas nem todos os dados apresentam os mesmos requisitos de segurança e de privacidade. O conhecimento do seu valor e do risco associado à sua utilização permitem compreender a importância destes na continuidade da atividade de uma organização.

A proposição *P6. Dados e manipulação de dados*, focada na principal justificação deste estudo – os dados em contextos de interoperabilidade, tem por objetivo a análise de quatro aspetos/questões com forte influência sobre a privacidade dos dados, e interoperáveis com base na colaboração entre as organizações. São questões em que a privacidade é relacionada com o ciclo de vida dos dados, a gestão da informação, as nomenclaturas de classificação, e a dependência das decisões ao nível da proteção dos dados. Na seção 4.4.1.4 (Tabela 19) foram apresentadas as quatro variáveis dependentes formuladas, assim como os seis itens de ligação com as fontes de evidências, que constituem a estrutura para o estudo desta proposição.

Esta é uma proposição que perspetivamos está relacionada com as proposições P3 e P4, com uma influência direta sobre a privacidade dos dados, mas inferior em relação a outras proposições, como representado na *framework* conceptual da Figura 14 (página 142). Em termos de interoperabilidade a proposição P6 está incluída no atributo *compreensão* do modelo OIM, e desta forma relacionada com a capacidade de partilha de informação e conhecimento, e com o desenvolvimento de um nível de entendimento nestas questões, capazes de influenciar a capacidade de interoperabilidade.

Do processo de análise sobre todos os itens de dados recolhidos no âmbito da proposição P6, resultou a matriz de análise de opinião apresentada na Tabela 31, assim como os seguintes resultados para cada uma das variáveis dependentes:

P6.V1 – As organizações apresentam um conhecimento insuficiente sobre as limitações que existem na recolha, utilização, partilha e retenção de dados, quer no interior das fronteiras dos seus SI, quer no ambiente de partilha de dados com outras organizações. Na área da saúde, as organizações, com situações muito similares de utilização de dados, estão cada vez mais confrontadas com a necessidade de armazenar um maior e mais diversificado volume de dados, e com uma multiutilização cada vez mais intensiva dos dados. O incentivo à gestão da informação e à sua proteção não acompanha o incentivo à recolha do maior volume possível de dados. Desta forma, o conhecimento e o trabalho ao nível dos dados são muito diferenciados entre organizações e nitidamente insuficiente.

Tabela 31 - Matriz de análise da opinião sobre P6. Dados e manipulação de dados

P6	**Matriz de análise da opinião sobre P6. Dados e manipulação de dados**		
Variáveis dependentes	*Padrão encontrado*	*Suporte ao conhecimento sobre os dados* *(Que ferramentas e conhecimentos a desenvolver no domínio dos dados)*	*Desenvolvimento através da colaboração* *(itens ou questões com potencialidade de interoperabilidade)*
P6.v1. À semelhança da proteção de dados, a privacidade de dados deve ser preocupação constante durante todo o ciclo de vida dos dados em ambientes de interoperabilidade.	Conhecimento insuficiente Falta de informação Medidas específicas	O conhecimento sobre as limitações da utilização dos dados é insuficiente. As limitações não estão presentes. É necessário uma maior preparação organizacional sobre a gestão dos dados - ausência de proatividade. Aprofundar o conhecimento (atualmente insuficiente) sobre os limites na utilização dos dados e os riscos associados. Profissionais especializados para o suporte à proteção de dados. Existe um maior conhecimento das fases de criação e utilização dos dados. A transferência de dados está a apresentar grandes desafios e preocupações.	Definição de direitos e obrigações e as melhores práticas de utilização de dados. Desenvolvimento da gestão da informação. Conhecimento partilhado sobre o funcionamento dos processos de partilha de dados entre organizações. Alinhamento de medidas de proteção para situações de transferência de dados/partilha de dados. Apresentar medidas específicas para todo o ciclo de vida dos dados. Diretrizes de arquivo e armazenamento de dados.
P6.v2. A existência de procedimentos para analisar o tipo e quantidade de dados pessoais recolhidos (a sua adequação e relevância) em relação ao(s) objetivo(s) definido(s), o seu período de retenção (não mais que o necessário), assim como a transparência, clarificação e publicação destes procedimentos são essenciais à compreensão e definição de medidas de proteção da privacidade dos dados.	Gestão da informação Responsabilidade Facilita, útil	Somente com uma maior experiência e conhecimento ao nível dos dados é possível implementar políticas de privacidade que sejam facilmente compreendidas. No meio da saúde, se se pretende implementar políticas rigorosas de privacidade é exigível às pessoas que conheçam o objetivo para que se está a recolher os dados. É importante, útil, vantajoso, existir um maior conhecimento e informação sobre os dados, o objetivo da sua recolha. A organização da informação é um ponto de partida. É necessário documentar todos os processos. Ajustar a proteção de dados à criticidade de cada processo. A maturidade ao nível da gestão da informação é fundamental.	Desenvolvimento de princípios orientadores para as organizações com processos comuns de recolha de dados. Desenvolvimento das melhores práticas de documentação do objetivo do processo de recolha de dados, dos detalhes dos dados, das limitações de utilização, das consequências da má utilização dos dados. Criar condições para a demonstração do compromisso para com a proteção de dados e para a realização de auditorias. Desenvolvimento da gestão da informação no suporte ao conhecimento sobre os dados, os processos, e no desenvolvimento conjunto de políticas de proteção. Preparar profissionais em gestão da informação.
P6.v3. A classificação, dinâmica (durante todo o seu ciclo de vida), dos dados é essencial à definição dos níveis de proteção e privacidade pretendidos, assim como os domínios onde pode circular, isto é dentro da organização e entre organizações.	Padrão/*standard* Acesso aos dados Gestão da informação	Faz sentido um padrão, uma nomenclatura de classificação dos dados – facilita o desenvolvimento e aplicação de políticas de privacidade. Neste momento o acesso aos dados é apenas controlado com base no perfil de utilizador. Facilita o conhecimento da criticidade, sensibilidade, disponibilidade e risco associado aos dados. Nomenclatura de classificação para todo o ciclo de vida.	Desenvolvimento ou adaptação de um *standard* para a classificação dos dados. Uniformização das medidas de proteção para os processos de partilha de dados. Alinhamento das políticas de partilha de dados. Garantir que a classificação de dados não se altera quando estes são partilhados entre sistemas.
P6.v4. A privacidade dos dados depende diretamente (1) do âmbito, (2) das tecnologias aplicadas e (3) dos *standards* usados da/na proteção de dados, implementados localmente e em ambientes de interoperabilidade. Quanto mais granular melhor. Quanto mais interoperáveis melhor.	Uniformização tecnológica *Standard* Proteção centrada nos dados	Uma harmonização tecnológica, integridade tecnológica podem facilitar a proteção de dados. É necessário regularizar a evolução tenológica. A estruturação dos dados e a organização da informação, são um fator de maior importância. São necessários padrões/standards no suporte à classificação dos dados, das melhores práticas de segurança e do funcionamento da interoperabilidade.	Definição de objetivos comuns para a privacidade dos dados. Definição nos padrões de suporte ao programa de proteção de dados. Desenvolvimento de estruturas de dados (Ex: conceito de processo clinico eletrónico). Meios humanos especializados em proteção de dados, capazes de fomentar uma proteção mais centrada nos dados. É necessário que as pessoas não contornem o risco.

É necessário que as organizações entendam os limites quanto à utilização dos dados, assim como os dados que podem, devem e estão obrigadas a partilhar. Esta falta de consciência em relação a estes limites pode resultar no uso ou exposição indevida de dados.

A partilha de dados entre organizações (que deu um passo significativo com a implementação a nível nacional da PDS) provocou uma maior atenção em relação a estas questões. Esta atenção crescente para com os dados, exige a disponibilidade de informação que promova a sua correta utilização, tendo em conta o tipo de dados envolvidos e o contexto de utilização.

Este contexto problemático é muito justificado pela não existência nas organizações de profissionais ou de estruturas especializadas que possam promover um programa em privacidade com qualidade ao nível dos dados, do seu conhecimento, da sua estrutura e posteriormente da sua proteção.

Existe a perceção de que os dados têm um ciclo de vida, com cada uma das fases a justificar medidas específicas que assegurem a sua privacidade. Atuar ou concentrar recursos apenas em algumas fases, pode comprometer a privacidade nas fases não asseguradas. O conceito de privacidade, no que diz respeito à exposição incorreta de dados está muito relacionado com as fases de criação e utilização de dados. Por seu lado as fases de armazenamento, transferência, arquivo e destruição estão mais relacionadas com medidas de segurança.

Sem dúvida que as fases de criação e utilização dos dados concentram as maiores preocupações. A transferência de dados, incrementada com a implementação da PDS, e devido à maior exposição dos dados, exige no curto prazo uma visão integrada para o conjunto das organizações. Em simultâneo, a intenção de disponibilizar eternamente os dados com interesse clínico, está a revelar-se crítica para os sistemas de armazenamento sobrecarregados de dados. Dado que a gestão da informação não está a contemplar o arquivo e a destruição deste tipo de dados, dificilmente se podem desenvolver políticas de privacidade. A orientação e o desenvolvimento de diretrizes de arquivo e destruição de dados podem surgir da colaboração entre organizações.

P6.V2 – Para a área da saúde, a implementação de políticas de privacidade dos dados está diretamente dependente do nível de conhecimento e informação existentes sobre os processos que envolvam dados pessoais. Se se pretende implementar políticas rigorosas de privacidade, é exigível às pessoas que conheçam o

objetivo para que se está a recolher os dados, isto porque as organizações estão a estruturar e armazenar maiores volumes de dados, e a investirem em meios que aumentam a sua disponibilidade. Estes processos não estão a ser estruturados com base numa avaliação prévia da sua viabilidade no que diz respeito à recolha e utilização dos dados, de acordo com os requisitos da legislação em vigor. Tanto o objetivo, como o destino da utilização destes dados são pouco questionados e documentados.

É importante, útil e vantajoso, existir um maior conhecimento e informação sobre os dados e sobre o objetivo da sua recolha. A organização da informação é um ponto de partida, uma vez que permite documentar todos os processos, e desta forma ajustar a proteção de dados à sua criticidade. Para o ambiente de partilha de dados é fundamental que da colaboração entre as organizações surjam princípios orientadores e a definição das melhores práticas de documentação do objetivo dos processos de recolha de dados, dos detalhes dos dados, das limitações de utilização e das consequências de má utilização dos dados. Desta forma, é possível criar condições para a demonstração do compromisso da organização para com a proteção de dados, e para a realização de auditorias.

A maturidade ao nível da gestão da informação é apontada como fundamental, para um maior conhecimento sobre os dados e sobre os processos, e para o desenvolvimento conjunto de políticas de proteção de dados. É necessário que existam profissionais com preparação adequada em gestão da informação.

P6.V3 – Uma nomenclatura de classificação dos dados, ao permitir a classificação dos dados durante o seu ciclo de vida vai facilitar a definição e aplicação de medidas de proteção e de segurança, orientadas aos dados. Semelhante a um padrão, pode resultar da adaptação de um *standard* publicado ou desenvolvido pelas organizações. Desta forma é possível assegurar que o significado atribuído aos dados será semelhante quando partilhado ou transferido entre sistemas dentro da organização, e entre sistemas de organizações diferentes. A implementação de mecanismos de controlo da privacidade no universo da saúde, passa muito por conhecer que dados podem ser consultados, por que profissionais e em que contexto. O acesso aos dados é realizado preferencialmente com base no perfil profissional e numa classificação muito macro dos dados, que difere entre aplicações.

O desenvolvimento de uma nomenclatura para a classificação dos dados, que responda aos requisitos de proteção dos dados em situações de partilha entre sistemas, apresenta vários desafios, nomeadamente: (1) é necessário que esta nomenclatura contemple a exigência de proteção diferenciada dos dados, e considere a sua criticidade, sensibilidade, disponibilidade, e o seu risco; (2) deve contribuir para que as organizações compreendam da mesma forma, o significado dos dados, a sua estrutura, e utilizem esta linguagem comum de classificação no suporte à definição de medidas de proteção; (3) garantir que a sinalização inicial realizada aos dados num determinado sistema, permanece inalterada quando estes dados são utilizados fora do contexto onde foram criados, assegurando-se assim o propósito da partilha de dados.

A interoperabilidade entre sistemas e entre organizações fica deste modo facilitada com a utilização desta ferramenta ao auxiliar na definição de políticas de partilha de dados, e de políticas de proteção destes dados.

P6.V4 – Para o ambiente alargado de colaboração entre organizações, com a consequente partilha de dados, a privacidade depende do trabalho desenvolvido ao nível da proteção de dados, seja numa perspetiva tecnológica, seja de preparação organizacional. A privacidade é, em parte, uma consequência da proteção de dados. A otimização desta dependência, e considerando a heterogeneidade técnica e de funcionamento dos sistemas, está muito dependente de uma maior uniformização tecnológica, essencialmente no suporte à segurança dos dados. A crescente dependência tecnológica carece contudo de regularização, no sentido de promover o desenvolvimento de soluções interoperáveis.

Contudo, a estruturação dos dados é apontada como fator de maior importância para o sucesso da proteção de dados. Nunca se conseguirá otimizar a relação proteção-privacidade dos dados, se os dados não forem estruturados de forma semelhante. Neste sentido, é necessário um consenso sobre os dados, processos, e sobre as medidas de proteção. A utilização de padrões é vital a este processo, com regras comuns para a classificação dos dados, para a segurança, e para a interoperabilidade. Num plano superior à tecnologia, a privacidade dos dados tem que ser um objetivo comum a todas as organizações, com meios humanos dedicados, capazes de mover a proteção centrada nas infraestruturas para uma proteção centrada nos dados e no

cidadão. É necessário desenvolver soluções para que as pessoas não contornem os riscos identificados.

5.1.7 Proposição P7. Estratégia para a privacidade

Para organizações com forte dependência da utilização e tratamento de dados pessoais, os dados e a sua privacidade devem ser considerados como um fator estratégico. A privacidade dos dados é, desta forma, reconhecida como um fator de grande importância para a realização dos objetivos da organização. Por falta de conhecimento ou de preparação, alguns responsáveis podem pensar que já cumprem com os requisitos de privacidade dos dados, desconhecendo que muitos dos dados sob a responsabilidade da sua organização estão a ser incorretamente manipulados.

A visão da privacidade dos dados como um fator estratégico é desta forma abordada através da proposição *P7. Estratégia para a privacidade,* com o objetivo de identificar aquilo que é preponderante para que os gestores executivos assumam a necessidade de uma estratégia para a privacidade dos dados, integrada com a visão estratégica para os SI.

Na seção 4.4.1.4 (Tabela 19) foram apresentadas as cinco variáveis dependentes formuladas, assim como os seis itens de ligação com as fontes de evidências, que constituem a estrutura para o estudo desta proposição.

Esta é uma proposição que pensamos relacionada com as proposições P2 e P5, com uma influência direta sobre a privacidade dos dados, mas de influência inferior em relação a estas proposições, como representado na *framework* conceptual da Figura 14 (página 142). Em termos de interoperabilidade a proposição P7 está incluída no atributo *coordenação* do modelo OIM, e desta forma relacionada com a compatibilidade entre as várias organizações, nomeadamente estruturas de coordenação e estilos de liderança, coordenação de iniciativas de interoperabilidade, e formas de acomodação das diferenças organizativas.

Do processo de análise sobre todos os itens de dados recolhidos no âmbito da proposição P7, resultou a matriz de análise de opinião apresentada na Tabela 32, assim como os seguintes resultados para cada uma das variáveis dependentes:

Tabela 32 - Matriz de análise da opinião sobre P7. Estratégia para a privacidade

P7	**Matriz de análise da opinião sobre P7. Estratégia para a privacidade**		
Variáveis dependentes	*Padrão encontrado*	*A privacidade como um fator estratégico* *(Uma estratégia deve estar na base de um programa integrado e continuo de proteção dos dados)*	*Colaboração necessária para uma visão estratégica para a privacidade* *(questões que dependem da interoperabilidade organizacional)*
P7.v1. Uma estratégia para a privacidade está associada ao reconhecimento da privacidade como fator estratégico para a organização, e da sua responsabilidade sobre este assunto.	Valor organizacional Responsabilidade	Os dados não podem ser apenas matéria-prima. O reconhecimento dos dados e da privacidade como um valor para a instituição vai facilitar uma estratégia para a sua proteção. A privacidade é um valor, que não se pode desvalorizar, nem corromper, e que tem que ser pensada de uma forma estratégica.	Acima de tudo é necessário desenvolver uma estratégia comum. A proteção de dados é uma das maiores responsabilidades ao nível da gestão. Pode existir colaboração a este nível.
P7.v2. Uma estratégia para a privacidade constitui uma ferramenta essencial ao planeamento e integração de mecanismos de proteção e controlo da privacidade.	Importante Colaboração	Faz sentido a existência de uma estratégia de desenvolvimento da privacidade como um todo. Os gestores devem ser os dinamizadores e promover a preparação dos profissionais. Incluir a privacidade no desenvolvimento estratégico dos SI.	Colaboração, interação entre responsáveis das organizações no desenvolvimento de uma estratégia comum. Desenvolver a proteção de dados para as situações de partilha de serviços e de informação. O Ministério deve promover a colaboração necessária ao desenvolvimento de uma estratégia integrada.
P7.v3. O conhecimento e consciência das práticas existentes de processamento de dados e a identificação do risco associado à ausência de políticas de proteção da privacidade e proteção de dados são impulsionadores de uma visão estratégica para a privacidade.	"Não encontrado"	O conhecimento dos riscos das situações de utilização e partilha de dados muda a atitude e preocupação existentes a nível coletivo. A análise de risco ainda é insuficiente, não inclui a privacidade dos dados. Os riscos atuais com a informação em suporte digital são muito elevados e devem ser identificados.	Análise do risco para as situações de partilha de dados. Analisar o impacto da ausência de partilha de dados, o risco de os dados não estarem acessíveis. É essencial para minimizar os eventos adversos que possam surgir, porque estamos a falar de partilha de dados, em que coexistem uma multiplicidade de SI.
P7.v4. Uma estratégia para a privacidade é promotora de uma cultura de privacidade. Uma cultura de privacidade emerge em cenários em que as questões associadas à privacidade e proteção dos dados têm por base uma estratégia de desenvolvimento em detrimento de auditorias pontuais de conformidade.	Influencia a cultura de privacidade	A estratégia primeiro, e depois como consequência desta a cultura de privacidade. Uma estratégia de topo para a privacidade facilita o desenvolvimento de uma cultura de privacidade. A cultura não aparece sem uma estratégia bem definida.	Desenvolvimento de uma estratégia concertada, que tenha como objetivo criar uma plataforma comum, uma abordagem comum. Definição do âmbito para esta estratégia, que permita orientar o conjunto de ações necessárias à sua implementação.
P7.v5. Em ambientes de interoperabilidade, a colaboração para o desenvolvimento de uma estratégia conjunta para a privacidade potenciaria o desenvolvimento de uma plataforma confiável para a recolha, partilha e utilização de dados pessoais.	Necessária mais colaboração Estratégia comum	O futuro passa pelas soluções de interoperabilidade. As pessoas estão sensíveis para estas questões da privacidade, pretendem desenvolvê-las, mas apercebem-se que sozinhos não conseguem. Têm de ter por base uma estratégia global. Existem aspetos que têm a ver com a informação que são transversais a todas as organizações. A falta de conhecimento e formação podem impedir o desenvolvimento da colaboração necessária. Tudo o que implica partilha, gera desconfiança.	O alinhamento de todas as estratégias em termos organizacionais depende da tutela, do Ministério da Saúde. Todas as instituições da administração pública devem partilhar da mesma estratégia comum para este problema. Necessário promover a partilha de experiências, e a definição de diretrizes comuns. São questões similares entre organizações.

P7.V1 – O reconhecimento dos dados e da sua privacidade como um valor para a organização, é o fator determinante para que os responsáveis ao nível executivo assumam a necessidade de uma estratégia para a privacidade. Um valor que não se questiona, que não se pode desvalorizar, nem corromper.

Este reconhecimento faz com que sejam necessárias ferramentas ao nível da gestão da privacidade que deem garantias da qualidade do tratamento de dados. Apesar de reconhecida como uma função de gestão de enorme responsabilidade, a intervenção dos gestores ao nível da proteção de dados é pontual e quase sempre limitada à análise da sua conformidade legal.

Não existem dúvidas de que o desenvolvimento de uma estratégia para a privacidade é uma responsabilidade dos gestores executivos, em conjunto com outros responsáveis. Este reconhecimento é decisivo para que estes assumam uma maior responsabilidade sobre as questões relacionadas com a proteção de dados, promovendo uma visão estratégica para este domínio. Este planeamento é uma ferramenta ou instrumento indispensável ao desenvolvimento de um programa de proteção de dados. Esta visão estratégica para o desenvolvimento da privacidade e da proteção de dados, não deve acontecer de uma forma isolada, mas sim integrada no planeamento estratégico para os SI.

P7.V2 – Uma visão integrada de todas as questões e decisões para o domínio da privacidade dos dados, deve apresentar na sua base uma estratégia de desenvolvimento, no seguimento da estratégia desenhada para os SI. Ao nível local é necessária uma preparação em termos de competências e conhecimentos necessários à operacionalização de um processo com estas características.

A partilha de serviços e de informação entre organizações levanta problemas relacionados com os dados e com a sua proteção. A PDS é disto um bom exemplo, apesar de a solução de partilha de dados ser a correta. A transição da informação em suporte papel para o digital não sofreu a atenção necessária, nomeadamente na sua estruturação e gestão. É necessária a colaboração entre os responsáveis das organizações no sentido de desenvolver uma visão estratégica para o conjunto das organizações, com base em orientações a um nível superior, neste caso o Ministério da Saúde.

P7.V3 – O conhecimento do risco muda a atitude e preocupação existentes a nível coletivo. O desconhecimento do risco pode contribuir para que não se atue de uma

forma proativa. Os riscos atuais com a informação em suporte digital são muito elevados e devem ser identificados. Existe já alguma experiência na análise do risco, mas limitada aos aspetos técnicos de segurança.

Com a implementação de processos de partilha de dados entre organizações, em que coexistem uma multiplicidade de sistemas, é essencial minimizar os eventos adversos que possam surgir em relação aos dados. Por um lado, eventos que coloquem em causa a privacidade dos dados, e por outro, eventos com impacto sobre a disponibilidade e partilha dos dados, que de alguma forma impeçam o acesso necessário aos dados. Ou seja, é necessário também considerar o risco de os dados não estarem acessíveis devido ao excesso de regras de proteção.

P7.V4 – Existe uma influência considerável sobre a cultura coletiva em privacidade, pelo facto de a organização apresentar uma visão estratégica para esta problemática. Havendo uma estratégia para a privacidade dos dados, a cultura em privacidade (P2) desenvolve-se com mais facilidade, com mais agilidade. Uma cultura de privacidade necessita de orientação, de conhecimento. Caso contrário esta não aparece, não se desenvolve.

Para um ambiente alargado de partilha de dados, é necessário uma estratégia concertada, que tenha como objetivo criar uma plataforma comum, uma abordagem comum, e como consequência promover uma cultura alargada a todas as organizações. É necessário definir o âmbito para esta estratégia, que posteriormente permita orientar o conjunto de ações necessárias à sua implementação.

P7.V5 – O futuro da área da saúde passa pelas soluções de interoperabilidade com o objetivo de melhorar a disponibilidade da informação clínica. Contudo, as organizações continuam a trabalhar de uma forma muito isolada, a olhar apenas para o interior dos seus sistemas. A falta de conhecimento e de formação podem impedir o desenvolvimento da colaboração necessária à definição de uma estratégia alargada para as questões relacionadas com os dados. As situações que impliquem "partilha" geram desconfiança entre as organizações, a qual tem que ser gerida.

O facto de existirem aspetos que são transversais a todas as organizações em relação à informação, tem contribuído para que as pessoas estejam mais sensíveis para as questões da privacidade, mas com a noção de que o seu desenvolvimento depende de uma estratégia global. Neste sentido, com o recurso à colaboração entre organizações e à partilha de experiências, será possível definir diretrizes comuns, assim como

definir e partilhar a mesma estratégia para este problema. Em simultâneo, a um nível superior, o Ministério da Saúde pode definir uma estratégia global, capaz de desencadear estas questões localmente.

5.1.8 Proposição P8. Confiança e gestão da confiança

Partilhar dados de elevada criticidade, como são os dados clínicos na sua globalidade, implica confiança a vários níveis entre as organizações envolvidas, tanto tecnológicos como organizacionais. A proteção de dados é um destes níveis, para o qual é necessário que se mantenha um nível de confiança para os contextos de partilha de dados, semelhante ao conseguido nas organizações para os seus SI. Contudo, as iniciativas de partilha de dados introduzem uma série de novas dificuldades à proteção de dados e à confiança entre as organizações.

A confiança entre organizações, subjacente a projetos que contemplem a partilha de dados e de serviços, é muitas vezes implícita. Confia-se na forma como as outras organizações e os seus profissionais vão utilizar os dados, mesmo com um conhecimento sobre os riscos envolvidos. Risco este que é necessário gerir no sentido de manter o nível necessário de confiança que suporte a partilha de dados. A privacidade e a confiança são sem dúvida conceitos intimamente relacionados em sistemas que envolvam tecnologias, e não deve ser descuidada esta dependência. Neste sentido, pretende-se com a proposição *P8. Confiança e gestão da confiança* identificar aquilo que pode influenciar negativamente a confiança entre organizações no que diz respeito à privacidade dos dados, assim como aquilo que pode gerar confiança.

Na seção 4.4.1.4 (Tabela 20) foram apresentadas as três variáveis dependentes formuladas, assim como os três itens de ligação com as fontes de evidências, que constituem a estrutura para o estudo desta proposição.

Em termos de interoperabilidade a proposição P8 está ligada ao atributo *ética* do modelo OIM, e desta forma relacionada com a natureza das organizações, a confiança e confiabilidade de cada organização, aspetos capazes de comprometer os objetivos da colaboração, e o sucesso da proteção da privacidade dos dados. Constitui uma proposição que de acordo com a *framework* conceptual apresentada na Figura 14 (página 142), apresenta uma influência indireta e um peso menor sobre as questões

da privacidade dos dados, e com influência sobre as questões abordadas nas proposições P3 e P9.

Do processo de análise sobre todos os itens de dados recolhidos no âmbito da proposição P8, resultou a matriz de análise de opinião apresentada na Tabela 33, assim como os seguintes resultados para cada uma das variáveis dependentes:

P8.v1 – A realização de iniciativas de interoperabilidade organizacional está muito dependente da confiança conseguida entre as partes envolvidas. A confiança é um pilar fundamental às iniciativas de colaboração. Existe hoje uma maior facilidade de colaboração entre as organizações, as suas estruturas e os seus profissionais.

Para a área da saúde, verifica-se que os SI desenvolvidos entre organizações apresentam à partida uma confiança intrínseca. Confia-se por um lado em situações de partilha de dados, apesar de nem os critérios para a segurança nem para a proteção de dados estarem totalmente definidos, e por outro em situações de partilha de serviços, dado que a sua eficiência depende da colaboração entre todas as partes.

Se existe um SI não confiável, não seguro, dificilmente se partilha dados com esse sistema. Contudo, a partilha de dados é determinante para o sucesso na prestação de cuidados de saúde [serviços], o que leva ao desenvolvimento de atividades de integração de processos com a noção dos riscos existentes ao nível da proteção de dados. É necessário um desenvolvimento concertado, bem planeado, com origem na colaboração entre organizações, que conduza à adoção de soluções conjuntas de acordo com os objetivos definidos para a partilha de dados.

P8.v2 – O facto de o trabalho dos profissionais depender cada vez mais da utilização de múltiplos sistemas influencia e condiciona a sua confiança nestes sistemas. Enquanto no interior da própria instituição os profissionais ainda questionam pouco o funcionamento dos sistemas quanto aos dados, confiando nas aplicações que lhe são disponibilizadas, o mesmo não acontece quando são obrigados a utilizar aplicações do exterior, em que manifestam desconfiança, nomeadamente na forma de partilhar os dados. A utilização de múltiplos sistemas não é totalmente transparente.

Tecnicamente, o que mais preocupa os profissionais é perderem o controlo dos dados quando estes são transferidos para um sistema de outra organização, apesar de a partilha de dados ser um sinónimo de melhoria dos cuidados de saúde.

Tabela 33 - Matriz de análise da opinião sobre P8. Confiança/gestão da confiança

P8	**Matriz de análise da opinião sobre P8. Confiança/gestão da confiança**		
Variáveis dependentes	*Padrão encontrado*	*Confiança no suporte à interoperabilidade* *(Importância da confiança no funcionamento de um ambiente de partilha de dados)*	*Confiança e privacidade* *(Influência do fator confiança sobre o sucesso da privacidade dos dados)*
P8.v1. A confiança constitui um dos pilares fundamentais aos processos de colaboração entre as organizações num ambiente de interoperabilidade.	Essencial à partilha de dados Importante	É necessário gerir a confiança. A experiência aumenta a confiança na interoperabilidade organizacional.	É sempre muito complicado disponibilizar dados quando podem acarretar riscos de responsabilização se não for acautelada a sua proteção. É necessária uma colaboração das organizações na adoção de soluções conjuntas.
		Existe hoje uma maior facilidade de colaboração entre organizações.	Existe a noção que é necessário correr riscos na implementação de processos de integração no sentido de atingir objetivos para a partilha de dados.
		Os SI interorganizações apresentam uma confiança intrínseca. Tomam-se medidas porque se percebe que existem falhas de segurança.	Dificilmente se partilham dados sempre que do outro lado está um sistema de informação não confiável.
		A confiança é importante, tecnicamente, numa situação de partilha de serviços, em que a sua eficiência depende de todas as partes.	É necessário um desenvolvimento concertado, por forma a influenciar todas as organizações.
		A confiança entre organizações é importante para iniciativas de colaboração. São um pilar das pontes de colaboração.	
P8.v2. O contexto de interoperabilidade influencia a atitude e a confiança de uma organização em relação às restantes, com implicação sobre a privacidade dos dados partilhados.	Influência Controlo dos dados	Do ponto de vista técnico a influência é muito grande. O caminho passa por criar sistemas mais homogéneos.	Na partilha de dados com outras organizações podemos perder o rasto de quem está a consultar os dados.
		A interoperabilidade é um meio de reutilização de dados.	A partir do momento em que os dados são transferidos para outro sistema, para serem reutilizados, perco a noção de onde estão estes dados, e isto é uma preocupação, apesar de esta reutilização ser um sinónimo de melhoria.
		Se houver um alinhamento dos requisitos de privacidade entre as organizações, vai no fundo aumentar a confiança das pessoas em relação àquilo que estão a partilhar.	Tem que haver uma base comum a todos os sistemas, para que depois seja mais fácil a sua utilização.
		A confiança é essencialmente gerida através da segurança.	As pessoas começam a perceber que se acontecem quebras de privacidade nas redes sociais, podem também acontecer em outros sistemas.
		Depende do tipo de dados que estamos a partilhar.	Depois não há transparência em relação ao que a PDS faz.
		Existe nos profissionais de saúde uma aceitação da partilha de dados, uma vez que é para seu bem.	
		São necessárias políticas bem definidas e procedimentos muito baseados numa boa gestão da identidade digital.	
P8.v3. A utilização de tecnologias inerentemente invasivas da privacidade, tecnologias novas que apresentam ameaças e que provocam demasiado interesse público, representam um risco à confiança sobre o sistema.	Análise prévia Princípio	Deveria investir-se mais numa análise prévia. Avaliar o impacto sobre a privacidade deveria ser um princípio.	Sim, deveria haver uma matriz de risco.
		Na prática primeiro pensa-se em determinada solução e só depois é que se pensa em licenciar, em proteção de dados. Os SI são desenhados com base em objetivos, sem a análise do risco em relação à privacidade.	A transmissão aos profissionais de saúde de que determinada solução foi testada quando à privacidade funcionava como um selo de confiança.
		Este modelo pode ser utilizado para tomar decisões relativamente aos procedimentos a ter ao nível de investimento ou de certificação.	A privacidade não significa manter tudo em segredo, mas sim manter seguro e utilizar de forma correta.
		Deveríamos ter linhas orientadoras, um determinado padrão.	Privacidade e proteção são de alguma forma tudo risco. A ISO 27005 ajuda na identificação e prova de que existe risco. O epSOS baseia-se nesta norma.
		Não temos ainda a noção do risco, uma vez que a nossa análise do risco é ainda muito limitada à segurança.	Deveríamos perceber logo à partida qual o impacto sobre a privacidade, os efeitos negativos sobre a privacidade.
		É com base no risco que nós conseguimos sustentar na opinião pública, nos parceiros, o que é que está em causa.	A utilização das tecnologias já não é um problema. Tornamo-nos dependentes dos computadores, e em todo o lado tem que haver um computador. O problema agora são os dados, o acesso a todos os dados.
		Criava uma maior confiança e uma maior qualidade dos dados transportados, e uma verdadeira rede colaborativa.	

A interoperabilidade é um meio de reutilização de dados, mas devido à maior exposição dos dados que daqui resulta, pode gerar desconfiança entre os participantes. O tipo de dados partilhados pode agravar esta desconfiança. O alinhamento dos requisitos de privacidade entre as organizações e o desenho de soluções e medidas, vão contribuir para o aumento da confiança dos utilizadores relativamente ao meio e aos dados partilhados. Atualmente o grau de confiança existente é assegurado essencialmente por medidas de segurança, onde a identidade digital tem uma função importante. Deve existir uma base comum que regule a partilha de dados, o seu controlo e a sua proteção. É necessário mais informação e transparência destes processos.

P8.v3 – Um levantamento inicial do risco com base numa análise do impacto sobre a privacidade estimula a confiança dos profissionais sobre as tecnologias utilizadas, sobre os fins para a recolha e partilha de dados. Ao transmitir-se a informação de que determinada solução foi testada positivamente quanto aos requisitos de privacidade, esta funciona como um selo de confiança. Desta forma, é mais fácil passar a mensagem que a "privacidade" não significa manter tudo em segredo, mas sim utilizar de forma segura e correta.

Uma grande parte dos sistemas em funcionamento foram desenvolvidos para cumprir determinados objetivos, para acumular dados, e não considerou a proteção do indivíduo (titular dos dados). As questões da privacidade, quando surgem, só são colocadas normalmente depois do início da sua atividade. Uma análise prévia dos riscos e efeitos negativos sobre a privacidade de uma solução tecnológica deveria ser realizada atempadamente, de forma a serem definidos os requisitos em termos de proteção de dados a serem integrados na fase de desenvolvimento. Apesar de ainda não ser prática comum, é reconhecida a importância deste procedimento, ao ser identificado como um princípio a instituir, a aplicar no domínio da proteção de dados.

Uma análise atempada do impacto sobre a privacidade pode fornecer um conjunto valioso de informação, de suporte a outros processos no domínio da privacidade, como planos de contingência, análise de conformidade e mesmo processos de certificação. São necessárias linhas orientadoras, procedimentos, um padrão, que suporte este tipo de análise do risco, como um modelo processual. A norma ISO/EIC 27005 é um bom exemplo no suporte à identificação e conhecimento do risco.

5.1.9 Proposição P9. Ética e cooperação humana

A expansão das situações de partilha de dados, ao aumentar consideravelmente a disponibilidade dos dados, seguramente aumenta as ameaças e riscos à privacidade dos dados. Isto porque, aumenta o número e variedade de atores que de uma forma contínua acedem aos dados, e aumenta a complexidade das interações que envolvem dados pessoais.

A atitude do titular dos dados e dos vários profissionais que diariamente atuam em ambientes de partilha de dados, pode mudar perante as alterações introduzidas, quer ao nível tecnológico de controlo, quer ao nível dos processos de utilização dos dados. Importa assim, compreender aquilo que é importante em matéria de proteção de dados, com impacto sobre a confiança dos vários profissionais e sobre o titular dos dados, que deve ser considerado no desenvolvimento de iniciativas de partilha de dados. Com base neste objetivo foi introduzida no *estudo de caso* a proposição com a denominação *P9. Ética e cooperação humana*, no sentido de compreender aquilo que pode influenciar a postura, a avaliação, a aceitação ou oposição manifestadas pelos profissionais de uma organização e pelos titulares dos dados em relação às mudanças que possam decorrer do facto das organizações desenvolverem iniciativas de interoperabilidade de suporte à partilha de dados.

A estrutura para o estudo desta proposição foi apresentada na seção 4.4.1.4 (Tabela 21), constituída por três variáveis dependentes, e por dezasseis itens de ligação com as fontes de evidências. As duas primeiras variáveis dependentes (P9.v1 e P9.v2) foram desenvolvidas por forma a serem validades com recurso a dados quantitativos, obtidos através da realização de um inquérito.

O inquérito, apresentado no Anexo IX, foi realizado através da Internet, e esteve disponível para respostas entre os dias 17 de outubro de 2014 e 7 de novembro de 2014. Não sendo viável a recolha de dados através de entrevistas aos utilizadores do Portal do Utente, optou-se neste caso por recolher os dados através da realização de um inquérito. São dados essenciais para a compreensão do que pode influenciar a atitude e o conhecimento do titular dos dados (utente do SNS) em relação à privacidade dos seus dados pessoais no contexto alargado de partilha de dados, representado pela PDS. A privacidade é desta forma analisada com base num tipo de informação pessoal, a informação de saúde, num determinado contexto de utilização.

A SPMS dispõe de um grupo de 1200 beta-tester, utentes do SNS registados no Portal do Utente, que colaboram regularmente na análise e avaliação das soluções implementadas para o domínio do SNS, onde se inclui o Portal do Utente. Dada a exigência das questões do inquérito, nomeadamente em assuntos relacionados com a proteção de dados, o conhecimento e a maturidade deste grupo de utentes são sem dúvida um indicador importante e essencial à qualidade que se pretende para os dados. O processo iniciou-se com o envio de uma mensagem por correio eletrónico (Anexo X) pela SPMS ao grupo de beta-tester, onde é resumido o objetivo do estudo e se explica a importância da colaboração do grupo. Foram recebidas no total 125 participações.

Em termos de interoperabilidade a proposição P9 está ligada ao atributo *ética* do modelo OIM, e desta forma relacionada com os aspetos socioculturais capazes de comprometer os objetivos da colaboração, e com um impacto negativo sobre as questões relacionadas com a privacidade dos dados. Constitui uma proposição que de acordo com a *framework* conceptual apresentada na Figura 14 (página 142), apresenta uma influência indireta e um peso menor sobre as questões da privacidade dos dados, e com influência sobre as questões abordadas nas proposições P2 e P8.

P9.v1 e P9.v2 (resultados obtidos com a realização do inquérito) - Sendo a temática em estudo a privacidade dos dados em contextos de partilha de dados entre organizações, a sua relevância está muito dependente do facto de as pessoas se identificarem com este tipo de privacidade em relação a outros tipos de privacidade, comuns no seu dia-a-dia. Com a 1ª questão do inquérito, procurou-se assim um alinhamento de opiniões em relação às três situações mais comuns de privacidade, com o pressuposto de que a maioria estaria centrada nos dados e na sua privacidade. O resultado apresentado no Gráfico 1 confirmou este pressuposto, sendo possível com base nos dados representados graficamente, demonstrar que 71% dos participantes centra a sua preocupação na privacidade dos dados pessoais, 19% dos participantes na privacidade das comunicações pessoais, e 10% dos participantes na privacidade em espaços públicos.

É um resultado importante e sem dúvida revelador de que existe uma maior atenção por parte das pessoas em relação aos seus dados pessoais. A análise das questões

seguintes permitirá compreender a atitude e opinião dos participantes em relação a questões mais específicas da privacidade dos dados.

O tratamento de dados pessoais para outros fins apenas deve ser autorizado se for compatível com as finalidades para as quais os dados foram inicialmente recolhidos, particularmente para fins de investigação histórica, estatística ou científica (GDPR, 2012). O desenvolvimento tecnológico facilitou a reutilização e a partilha dos dados entre sistemas e entre organizações. Independentemente de todos estes processos de tratamento serem compatíveis com a finalidade inicial, o risco que apresentam em termos de privacidade é diferente.

Gráfico 1 - Resultados da 1ª questão do inquérito, P9.v1.1

Atualmente, no domínio da prestação de cuidados de saúde, a partilha de dados é um requisito essencial ao funcionamento e à eficiência de serviços e unidades. Esta partilha de dados pode acontecer em três cenários: (1) entre os profissionais de saúde, (2) entre as organizações no setor da saúde, e (3) entre as várias estruturas administrativas dentro da organização. A 2ª questão do inquérito procurou assim compreender qual destes cenários suscita mais preocupações quanto à proteção e à privacidade dos dados.

Com base nos resultados apresentados na Tabela 34, podemos desta forma verificar que 80% dos participantes demonstram uma maior preocupação relativamente a situações de utilização dos seus dados pessoais no contacto com outras instituições do setor da saúde, do que com situações de suporte ao funcionamento da organização

(9,6%), ou no apoio aos tratamentos de saúde (10,4%). Este resultado pode significar o reconhecimento de um maior risco para a privacidade dos dados sempre que partilhados com outras organizações, e um menor risco quando os dados são partilhados dentro das fronteiras dos SI locais.

O facto de 80% dos participantes indicarem as situações de partilha de dados com outras instituições do setor da saúde como o contexto mais preocupante, justifica a necessidade de um maior conhecimento sobre o seu funcionamento e requisitos em relação à proteção da privacidade dos dados. Em nosso entender, esta situação está relacionada com a qualidade da informação disponibilizada e a transparência destas situações, para com o titular dos dados. Os resultados da 3ª e da 4ª questão podem conter dados que confirmam ou não esta convicção.

Tabela 34 - Resultados da 2ª questão do inquérito, P9.v1.2

[2] Qual a situação de utilização e partilha dos seus dados, que lhe suscita mais preocupações quanto à sua proteção e privacidade?	
a. No apoio aos tratamentos de saúde, em que os seus dados de saúde podem ser partilhados entre profissionais de saúde.	**13** (10,4%)
b. No contato com outras instituições do setor da saúde, em que os seus dados podem ser partilhados para faturação dos serviços de saúde a outras entidades.	**100** (80%)
c. No funcionamento da organização hospitalar, em que os seus dados podem ser utilizados e partilhados internamente, para melhorar o apoio médico, melhorar o atendimento e se necessário contatá-lo pessoalmente.	**12** (9,6%)
Total	125

No domínio da informação, foi pedido aos participantes que atribuíssem um grau de importância a quatro grupos de informação, que consideramos essenciais a um maior conhecimento sobre as situações de partilha de dados. Para todos estes grupos, e com base nos resultados apresentados na Tabela 35, constatamos que em todos os grupos de informação mais de ¾ dos participantes atribui um grau de importante (4) ou muito importante (5) à sua disponibilização.

Tabela 35 - Resultados da 3ª questão do inquérito, P9.v2.5

[3] Sempre que os seus dados forem suscetíveis de serem legitimamente partilhados com outros utilizadores/organizações, que informação considera importante que lhe seja enviada. Atribua um grau de importância entre 1 (nada importante) e 5 (muito importante).					
	1	2	3	4	5
a. Os tipos de dados partilhados	2	5	14	***25***	***79***
b. A identificação do utilizador/organização que vai receber os dados	4	1	12	***17***	***91***
c. O propósito da partilha dos dados	3	6	10	***18***	***88***
d. As medidas adotadas para a proteção dos dados	7	3	14	***18***	***83***

O princípio da transparência vai exigir que qualquer informação destinada ao público ou ao titular dos dados seja de fácil acesso e compreensão, e formulada numa linguagem clara e simples (GDPR, 2012). Isto é especialmente relevante em contextos de partilha de dados entre organizações. Havendo processos, serviços ou profissionais que de uma forma regular e legítima realizam trocas de dados entre si, então a organização deve reconhecer esta prática e disponibilizar informação que permita ao titular dos dados, por um lado conhecer estas situações, e por outro conhecer as situações em que os seus dados nunca serão utilizados ou cedidos a terceiros – é uma questão de transparência.

Ao analisar os resultados da 4ª questão, representados no Gráfico 2, pode verificar-se que 62,4% dos participantes não consegue distinguir, com base na informação que lhe é disponibilizada, entre situações legítimas de partilha de dados nos vários cenários apresentados na Tabela 34, e situações onde a partilha de dados não vai acontecer. É um valor alto, que quando conjugado com os 80% de participantes que na 2ª questão apontam para as situações de partilha de dados entre organizações como as mais preocupantes, e com os ¾ dos participantes que na 3ª questão consideraram importante a disponibilização de mais informação sobre este contexto de partilha de dados, permite apontar para um cenário que carece de mais informação.

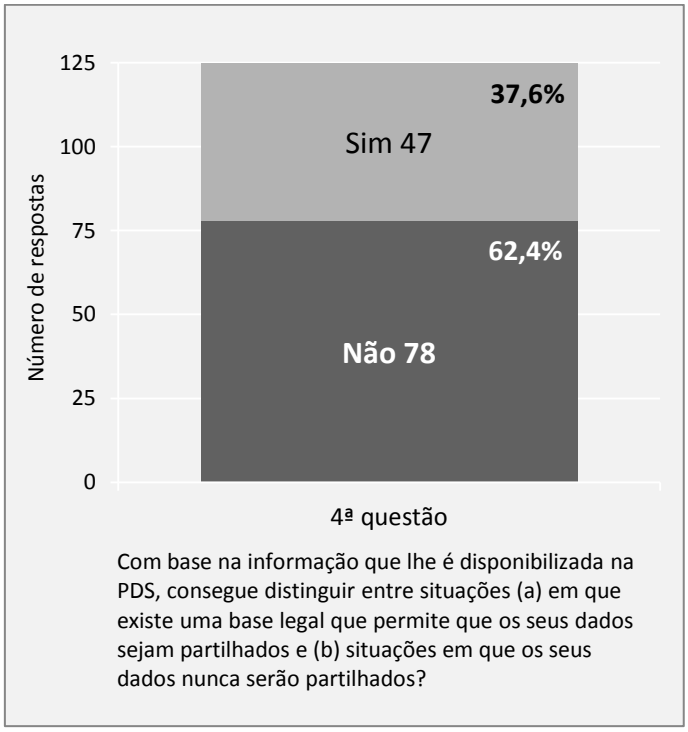

Gráfico 2 - Resultados da 4ª questão do inquérito, P9.v2.4

Ainda no âmbito da 4ª questão, é importante identificar a origem da elevada percentagem (62,4%) de participantes que não consegue distinguir entre situações passíveis ou não de partilha de dados. Através do Gráfico 3 pode constatar-se que tanto para as pessoas mais preocupadas com a privacidade dos dados, como das comunicações, ou dos espaços públicos, são mais as pessoas que reconhecem ter dificuldades no reconhecimento destas situações, do que as que respondem não ter ou apresentar dificuldades. Contudo, esta diferença é maior para o grupo de pessoas mais preocupadas com a "violação da privacidade dos seus dados pessoais", em que 58/89, 65%, reconhecem que não são capazes de distinguir, com base na informação disponível, se a situação de partilha de dados está enquadrada legalmente.

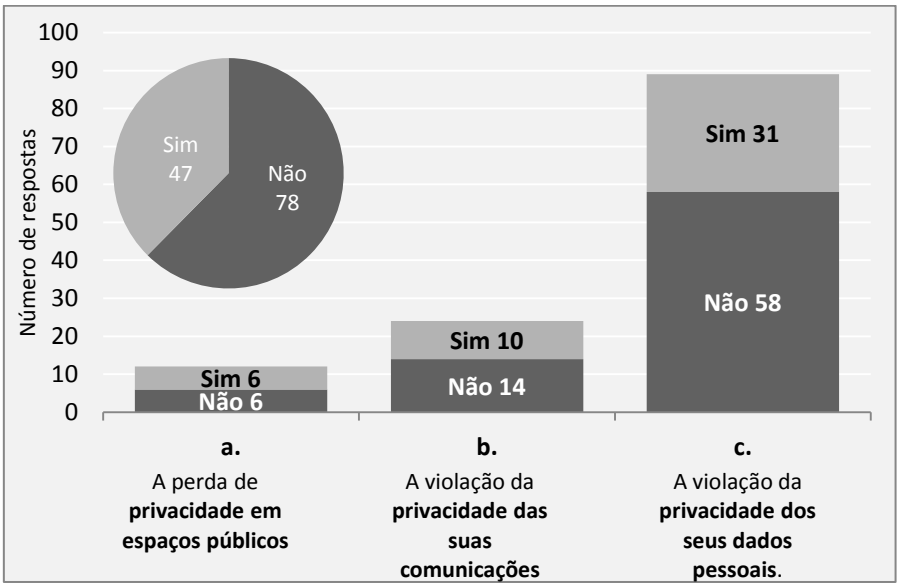

Gráfico 3 - Cruzamento de resultados entre a 4ª e a 1ª questão do inquérito

Os dados resultantes das 3ª e 4ª questões evidenciam a necessidade de as organizações disponibilizarem mais informação que suporte o titular dos dados na formulação de uma opinião e conhecimento, especialmente sobre as situações em que os seus dados podem ser partilhadas com outras organizações. A confiança do titular dos dados em relação à organização pode ser influenciada pela clareza e transparência destas situações.

Os princípios de tratamento leal e transparente vão exigir que o titular dos dados seja informado, em especial, da existência da operação de tratamento de dados e das suas finalidades, do período de conservação dos dados, da existência do direito de acesso, da retificação ou de apagamento, bem como do direito de apresentar uma queixa (GDPR, 2012).

Foram considerados na 6ª questão, quatro conjuntos de informação que se consideram importantes para o objetivo de informar o titular dos dados. Pretende-se desta forma compreender qual a importância que os participantes atribuem às políticas de privacidade, à publicação de informação sobre os direitos do titular dos dados, à informação que demonstre o compromisso da organização para com a privacidade e a proteção dos dados, e à informação sobre os contextos e finalidades dos processos de tratamento de dados.

Pela análise dos resultados apresentados na Tabela 36, os quatro conjuntos de informação recebem um grau elevado de importância quanto à sua disponibilização para consulta pública. Estes quatro conjuntos de informação podem, assim, ser preponderantes para um maior conhecimento do titular dos dados e, consequentemente, para uma maior confiança nas organizações.

Tabela 36 - Resultados da 6ª questão do inquérito, P9.V1.6

[6] A confiança do titular dos dados (utente) na organização a quem facultou os seus dados pessoais é determinante para a gestão da privacidade. Atribua um grau de importância (1 - nada importante; 5 - muito importante) aos seguintes conjuntos de informação, que sendo públicos, podem influenciar a confiança do titular dos dados na organização:					
	1	2	3	4	5
a. A publicação das políticas de privacidade e proteção de dados.	7	2	31	**31**	**54**
b. A publicação dos direitos que o titular dos dados (utente) tem sobre os seus dados pessoais.	1	5	16	**40**	**63**
c. A demonstração do cumprimento, por parte da organização, dos requisitos legais no domínio da proteção e privacidade dos dados.	2	3	13	**16**	**91**
d. A publicação dos contextos e finalidades de utilização dos dados.	1	6	13	**36**	**69**

A proteção dos direitos do titular dos dados em relação ao tratamento dos seus dados pessoais, exige que a organização tome medidas técnicas e organizacionais adequadas, em linha com os requisitos da legislação aplicável. É fundamental que estas medidas, por um lado, se baseiem no risco identificado e, por outro, na natureza dos dados pessoais que é necessário proteger.

A opção c) da 6ª questão, ao procurar analisar a importância atribuída à disponibilização pública de informação que permita demonstrar o compromisso da organização para com a proteção e privacidade dos dados, de uma forma indireta questionou os participantes sobre a importância de a organização tornar públicas as medidas técnicas e organizacionais que adaptou ao risco e ao contexto de utilização

de dados. Dos 125 participantes, 107 (16+91) atribuem uma importância elevada à disponibilização deste tipo de informação, a qual permite demonstrar que a organização tomou medidas de proteção, de acordo com os requisitos legais.

Contudo, quando através da 7ª questão é solicitado aos participantes uma avaliação da informação existente, os resultados apresentados na Tabela 37 permitem concluir que existe um défice muito grande na disponibilização pública deste tipo de informação. Do total de participantes, 40% não têm conhecimento da disponibilização desta informação, enquanto 58,4% reconhece a existência desta informação, mas reconhece também que a informação não é clara (36,8%), nem existe qualquer evidência de que a organização cumpriu com as obrigações que indicou (21,6%). Apenas 1.6% consideram a informação suficiente.

Tabela 37 - Resultados da 7ª questão do inquérito, P9.V2.1

[7] A legislação sobre proteção de dados exige às organizações que utilizam os seus dados pessoais, determinadas obrigações (responsabilidades). Qual a sua opinião sobre estas obrigações?		
a.	Existem e permitem compreender as medidas de proteção implementadas.	**2** (1,6%)
b.	Existem, mas não são claras para a maioria dos utentes.	**46** (36,8%)
c.	Existem, são compreensíveis, mas as organizações não apresentam provas quanto ao seu cumprimento.	**27** (21,6%)
d.	Não são do conhecimento generalizado dos utentes.	**50** (40%)
	Total	125

As organizações devem contemplar modalidades para facilitar o exercício, pelo titular dos dados, dos direitos que lhe são conferidos, incluindo mecanismos para solicitar, a título gratuito, em especial o acesso aos dados, a retificação, a supressão e o exercício do seu direito de oposição (GDPR, 2012). A questão dos direitos que assistem o titular dos dados, integrada na 6ª questão com o objetivo de perceber se é importante ou não a disponibilização de informação sobre os direitos do titular dos dados, revelou que 103 dos 125 dos participantes atribuem uma importância elevada à disponibilização de informação que os ajude a compreender os seus direitos em matérias de proteção de dados, dada a especificidade e exigência do domínio da saúde.

Contudo, quando lhes é solicitado (ver dados na Tabela 38 relativos à 8ª questão) que classifiquem a informação pública a que têm acesso quanto aos seus direitos como titular dos dados, verifica-se que 88 consideram a informação insuficiente, e 19 nem sequer conseguem localizar informação sobre os seus direitos. Apenas 14 considera a informação existente suficiente, de fácil acesso e compreensão. Esta situação dificulta

sem dúvida a atitude do titular dos dados perante um contexto de utilização de dados pessoais que lhe suscite alguma dúvida.

Tabela 38 - Resultados da 8ª questão do inquérito, P9.v2.2

[8] Como classifica a informação que lhe é disponibilizada sobre os seus direitos em termos de privacidade e proteção dos seus dados		
a.	A informação existente é mínima, e não permite compreender quais os direitos que assistem o titular dos dados.	**88** (70,0%)
b.	A informação existente é suficiente, é de fácil acesso e compreensão, formulada numa linguagem clara e simples, para um conhecimento detalhado dos direitos do titular dos dados.	**14** (11,2%)
c.	Não foi possível encontrar qualquer informação.	**19** (15,2%)
	Total	**125**

Qualquer pessoa deve ter o direito de acesso aos dados recolhidos sobre si e de exercer facilmente este direito, a fim de conhecer e verificar a licitude do tratamento (GDPR, 2012). Isto pressupõe a existência de meios que facilitem o exercício, pelo titular dos dados, dos direitos que lhe são conferidos. A sua não existência limita a atitude do titular dos dados quando confrontado com situações que lhe possam suscitar dúvidas, seja na recolha, no tratamento ou na partilha dos seus dados pessoais.

De acordo com os resultados da 9ª questão do inquérito (ver Tabela 39), e para o contexto em estudo, se o titular dos dados for confrontado com dúvidas em relação à licitude, lealdade ou à transparência de um determinado processo, verifica-se que 83/125 não consegue identificar os meios para apresentar uma dúvida, 105/125 não consegue identificar sobre quem recai a responsabilidade pelo processo de tratamento de dados, e 101/125 reconhece dificuldades no contacto com este responsável.

Tabela 39 - Resultados da 9ª questão do inquérito, P9.v2.3

[9] Confrontado com uma situação que lhe suscita preocupações em relação à utilização dos seus dados pessoais, consegue com base na informação que lhe é disponibilizada:			
		Não	Sim
a.	Identificar com facilidade os meios disponíveis para apresentar as dúvidas existentes?	83	42
b.	Identificar a pessoa responsável pela utilização dos seus dados dentro da organização?	105	20
c.	Contactar com facilidade o responsável na organização pela utilização dos seus dados?	101	24

O resultado da opção d) da 6ª questão (ver Tabela 36), com 4/5 dos participantes (36+69) a atribuir uma importância elevada à disponibilização de informação sobre os contextos e finalidades de recolha e utilização dos dados, está muito relacionado com os resultados obtidos com a 9ª questão. É assim urgente, disponibilizar informação e meios que facilitem a iniciativa individual do titular dos dados em situações que lhe suscitem dúvidas.

O titular dos dados é o primeiro interessado na privacidade dos seus dados, e em garantir que os dados sobre si mesmo estão protegidos. Uma exposição não controlada dos seus dados pessoais pode causar danos significativos na sua reputação, humilhações, roubo ou usurpação de identidade, para a pessoa ou para um grupo de pessoas em causa. Caso o titular dos dados, pretenda intervir na gestão da privacidade dos seus dados pessoais, dispõe de algumas funcionalidades reconhecidas pela legislação, nomeadamente: a atualização e correção dos seus dados pessoais, a sua portabilidade, o consentimento, e o controlo e a monitorização da utilização dos seus dados pessoais (GDPR, 2012). Estas funcionalidades, quando implementadas, podem apresentar um impacto positivo sobre a proteção da privacidade dos dados.

Com base nos resultados apresentados no Gráfico 4, verifica-se que o consentimento é a funcionalidade que recolhe mais respostas. Confirma-se, assim, uma maior importância desta funcionalidade em relação às restantes. Contudo, e muito próximo do consentimento, 97/125 dos participantes apontam o controlo e a monitorização dos dados, como uma funcionalidade fundamental. Este valor pode estar relacionado com a necessidade de mais informação no suporte ao consentimento.

Mesmo a portabilidade dos dados, uma das ferramentas menos conhecida e utilizada, reúne 51/125 manifestações de importância.

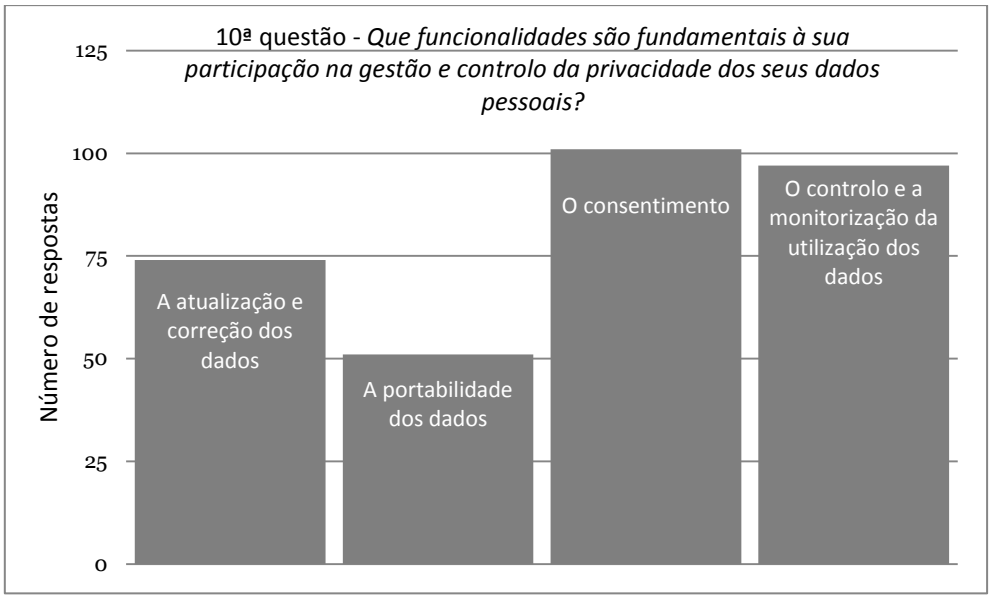

Gráfico 4 - Resultados da 10ª questão do inquérito, P9.v1.4

Para que um tratamento seja lícito, os dados pessoais devem ser tratados com base no consentimento da pessoa em causa ou noutro fundamento legítimo, previsto por lei (GDPR, 2012). Tendo sido atribuída uma importância elevada à funcionalidade do consentimento, é expectável que as pessoas conheçam e dominem esta funcionalidade em situações onde o consentimento é exigível.

Os resultados representados no Gráfico 5 confirmam em grande parte esta expetativa, com 22/125 dos participantes a reconhecer que consegue gerir as situações de privacidade onde é necessário o seu consentimento, e com 70/125 das pessoas a reconhecer uma compreensão deste conceito e das situações que requerem o seu consentimento, mas a reconhecer também uma dificuldade na forma como o consentimento é atribuído ou retirado, assim como na sua monitorização ou controlo. Contudo, 33/125 dos participantes, aproximadamente ¼ dos participantes, reconhece que as situações de consentimento não são claras nem compreensíveis. Ou seja, apesar do resultado bastante positivo quanto à funcionalidade do consentimento, é necessário que esta evolua no sentido de se apresentar de mais fácil compreensão, e consequentemente de mais fácil gestão e controlo. A qualidade e clareza da informação disponibilizada pode mais uma vez estar a comprometer uma funcionalidade tão importante para o titular dos dados.

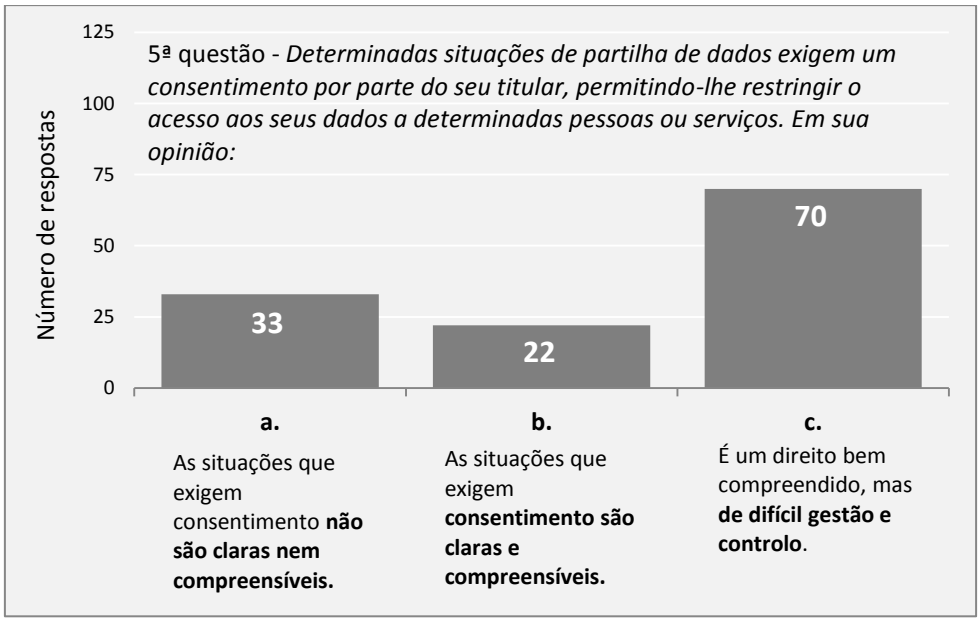

Gráfico 5 - Resultados da 5ª questão do inquérito, P9,v1.5

Independentemente das dificuldades já identificadas, essencialmente relacionadas com a qualidade da informação, transparência e proatividade das organizações, assim como no acesso às funcionalidades de gestão da privacidade, os titulares dos dados continuam a acreditar que têm um papel significativo sobre a gestão dos seus dados pessoais. No Gráfico 6 é verificável este facto. Não é surpreendente, desta forma, que a PDS seja apontada por 106/125 dos participantes como uma oportunidade para melhorar o conhecimento individual e coletivo sobre a privacidade dos dados.

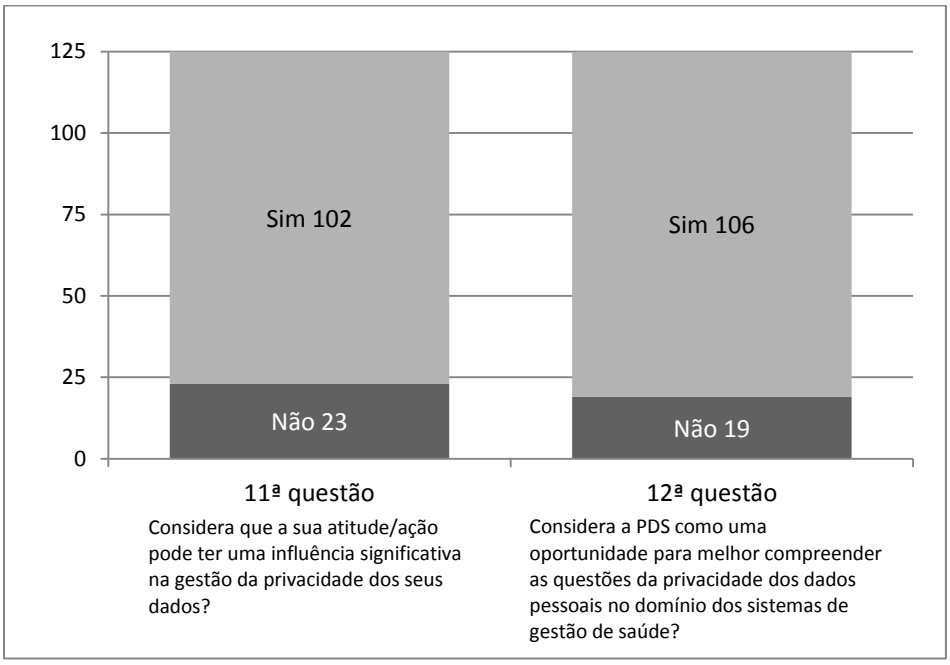

Gráfico 6 - Resultados da 11ª e da 12ª questão do inquérito, P9,v1.6

P9.v3 – Do processo de análise sobre todos os itens de dados recolhidos no âmbito desta variável dependente da proposição P9, resultou a matriz de análise de opinião apresentada na Tabela 40, e com base nesta os seguintes resultados:

Existe uma mudança de atitude dos profissionais de saúde face aos requisitos que resultam das iniciativas de colaboração, com o propósito de partilha de dados. Esta mudança de atitude está a manifestar-se, por um lado, na retração ou resistência de alguns profissionais a estas iniciativas, e por outro, num aumento das preocupações em relação à qualidade dos dados e à sua maior exposição, a qual pode afetar a sua privacidade profissional.

Apesar de muitos profissionais serem avessos à mudança, gradualmente apercebem-se das oportunidades de melhoria dos serviços, das facilidades obtidas com a partilha de dados, e acabam por aderir. Muitas das dificuldades de adesão são explicadas pela falta de informação sobre a exigência e as obrigações da sua participação.

Com a expansão do ambiente de partilha de dados e com o aumento da mobilidade de profissionais, existe a noção de que os profissionais têm acesso a mais informação, e a informação com mais qualidade.

Melhorou a preocupação para com o que se regista e na forma como se regista, assim como no rigor com que se lida com os dados. Contudo, a noção de reutilização dos dados por outros profissionais e a sua confidencialidade, geram preocupações quanto à sua privacidade profissional. É o início de um processo de mudança cultural, em que as gerações mais recentes estão mais adaptadas à evolução tecnológica. Existe a necessidade de gerir a mudança no sentido de evitar efeitos negativos sobre os objetivos da colaboração.

Com cada vez mais informação em suporte digital, o profissional tem consciência que existe um maior controlo, um controlo tecnológico sempre presente sobre o seu trabalho diário, e que degrada o seu direito e expetativa de privacidade profissional. Este controlo pode mesmo condicionar a sua atividade e a sua adesão em pleno. Os contextos de colaboração aumentam por um lado a exposição e o acesso aos dados, e por outro, a exposição do próprio profissional a vários níveis. O mais preocupante diz respeito à exposição do seu pensamento e raciocínio clínico. Os profissionais têm a consciência que não estão a trabalhar sozinhos, mas cada vez mais em paralelo, e em rede com outros profissionais.

Tabela 40 - Matriz de análise da opinião sobre P9. Ética e cooperação humana

P9	**Matriz de análise da opinião sobre P9. Ética e cooperação humana**		
Variável dependente	*Padrão encontrado*	*Adaptação à mudança* *(De que forma os profissionais encaram as mudanças resultantes da partilha de dados e de serviços)*	*Influência sobre a partilha de dados* *(Que aspetos pode influências a partilha de dados e que podem ser desenvolvidos em conjunto)*
P9.v3. A atitude dos profissionais face à mudança que decorre dos novos requisitos do ambiente de colaboração, assim como a sua atitude face à deterioração da sua privacidade profissional, podem apresentar efeitos negativos para o sucesso das políticas de privacidade para o contexto da colaboração.	Mudança de atitude Falta de informação Privacidade profissional	Há uma mudança de atitude, muito grande. Muitos profissionais são avessos a estas mudanças. Há profissionais de saúde pró-ativos em relação a esta mudança. Existem outros mais renitentes.	Não é claro para os profissionais este formato de funcionamento.
			Deveria haver uma maior atenção quando se exige que um profissional lide com vários sistemas. Perceber qual a atitude e a adesão.
		Contudo, um conjunto de pessoas vê uma oportunidade de melhoria. Progressivamente esta relutância foi-se diluindo com as facilidades obtidas com o uso das ferramentas informáticas.	Leva a um maior cuidado na forma como registamos os dados. Os dados estão a ser partilhados. Daí existir um maior rigor assim como um maior cuidado na forma como lidamos com esses dados.
		A informação sobre a participação e as obrigações neste domínio de colaboração não é clara. Deveria haver mais informação.	A confidencialidade dos dados é o que leva a que muitos médicos não adiram.
		Não é claro para os profissionais o formato de funcionamento em ambiente de colaboração, integrado com outras instituições. Deveria haver mais informação.	Hoje os profissionais têm acesso a informação que antes não tinham, uma mais-valia.
		Esta mudança tem que ser mais bem gerida.	O facto de os sistemas estarem a ser cada vez mais intrusivos coloca em causa aquilo que é a privacidade profissional.
	Maior controlo Aspetos positivos	Têm um receio face a este controlo invisível. Mas acaba também por ser um fator de proteção para a nossa atividade.	Não posso por em causa o exercício da minha atividade porque não quero aderir a algo que interfere na minha privacidade profissional.
		As pessoas de facto percebem que têm uma exposição maior daquilo que é o seu pensamento clínico.	Não digo influenciar a sua colaboração, mas mais o desempenho do profissional de saúde. Condiciona o seu comportamento. O próprio trabalho do profissional fica mais exposto.
		Hoje as pessoas têm que ser responsabilizadas.	
		Este controlo condiciona a própria privacidade profissional.	Pode influenciar a cooperação com um ambiente de colaboração. A transparência é fundamental nestas situações.
		As pessoas têm consciência do controlo efetuado através das tecnologias, é intrínseco. Sabem que o seu trabalho é realizado paralelamente com outros.	É necessário um maior conhecimento sobre os direitos e obrigações dos profissionais em relação à sua privacidade profissional. Este controlo invisível tem que ter um limite. Tem que estar enraizado nas pessoas os limites quanto à utilização de dados.
		Com cada vez mais informação em suporte digital, o profissional sente que existe um maior controlo, um controlo sempre presente sobre a sua tarefa diária.	
		Este controlo tecnológico invisível começa por ser difícil no dia-a-dia à adesão plena a um registo informático dos dados.	Nota-se algum receio de algumas instituições em participar, em partilhar os dados.
		A instituição tem obrigatoriamente que ser mais eficaz, e só o consegue fazer se analisar as práticas.	Quando eu estou a avaliar a qualidade da prestação, do desempenho e a estou a divulgar, então posso estar a ultrapassar o âmbito da privacidade. Estou a expor aquela pessoa.
	Ética Colaboração Consequências	Sim é uma questão ética muito presente. Em ambientes de colaboração agrava-se. Cada vez trabalhamos mais em rede e se eu não registar algo importante, posso condicionar os cuidados de saúde numa outra instituição.	Um serviço hoje em dia já é cada vez mais da responsabilidade de várias instituições. A colaboração é imprescindível.
			A omissão de informação pode comprometer outros diagnósticos.
			Existem áreas onde a informação é mais crítica do que em outras. Deveria trabalhar-se mais nestas áreas. Um doente crónico sofre de mais perigos de privacidade.
		A minha ação ou a minha inação vai ter consequências. Se existe um dado que é muito importante, e que eu não registei, e que por isso não é partilhado, pode por em causa a continuidade dos cuidados numa outra instituição, por um outro profissional.	Os profissionais percebem que os dados cada vez mais acompanham os movimentos do utente com maior facilidade.
		Têm a noção que se abreviarem alguns passos ou se não cumprirem alguns procedimentos incorrem em procedimentos legais.	Tem que ser cada vez mais desenvolvida uma apetência para a colaboração, o trabalho em rede com outras instituições.
			Não existem normas para o registo clínico. Deveria haver normas adaptadas à realidade.

Contudo, apontam o facto de este controlo tecnológico poder atuar como protetor da atividade do profissional e da instituição, como um aspeto positivo. Os dados que resultam destes processos de controlo podem funcionar como um fator de proteção para o profissional. No entanto, e à semelhança de outros dados, é necessário considerar a privacidade destes dados de controlo. Apesar dos benefícios para o profissional, nomeadamente no suporte à avaliação do seu desempenho, o destino e uso desta informação pode expor de forma incorreta o profissional.

O controlo tecnológico tem influência sobre o comportamento dos profissionais, uma vez que os dados clínicos registados por si, podem ser facilmente consultados e partilhados com outros, e neste sentido influencia a sua cooperação num ambiente de colaboração. Apesar de existirem questões ou situações que podem colocar em causa a sua privacidade profissional, os profissionais são da opinião que estas não colocam em causa o exercício da sua atividade, e que a sua não adesão teria consequências para o utente. Não existe assim a noção de que a sua privacidade profissional é violada em relação às situações de partilha de dados. O grande condicionalismo surge na possibilidade de utilização indevida dos dados que resultam dos processos de monitorização da sua atividade como profissional, por exemplo processos de análise de produtividade e desempenho. A utilização indevida destes dados vai expor o profissional e comprometer o direito à sua privacidade profissional.

É necessária uma maior transparência das situações de partilha de dados e de colaboração, nomeadamente através de informação sobre os direitos e obrigações dos profissionais em relação à sua privacidade profissional. É necessário compreender quais os limites do controlo da sua atividade, assim como aquilo que pode ou não ser partilhado no que diz respeito ao histórico clínico do utente.

Os profissionais de saúde têm a noção que a sua própria ação ou omissão (ética profissional) tem uma influência significativa no sucesso das situações de partilha de dados com profissionais de outras organizações. O facto de um profissional omitir informação no âmbito da sua atividade, pode comprometer a continuidade dos cuidados de saúde numa outra organização, por outro profissional. A sua ação ou inação pode ter consequências, inclusive legais. A colaboração é desta forma imprescindível. Existe, contudo, a perceção que nem todos os dados registados devem automaticamente tornar-se públicos para todos os profissionais de saúde. Existem

áreas onde a informação é mais crítica do que em outras, onde os riscos para a privacidade são maiores.

É necessária uma maior transparência nas regras de acesso à informação, assim como normas para o registo clínico, adaptadas a esta realidade. Realidade que assenta cada vez mais numa malha de sistemas e em que um serviço hoje em dia já é cada vez mais da responsabilidade de várias organizações.

5.1.10 Proposição P10. Estrutura organizativa

Os desafios para a privacidade dos dados, quando estão envolvidas várias organizações com estruturas e modelos de funcionamento diferentes, são sem dúvida bastante complexos. Vários problemas podem comprometer a colaboração necessária para estas questões.

O sucesso da interoperabilidade como estrutura de suporte à partilha de dados depende das estruturas organizativas, e do conhecimento das restrições que podem condicionar tanto a sua disponibilidade como a sua agilidade. Este conhecimento pode facilitar o alinhamento pretendido e necessário entre as organizações envolvidas, no sentido de aumentar o nível de interoperabilidade. Este facto faz da capacidade operacional para a colaboração um fator decisivo ao alinhamento e padronização das questões da privacidade dos dados, que permitam a sua partilha entre organizações de uma forma continuada, num ambiente que se pretende seja seguro e confiável.

Pretendeu-se com a inclusão da proposição *P10. Estrutura organizativa* neste estudo identificar os aspetos essenciais ao desenvolvimento de uma maior capacidade de colaboração numa organização, assim como da abordagem ideal para o desenvolvimento das questões da privacidade para o conjunto das organizações.

Esta é uma proposição que apresenta uma variável dependente e dois itens de ligação com as fontes de evidências, como foi apresentado na seção 4.4.1.4 (Tabela 22).

É uma proposição que pensamos relacionada com as proposições P1 e P5, com uma influência direta sobre a privacidade dos dados, mas de influência inferior em relação a estas proposições, como representado na *framework* conceptual da Figura 14 (página 142). Em termos de interoperabilidade a proposição P10 está incluída no atributo *coordenação* do modelo OIM, e desta forma relacionada com a

compatibilidade entre as várias organizações, nomeadamente estruturas de coordenação e estilos de liderança, coordenação de iniciativas de interoperabilidade, e formas de acomodação das diferenças organizativas.

Do processo de análise sobre todos os itens de dados recolhidos no âmbito desta variável dependente da proposição P10, resultou a matriz de análise de opinião apresentada na Tabela 41, e com base nesta os seguintes resultados:

P10.v1 - Atendendo à complexidade das questões da privacidade dos dados para o contexto de colaboração, uma abordagem conjunta e integrada desta problemática, é a abordagem que melhor se adapta a esta complexidade. Não é garantidamente um requisito que possa ser resolvido isoladamente, com cada organização virada apenas para si. A experiência em interoperabilidade, técnica e organizacional, apesar de muito díspar entre organizações, é fundamental ao desenvolvimento de práticas orientadas à proteção dos dados. A proteção dos dados é um assunto que diz respeito a todas as organizações, dado que cada vez mais a informação é reutilizada por várias organizações. A definição de uma estratégia global para a privacidade dos dados pode depois refletir-se numa estratégia individual em cada organização, adaptada em função da sua atividade e contexto de utilização dos dados.

A colaboração/interoperabilidade entre organizações, e a existência de recursos humanos especializados e dedicados, são essenciais ao desenvolvimento e sucesso desta estratégia conjunta.

Este é um processo que deve ser liderado pelos responsáveis ao mais alto nível nas organizações. A operacionalização de uma abordagem conjunta depende também da intervenção de uma instituição com influência direta sobre todas as organizações participantes, neste caso o Ministério da Saúde ou a SPMS, através da regulação e definição de regras para a partilha de dados e para a sua proteção.

À semelhança da mudança de atitude em relação à segurança, provocada pelo desenvolvimento da PDS, deveria haver um percurso semelhante para as questões da privacidade e proteção de dados. É necessário que esta questão se torne uma prioridade, e sejam traçados objetivos comuns, com base numa estratégia que seja capaz de influenciar a agilidade das instituições.

Tabela 41 - Matriz de análise da opinião sobre P10. Estrutura Organizativa

P10	**Matriz de análise da opinião sobre P10. Estrutura Organizativa**		
Variáveis dependentes	*Padrão encontrado*	*Estrutura de suporte à interoperabilidade* *(Como abordar a complexidade das questões da privacidade dos dados para o contexto de partilha de dados)*	*Requisito "colaboração"* *(Colaboração no suporte ao desenvolvimento conjunto das questões da privacidade dos dados)*
P10.v1. A resolução das dificuldades em ambientes de colaboração em matéria de privacidade dos dados resultantes da heterogeneidade organizacional depende da compreensão comum da importância da interoperabilidade organizacional e de uma estratégia e acordos comuns para o seu desenvolvimento (cultura de interoperabilidade).	Abordagem conjunta Colaboração Estratégia global	Por iniciativa própria e de forma autónoma as organizações não vão conseguir. Tem que ser uma coisa integrada.	Não é fácil. Principalmente ao nível da interoperabilidade. É uma questão que tem vindo a ganhar importância, e em que se começa a pensar muito recentemente, mas nota-se que de instituição para instituição a própria experiência é muito díspar.
		Isto é um assunto que diz respeito a todas as organizações. Não é um problema isolado, da minha ilha.	
		Deve haver um modelo único para todas as organizações, e depois cada organização adaptá-lo à sua realidade. Tem que obrigatoriamente ser uma visão de conjunto.	É necessário haver recursos humanos e técnicos dedicados para a sua operacionalização. Uma maior preparação de quem está a coordenar as organizações. Uma maior partilha de experiências entre as organizações, assim como de conhecimento desta problemática.
		Tem que haver um desenvolvimento conjunto. Cada vez mais a informação não é das organizações. Claro que é muito mais complexo, mas acho que iria dar bom resultado. Depois em casos particulares, em situações pontuais, em determinadas instituições poderá ser necessário uma abordagem mais específica.	Será necessário uma decisão transversal do Ministério para operacionalizar uma abordagem conjunta. A decisão não significa "impor", não é o melhor caminho, mas passar a integrar os objetivos estratégicos, a cumprir, assumidos por todas as instituições para um determinado prazo.
		Depende da definição de uma estratégia global para a privacidade, que depois se vai refletir numa estratégia individual em cada organização.	Tipicamente se esta questão é levada diretamente para a área do IT morre imediatamente. Isto deve começar ao mais alto nível.
		Tem sempre que ser o Ministério da Saúde a implementar um processo como este.	O que o Ministério deveria fazer é concentrar-se em regular. Definir as regras para a partilha de dados, da garantia da confidencialidade. E depois as instituições têm que atuar, fazer.
	Agilidade Orientação Colaboração	Por exemplo ao nível da segurança não existe partilha de soluções, de boas práticas entre as organizações. A SPMS, com a PDS estão a dar um salto qualitativo neste âmbito. A troca de informação passa a ser multiplataforma. E quando se sensibiliza o IT Management para esta questão, estamos a implementar uma camada de segurança para estas questões.	Gradualmente o fator colaboração, passou a ser um fator de sucesso. No âmbito da privacidade de proteção de dados teremos de caminhar neste sentido.
		É necessário que esta questão se torne numa prioridade.	É importante que se perceba de forma clara este conceito de proteção de dados, quais são os limites da proteção e da não proteção. Isto tem de estar muito bem definido, e não está.
		Esta questão deveria ser vista como uma questão estratégica. Definir um conjunto de fases a atingir e ir aos pouco influenciar aquilo que é a agilidade das instituições.	Internamente é necessário promover uma maior agilidade para a colaboração, para o desenvolvimento de soluções conjuntas. Isto não é difícil de ultrapassar.
		Deveria surgir ao nível do Ministério da Saúde a orientação necessária.	Deveriam existir mais iniciativas de colaboração. Muitas instituições ainda olham muito apenas para a sua "quinta". Deveria haver alguém acima das instituições que mostre que os problemas são transversais e que dependem de um trabalho em conjunto.
		Teremos de ser ágeis. Se as situações estiverem bem definidas e documentadas podemos ser ágeis.	Se forem traçados alguns objetivos comuns, provavelmente as pessoas começavam a ter mais agilidade internamente para depois trabalhar estes objetivos.
		Com uma orientação vinda do Ministério ou da SPMS, as pessoas ficariam mais confortáveis, porque teriam à partida alguém com conhecimento na área.	Temos que perceber qual é nosso caminho de evolução tecnológica e incorporar já mecanismos de proteção da privacidade.
		A SPMS pode ser um órgão agregador e facilitador, que unifique esta gente toda e as faça trabalhar em conjunto. Mais do que se promover dentro da organização, a promoção do diálogo e entreajuda entre as várias instituições, tem que acontecer acima da organização.	São necessários recursos humanos, técnicos especialistas para intervir nesta área. Técnicos dedicados a esta área. Caso contrário estas questões passam para segundo nível.

Pode a este nível surgir por parte do Ministério da Saúde/SPMS a definição clara do conceito e da aplicabilidade da proteção e dados, e a promoção do diálogo e entreajuda entre as várias organizações no desenvolvimento de uma solução conjunta. A agilidade das organizações sai beneficiada se as situações estiverem bem definidas e bem documentadas.

Para o âmbito da privacidade e proteção de dados o fator colaboração é sem dúvida um fator de sucesso. Contudo, a preparação das organizações ao nível da privacidade e da interoperabilidade ainda são insuficientes. São necessários técnicos especialistas para intervir nesta área e completamente dedicados a esta área. Considerando que estão em causa problemas transversais a todas as organizações, é necessário promover iniciativas de colaboração, partilha de experiências, e transferência de conhecimentos. É necessário perceber qual a evolução tecnológica e incorporar mecanismos de proteção da privacidade.

5.2 Resultados finais das proposições do estudo

A formulação de proposições, e a sua divisão em variáveis dependentes, foi o instrumento utilizado para identificar e estudar os fatores com influência sobre a privacidade dos dados com o rigor científico exigível. As proposições permitem sem dúvida direcionar a nossa atenção para algo que deve ser estudado no âmbito da questão de estudo.

No ponto 5.1 foram apresentados os resultados obtidos ao nível de cada variável dependente. Todos os resultados foram apresentados isoladamente e não foi realizado qualquer cruzamento com os resultados de outras variáveis dependentes, ainda que incluídas na mesma proposição. A análise conjunta dos resultados obtidos em cada variável dependente, considerando o método *estudo de caso*, é decisiva sobre as conclusões a ter em relação à solidez dos pressupostos ao nível das proposições. Ou seja, tendo sempre presente as conclusões apresentadas anteriormente para cada variável dependente, é necessário numa fase posterior e a um nível superior, analisar estes resultados como um todo, e apresentar as conclusões para cada uma das dez proposições. Assim, e num primeiro momento, será apresentada para cada proposição a decisão sobre a validade do seu pressuposto; num segundo momento, são apresentadas as conclusões sobre a proposição que surgem das evidências

obtidas; por fim, e caso se justifique, será ajustada a *framework* conceptual do estudo de acordo com os resultados finais sobre as proposições.

P1. Experiência - O pressuposto da proposição *P1. Experiência* é que o planeamento conjunto de medidas transversais e eficazes para a proteção da privacidade dos dados em contextos de interoperabilidade, e consequente partilha de dados, está dependente da experiência (preparação) e da compreensão coletiva das questões da interoperabilidade e da proteção e privacidade dos dados.

> A qualidade dos resultados obtidos em cada uma das quatro variáveis dependentes, apresentados com detalhe na secção 5.1.1, confirma os pressupostos iniciais apresentados na secção 4.4.1.4 (Tabela 13), pelo que podemos considerar como válido e correto o pressuposto da proposição P1.

Muitas vezes o acesso e a partilha de informação entre profissionais e entre serviços dentro de uma instituição são deficientes. Esta situação deve-se a diversos fatores, entre os quais se destacam: a complexidade na integração e interoperabilidade; a falta de recursos especializados dentro de algumas instituições; a falta de imposição de regras claras ao setor da indústria de *software*; a deficiente arquitetura e tecnologia de muitos desses sistemas e, por fim, a não proliferação de integrações *via standards* internacionalmente reconhecidos (Reis, 2012).

A preocupação com os dados e com a sua proteção está a surgir nas organizações da área da saúde. Contudo, a preparação existente não é a suficiente face aos requisitos complexos da proteção de dados e dos ambientes de partilha de dados. As iniciativas estruturadas de partilha de dados entre serviços de várias instituições, apesar de existir uma unanimidade em relação às vantagens que apresentam, colocam numa fase inicial muitas questões aos responsáveis pela sua implementação. As questões técnicas de interoperabilidade são nesta fase as mais fáceis de ultrapassar. O mesmo não se consegue com a proteção de dados. A inversão desta situação só será possível se os profissionais apostarem numa maior experiência nas questões de interoperabilidade, e em projetos que envolvam a disponibilidade de dados a outras organizações. Por acréscimo ganha-se experiência na proteção de dados. Esta experiência vai permitir uma atuação proativa em relação às questões da privacidade dos dados, e fomentar uma visão estratégica para o seu desenvolvimento, em detrimento de soluções pontuais sem continuidade.

Esta evolução vai contribuir para que a experiência atual em proteção de dados, não se limite às tecnologias de segurança, e evolua para a perspetiva dos dados. É necessário um processo de mudança, suportado por profissionais com especialização em proteção e privacidade dos dados, capazes de desenvolver ao nível local um programa contínuo de proteção de dados, e interagir com profissionais de outras organizações no alinhamento de princípios e medidas, reunidas num programa alargado, aceite e aplicado às situações de partilha de dados sob a forma de um padrão.

Tal como aconteceu com outras iniciativas de colaboração (por exemplo, a implementação da RIS), em que o seu sucesso apenas aconteceu porque existia uma equipa coordenadora da iniciativa, com conhecimento e capacidade de influenciar o rumo dos SI ao nível local, o desenvolvimento de um plano comum a todas as organizações, que participam na PDS, para a proteção da privacidade dos dados, depende da criação de uma equipa permanente ao nível do Ministério da Saúde ou da SPMS. A sua experiência em projetos de interoperabilidade, em segurança, e em proteção de dados, são determinantes para que um processo orientado à proteção da privacidade dos dados se inicie com a solidez necessária. A prioridade deve ser a definição dos princípios e das orientações necessárias à implementação de medidas de proteção para os dados, e claro a sua privacidade.

A integração de sistemas de várias organizações, aumenta consideravelmente o número e tipo de profissionais com possibilidades reais de acesso a um maior conjunto de dados clínicos. Esta utilização requer uma utilização responsável da parte de todos os profissionais. Isto faz com que a preparação em proteção de dados não deva acontecer apenas ao nível dos profissionais responsáveis pela evolução tecnológica e pelos SI, mas sim incluir todos os profissionais para os quais existe uma justificação para o acesso aos dados. E neste sentido devem ser disponibilizados os meios necessários à melhoria desta preparação coletiva, nomeadamente baseados na publicação de informação, e em eventos que promovam o debate e a partilha de conhecimento em privacidade dos dados e em todas as questões relacionadas com este requisito. Têm que ser eventos construídos para diferentes públicos e para diferentes meios de comunicação. Chegar ao utente do SNS requer meios e recursos diferentes dos necessários para se chegar aos profissionais de saúde.

P2. Cultura de privacidade - Na base da proposição *P2. Cultura de privacidade,* encontramos uma forte convicção de que uma organização só terá sucesso no desenvolvimento das melhores práticas de gestão e utilização dos dados que respeitem a privacidade, quando esta constituir uma parte integrante da cultura organizacional, à semelhança do que acontece com outros valores. Aquilo a que chamamos de cultura de privacidade.

> Os pressupostos iniciais para as três variáveis dependentes, apresentados na secção 4.4.1.4 através da Tabela 14, foram confirmados na íntegra pela forte convergência dos resultados obtidos e apresentados na seção 5.1.2. Uma vez que se conseguiu atingir o padrão geral previsto para cada variável dependente, podemos aceitar como correto o pressuposto da proposição P2.

Não podemos pensar na privacidade como um requisito temporário, pontual, que diz respeito apenas aos dados sensíveis, e a uma determinada classe ou grupo profissional. Não podemos atuar apenas quando confrontados com situações de violação da confidencialidade de um conjunto alargado de dados. Devemos sim, pensar na privacidade como uma cultura de respeito pela vida privada e essencial à continuidade da atividade das organizações. As organizações devem incorporar a privacidade nos seus processos de negócio da mesma forma que incorporam outros valores fundamentais como a justiça e a transparência (Ernst & Young, 2013). É necessário integrar a privacidade na arquitetura dos sistemas e nas práticas organizacionais (Cavoukian, 2009).

O facto de as organizações reconhecerem o *valor* que constituem as boas práticas de utilização dos dados e a proteção da sua privacidade, constitui sem dúvida um passo decisivo para que este *valor* seja considerado de uma forma constante no ciclo de vida dos sistemas e dos dados. Podemos, com base nos dados deste estudo, afirmar que existe uma relação linear entre a existência de uma cultura em privacidade transversal a todas as organizações e o sucesso da privacidade dos dados, quer em situações de tratamento pontuais e isoladas, quer em situações de partilha contínua de dados.

Uma cultura de privacidade que se deve materializar nas organizações num maior conhecimento sobre os dados e sobre os riscos associados aos contextos de utilização, numa melhor compreensão do objetivo e do contexto de utilização dos dados, numa melhor perceção sobre as questões da privacidade, numa maior responsabilidade na

utilização e partilha de dados, e numa maior recetividade para com a implementação de medidas de proteção. O desenvolvimento de um ambiente de partilha de dados seguro e confiável, depende desta "*forma de pensar e agir*" face à exigência de respeito pela privacidade em geral e a privacidade dos dados em particular. Uma cultura de privacidade significa uma atitude responsável e uma compreensão coletiva das questões da privacidade dos dados.

Contudo, as dificuldades na definição dos conceitos associados à privacidade contribuem para que seja confundida com outros conceitos (Tavani, 2007). Saber atuar perante situações em que está em causa a privacidade da pessoa, ou da sua esfera pessoal, das suas comunicações pessoais, ou dos seus dados pessoais, ainda é uma dificuldade para a maioria dos profissionais. É desta forma importante identificar os aspetos da privacidade que nos permitem compreender e definir a privacidade (Introna, 1997).

Se as organizações promoverem o desenvolvimento de uma cultura em privacidade, conseguem definir com maior facilidade e clareza as situações de privacidade, os seus requisitos de proteção, assim como desenvolver a colaboração necessária com outras organizações no alinhamento destes conceitos e requisitos de privacidade. Só desta forma é possível que as organizações partilhem o mesmo conceito e objetivos para a privacidade dos dados, e que situações similares de privacidade existentes nas várias organizações sejam uniformemente protegidas. Este processo de mudança vai fomentar uma maior consciência nas pessoas para com a necessidade de garantir um elevado nível de proteção da privacidade, e um maior conhecimento sobre os riscos associados à sua não proteção. Podem desta forma anular-se situações problemáticas quanto ao tratamento de dados.

Os profissionais na área da saúde apresentam uma dificuldade na identificação dos diferentes tipos de privacidade, e no saber atuar perante diferentes situações de privacidade. A privacidade dos dados é de imediato associada à confidencialidade dos dados, e esta, por sua vez, única e exclusivamente relacionada com a necessidade de proteção da identidade do titular dos dados, neste caso o utente do SNS. A confidencialidade é na realidade a questão mais associada à privacidade dos dados. A dificuldade é ainda maior quando é necessário reconhecer aquilo que são medidas de segurança e aquilo que são medidas de privacidade dos dados.

Se as organizações estão a partilhar dados de uma forma contínua, então é necessário que apresentem medidas conjuntas de segurança e de proteção de dados. No cenário atual, a colaboração não está a ter o desempenho necessário a estes níveis, por forma a ser capaz de desenvolver medidas distintas para o nível da segurança e para o nível da privacidade dos dados partilhados. Este facto está relacionado com a insuficiente preparação nestas questões em todas as organizações. Mesmo medidas de segurança que à partida parecem simples, com regularidade são de difícil aplicação prática. É opinião dos participantes no estudo, que uma cultura em privacidade pode contribuir significativamente para que este cenário de utilização de dados se altere, melhorando a preparação de todos os profissionais no reconhecimento das questões da segurança, proteção, e da privacidade dos dados e na compreensão e cumprimento das medidas adotadas para estes níveis. É, contudo, muito claro que é necessário conciliar o desenvolvimento de uma cultura em privacidade, com a criação de condições para que as organizações apostem em profissionais especializados neste domínio. O apelo a que exista nas organizações um ou mais profissionais especializados nestas questões é generalizado, tendo em conta que os problemas relacionados com a incorreta utilização dos dados de saúde podem vir a agravar-se se as organizações não adotarem uma postura mais responsável.

P3. Segurança e infraestruturas - A proposição *P3. Segurança e infraestruturas,* assenta no pressuposto de que o sucesso e viabilidade das medidas de proteção para o nível da privacidade dos dados dependem da maturidade existente na interoperabilidade ao nível das medidas de segurança. Ou seja, é necessário compreender quais as soluções ao nível da segurança necessárias para se garantir que as obrigações de privacidade dos dados para todo o ambiente de interoperabilidade são cumpridas, assim como, qual a interoperabilidade necessária a este nível.

> Os resultados obtidos ao nível das cinco variáveis dependentes, apresentados na secção 5.1.3, estão de acordo com o padrão geral previsto para estas variáveis dependentes, não tendo sido identificado nenhum padrão alternativo. Considera-se assim válida a proposição P3.

De acordo com o regulamento geral sobre a proteção de dados (GDPR, 2012), em fase de debate público e aprovação, e que deverá substituir a atual diretiva de proteção de dados (CE, 1995) para o espaço europeu, deve ser assegurado um nível de segurança adaptado aos riscos que o tratamento representa e à natureza dos dados pessoais a

proteger. Falamos do risco associado à destruição acidental ou ilícita e a perda acidental, assim como ao tratamento ilícito, em especial a divulgação, a difusão, ou o acesso, não autorizados, ou a alteração de dados pessoais. As organizações devem adotar medidas técnicas ou organizativas necessárias a impedir o acesso de pessoas não autorizadas aos dados pessoais, impedir qualquer forma não autorizada de utilização de dados pessoais, e assegurar a avaliação da licitude das situações de utilização e tratamento de dados.

Os dados são um bem importante. Diversos dados que normalmente estão destinados a uso exclusivo das organizações de saúde, podem passar a ser de domínio público. Qualquer perturbação na qualidade, quantidade, distribuição ou pertinência dos SI pode expor a organização ao risco de sofrer ataques de fontes externas. Esta é razão pela qual se torna necessário gerir ativamente a segurança dos SI, bem como de dados críticos, não só para dar segurança aos profissionais de saúde e partes interessadas, mas também a todos os utentes do SNS, com os quais estes dados possam ser partilhados (Campos, 2012).

Apesar de os dados de saúde serem fundamentais à atuação conjunta das organizações do SNS, a segurança física e a disponibilidade dos sistemas continuam a ser as principais preocupações para os seus responsáveis. Cientes deste facto, tanto os responsáveis pelos SI, como outros técnicos com responsabilidade sobre o desenvolvimento da PDS, apontam para a necessidade de a segurança evoluir, por forma a melhor suportar os requisitos da privacidade dos dados.

No imediato, e com base na colaboração e partilha de experiências, as organizações devem padronizar as medidas e as melhores práticas de segurança de acordo com o contexto de partilha de dados. Esta uniformização vai permitir que cada organização adeque o seu nível de segurança no suporte ao nível de confiança estabelecido para a partilha de dados. Esta experiência é fundamental para que a colaboração possa evoluir para medidas direcionadas à privacidade dos dados, integradas com medidas de proteção ao nível da segurança.

A evolução que se pretende que aconteça ao nível da segurança é justificada pelo requisito de rastreabilidade dos dados e a possibilidade de se conseguir uma visão integrada da utilização dos dados não apenas para o interior das organizações, mas também quando os dados são transportados para outros sistemas. É necessário que se consiga em qualquer momento saber qual a localização dos dados, e quais os

utilizadores e processos envolvidos. Ou seja, devem ser disponibilizadas ferramentas que permitam a qualquer momento dispor de provas que revelem uma utilização responsável dos dados, e atuar perante situações desviantes e não cumpridoras das medidas em vigor. Os requisitos da rastreabilidade dos dados e da ativação de processos de responsabilização, apenas serão possíveis se existir uma evolução concertada dos conceitos de identidade digital e dos sistemas de controlo da identidade digital. A sua arquitetura deve evoluir, devendo no futuro suportar tanto a mobilidade dos profissionais, como dos dados. O desenvolvimento de uma federação que estabeleça ligações de confiança entre os sistemas instalados e a consequente partilha de dados de identidade digital é uma das hipóteses a considerar.

A realidade dos nossos sistemas de saúde, não é, na sua grande maioria, esta. Não é raro o profissional de saúde ter de se movimentar por várias aplicações que transportam dados entre si, com interfaces distintos, e em alguns casos obrigando mesmo a apresentação repetida de credenciais aplicativas, ao longo do mesmo processo (APDSI, 2013).

Um outro tema ainda limitado às infraestruturas e à segurança física, e que reúne um forte consenso quanto à sua evolução, constitui a análise do risco. O risco é o denominador comum em todas as questões no domínio da segurança. Apesar de pouco instituída, a análise de risco é considerada por todos como fundamental ao alinhamento de medidas de proteção dos dados, face aos riscos conhecidos, e muito comuns a todas as organizações. São necessários profissionais com um conhecimento suficiente neste formato de análises, capazes de por exemplo realizar análises de impacto sobre a privacidade, sempre que é considerada a aquisição ou desenvolvimento de uma nova solução que envolva a utilização de dados pessoais. Desta forma, a segurança da informação pode evoluir e incluir a privacidade dos dados, com resultados efetivos.

O risco é também uma constante nas situações de utilização secundária dos dados, ou reutilização dos dados, que no geral estão a causar muitas preocupações a todas as organizações. Regularmente são confrontadas com cada vez mais pedidos, tanto internos como externos, de utilização dos dados de saúde para determinadas finalidades que não a finalidade principal que deu origem à recolha destes dados. A atuação das organizações é muito similar e reconhecidamente insuficiente, procurando concentrar todo o processo de autorização de acesso aos dados sob a

responsabilidade de uma só pessoa, e em alguns casos disponibilizando algumas normas orientadoras.

Muitas tecnologias têm um impacto negativo sobre a privacidade. Tecnologias de *data warewhousing*, *data mining*, *data fusion* e *data meshing* foram desenvolvidas com o objetivo de explorar a informação que resulta da agregação de múltiplas fontes (Jericho Forum, 2007b). As situações de utilização secundária dos dados são muito similares entre as organizações e começam a ser transversais a todas elas. A recolha e reutilização dos dados tende no futuro a abranger mais que uma organização. As soluções de proteção dos dados devem assim adaptar-se ao contexto de utilização secundária e à natureza dos dados envolvidos. A colaboração entre organizações é decisiva para que as situações de utilização secundária dos dados apresentem um nível idêntico de proteção.

A disponibilidade dos dados é considerada tão importante quanto a disponibilidade dos sistemas, mas evitar a falência dos sistemas continua a ser prioritária em termos de recursos. Quanto aos dados, a segurança é responsável pela sua disponibilidade e em simultâneo garantir a sua correta utilização. Contudo, é necessário considerar casos de violação de dados pessoais, que devido à ausência de medidas de segurança ou ao não cumprimento das medidas existentes, afetou negativamente a privacidade do titular dos dados. As organizações devem neste sentido apresentar planos de contingência que lhes permitam no imediato anular os impactos negativos detetados e repor os dados comprometidos. As colaborações entre as organizações e a partilha de experiências são fundamentais ao desenvolvimento, e à sua otimização, de um plano de contingência de acordo com a criticidade dos dados e os riscos já conhecidos.

P4. Linguagem de privacidade (taxonomia) - A proposição *P4. Linguagem de privacidade* apresenta o pressuposto de que a definição clara e inequívoca das questões que dizem respeito à privacidade dos dados, assim como o esforço conjunto na definição de medidas de proteção, beneficia com a utilização partilhada de uma taxonomia em privacidade.

> Foram confirmados os pressupostos inicialmente apresentados para as duas variáveis dependentes, relacionados com as vantagens obtidas na definição das questões da privacidade, e com a agilidade na aplicação de medidas para o

ambiente alargado de partilha de dados, que podem surgir através da utilização de uma taxonomia. Os resultados obtidos, apresentados anteriormente na seção 5.1.4, permitem assim decidir pela aceitação do pressuposto apresentado para a proposição P4.

A privacidade dos dados é um domínio de investigação com uma importância crescente, nomeadamente na pesquisa de definições e terminologias que permitam uma melhor compreensão e classificação dos conceitos e termos da privacidade dos dados, com especial destaque nas necessidades que surgem com a expansão de ambientes colaborativos (Skinner et al., 2006). O desenvolvimento de ambientes colaborativos, como é o caso do setor da saúde, faz surgir inúmeros problemas de privacidade dos dados pessoais que é necessário resolver.

A utilização de taxonomias na área da saúde é uma prática regular e com resultados comprovados, essencialmente ao nível da qualidade e da estruturação da informação. O registo de muitos dos atos médicos depende da utilização rigorosa de taxonomias de âmbito internacional. Considerando a complexidade da problemática da privacidade dos dados, uma taxonomia pode influenciar a capacidade de partilha de informação e conhecimento das organizações a este nível, e desta forma influenciar a sua capacidade e agilidade de interoperabilidade. Uma taxonomia é sem dúvida uma ferramenta, um facilitador na definição precisa e no alinhamento das questões da privacidade entre todas as organizações. Em paralelo ou integrada com outras taxonomias, uma taxonomia específica para a privacidade dos dados vai contribuir para que, com maior facilidade, esta seja contemplada no ciclo de vida dos sistemas e dos dados.

P5. *Accountability* – responsabilidade e conformidade - A proposição *P5. Accountability – responsabilidade e conformidade* está relacionada com a necessidade de as organizações repensarem a sua abordagem à privacidade dos dados. A alteração que se avizinha no quadro legal de proteção de dados, por si só, não vai promover esta mudança de abordagem, que se pretende que aconteça. É essencial que a organização se sinta responsável pelos dados sob o seu controlo, e opte por um trabalho proativo em relação à proteção de dados. Neste sentido, e de acordo com o pressuposto da proposição P5, o sucesso da proteção da privacidade num ambiente de colaboração está dependente do desenvolvimento ao nível local de

um programa contínuo de análise de conformidade e monitorização da utilização dos dados, que demonstre o compromisso da organização para com o desenvolvimento de boas práticas na utilização dos dados.

> Os resultados obtidos nas quatro variáveis dependentes, apresentados em detalhe na secção 5.1.5, confirmam os pressupostos iniciais para todas as variáveis dependentes (ver Tabela 17, na página 152), não tendo surgido qualquer padrão alternativo. A qualidade destes resultados permitem-nos considerar o pressuposto desta proposição como correto.

Os dados obtidos nesta proposição demonstram uma realidade comum a todas as organizações: (1) os seus responsáveis, a todos os níveis, sabem da obrigação e responsabilidade em garantir a privacidade dos dados, dos seus utentes, dos seus profissionais, dos seus parceiros e da própria organização; mas (2) reconhecem não ter a preparação necessária que lhes permita identificar a forma e os meios para cumprir com esta obrigação. Colocar em prática medidas adequadas e eficazes com base nas obrigações e princípios da legislação em vigor em proteção de dados, assim como em normativos específicos da área da saúde, pode ser conseguido através de um programa de responsabilidade, capaz de alterar a atitude e o compromisso da organização para com estas questões. É o catalisador adequado face à complexidade deste problema.

Desenvolver um programa de responsabilidade, e de uma forma contínua monitorizar o sucesso da aplicabilidade de todas as medidas, tanto técnicas como organizativas, requer que em cada organização exista uma equipa multidisciplinar, que reúna profissionais com diferentes responsabilidades ou interesse sobre a privacidade dos dados. Enquadra-se perfeitamente nesta equipa a figura de profissionais especializados em privacidade, os quais darão melhores condições ao desenvolvimento de um programa, o mais abrangente possível, para a proteção de dados.

Os riscos associados aos processos de partilha de dados, assim como ao desenvolvimento de serviços comuns, fazem com que todas as organizações sintam a necessidade de evoluir, e colocar em prática medidas que salvaguardem a confiança na sua atividade. A confiança que se pretende que continue a existir entre organizações depende em parte desta evolução. E neste aspeto, a colaboração entre organizações pode e deve contribuir para a definição e uniformização de diretrizes e

de níveis de proteção de acordo com o contexto de partilha de dados, que devem estar na origem de um programa de responsabilidade.

Um programa de responsabilidade pressupõe o início de um processo contínuo de desenvolvimento, e à semelhança de outros processos de gestão, a monitorização e a análise de conformidade das medidas aplicadas, é uma tarefa obrigatória. Deve, desta forma, ser avaliado o cumprimento das medidas aplicadas e promover um melhor conhecimento sobre todas as situações de exposição de dados. Caso contrário, a continuidade deste processo fica comprometida. É necessário que se produzam resultados concretos sobre o estado da utilização dos dados, capazes de influenciar decisões de melhoria, assim como a confiança de todos em relação à forma responsável como os dados estão a ser utilizados.

Com os dados cada vez mais expostos ao exterior e a serem transportados entre sistemas, dispor de provas de evidência quanto à sua utilização é um desafio para os responsáveis pelos SI, preocupados com a perda de controlo sobre estes dados, e com a incapacidade de rastrear a sua utilização. Atualmente o registo (*account)* está vocacionado para o controlo de eventos de acesso de utilizadores ou equipamentos aos serviços (aplicações) e às infraestruturas, e não para o registo das ações efetuadas sobre os dados. Algumas aplicações já o fazem, mas ainda de uma forma isolada, com níveis de detalhe muito diferentes, e que dificilmente permite ir de encontro a um requisito já abordado neste estudo – a visão integrada da atividade de um utilizador.

Aquilo que deve constituir um registo que documente uma ação realizada sobre um dado ou um conjunto de dados, a evolução das arquiteturas dos sistemas de *accountability,* assim como a interoperabilidade necessária entre estes sistemas, deve acontecer através da colaboração entre organizações.

A certificação das organizações, e da forma correta e responsável como gerem os dados, é apontada por todos como um caminho a seguir, e com influência sobre a confiança entre as organizações. Apesar de não poder ser vista como a garantia do funcionamento efetivo da proteção de dados, resultaria num maior rigor para com a gestão de dados e na normalização de medidas de políticas de proteção. Contudo, experiências em outros processos de certificação levaram a que todos apontassem para a necessidade de existirem cautelas especiais neste processo. O custo e a complexidade envolvida, a par da insuficiente preparação de todos os profissionais, pesam sobre o receio existente.

A certificação dos SI pode transformar toda a cultura empresarial, tanto interna como externamente. Melhora a ética dos profissionais de saúde e a noção de confidencialidade que abrange todo o âmbito de trabalho deste setor. Permite à organização de saúde pôr em vigor a segurança da informação e reduzir a probabilidade de riscos de fraude, perda, e revelação de informação confidencial (Campos, 2012).

P6. Dados e manipulação de dados - O pressuposto da proposição *P6. Dados e manipulação de dados*, entendendo-se manipulação como tratamento, coloca a privacidade dos dados na dependência do conhecimento existente sobre os dados e da transparência dos processos de tratamento, em cada fase do ciclo de vida dos dados num ambiente de interoperabilidade. Está em causa o conhecimento sobre os dados e os processos que a organização tem e utiliza, para com base neste conhecimento conseguir proteger melhor. Ou seja, se esta não conhece os seus dados, e/ou os seus processos, dificilmente vai conseguir apostar num modelo de proteção centrado nos dados. As medidas que possam ser enunciadas não vão passar da teoria.

> Com base nos resultados obtidos com as quatro variáveis dependentes abordadas nesta proposição, e apresentados na seção 5.1.6, podemos concluir que estes validam os pressupostos iniciais das variáveis dependentes, assim como o pressuposto desta proposição. O padrão que resulta do tratamento dos dados obtidos é muito representativo. De salientar que ao nível desta proposição, foi possível identificar um novo tema padrão, não previsto e não alternativo, e que reuniu um elevado consenso de todos os participantes – a gestão da informação. Face à qualidade destes resultados, alterou-se a conceção inicial em relação a esta proposição, nomeadamente no que diz respeito à sua importância para a privacidade dos dados. Esta alteração será posteriormente refletida na versão final da *framework* conceptual.

A adesão das organizações à PDS, assim como a outras solicitações de colaboração em rede, demonstrou que o trabalho ao nível dos dados é nitidamente insuficiente e pouco qualificado. A obrigatoriedade de partilhar dados, não recolhidos para esse efeito, está a provocar reações em relação às estruturas de dados, e aos meios utilizados para armazenar, utilizar e partilhar dados. É uma reação tardia e que não vai provocar, no curto prazo, muitas alterações na atuação das organizações a este

nível. Isto porque, o conhecimento existente sobre os dados, o objetivo da sua recolha, as limitações de utilização, e a obrigatoriedade de proteção, não é o suficiente e está a condicionar a alteração necessária na atitude das organizações para com os dados. É uma realidade preocupante e que condiciona a capacidade da organização em desenvolver projetos de interoperabilidade e de proteção de dados, assim como o necessário reconhecimento do valor estratégico dos dados e dos riscos envolvidos na sua utilização. Provavelmente uma consequência da falta de profissionais especializados na gestão de dados, e na intenção de que outros profissionais abranjam estes domínios.

Até há pouco tempo, a gestão de dados foi vista apenas como uma das responsabilidades dos departamentos de TI. Este pensamento está gradualmente a alterar-se, com várias organizações finalmente a perceberem que os dados são acima de tudo uma responsabilidade organizacional. A prova disto são o desenvolvimento do conceito de *data governance*, e o início de programas neste domínio em muitas organizações (Moss & Adelman, 2015).

Na generalidade das organizações existe um entendimento sobre o conceito de ciclo de vida dos dados, sendo inclusive algumas das suas fases muito consideradas no desenvolvimento de sistemas, apesar de uma forma não estruturada. Contudo, ainda não se assiste à distinção dos requisitos de privacidade exigidos em cada fase do ciclo de vida dos dados. As fases de criação e utilização dos dados são mais associadas aos conceitos de privacidade, essencialmente porque se considera existirem mais riscos com a maior exposição dos dados. As fases de armazenamento, transferência (partilha), arquivo e destruição são por seu lado mais relacionadas com a segurança dos dados. Atualmente, o arquivo e a destruição de dados não estão a receber qualquer medida relacionada com a privacidade dos dados. As organizações tentam reter os dados o máximo de tempo possível, estendendo mesmo, para este efeito, o tempo de vida útil de algumas aplicações. No âmbito da PDS as fases de recolha/criação, utilização e transferência de dados, são as fases mais apontadas como prioritárias em relação à privacidade dos dados de saúde.

A orientação e o desenvolvimento de diretrizes e medidas para a proteção dos dados para todas as fases do ciclo de vida dos dados podem surgir da colaboração entre organizações, uma vez que os problemas são muito semelhantes a todas as

organizações, para os quais podem ser encontradas soluções aplicáveis a todo o contexto de colaboração.

A organização da informação, ao contribuir para a documentação e conhecimento de todos os processos de utilização de dados pessoais, para um conhecimento qualificado das situações que exigem medidas de proteção, são um elemento da gestão dos SI, de vital importância no suporte ao desenvolvimento de políticas de proteção dos dados de âmbito local, assim como o seu alinhamento com outras organizações. Facilita-se desta forma a compreensão do porquê das políticas de privacidade. A experiência que resulta da gestão da informação vai permitir às organizações: (1) conhecer com detalhe os dados, a sua criticidade e a sua disponibilidade; (2) clarificar para todos os profissionais o objetivo da recolha dos dados; (3) apresentar os limites da utilização dos dados; (4) facilitar a compreensão das medidas de proteção; (5) responsabilizar os profissionais face a situações irregulares de utilização de dados; (6) e sempre que necessário demonstrar da conformidade (P5) e compromisso da organização para com um programa de proteção dos dados.

As organizações estão a estruturar e armazenar maiores volumes de dados, e a investirem em meios que aumentam a sua disponibilidade. Estes processos não estão a ser estruturados com base numa avaliação prévia que analise a sua viabilidade em relação à intenção de recolha e utilização dos dados, de acordo com os requisitos da legislação em vigor. Tanto o objetivo, como o destino da utilização destes dados são pouco questionados e documentados.

Devemos aproximar tanto quanto possível as medidas de proteção dos dados, da sua unidade mais granular. Só desta forma podemos adaptar medidas de proteção sempre que a criticidade dos dados se altera em cada uma das fases do ciclo de vida. A existência de uma nomenclatura de classificação dos dados, ao permitir a classificação dos dados durante o seu ciclo de vida, vai facilitar a definição e aplicação de medidas de proteção e de segurança, orientadas aos dados. O acesso aos dados realizado atualmente com base no perfil profissional, não é suficiente para garantir que os dados mantêm medidas de proteção semelhantes quando são transferidos entre sistemas heterogéneos. Uma nomenclatura de classificação dos dados é fundamental na adaptação de medidas à criticidade e sensibilidade dos dados, e na garantia de que a sinalização inicial realizada aos dados num determinado sistema,

permanece inalterada quando os dados são utilizados fora do contexto onde foram gerados, assegurando-se assim o propósito da partilha de dados.

A heterogeneidade tecnológica e de funcionamento dos sistemas instalados nas organizações do setor da saúde podem constituir um forte condicionalismo ao desenvolvimento de políticas de proteção da privacidade aplicáveis ao ambiente de colaboração. A estruturação dos dados é o primeiro passo, para se conseguir, com base em padrões comuns, com regras para a classificação dos dados, regras de interoperabilidade, aplicar medidas de sucesso ao nível da proteção de dados. O sucesso a este nível tem influência direta sobre a melhoria das condições, para que se evolua nas questões da privacidade dos dados. É necessário criar as condições necessárias para que se mova a proteção, apenas centradas nas infraestruturas, para uma proteção centrada nos dados.

P7. Estratégia para a privacidade - O pressuposto da proposição *P7. Estratégia para a privacidade*, em linha com outras proposições mais relacionadas com o posicionamento das organizações e dos seus responsáveis para com as questões da privacidade, está relacionado com a necessidade de existir para o ambiente de colaboração uma estratégia para a privacidade dos dados, ligada com a estratégia de cada organização, que garanta o desenvolvimento contínuo de um programa de proteção da privacidade dos dados.

> Com base nos resultados obtidos ao nível das variáveis dependentes, apresentados na secção 5.1.7, apenas podemos afirmar que o pressuposto da proposição apresentado é plausível, faz sentido, uma vez que não se conseguiu confirmar na totalidade os pressupostos iniciais de todas as variáveis dependentes. As dificuldades registadas na variável dependente P7.v3 levaram a que não se tenha confirmado o pressuposto inicial desta variável, inviabilizando assim a validação total da proposição. Não se obteve contudo um padrão concorrente ou oposto, pelo que pensamos serem necessários mais estudos e mais dados que permitam obter mais certezas em relação a esta variável dependente. Apesar da dificuldade surgida, esta não é suficiente para alterar a conceção inicial em relação a esta proposição, naquilo que diz respeito à sua importância para a privacidade dos dados. Contudo, esta

dificuldade será posteriormente refletida na versão final da *framework* conceptual.

Os SI são para uma organização um fator estratégico de elevada importância no seu alinhamento e agilidade na resposta à mudança, que se pretende que aconteça nos próximos anos na área da saúde. A interoperabilidade entre sistemas é um dos pilares de suporte a esta mudança. É essencial para o aumento da disponibilidade de dados clínicos, assim como para o funcionamento de serviços partilhados. As organizações aumentam desta forma a sua dependência em relação aos dados, quer estes estejam sob o seu controlo, quer sob o controlo de outras organizações. Gradualmente começa a esbater-se a distinção entre aquilo que são dados gerados localmente e dados obtidos de um sistema externo. Evolui-se para o conceito de independência dos dados em relação às organizações de origem. A PDS é disto um excelente exemplo, com as barreiras técnicas que impediram a disponibilização dos dados a serem ultrapassadas com alguma facilidade.

Esta evolução faz com que os dados e a sua privacidade sejam atualmente, e cada vez mais, um recurso crítico e essencial à continuidade da atividade de uma organização na área da saúde, e no desempenho do SNS a nível nacional. São um fator com um peso significativo sobre a sua resiliência organizacional. Isto justifica que se desenvolva uma estratégia orientada para os dados e para a sua privacidade, devidamente enquadrada com os objetivos da organização, e que se assuma como um compromisso organizacional. A intervenção dos responsáveis de topo nas organizações no desenvolvimento de uma estratégia para estas questões é sem dúvida imprescindível. Estes reconhecem a sua responsabilidade no desenvolvimento de uma estratégia para a proteção e privacidade dos dados, num trabalho conjunto com outros profissionais, assim como as consequências que possam surgir com a ausência de atuação. Argumentam no sentido de esta estratégia ser integrada na visão estratégica dos SI.

A intervenção dos gestores ao nível dos dados e da sua proteção ainda é pontual, e não concertada com responsáveis de outras organizações. O não reconhecimento dos dados e da sua proteção como um valor estratégico contribui em parte para a não inclusão dos gestores executivos nesta problemática, e na ausência de medidas específicas para a privacidade dos dados ao nível dos SI.

As organizações devem promover uma visão integrada de todas as questões e decisões relacionadas com os dados e com a sua privacidade, nomeadamente com a visão estratégica existente para os SI e para as suas tecnologias. O facto de haver um desconhecimento dos riscos associados à maior exposição dos dados, resultante da sua massiva utilização em suporte digital, justifica em parte a ausência de uma estratégia clara. O conhecimento do risco é essencial para que se possa mudar a atitude não proativa instalada.

A solução de partilha de dados preconizada pela PDS, em que coexistem uma multiplicidade de sistemas, despertou e colocou dúvidas aos responsáveis das organizações em relação aos dados, às consequências da sua partilha, e à necessidade urgente de repensar o contexto de proteção destes dados. Face à necessidade transversal de soluções, apontam para a necessidade de uma estratégia abrangente e global a todas as organizações, com os gestores executivos com responsabilidades na replicação desta estratégia no interior das organizações.

Uma estratégia concertada de todas as organizações, que permita o desenvolvimento de uma abordagem comum para as questões da privacidade dos dados terá como consequência uma melhoria da cultura de privacidade (P2) existente. Todos estão de acordo que uma estratégia para a privacidade dos dados permite um desenvolvimento mais facilitado e mais ágil de uma cultura de privacidade. A definição dos princípios e das diretrizes que devem estar na base de uma estratégia local, assim como o seu alinhamento a este nível com outras organizações, deve resultar da colaboração e partilha de experiências entre organizações.

P8. Confiança e gestão da confiança - A proposição *P8. Confiança e gestão da confiança* está relacionada com a confiança entre organizações, como pilar fundamental à colaboração num ambiente de interoperabilidade, necessária à definição das questões da privacidade dos dados. Ou seja, pressupõe-se que só com base na confiança entre as organizações participantes, é possível aplicar com sucesso medidas de proteção da privacidade aceites por todas as organizações, e desta forma promover o desenvolvimento de um ambiente seguro e confiável para a partilha de dados e de serviços.

Para as três variáveis dependentes abordadas nesta proposição, os resultados obtidos (apresentados na seção 5.1.8) estão em consonância, alinhados com os

pressupostos iniciais formulados. Podemos desta forma considerar que o pressuposto desta proposição é correto.

A confiança intrínseca que esteve na base do desenvolvimento do ambiente alargado de partilha de dados e de serviços na área da saúde, pode não ser suficiente face ao aumento da complexidade das interações entre as organizações. São necessárias medidas adicionais, no sentido de fomentar uma maior confiança entre todos os participantes num ambiente de partilha de dados. Caso surja uma situação de utilização indevida de dados pessoais, que tenha um forte impacto sobre todo o ambiente de colaboração, assim como sobre a opinião pública, podem ficar comprometidos os objetivos na base da partilha de dados e diminuir significativamente a confiança das organizações e dos seus profissionais na solução implementada. É necessário garantir que a utilização dos dados é confiável. Contudo, é necessário compreender como é que uma organização sabe que pode confiar na utilização que outras fazem com os dados que lhes disponibilizou, assim como através de que meios pode avaliar este fator.

Neste sentido, um programa para a proteção de dados é essencial para a manutenção de um ambiente confiável e seguro de partilha de dados. A colaboração entre todas as organizações permite adaptar soluções conjuntas de proteção de dados de acordo com os riscos presentes nos processos de partilha de dados.

Através da interoperabilidade entre sistemas, a utilização e o controlo sobre os dados descentralizam-se. Aumenta a capacidade de reutilização dos dados e os riscos devido à maior disponibilidade dos dados. A interoperabilidade pode desta forma gerar desconfiança entre as organizações participantes, pelo facto de perderem o controlo sobre os "seus dados" a partir do momento em que são movidos para outro sistema.

A definição e acordo entre as organizações dos requisitos de privacidade, de medidas de segurança e de controlo da utilização dos dados, assim como uma maior transparência e informação sobre os processos de partilha de dados, vão contribuir para o aumento da confiança dos profissionais relativamente ao meio e aos dados partilhados.

A análise atempada do impacto sobre a privacidade que uma nova solução ou processo, que requeira a utilização de dados pessoais, possa apresentar, é reconhecida como um procedimento com influência sobre a confiança de todos os interessados na proteção da privacidade dos dados, procedimento este que já deveria

fazer parte das práticas de gestão. Ao transmitir-se a informação que esta análise foi realizada com sucesso, e que os riscos identificados foram considerados, consegue-se transmitir uma mensagem diferente de proteção da privacidade.

A informação que possa surgir, desta análise prévia dos riscos e efeitos negativos sobre a privacidade dos dados, é muito valiosa no suporte a outros processos integrados de gestão da privacidade.

P9. Ética e cooperação humana - A proposição *P9. Ética e Cooperação humana* apresenta como pressuposto que o sucesso das medidas para a proteção da privacidade dos dados, assim como dos objetivos que estão na origem da partilha de dados, dependem da iniciativa (atitude), confiança, transparência e conhecimento, em relação aos contextos de utilização de dados pessoais e clínicos, quer do titular dos dados, quer dos profissionais de saúde.

A compreensão sistemática das preocupações com a privacidade dos indivíduos ganha cada vez mais importância, uma vez que as tecnologias de informação estão a expandir a capacidade das organizações de armazenar, processar e explorar dados pessoais (Xu et al., 2008). O titular destes dados raramente tem conhecimento sobre como a organização está a utilizar os seus dados. Se o titular dos dados não for capaz de controlar a utilização normal ou abusiva dos seus dados, então quem será capaz? (Jericho Forum, 2007b).

> Os resultados obtidos e apresentados na seção 5.1.9 com as três variáveis dependentes abordadas nesta proposição permitiram validar os pressupostos iniciais formulados. A qualidade destes resultados permite-nos assim considerar o pressuposto desta proposição como correto. O recurso à utilização de dados quantitativos, por vezes desconsiderada em estudos interpretativos, demonstrou ser um instrumento muito útil de investigação e bem adaptado ao objeto de estudo, permitindo com sucesso a validação dos resultados esperados para as duas primeiras variáveis dependentes.

Podemos observar que num ambiente alargado de partilha de dados, neste caso a área da saúde, existe por parte de alguns agentes um interesse e uma influência diferenciados em relação à privacidade, ao seu funcionamento, e à sua proteção. O titular dos dados, o primeiro interessado na privacidade dos seus dados, é suportado por um conjunto de direitos, que lhe permitem exigir a proteção dos seus dados

pessoais e da sua privacidade pessoal, podendo também atuar, nomeadamente através do consentimento, sobre a gestão da privacidade dos seus dados. O profissional de saúde tem um interesse sobre a sua privacidade profissional, a qual depende da privacidade dos dados que resultam do ato médico e do controlo e monitorização da sua atividade profissional, e em simultâneo, um agente importantíssimo no desenvolvimento e no cumprimento de políticas de proteção da privacidade do titular dos dados. Os restantes profissionais, que apesar de não terem um interesse direto sobre a privacidade dos dados, podem utilizar os dados para outros fins, e apresentam uma influência de enorme responsabilidade sobre os sistemas que assistem a utilização de dados e sobre o desenvolvimento de medidas que garantam a sua utilização segura. A organização, interessada em manter a privacidade dos dados disponibilizados a outras organizações, é o principal agente com influência sobre o desenvolvimento de um programa de proteção, de acordo com as responsabilidades e obrigações da legislação e regulamentos setoriais.

O tratamento de dados pessoais deve ser concebido para servir as pessoas. A rápida evolução tecnológica criou a este nível novos desafios em matérias de proteção de dados, que em parte resultam do aumento considerável da partilha e recolha de dados. O setor da saúde é talvez o melhor exemplo deste aumento, onde se verificou um incremento assinalável na utilização de dados pessoais no exercício das suas atividades. Esta evolução exige às organizações a disponibilização de informação e meios que permitam ao titular dos dados poder controlar a utilização que é feita dos seus dados pessoais.

A possibilidade de o titular dos dados interagir com uma organização do SNS, no que diz respeito aos seus dados pessoais e de saúde, ganhou uma dimensão nunca antes atingida com a implementação da PDS. No passado, os meios ao dispor do titular dos dados, neste caso o utente do SNS, para que pudesse conhecer a utilização dos seus dados, não estavam previstos. Com a PDS, através do Portal do Utente, é dada ao titular dos dados, pela primeira vez, a oportunidade de participar, de agir. Acreditamos que, gradualmente, este vai ter uma atitude mais ativa e de maior exigência para com as organizações do SNS, que têm sob sua administração os seus dados de saúde.

A recolha de dados através da realização de um inquérito aos utentes do SNS, teve por objetivo conhecer aquilo que pode influenciar a sua atitude e compreensão em

relação à utilização dos seus dados, e de que forma podemos melhorar a sua compreensão sobre o funcionamento e a proteção de dados aplicada ao ambiente alargado de partilha de dados, neste caso o SNS.

Da análise dos dados obtidos, verificou-se que os participantes não têm dúvidas quanto ao seu papel na gestão da privacidade dos seus dados, apontando o consentimento como a funcionalidade de primeira linha, mas atribuindo às outras funcionalidades uma importância significativa. Apesar do avanço significativo na gestão do consentimento sobre os dados, reconhecem alguma dificuldade na clareza e compreensão das situações onde este é um requisito obrigatório.

Relativamente àquilo que é o contexto de partilha de dados, os resultados evidenciam uma percentagem elevada de 80% dos participantes, a classificarem as situações de partilha de dados entre instituições como as situações mais preocupantes em relação a outras situações, limitadas ao interior das instituições. No entanto, é preocupante o facto de 67% dos participantes não conseguir distinguir com base na informação disponível, quais as situações existentes de partilha de dados e quais as situações em que a partilha de dados não pode acontecer.

Quando falamos de informação sobre o funcionamento da proteção de dados, os dados recolhidos evidenciam um défice elevado, nomeadamente em informação sobre os direitos do titular dos dados, em informação sobre o compromisso e atividade da organização para com a proteção de dados, e em informação que permita ao titular dos dados atuar junto da organização face a uma situação suspeita de tratamento de dados. Mais de ¾ dos participantes atribui uma importância elevada ao envio de informação que caracterize o processo de partilha, e à disponibilização pública de conjuntos de informação que permitam uma maior transparência em relação às políticas, direitos, compromisso organizacional, e finalidades da utilização de dados.

A interoperabilidade entre sistemas é atualmente um meio de suporte à mobilidade do utente do SNS entre serviços e entre organizações, derivado ao aumento conseguido na acessibilidade aos dados clínicos, anteriormente muito limitada. Gradualmente é eliminada a necessidade de o utente se fazer acompanhar da sua informação clínica, nos mais variados formatos e suportes. Contudo, esta capacidade de mobilidade dos dados entre sistemas colocou, e está a colocar, enormes desafios em vários níveis organizacionais. Os profissionais de saúde são os primeiros a

questionar a segurança com que está a acontecer esta mobilidade de dados e a sua maior exposição.

Existe uma mudança na atitude dos profissionais de saúde face aos requisitos que resultam do ambiente de partilha de dados. Esta mudança é justificada por dois motivos: (1) a reutilização dos dados que resultam do pensamento e raciocínio clínico, por outros profissionais, e (2) o controlo tecnológico exercido cada vez mais sobre a sua atividade, podendo comprometer a sua privacidade profissional.

P10. Estrutura organizativa - O pressuposto da proposição *P10. Estrutura organizativa* está relacionado com o compromisso para com os valores e objetivos subjacentes à colaboração sob a forma de interoperabilidade organizacional, por forma a minimizar possíveis impactos sobre a privacidade dos dados que derivam de culturas e estruturas organizativas diferentes. Ou seja, a resolução das dificuldades que possam surgir em matéria de privacidade dos dados, comuns a várias organizações, depende da capacidade de colaboração destas organizações, no sentido de harmonizarem medidas de proteção para os dados partilhados.

> Os resultados obtidos com as três variáveis dependentes abordadas nesta proposição, anteriormente apresentados em detalhe na seção 5.1.9, permitiram validar os pressupostos iniciais destas variáveis. Podemos assim considerar a proposição como correta.

A partilha de dados entre organizações na área da saúde é um processo irreversível. Este processo está a ser concretizado quer por iniciativas do Ministério da Saúde, que normalmente abrangem um elevado número de organizações, quer por iniciativas isoladas, de duas ou mais organizações. A PDS constitui o projeto a nível nacional de partilha de dados com maior visibilidade, atendendo ao volume de dados partilhados e ao número de utilizadores envolvidos. Localmente estão a surgir projetos que contemplam na sua raiz a interoperabilidade entre aplicações locais ou entre aplicações dispersas geograficamente. As diferenças tecnológicas e aplicacionais não são, neste momento, um fator que condicione a integração completa de serviços ou a simples reutilização de dados de um outro sistema. Os dados, a sua estrutura, os seus requisitos de proteção, estes sim, são fatores que podem condicionar, ou mesmo impossibilitar, o nível de interoperabilidade desenhado para os sistemas. A

preparação das organizações a este nível é nitidamente insuficiente, como já referimos anteriormente.

Quer sejam projetos de partilha de dados de âmbito nacional ou projetos de menor dimensão, circunscritos a duas organizações, o sucesso das medidas de proteção de dados, com impacto sobre a sua privacidade, depende do fator colaboração – também denominada de interoperabilidade organizacional. A proteção de dados não é responsabilidade de uma das partes apenas. Para projetos como a PDS, é um problema e uma responsabilidade transversal a todo o SNS.

Neste sentido, os responsáveis quer ao nível executivo quer ao nível dos SI, defendem uma abordagem conjunta e integrada de todas as partes envolvidas, como forma de lidar com a complexidade e dinâmica das questões da privacidade dos dados. A definição de uma estratégia global para o seu desenvolvimento pode posteriormente ser adaptada à realidade de cada organização, em função da sua atividade e contexto de utilização dos dados. Estes responsáveis reconhecem que este é um processo totalmente dependente da interação entre as organizações, e da prestação dos profissionais com competências em privacidade dos dados, sempre com a liderança dos responsáveis executivos. Caso contrário este assunto nunca vai receber a prioridade necessária.

Para projetos de âmbito nacional a operacionalização de uma abordagem conjunta depende da liderança do Ministério da Saúde, e também da SPMS. É necessário definir e propagar regras para as estruturas de dados que facilitem a sua interoperabilidade, assim como regras de proteção. O ritmo de desenvolvimento de soluções, que consideram a utilização de dados pessoais e de saúde, não está a ser acompanhado por soluções concebidas desde o primeiro momento para a proteção destes dados. A proteção e a privacidade dos dados devem caminhar lado a lado com a evolução tecnológica, e serem consideradas logo no primeiro momento de desenvolvimento. É necessário estar sempre a olhar para o futuro e entender se o rumo tecnológico é o esperado, e qual o impacto que este pode ter para a privacidade e para a segurança (Kalish, 2015).

5.3 Adaptação da *framework* conceptual aos resultados do estudo

A *framework* conceptual é uma representação gráfica da questão de estudo e reflete a teoria subjacente a cada proposição. Permite compreender a importância de cada um dos subdomínios de fatores estudados, ao abrigo de cada proposição, a sua

prioridade, assim como a sua relação ou dependência com os restantes subdomínios. Neste sentido, é importante a sua revisão atendendo aos resultados finais obtidos. Durante a apresentação dos resultados finais ao nível das proposições do estudo, foram identificas situações com implicações na versão inicial da *framework* conceptual apresentada na Figura 14, na página 142. Neste sentido a versão final apresentada na Figura 21, apresenta quatro alterações em relação à versão inicial:

a. O aumento da importância do subdomínio de fatores associado à proposição P6. Dados e manipulação de dados;
b. A não validação integral da proposição P7;
c. A existência de influência entre as proposições P1 e P6;
d. A existência de influência entre as proposições P2 e P8.

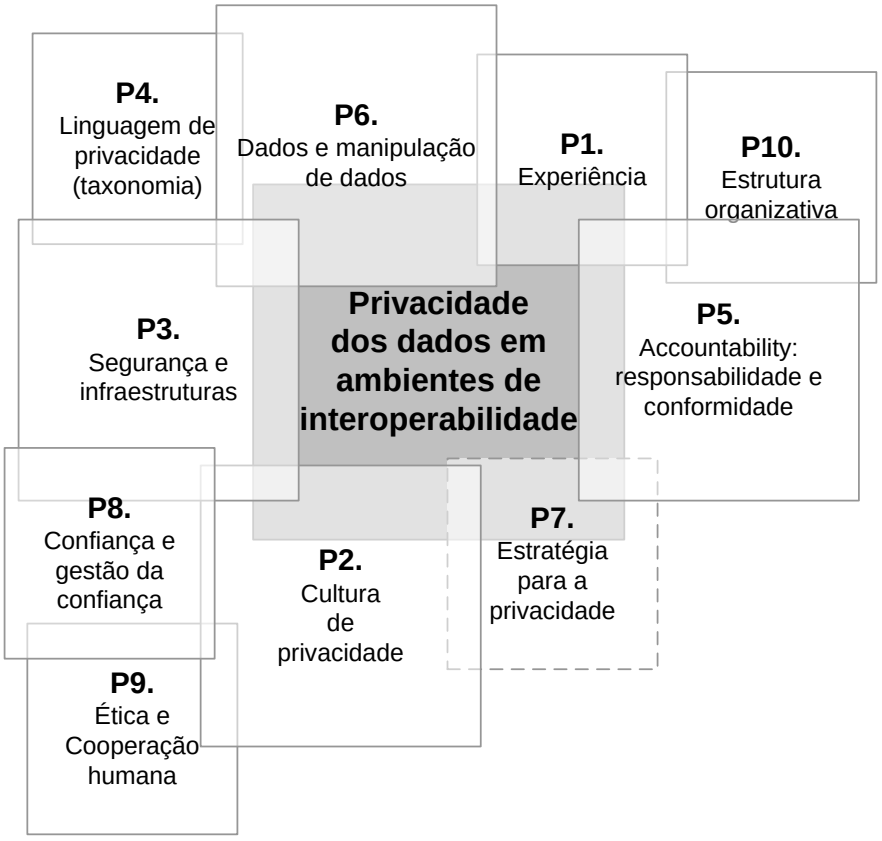

Figura 21 - *Framework* conceptual, versão final

Capítulo VI - Conclusões

No capítulo anterior foram apresentados, com o detalhe exigível, os resultados finais da investigação para cada uma das dez proposições, com base na análise dos dados obtidos ao nível das suas variáveis dependentes. Foram desta forma validadas a importância, a influência, e o foco de cada proposição em relação à problemática em estudo.

Neste último capítulo apresentam-se de forma sumária os resultados da investigação, nomeadamente as suas conclusões finais, as suas principais limitações, e oportunidades futuras de investigação.

6.1 Conclusões

Os objetivos definidos para este estudo previam que, da sua realização, resultassem determinados contributos teóricos e práticos. Neste sentido, importa neste último capítulo apresentar e refletir sobre as contribuições deste estudo à luz dos objetivos orientadores deste estudo.

Em termos **teóricos**, conseguiu-se com sucesso cumprir com o objetivo principal deste estudo, através de uma abordagem rigorosa tanto à problemática como ao domínio em estudo. Neste sentido, foi possível proceder à *identificação dos fatores com influência sobre a privacidade dos dados, em ambientes onde, por força da interoperabilidade estabelecida entre sistemas, estes são partilhados de forma estruturada e contínua.*

O primeiro objetivo específico contemplou assim, a *identificação e estudo dos fatores com influência sobre a dinâmica da privacidade dos dados, em contextos de interoperabilidade entre sistemas sociotécnicos*. O sucesso das medidas de proteção da privacidade dos dados depende num primeiro momento do sucesso alcançado ao nível organizacional, ou seja, da interoperabilidade conseguida entre pessoas e processos, e num segundo momento ao nível da interoperabilidade tecnológica. A colaboração entre organizações no desenvolvimento de medidas de proteção da privacidade dos dados, deve assim considerar os subdomínios de fatores como a experiência, a cultura de privacidade, a segurança e as infraestruturas, uma linguagem de privacidade, a *accountability* (responsabilidade e conformidade), os dados e a manipulação de dados, uma estratégia para a privacidade, a confiança e

gestão da confiança entre organizações, a ética e cooperação humana, e as estruturas organizativas.

O terceiro objetivo específico permitiu posteriormente proceder *à validação dos fatores com influência sobre a privacidade dos dados identificados* no âmbito do primeiro objetivo específico, no cenário privilegiado da área da saúde. Deste processo destacamos as seguintes conclusões finais:

- Os dados sempre receberam uma importância muito mais elevada na área da saúde, e a sua privacidade foi sempre muito debatida, mesmo quando o papel constituía o seu principal suporte. A exigência crescente de melhores serviços, de melhor informação, e de uma acessibilidade permanente e descentralizada aos sistemas, promoveu a revolução tecnológica a que temos assistido até aos dias de hoje, mas colocou as organizações num cenário precário quanto à proteção de dados.

  No geral, as organizações na área da saúde apresentam, em relação às questões da privacidade, uma visão "insuficiente" e por vezes "distorcida" do problema, que resulta de uma preparação pouco qualificada. Em cada classe profissional existe uma noção muito própria destas questões, que resulta da sua atividade profissional e do conhecimento dos riscos associados à utilização dos dados. Este conhecimento diferenciado de cada perfil profissional, em conjunto com aquilo que é a **experiência** da organização, foi essencial para compreender e validar os fatores identificados com influência sobre a complexidade da privacidade dos dados para o domínio da colaboração.

  É necessário que a preparação e **experiência** das organizações em relação à proteção dos dados evoluam, no sentido de responder à preocupação crescente para com a privacidade dos dados. Somente com uma maior experiência e conhecimento tanto em interoperabilidade como em proteção de dados, é viável o desenvolvimento de medidas transversais para a proteção da privacidade dos dados, aplicáveis ao ambiente de interoperabilidade. Esta é uma questão de *eficiência coletiva*.

  A necessidade de uma visão completa e integrada das questões da privacidade dos dados, assim como a complexidade dos requisitos para a sua proteção, requerem que existam nas organizações profissionais especializados e dedicados à privacidade dos dados.

- A privacidade é um compromisso e uma responsabilidade coletiva, sobretudo quando as organizações partilham dados pessoais e de saúde. A privacidade não pode resultar de uma visão caso-a-caso, isolada, mas sim de uma visão de conjunto, aplicada ao domínio da colaboração entre organizações. As melhores práticas de gestão e utilização de dados que respeitam a privacidade do seu titular, atualmente muito dependentes de medidas técnicas de segurança, estão também dependentes do reconhecimento da privacidade como parte integrante da cultura organizacional. A privacidade não é um requisito temporário, pontual, aplicável unicamente à sensibilidade dos dados de saúde, e da responsabilidade de uma única classe profissional, neste caso os profissionais de saúde. Antes pelo contrário, a privacidade é um *valor*, transversal a todas as organizações do SNS, a todas as situações de utilização de dados pessoais, especialmente dados de saúde, e que é da responsabilidade e do interesse de todos os profissionais que interagem através dos SI. Uma **cultura de privacidade** significa, assim, uma cultura responsável e um compromisso coletivo para com este *valor,* que é a privacidade dos dados. Pode contribuir significativamente para que o cenário atual de utilização de dados se altere.
- Os sistemas atuais foram desenvolvidos com o pressuposto de que tanto os dados como os mecanismos de segurança vão estar apenas sob a gestão e o controlo de uma organização. As situações que contemplam a partilha de dados, especialmente entre organizações, obrigaram a que este pressuposto fosse invariavelmente questionado. Atendendo a que os sistemas não consideram a privacidade dos dados como um requisito de primeira ordem, traduzido em mecanismos de segurança ajustáveis à sensibilidade dos dados, faz com que um contexto de partilha de dados seja ainda mais complexo. Na sua maioria, os sistemas controlam os dados na ótica do conjunto de registos e não na ótica do elemento de dados o mais granular possível.

  A interoperabilidade ao nível da camada de **segurança e infraestruturas** é a base sólida necessária ao desenvolvimento de um plano conjunto para a proteção da privacidade dos dados. A partilha de conhecimentos, soluções ou experiências, e a compreensão dos requisitos de segurança necessários, têm uma forte influência sobre a disponibilidade contínua dos sistemas que suportam a criticidade dos dados partilhados. O alinhamento de medidas de

segurança orientadas à privacidade dos dados, assim como medidas orientadas à resiliência das infraestruturas, devem resultar de iniciativas estruturadas de colaboração. A interoperabilidade a este nível deve contribuir para que as organizações evoluam em áreas como a análise do risco, os sistemas de identidade digital, na normalização de situações de utilização secundária de dados, e em planos de contingência para situações de violação da privacidade dos dados.

- Esta evolução das organizações em áreas tão distintas, pode ser facilitada pela adaptação de uma terminologia, uma **taxonomia** para as questões da privacidade dos dados, e no seu funcionamento em ambientes de interoperabilidade. É uma ferramenta imprescindível ao diálogo e ao desenvolvimento objetivo de medidas de proteção da privacidade. Muitas das dificuldades existentes no reconhecimento dos requisitos e noções, associadas à proteção de dados, na adaptação de medidas e na sua transposição para os SI, podem ser eliminadas se surgir uma **taxonomia**, um vocabulário em privacidade, para a especificidade da área da saúde, integrada com outras taxonomias, e aplicável ao ambiente de partilha de dados.
- Mudar a atitude atual das organizações, predominantemente reativa, para uma atitude pró-ativa em relação às questões da privacidade dos dados, à semelhança daquilo que presenciamos noutros domínios, requer um compromisso e uma maior **responsabilidade** das organizações na definição de objetivos para a proteção de dados. Reconhecer a importância da privacidade dos dados e dos riscos associados ao tratamento de dados, é o primeiro passo para que a organização disponibilize os recursos necessários, para que uma equipa multidisciplinar implemente um plano integrado de proteção dos dados e da sua privacidade. Em simultâneo, esta equipa deve ser capaz de operacionalizar processos de avaliação de **conformidade** das medidas implementadas, assim como colaborar com outras organizações no alinhamento de medidas de proteção para as situações de partilha de dados. As organizações necessitam de sair urgentemente da situação de indiferença para com os riscos associados à privacidade dos dados, e iniciar um processo de mudança com base num programa de responsabilidade a nível local, e na sua articulação com diretrizes para o ambiente de colaboração. A certificação destes processos pode, apesar dos custos e da complexidade, trazer às

organizações a normalização necessária das medidas de proteção, assim como uma maior dinâmica entre as estruturas envolvidas.

- Otimizar a relação privacidade-proteção-segurança dos dados em ambientes sistémica e tecnologicamente heterogéneos e desregulados, deve iniciar-se por soluções ao nível dos **dados**, nomeadamente ao nível da sua estrutura, dos processos de utilização e intercâmbio com base na interoperabilidade entre sistemas. Na área da saúde, o número de processos que envolvem dados pessoais é, comparado com outras áreas, muito elevado, e as organizações continuam a instalar soluções tecnológicas que aumentam a sua disponibilidade e consequentemente a sua maior exposição, sendo que gradualmente esta exposição ultrapassa os limites "geográficos" das organizações. Por defeito, estes processos não são documentados nem conhecidos, com base numa norma ou padrão estruturado, nem foram sujeitos a uma análise prévia de impacto sobre a privacidade, prospetora dos riscos existentes. Nem tão pouco se encontram definidos de forma clara os objetivos associados à recolha de dados, as limitações à sua utilização, o tempo máximo de retenção, e os procedimentos para eliminar dados.

  A gestão da informação (com evolução para o conceito de *Data Governance*), como ferramenta, pode gerar uma base de conhecimento devidamente estruturada, sobre todo o ciclo de vida dos dados, capaz de suportar processos de desenvolvimento de medidas práticas de proteção de dados, e em simultâneo valorizar um ativo essencial e crítico à continuidade das organizações – os dados. Se há algumas décadas atrás foi vital os dados serem independentes das aplicações, entramos hoje numa fase em que os dados gradualmente ficam independentes das organizações. Não pertencem a uma organização, mas a um conjunto de organizações, que os utilizam em simultâneo.

- Contudo, uma visão integrada de todas as questões e decisões para o domínio dos dados e da sua proteção, depende de uma **estratégia para a privacidade**, de preferência integrada com a estratégia conseguida para os SI. Não podemos ter a pretensão de atuar sobre a privacidade dos dados com a intenção de, no imediato, apresentar uma lista de medidas de proteção. Seria sem dúvida um trabalho inglório. O sucesso a este nível passa por (1) perceber

se o conhecimento existente é suficiente para colocar em prática um projeto tão ambicioso quanto o da proteção de dados; (2) conhecer as ferramentas necessárias ao suporte de um processo que nunca vai estar terminado; (3) avaliar o real compromisso da organização para com este objetivo; (4) apresentar uma capacidade e disponibilidade de colaboração com outras organizações na preparação de processos de partilha de dados; e (5) avaliar se a maturidade de gestão do sistema de informação é a suficiente.

A maior disponibilidade e exposição dos dados clínicos estão, em parte, a conseguir que os vários responsáveis pelo funcionamento dos SI assumam que é necessário uma visão de médio e longo prazo para as questões da privacidade dos dados. Em simultâneo, deparam-se com aspetos estruturantes que são transversais a todas as organizações em relação aos dados, para os quais é urgente uma estratégia global que defina diretrizes comuns para a sua integração e interoperabilidade.

- Apesar de existir hoje uma maior facilidade de colaboração, a vários níveis, entre as organizações, geralmente suportada numa confiança intrínseca e débil em medidas de proteção de dados e de privacidade, a perda de controlo sobre os dados partilhados e a perda da privacidade profissional podem condicionar a **confiança** necessária ao funcionamento transparente do ambiente de partilha de dados.
- Neste sentido, é importante compreender aquilo que, no domínio da **ética e cooperação humana**, pode influenciar a postura, a avaliação, a aceitação ou oposição manifestadas pelos profissionais de saúde, assim como pelos titulares de dados em relação às iniciativas de partilha de dados de saúde. São necessários meios e informação que vão de encontro à expetativa crescente do titular de dados, numa maior transparência e informação em relação à proteção de dados e da responsabilidade das organizações do SNS. O titular de dados pretende mais informação sobre o compromisso das organizações para com a proteção de dados, sobre os processos de partilha de dados e possíveis utilizações secundárias dos seus dados de saúde, assim como sobre os seus direitos em matérias de proteção de dados.
- Face a todos estes fatores, que apresentam como denominador comum a "colaboração", é necessário olharmos para a organização, e orientar a sua

estrutura organizacional, de modo a gerar capacidade de interoperabilidade. É necessário, para o sucesso da privacidade dos dados, que cada organização se adapte ao ambiente de colaboração, e desenvolva a interoperabilidade necessária e essencial à partilha de conceitos, ferramentas e medidas de proteção. Apenas se a privacidade dos dados se tornar numa prioridade para as organizações, é possível que um conjunto de objetivos desencadeie uma abordagem conjunta, capaz de influenciar a agilidade das organizações, na sua capacidade de colaboração e interação. Caso contrário, as organizações continuarão a participar em processos irreversíveis de partilha contínua de dados de saúde, com os requisitos de proteção ao nível da privacidade a não serem devidamente considerados. Os dados vão continuar a ser apenas protegidos com base no *invólucro* da segurança, insuficiente à proteção da sua privacidade.

Em paralelo com os objetivos específicos relacionados com a identificação e estudo dos fatores com influência sobre a privacidade dos dados em ambientes de interoperabilidade, o segundo objetivo específico contemplou a seleção e utilização de um modelo de interoperabilidade no suporte à temática em estudo. A utilização do modelo de maturidade da interoperabilidade OIM no suporte ao estudo numa perspetiva organizacional, revelou-se muito útil, obrigando-nos a estruturar o conhecimento desenvolvido de acordo com a estrutura funcional proposta por este modelo, já testado em vários contextos. Apenas desta forma, é possível distinguir os requisitos para a proteção de privacidade dos dados que resultam de um nível básico de interoperabilidade ou de um nível alto de interoperabilidade. Apesar do contexto de interoperabilidade se manter, a complexidade da proteção de dados aumenta quando passamos para níveis superiores de interoperabilidade. Em simultâneo, o alinhamento dos fatores estudados em relação aos quatro atributos do modelo, *preparação*, *compreensão*, *coordenação* e *ética*, facilitou o entendimento sobre a forma como estes fatores podem afetar ou influenciar, em termos tecnológicos e organizacionais, o funcionamento da interoperabilidade.

Pode, contudo, ser questionado porquê este modelo e não outro, dado que existem outros modelos que poderiam ser utilizados. A qualidade da informação acessível sobre este modelo teve um peso decisivo sobre esta decisão, assim como as várias melhorias que sofreu desde a sua publicação original. Contudo, existe a perceção de

que os fatores identificados com influência sobre a privacidade dos dados, com alguma facilidade podem ser adaptados a outro modelo de interoperabilidade, essencialmente por duas razões: primeiro, porque a filosofia de estruturar a interoperabilidade em níveis é comum à maioria dos modelos publicados, e segundo, porque muitos dos modelos mais recentes (alguns específicos para determinados domínios) se basearem nos primeiros modelos de interoperabilidade publicados.

Em termos **práticos,** e atendendo a que o quarto objetivo específico deste estudo (o objetivo d) apresentado na secção 1.3 do Capítulo I) pressupõe a compreensão dos requisitos que devem estar na base do desenvolvimento de um programa de proteção da privacidade dos dados para o contexto de interoperabilidade, foi possível compreender a complexidade desta questão e apresentar um contributo prático no suporte ao desenho e operacionalização de um programa orientado à privacidade dos dados.

Um programa sólido para proteção da privacidade dos dados deve resultar da solidez do trabalho realizado ao nível da estruturação e conhecimento dos dados, da segurança, da responsabilidade organizacional e da preparação coletiva. O sucesso de um programa para a privacidade dos dados depende do desenvolvimento de outros domínios como: os dados, a gestão da informação e a gestão do risco. Caso contrário, podemos elencar um conjunto de medidas e alinhá-las numa qualquer política de privacidade, sem nunca conseguirmos perceber se o objetivo foi atingido. A privacidade dos dados requer um trabalho efetivo de aplicação de medidas eficientes de proteção e, em simultâneo, requer que se prove que estas medidas estão ajustadas à realidade e aos perigos da utilização dos dados, e se consiga introduzir melhorias contínuas. É comum encontrarem-se medidas de segurança que, sem intenção, englobam as questões da privacidade. Este desconhecimento contribui para uma fraca eficiência destas medidas, pelo facto de não serem suficientemente compreendidas.

A capacidade de compreensão das questões com influência sobre a privacidade dos dados é diferente entre organizações e entre classes profissionais. Desenvolver um programa de proteção para a privacidade dos dados, implica que se contemplem vários subdomínios no interior de um sistema de informação, e se apresentem medidas práticas que todos compreendem e aplicam. A interoperabilidade entre

sistemas, que está na base da partilha de dados e de serviços, aumenta a complexidade das medidas de proteção, pois muitos dos requisitos de proteção dependem agora da colaboração entre organizações. Este é, garantidamente, um processo difícil de enraizar na cultura de utilização de dados.

Conceber e operacionalizar um programa de proteção entre várias organizações, adequado à especificidade do ambiente de partilha de dados, depende de uma abordagem complementar da apresentada na *framework* conceptual (ver Figura 21, na página 257). Os profissionais, com influência sobre o sucesso de um programa de proteção da privacidade dos dados, necessitam de ferramentas de apoio, (1) ao desenho de políticas de proteção orientadas à privacidade dos dados, integradas com outras medidas de proteção já em vigor, assim como (2) à operacionalização destas medidas, tanto a nível local como em colaboração com outras organizações. No fundo, obter suporte à criação e disponibilização de conhecimento no apoio ao desenho de medidas de proteção, e à ativação de forma efetiva e eficiente deste conjunto de medidas de proteção.

É assim importante dispor de instrumentos que permitam localmente suportar um desenvolvimento integrado de um programa para a proteção da privacidade dos dados, e ao mesmo tempo permitam agilizar a interoperabilidade necessária com programas similares que estão a acontecer nas restantes organizações. A qualidade das ferramentas e das fontes de informação que as organizações dispõem para o desenvolvimento de um programa de proteção da privacidade dos dados, é atualmente insuficiente. A segurança dos sistemas é comprovadamente a ferramenta mais desenvolvida, e que recebe mais recursos. Isto significa que um programa abrangente e integrado para a privacidade dos dados tem que, obrigatoriamente, ser antecedido por um trabalho de preparação e disponibilidade de mais ferramentas de suporte. E todas estas exigem profissionais com experiência em privacidade dos dados.

Com base no conhecimento adquirido nos subdomínios abordados no estudo, é possível apresentar uma proposta e indicar os instrumentos que devem estar na base da definição e operacionalização de um programa para a proteção da privacidade.

No que diz respeito às "ferramentas" necessárias ao desenvolvimento de um programa de proteção, e considerando todos os resultados anteriormente validados, podemos reunir todos os fatores estudados em três "ferramentas", as quais,

pensamos, devem estar na base da definição e justificação das medidas necessárias para a proteção da privacidade: a gestão da informação, a análise do risco, e a segurança dos SI e da informação, como representado na Figura 22. São três ferramentas essenciais no suporte à interoperabilidade entre organizações.

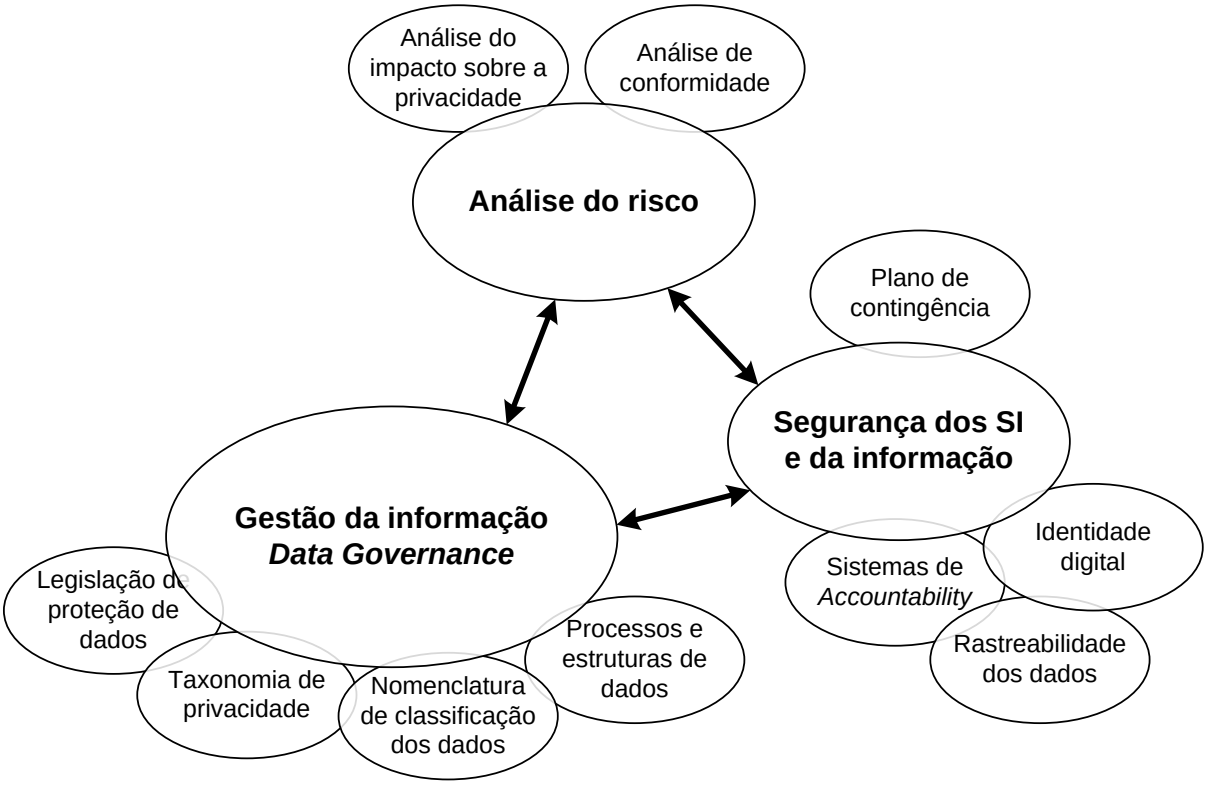

Figura 22 - Ferramentas de suporte ao desenho de um programa de proteção da privacidade dos dados

O maior protagonismo atribuído à **gestão da informação** está relacionado com a sua potencial intervenção sobre a gestão de todo o ciclo de vida dos dados. E neste sentido, pode integrar o desenvolvimento de alguns dos fatores como (1) a transposição dos requisitos da legislação para as práticas de utilização de dados, (2) o desenvolvimento de uma taxonomia específica para a privacidade dos dados que contribua para um diálogo e desenho de medidas mais objetivas, (3) uma nomenclatura de classificação dos dados, essencial para a atribuição de medidas de proteção com base no tipo e criticidade dos dados e não somente com base no perfil do utilizador, e (4) a documentação e conhecimento de todos os processos e estruturas de dados.

A **análise do risco** constitui uma ferramenta importantíssima de conhecimento das várias situações de utilização dos dados e dos riscos associados. O conhecimento do

risco vai desencadear medidas de proteção. Tanto a realização de processos de análise do impacto sobre a privacidade, como de processo de análise de conformidade, são ferramentas enquadráveis com a análise do risco. O risco está relacionado com ambas.

A **segurança dos SI e da informação** são importantes ao garantirem que determinadas medidas de proteção são cumpridas, assim como ao disponibilizarem provas que demonstrem a origem de situações anómalas de utilização de dados. No sentido de suportar um programa de proteção da privacidade dos dados, o domínio da segurança deve contemplar o desenvolvimento dos sistemas de identidade digital, dos sistemas de *accountability*, assim como suportar a rastreabilidade dos dados, quer ao nível local, quer entre organizações. Em simultâneo, deve adaptar os planos de contingência para que estes contemplem os dados, e todas as situações que possam comprometer a sua privacidade.

Operacionalizar medidas de proteção da privacidade depende da preparação e da agilidade da organização a vários níveis. A preparação dos gestores é o primeiro fator com influência sobre a operacionalização de um programa para este fim. Pensamos que um **programa de responsabilidade**, um **plano estratégico de desenvolvimento**, e a **colaboração ou interoperabilidade** com organizações com interesses semelhantes de proteção dos dados, são três componentes indispensáveis à implementação de um programa contínuo de proteção, assim como à interoperabilidade necessária com outras organizações. A Figura 23 representa uma abordagem integrada destes componentes, para um programa de proteção que se pretende ser o mais abrangente possível, e ágil em termos de colaboração. A proteção dos dados em trânsito depende da capacidade de **interoperabilidade** das organizações, não só ao nível das ferramentas de desenvolvimento de medidas de proteção, como ao nível de ferramentas operacionais.

Um **programa de responsabilidade** deve permitir à organização repensar a sua abordagem à privacidade, isto é, identificar perante que entidades devem ter uma atitude de responsabilidade, identificar o que está na base do seu desenvolvimento (exemplos: adaptação à legislação e regulamentação em vigor, como resposta à análise do risco efetuada, etc.), quais os requisitos que se devem implementar, e estar preparadas para demonstrar, a pedido das autoridades competentes, o seu compromisso para com a privacidade dos dados.

Figura 23 - Componentes de suporte à operacionalização de um programa de proteção da privacidade dos dados

Um **plano estratégico de desenvolvimento** é essencial para que a privacidade dos dados receba a prioridade e recursos necessários. Seja uma estratégia minimalista ou abrangente, esta pressupõe o compromisso no nível executivo da organização com um programa para a privacidade, a nomeação de responsáveis, e a definição das ações necessárias à sua construção, nomeadamente ações que melhorem a preparação coletiva em proteção de dados, e ações que promovam o desenvolvimento da cultura de privacidade existente. São ações orientadas para a criação e difusão de informação, tipificada para vários públicos, assim como para a realização de eventos formativos e de sensibilização, que promovam a aquisição de conhecimentos e o debate e partilha de experiências.

Tanto um programa de responsabilidade como um plano estratégico de desenvolvimento dependem da formação de uma equipa multidisciplinar, liderada por um elemento do nível executivo. Em simultâneo, esta deve coordenar as iniciativas de colaboração ou de interoperabilidade com outras organizações, de acordo com políticas de disponibilidade dos dados a outras organizações. A SPMS e o

Ministério da Saúde são as entidades externas capazes de promover iniciativas de colaboração quando estão em causa projetos de partilha de dados de âmbito nacional, como a PDS.

6.2 Outros contributos

Apesar de não estar elencado um objetivo específico relacionado com um possível contributo **metodológico** da investigação, pensamos ser importante apresentar o resultado que surgiu do desenho e operacionalização de um *estudo de caso* para o domínio dos SI, em nosso ver bem-sucedido. A disponibilidade de exemplos práticos de aplicação deste método, no domínio das ciências sociais e mais especificamente no estudo dos SI, à globalidade do processo de investigação é escassa. Ainda assim, existem vários estudos publicados que adaptam este método de investigação apenas à fase inicial de desenho do processo de investigação, e que recorrem posteriormente a outros métodos no suporte à recolha e tratamento de dados. O objetivo de utilizar o método de investigação *estudo de caso* como uma estratégia de pesquisa abrangente, e como ferramenta de suporte ao desenho da globalidade do estudo, foi assim um desafio adicional para a investigação.

Demonstrou-se com esta investigação, que num *estudo de caso* determinados componentes são fundamentais para a aplicação deste método no domínio específico dos SI, nomeadamente ao nível da conceção teórica do estudo, da recolha de dados, e da análise dos dados recolhidos. São componentes que não podem num processo tão exigente ser construídos de uma forma isolada.

Na conceção teórica do estudo, o conhecimento que resultou da revisão bibliográfica sobre a temática em estudo é estruturado através do desenho do *projeto de pesquisa* (apresentado na seção 4.5.1 do Capítulo IV). Este é uma ferramenta essencial para a estruturação daquilo que se quer estudar, onde se quer estudar, que dados se devem recolher, e como devem ser interpretados estes dados. Apesar de ser uma ferramenta de difícil conceção, esta deve ser capaz de captar os mais diferentes aspetos inerentes à complexidade da questão de estudo, e desta forma evitar que o investigador recolha e acumule quantidades de dados que não vão viabilizar o estudo.

Demonstrou-se assim, que o *projeto de pesquisa* é fundamental para se conseguir num *estudo de caso* manter aquilo que Yin (2009) define como encadeamento de

evidências. Ou seja, um observador deve ser capaz de seguir as etapas do estudo em qualquer direção, tanto das conclusões para as questões iniciais da pesquisa, como das questões iniciais até às evidências recolhidas e às conclusões.

No momento da recolha de dados é quando ocorre o primeiro contacto do investigador com as instituições e com os seus profissionais. Foi sem qualquer dúvida o melhor momento deste estudo, depois do trabalho exaustivo de desenvolvimento do *projeto de pesquisa*, poder iniciar a sua validação. Foi contudo importante definir, com o maior rigor possível, a rotina dos processos de recolha de dados, assim como disponibilizar às instituições informação detalhada sobre o estudo, sobre os dados que se pretendiam recolher, sobre os meios de recolha, e os profissionais envolvidos. Este é um momento que está na íntegra dependente da qualidade do *protocolo para o estudo de caso* (Anexo I), e na sua capacidade em operacionalizar e orientar o investigador no momento de recolha de dados. O sucesso do momento de recolha de dados, muito dependente desta ferramenta, é também muito influenciado pela: (1) capacidade de o investigador ser flexível, agir como observador, e adaptar o estudo a novos conceitos, novas pistas de estudo, que surgem durante a fase de recolha de dados; (2) importância de um interlocutor local em cada unidade de análise, que se identifique com o estudo, que nos identifique os potenciais colaboradores, e que agilize internamente a operacionalização do estudo; e (3) persistência e adaptação contínua do investigador às exigências específicas de cada organização e de cada colaborador.

O momento de análise dos dados recolhidos é um momento crítico para o investigador face à quantidade de dados acumulados. A primeira sensação que se tem é de que os dados recolhidos não vão permitir validar as proposições em estudo. No entanto, se a análise dos dados for planeada antes da sua recolha, e desenhadas as ferramentas necessárias à sua análise de acordo com as técnicas disponíveis, aos poucos esta sensação vai-se dissipando. Num *estudo de caso*, o investigador não deve recolher os dados e só depois decidir quais as ferramentas e técnicas de análise a aplicar. Esta decisão pode ter como consequência a inviabilização do estudo.

Face à complexidade da temática em estudo, à exigência da unidade de estudo, aos diferentes perfis profissionais abrangidos, demonstrou-se com base na investigação realizada, que a utilização do método *estudo de caso* é um modo de investigação apropriado, com instrumentos eficientes para o acesso ao ambiente natural do SI, e à

recolha de dados, qualitativos e quantitativos, para validação das proposições teóricas em estudo. A experiência conseguida com a aplicação deste método, e a disponibilização de informação que documenta tão detalhadamente esta experiência, é sem dúvida importante no suporte, e mesmo no incentivo, para futuras aplicações práticas deste método, no estudo de mais casos no domínio dos SI.

6.3 Limitações de pesquisa

A principal limitação do estudo surgiu da necessidade de condicionar o âmbito do estudo aos recursos e ao tempo útil disponíveis. Tratando-se de um estudo desenvolvido ao abrigo do programa de doutoramento, foi desta forma necessário definir para a questão de estudo, aquilo que seria possível estudar com os recursos disponíveis. Esta limitação levou, por exemplo, a não ser possível que fossem consideradas mais unidades de análise, nomeadamente a Saúde 24 e uma unidade hospitalar do setor privado, participantes na PDS.

A Saúde 24 representa um cenário único de utilização de dados de saúde, e que traria a este estudo uma experiência diferente da existente ao nível das unidades de estudo contempladas. Por outro lado, incluir uma unidade hospitalar do setor privado, permitiria para o domínio da proteção de dados, estabelecer uma comparação com as práticas de proteção de dados do setor público.

O acesso às organizações na área da saúde foi facilitado, por um lado, pela aprovação do estudo por parte dos responsáveis da SPMS, e por outro, pela identificação de um interlocutor local para a operacionalização do estudo. Caso contrário, teria sido muito difícil aceder às organizações de saúde. No entanto, apesar da excelente abertura à colaboração no estudo, foi necessário acomodar as diferenças organizacionais em relação à problemática em estudo. Em algumas situações foi necessário eliminar a perceção errada de alguns responsáveis em que o nosso objetivo era "avaliar" a organização, assim como a suspeita de que algumas questões poderiam comprometer a imagem da organização ou dos próprios profissionais. Estas situações podem ter limitado a prestação de alguns participantes em alguns itens da recolha de dados.

Dos cinco perfis de profissionais que colaboraram no estudo, existiu uma dificuldade não prevista, em relação aos profissionais do perfil 4, perfil destinado aos administradores executivos em cada unidade de estudo. Além de se ter conseguido

apenas um participante por unidade de estudo, verificou-se que a sua responsabilidade e intervenção sobre as questões da proteção e privacidade dos dados é diminuta, o que pode ter comprometido a qualidade esperada no processo de recolha de dados em alguns itens do elenco de questões da entrevista.

Durante a fase de recolha de dados, em colaboração com os interlocutores ao nível de cada unidade de análise, sentimos nestes algum receio em relação à nossa pretensão de recolher um conjunto de documentos relacionados com a problemática em estudo. Este receio está muito relacionado com a estrutura e a qualidade destes documentos, construídos para utilização interna, e como tal, não queriam que, através deste estudo, estes fossem tornados públicos. Conseguiu-se recolher alguns documentos de várias unidades de análise, mas na sua maioria pouco relacionados com a temática em estudo, o que dificultou o processo de validação de algumas variáveis dependentes do estudo.

6.4 Oportunidades futuras de investigação

No decorrer deste trabalho foi possível identificar temas relacionados com a privacidade dos dados e com a interoperabilidade, que podem constituir temáticas a abordar noutros estudos. Neste sentido deixamos em aberto alguns temas ou oportunidades de investigação:

a. Desenvolvimento de uma *framework* de suporte à realização de processos de análise do risco orientados à privacidade dos dados. Apresenta-se como uma ferramenta fundamental ao planeamento dos SI, permitindo identificar os contextos de utilização de dados pessoais, as situações que apresentam riscos para a privacidade destes dados, o conhecimento dos riscos existentes, e a consequente adaptação de medidas de correção.
b. Replicação da temática da privacidade dos dados em ambientes de colaboração/interoperabilidade, através de outros *estudos de caso,* em áreas como a justiça, a administração interna e as finanças (DGCI), assim como na área da saúde de um outro país europeu. Somente através desta replicação do estudo e a validação dos fatores com influência sobre a privacidade dos dados noutro domínio, se pode generalizar os resultados obtidos.
c. Desenvolvimento do conceito *Unified Privacy Program*, que permita aos responsáveis pelas questões da privacidade e da proteção de dados,

desenvolver um programa unificado de políticas de privacidade para os dados, de âmbito mais alargado, e não confinado à interoperabilidade. Existem atualmente vários domínios onde as questões da privacidade são um desafio constante, e que não podem ser desenvolvidos isoladamente, como são a privacidade dos dados nos serviços da *Cloud*, na Internet das Coisas (IoT), nas *SmartCities*, e nas comunicações ao nível da Internet. A realização de casos de estudo nos domínios apresentados pode gerar o conhecimento necessário ao desenvolvimento deste conceito.

d. Desenvolvimento de uma taxonomia para a privacidade dos dados na área da saúde, de suporte à interoperabilidade entre organizações. Uma taxonomia para a privacidade dos dados, apesar de reconhecida como de desenvolvimento obrigatório, se estiver focada apenas nas questões da privacidade dos dados pode, à partida, não receber a recetividade esperada. É importante, por exemplo, que inclua uma nomenclatura para classificação dos dados de saúde, adaptável ao ciclo de vida dos dados, e uma classificação de perfis de utilizadores. Desta forma pode caminhar-se para um *standard* que se pode generalizar a todas as organizações na área da saúde.

Anexos

Anexo I - Protocolo para o *estudo de caso*

Privacidade dos dados

em ambientes de interoperabilidade - a área da saúde

Protocolo para o *estudo de caso*

Conteúdo

Secundino Lopes

Doutorando do programa de doutoramento em gestão, especialidade em sistemas de informação, da Universidade de Évora.

Instituto Politécnico de Portalegre; Escola Superior de Tecnologia e Gestão; Portalegre, Portugal; secundino.lopes@estgp.pt

Rui Quaresma

Professor auxiliar da Universidade de Évora e orientador do projeto de investigação

CEFAGE-UE

Universidade de Évora; Évora, Portugal; quaresma@uevora.pt

Resumo

O presente documento constitui um dos componentes do método de investigação "*Case Study*" e tem por objetivo apresentar aos participantes do estudo de forma sucinta e objetiva, o projeto de investigação "*Privacidade dos dados em ambientes de interoperabilidade*", as questões necessárias à operacionalização da fase de recolha dos dados para validação da questão e das proposições de estudo, e o contributo esperado por cada perfil de participante.

O projeto de investigação, na área dos sistemas de informação, apresenta como principal objetivo a identificação e o estudo dos fatores críticos à privacidade dos dados em contextos de colaboração entre organizações, onde existe partilha de dados entre sistemas de informação heterogéneos.

A Plataforma de Dado da Saúde (PDS) constitui um ambiente de interoperabilidade no domínio da saúde, classificada neste estudo como a *unidade de estudo*, contexto real para a recolha de dados de validação da problemática em estudo - a privacidade dos dados.

1. Descrição do projeto de investigação

1.1 Objetivos

O projeto de investigação foca-se num fenómeno mal compreendido (a privacidade dos dados), e relativamente ao qual existe um interesse particular por parte das organizações em entender a dinâmica deste fenómeno no interior do seu sistema de informação e em ambientes de colaboração. Estamos perante uma realidade complexa, subjetiva, para a qual é essencial o seu estudo em contexto real, onde a compreensão do contexto de ação e as experiências individuais são muito relevantes para a identificação dos fatores relacionados com a "atividade humana" que podem condicionar a privacidade dos dados em processos de colaboração inter-organizacional. A opinião, a experiência e o conhecimento dos vários atores num fenómeno com estas características constituem a principal, senão única, fonte primária de informação.

Para a problemática em estudo, foram definidos os seguintes objetivos de investigação:

a. Identificação e estudo dos principais fatores com influência sobre a dinâmica da privacidade dos dados em contextos de interoperabilidade entre sistemas sociotécnicos. Estruturação deste conhecimento para aplicação prática futura no suporte, quer ao desenvolvimento de sistemas onde a privacidade dos dados é um requisito fundamental, quer à análise de conformidade dos sistemas em funcionamento em relação aos requisitos externos e internos quanto à privacidade dos dados.
b. A seleção e utilização de um modelo de interoperabilidade, ferramenta essencial para lidar com a complexidade dos vários níveis de exigência de interoperabilidade entre sistemas, neste caso em relação às questões associadas à privacidade dos dados. Pretende-se que esta ferramenta apoie os responsáveis pelos sistemas no planeamento da evolução da interoperabilidade com outros sistemas para níveis superiores.
c. Validação do estudo através da recolha da opinião e experiência de várias categorias de profissionais, num cenário privilegiado para o estudo da privacidade dos dados, dada a sensibilidade dos dados utilizados e o ambiente de partilha de dados em desenvolvimento – a área da saúde.

Será utilizado o método *estudo de caso* ("*case study*"), um método bem adaptado à investigação em sistemas de informação e às características deste projeto de investigação.

1.2 Unidade de estudo – unidades de análise

A PDS, projeto desenvolvido e coordenado pela Comissão para a Informatização Clínica (CIC) e pelos Serviços Partilhados do Ministério da Saúde (SPMS), constitui a unidade de estudo ou o "caso de estudo". Esta escolha é justificável por três razões: (1) o facto de a PDS reunir vários sistemas de informação heterogéneos com um objetivo comum – a construção de um sistema de colaboração e partilha de dados/serviços de saúde; (2) dada a natureza dos dados partilhados, a sua proteção e a sua privacidade constituem um aspeto crítico com significativa influência sobre a confiança dos utilizadores sobre o sistema; (3) a interoperabilidade entre os vários sistemas em franca expansão e a perspetiva futura de interoperabilidade com sistemas similares no espaço europeu.

Sendo inviável a cobertura total e de todas as instituições participantes na PDS, foram selecionadas as seguintes unidades de análise, dentro da unidade de estudo:

a. *Projeto-piloto – Unidade Local de Saúde do Norte Alentejano, Portalegre (ULSNA);*
b. Hospital do Espírito Santo E.P.E, Évora (HES);
c. USF Saúde Mais, Santa Maria da Feira (USF);
d. Hospital Professor Doutor Fernando Fonseca E.P.E., Amadora (HFF);
e. Instituto Nacional de Emergência Médica, Lisboa (INEM);
f. Serviços Partilhados do Ministério da Saúde E.P.E. (SPMS);
g. Grupo de *beta-tester* de Utentes.

2. Procedimentos (de campo)

Para uma operacionalização eficiente da fase de recolha de dados, é vital a colaboração de dois participantes:

1. Os responsáveis pela implementação a nível nacional da PDS;
2. O responsável, em cada uma das cinco unidades de análise, pela interligação do sistema de informação com a PDS. Será através deste responsável que a equipa de investigação pretende desenvolver todos os contactos que conduzam

à identificação do elenco de profissionais a incluir na fase de recolha de dados, com recurso a entrevistas.

Neste sentido é vital que ambos conheçam os objetivos do projeto de investigação e com base neste conhecimento identifiquem as *pessoas-chave* em cada organização em que o seu contributo é uma mais-valia (de acordo com os perfis identificados na tabela 1 e o número de entrevistas por perfil previstos na tabela 2).

Uma vez identificados todos os participantes, será realizado um contacto individual com o objetivo de realizar um acordo tácito de colaboração, após o qual será agendada a entrevista e/ou a recolha de outros dados.

Para a recolha de dados serão utilizados dois métodos: entrevistas semiestruturadas e documentos. Em relação às **entrevistas semiestruturadas,** estas apresentam as seguintes características:

a. Uma duração de aproximadamente **30 minutos** por cada participante;
b. A participação é voluntária, *sendo que se pretende transmitir ao participante que a sua opinião é fundamental ao desenvolvimento do sistema de informação no que toca à privacidade dos dados;*
c. Será recolhida a opinião da pessoa sobre as proposições em estudo, e em nenhuma situação será recolhida a opinião da pessoa sobre a instituição, nem sobre a forma como esta funciona. Sempre que o participante o permitir será utilizado um gravador digital para recolha dos dados para futuro tratamento;
d. Todos os dados serão tratados de forma confidencial, não sendo em nenhuma situação identificada nem publicada a identidade do autor de uma resposta/opinião. A obrigação de confidencialidade vigorará após a conclusão do estudo referido;
e. Os dados recolhidos serão **apenas** tratados no âmbito da investigação em curso, não sendo possível que outras pessoas ou entidades externas utilizarem estes dados para outro fim;
f. Os resultados obtidos com o tratamento dos dados recolhidos serão apenas publicados no documento final da tese de doutoramento e em artigos científicos da especialidade, sendo que nesta situação deve existir um acordo prévio da CIC.

Perfis de participantes nas unidades de análise

ID	Descrição
Perfil 1 Responsáveis locais pela implementação e coordenação da PDS	Perfil que inclui os responsáveis, em cada organização, pela implementação e coordenação da PDS. *Estão-lhe destinadas questões relacionadas com a exigência que resulta da colaboração e partilha de dados entre as várias organizações.*
Perfil 2 Técnicos e responsáveis pelos sistemas de informação	Incluem-se neste perfil os responsáveis, em cada unidade de análise, pela coordenação global de todos os serviços informáticos, assim como os técnicos fundamentais à operacionalização do sistema como um todo e à PDS em particular. São os casos de técnicos especializados em segurança e técnicos especializados em questões de proteção de dados. Inclui-se neste perfil o responsável local pelo tratamento de dados (artigo 2º, alínea d, da Diretiva 95/46/CE) quando identificável. *Estão-lhe destinadas questões relacionadas com o funcionamento dos sistemas de informação no domínio da segurança, proteção e privacidade dos dados.*
Perfil 3 Profissionais de saúde	Perfil que inclui médicos, enfermeiros e outros profissionais da área da saúde. Constituem os utilizadores principais da PDS e para os quais os dados são essenciais à realização da sua atividade profissional. *Estão-lhe destinadas questões relacionadas com a ética e atitude humana em relação às alterações resultantes do ambiente de colaboração e partilha de dados.*
Perfil 4 Gestores e administradores	Perfil destinado aos administradores executivos das organizações que constituem uma unidade de análise. *Estão-lhe destinadas questões organizativas e de estratégia em relação à privacidade no geral e à privacidade dos dados em particular.*
Perfil 5 Titular dos dados	Grupo de "beta tester" existente para a validação/avaliação dos serviços disponibilizados pela PDS, através do *Portal do Utente (*https://servicos.min-saude.pt/utente/portal/paginas/default.aspx). *Estão-lhe destinadas questões para analisar a sua confiança e atitude em relação à partilha de dados entre organizações, assim como a necessidade ou não de mais informação (transparência) sobre este novo contexto.*

Tabela 1 – Perfis de participantes

Número de processos de recolha de dados por perfil/unidade de análise
Previsão inicial do número de processos de recolha de dados a realizar.

	Unidades de análise						
ID	ULSNA	HES	USF	HFF	INEM	SPMS	Utentes
Perfil 1 Responsáveis locais pela implementação e coordenação da PDS	1	1-2	1-2	1-2	1-2	1-2	n/a
Perfil 2 Técnicos e responsáveis pelos sistemas de informação	2	2-5	2-5	2-5	2-5	2-5	n/a
Perfil 3 Profissionais de saúde	3	2-5	2-5	2-5	2-5	n/a	n/a
Perfil 4 Gestores e administradores	1	1-2	1-2	1-2	1-2	n/a	n/a
Perfil 5 Titular dos dados	n/a	n/a	n/a	n/a	n/a	n/a	1-300

Tabela 2 – Processos de recolha por perfil/unidade de análise

3. Questões de estudo – o que se pretende estudar?

Para o método de investigação *estudo de caso* são especialmente importantes (1) a questão de estudo, (2) as suas proposições e (3) a (s) unidade (s) de estudo.

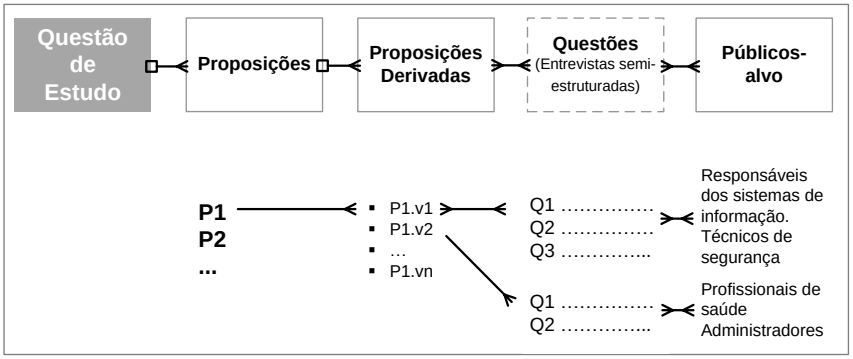

Figura 1: Ligação entre a questão de estudo, as suas proposições e as fontes de informação

Um elemento essencial à definição da melhor estratégia de investigação, e formulada de forma independente e não associada à unidade de estudo (neste caso a PDS), é **a questão de estudo**, a qual serve de orientação para o projeto de investigação. Neste estudo, a questão de estudo definida é a seguinte:

> *"Quais os fatores críticos à privacidade de dados em ambientes heterogéneos de interoperabilidade entre sistemas sociotécnicos e como podem estes fatores ser alinhados com os vários níveis e atributos de interoperabilidade do modelo Organizational Interoperability Maturity (OIM)?"*

As proposições de estudo, que derivam da questão de estudo, focam-se nos aspetos a serem estudados dentro da questão de estudo, clarificando e identificando onde devemos procurar evidências relevantes. Pretende-se que a formulação de proposições possa contribuir para a identificação dos fatores críticos a estudar. Para a questão de estudo em causa foram identificadas as proposições apresentadas na tabela 3 (P1, P2, ..., P10) que, como se pode observar na figura 1, vão dar origem às questões a colocar às pessoas-chave, para a recolha de dados, nomeadamente através de entrevistas.

Ou seja, os dados a recolher vão permitir validar ou não as proposições formuladas (tabela 3). Esta validação é, contudo, realizada através da decomposição de cada uma das proposições em proposições mais específicas denominadas de *proposições derivadas*, apresentadas da tabela 4 à tabela 13. Nestas tabelas é apresentada a descrição da proposição derivada assim como a sua fundamentação.

Proposições

Designação da proposição	Descrição
P1. "Experiência"	Num contexto de interoperabilidade, a experiência e a compreensão coletiva das questões da interoperabilidade e da proteção e privacidade são essenciais ao planeamento conjunto de medidas transversais e eficazes para a proteção da privacidade.
P2."Cultura de privacidade"	A implementação eficaz das soluções tecnológicas e das políticas de privacidade está dependente do compromisso das organizações no desenvolvimento das melhores práticas de gestão da informação que respeitem a privacidade. Este contexto só é alcançável quando a privacidade constituir uma parte integrante da cultura organizacional.
*P3."*Segurança e infraestruturas"	A colaboração e a interoperabilidade técnica entre as várias soluções de segurança e infraestruturas de armazenamento de dados são essenciais ao suporte e à viabilidade das medidas adotadas nos níveis superiores de proteção e privacidade dos dados.
P4."Linguagem de privacidade (*taxonomia*)"	A existência de uma linguagem comum nos domínios da proteção e da privacidade é essencial à definição clara e inequívoca das questões associadas à privacidade dos dados, e ao esforço comum no compromisso para a sua preservação.
P5." Accountability - responsabilidade e conformidade"	Um programa continuado de análise de conformidade, de monitorização dos controlos de proteção e privacidade, assim como a disponibilização de provas de evidência sobre quebras detetadas, são ferramentas essenciais à proteção da privacidade num ambiente de colaboração.
*P6."*Dados e manipulação de dados"	A privacidade dos dados está dependente do conhecimento desenvolvido pelas instituições sobre os dados que utiliza e da transparência e qualidade dos processos de tratamento em todo o seu ciclo de vida num ambiente de interoperabilidade.
*P7."*Estratégia para a privacidade"	Num ambiente de colaboração com outras organizações, impõe-se a existência de estratégias individuais (e a sua harmonização) para a privacidade como um todo e em particular para a proteção e privacidade dos dados.
*P8."*Confiança e gestão da confiança"	É essencial à privacidade dos dados a confiança entre as organizações participantes, como pilar fundamental à colaboração num ambiente de interoperabilidade.
P9."Ética e cooperação humana"	No domínio da ética, a iniciativa (atitude), confiança e conhecimento por parte do titular dos dados do novo contexto de utilização dos seus dados pessoais, assim como a atitude face à mudança por parte dos profissionais, podem comprometer os objetivos para a colaboração, e consequentemente o sucesso das medidas para proteção da privacidade dos dados.
*P10."*Estrutura organizativa"	O compromisso para com os valores e objetivos subjacentes à colaboração sob a forma de interoperabilidade organizacional é essencial para minimizar possíveis impactos sobre a privacidade que derivam de culturas e estruturas organizativas diferentes.

Tabela 3 – Proposições de estudo

Proposição – descrição, enquadramento e fundamentação

P1. "Experiência"

Variáveis Dependentes – ID e descrição *[1] O que se pretende conhecer?* [2] O motivo da recolha da informação
P1.v1. É fundamental uma experiência em partilha de dados, em interoperabilidade, em projetos internos do próprio sistema de informação e em projetos de colaboração com outras organizações. *[1] Identificar situações/projetos de partilha de dados, de interoperabilidade (locais ou com outras organizações) em que a organização em estudo participou. Perceber qual a importância atribuída às questões da interoperabilidade, e se estrategicamente é uma aposta de futuro. Identificar projetos futuros de interoperabilidade.* [2] Perceber se o fator "experiência em interoperabilidade" é importante à privacidade dos dados, e se a ausência de experiência constitui uma barreira à sua proteção.
P1.v2. Experiência em questões de privacidade[72], em proteção de dados, no seu enquadramento legislativo (nacional e internacional), em avaliações do impacto sobre a privacidade (PIA), ao nível dos sistemas locais permitem uma colaboração mais produtiva com outras organizações no desenvolvimento de um ambiente seguro de partilha de dados. *[1] Compreender se o conhecimento nos domínios da privacidade, da proteção de dados, é um facilitador para a abordagem da privacidade dos dados num contexto de colaboração com outros sistemas. Identificar práticas de proteção de dados, tanto em projetos locais como em projetos de partilha de informação com outras organizações, mesmo que com total ausência de interoperabilidade.* [2] Perceber se a experiencia em privacidade e proteção de dados é importante quando a organização implementa interfaces para partilha de informação ou serviços com outras organizações.
P1.v3. É essencial a existência de profissionais especializados em proteção e privacidade, a cooperação entre estes, e de um órgão de supervisão para o contexto da colaboração, para garantir que as políticas de privacidade são atendidas por todos. *[1] Analisar se é essencial à experiência global da organização, a existência de profissionais permanentes especializados em proteção e privacidade dos dados, e neste sentido, mais bem preparados para os desafios que surgem das exigências da interoperabilidade organizacional* [2] Verificar se a existência de profissionais com competências em proteção e privacidade de dados é importante ao desenvolvimento de programas integrados de proteção e privacidade dos dados. Compreender que profissionais devem incorporar competências em proteção e privacidade dos dados.
P1.v4. Eventos como programas periódicos de educação, formação e sensibilização entre os profissionais da organização, participação em workshops, seminários nacionais ou internacionais, no domínio da privacidade e proteção de dados, são importantes para uma melhor experiência e preparação coletiva. *[1] Analisar a formação disponibilizada nas organizações que melhore a sua preparação em questões associadas à proteção e privacidade de dados. Qual a regularidade destas ações. Qual o grau de adesão.* [2] É importante perceber qual o contributo de ações de formação ou sensibilização para a formação de uma consciência coletiva da problemática da privacidade de dados.

Tabela 4: Estrutura da proposição P1

[72] Não apenas em situações de privacidade dos dados, mas também um conhecimento de situações de privacidade da pessoa ou corporal, privacidade do comportamento ou esfera pessoal e privacidade das comunicações pessoais.

Proposição – descrição, enquadramento e fundamentação

P2.*"Cultura de privacidade"*

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P2.v1. A existência de uma cultura de privacidade é sinónimo de uma melhor preparação organizacional para agir em situações/contextos de privacidade. A privacidade dos dados ao ser reconhecida como um *valor*, é integrada nas práticas de uma organização e considerada durante todo o ciclo de vida de um sistema.

[1] Analisar a relação e dependência da privacidade dos dados com uma cultura de privacidade em toda a organização, assim como a necessidade de esta ser reconhecida como um valor para que seja considerada no desenvolvimento de um sistema (privacy by design).

[2] Validar a proposição P2 em relação à necessidade de que as questões da privacidade dos dados sejam parte integrante de uma cultura de privacidade em toda a organização.

P2.v2. Uma cultura de privacidade é fundamental (1) à identificação e definição de *situações* de privacidade dentro de uma *zona* maior de privacidade, (2) à sua justificação e (3) à sua posterior implementação e gestão, assim como à previsão de exceções às políticas de privacidade desenvolvidas.

[1] Compreender se uma cultura em privacidade é fundamental para que os profissionais saibam identificar e planear o funcionamento de uma situação de privacidade, assim como serem capazes de interligar[73] (interoperabilidade organizacional) uma situação com uma similar em outras organizações.

[2] Validar a relação dos vários profissionais em relação à proposição P2, como condição para lidarem com contextos de informação sensível.

P2.v3. Uma cultura de privacidade é essencial à distinção dos vários tipos de privacidade, e no domínio da privacidade dos dados compreender as diferenças e dependências em relação à proteção de dados e à segurança dos dados.

[1] Normalmente a privacidade dos dados é confundida com segurança e proteção de dados. Importa perceber se organizações com uma cultura forte em privacidade distinguem e identificam com facilidade estes três contextos e a sua interdependência.

[2] Validar a proposição P2 em relação à definição e distinção do conceito de privacidade dos dados, dos conceitos proteção de dados e segurança de dados.

Tabela 5: Estrutura da proposição P2

[73] Podem existir situações similares de privacidade em várias organizações, já identificadas (ou não), mas a funcionar com políticas de privacidade díspares (ou sem qualquer política de privacidade). O desafio passa por integrar estas regras de funcionamento para o contexto de interoperabilidade. Aqui tem um papel decisivo o órgão de supervisão para o contexto da colaboração em questões de privacidade dos dados.

Proposição – descrição, enquadramento e fundamentação

P3. *"*Segurança e infraestruturas"

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P3.v1. A segurança de infraestruturas locais e de comunicação, a sua interoperabilidade técnica e não-técnica (*a "padronização das melhores práticas de segurança" específicas de cada sistema são essenciais ao desenvolvimento de uma plataforma segura e de confiança*), são preponderantes para camadas superiores de segurança, nomeadamente a privacidade dos dados.

[1] Compreender se os profissionais identificam a relação de dependência da privacidade dos dados em relação às questões da segurança para o contexto de colaboração. Analisar qual o contributo e importância da interoperabilidade organizacional a este nível.

[2] Validar a proposição P3 em relação à interoperabilidade técnica e não técnica entre infraestruturas.

P3.v2.Uma análise de risco em segurança e uma análise do impacto sobre a privacidade (PIA), que englobem todos os equipamentos e situações de recolha, armazenamento, utilização e partilha de dados, são dois instrumentos decisivos para o enquadramento e conhecimento das situações problemáticas à privacidade dos dados.

[1] Compreender se para os responsáveis pelos sistemas de informação a existência de análise de risco é uma ferramenta imprescindível e ponto de partida para o desenvolvimento de medidas que permitam corrigir os riscos identificados.

[2] Validar a proposição P3 em relação à dependência de um programa de segurança que tenha na sua origem uma análise de risco.

P3.v3. No domínio da segurança e infraestruturas, a identidade digital, os sistemas de gestão de identidade, e a confiança (federação) e interoperabilidade entre estes sistemas, são um componente essencial à gestão e monitorização da confidencialidade e privacidade dos dados.

[1] É unânime que a identidade digital é fundamental ao controlo da exposição de dados pessoais e é um fator decisivo para a privacidade de dados em contextos de interoperabilidade. É contudo necessário verificar como estes sistemas devem evoluir para cumprir eficientemente com este requisito.

[2] Validar a proposição P3 em relação aos conceitos de gestão da identidade e federação de sistemas, assim como a sua influência sobre a proposição P5.

P3.v4. A segurança em cenários de exposição de dados a ambientes vulneráveis de "não-produção" é essencial a preservação da sua privacidade. Os requisitos de privacidade dos dados nestes contextos devem cumprir com os requisitos legais.

[1] Determinar se ambientes de não-produção, ou seja, processos ou tarefas que estão fora do âmbito e objetivo principal para a recolha de dados, não constituem lacunas no que diz respeito à privacidade dos dados.

[2] Validar a proposição P3 em relação à necessidade de medidas de segurança de preservação da privacidade dos dados quando utilizados para outros objetivos que não os inicialmente propostos (principio relativo à qualidade dos dados).

P3.v5. A existência de um plano de contingência para lidar com os efeitos de eventos não previstos como a perda acidental, destruição ou deterioração de dados pessoais, e tratamentos ilegais e não autorizados, contribui para anular possíveis quebras de privacidades destes dados.

[1] Verificar se a privacidade dos dados é uma das preocupações na base do desenvolvimento de planos de contingência.

[2] Validar a proposição P3 em relação à inclusão da privacidade dos dados no plano de contingência desenhado para o sistema.

Tabela 6: Estrutura da proposição P3

Proposição – descrição, enquadramento e fundamentação

P4.*"Linguagem de privacidade* (*taxonomia*) "

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P4.v1. Uma linguagem ou taxonomia comum de suporte à definição, justificação e gestão de zonas e situações de privacidade constitui um auxiliar importante para analisar de uma forma clara e inequívoca as questões da privacidade tanto no interior de uma organização como na sua integração com outras organizações.

[1] Sendo a privacidade dos dados de difícil definição uma taxonomia comum facilitaria o seu desenvolvimento em todas as organizações. Importa perceber qual a sensibilidade dos responsáveis pelas questões da privacidade dentro das organizações em relação à existência desta ferramenta de trabalho – uma Framework de suporte ao desenvolvimento de políticas de privacidade.

[2] Validar o contributo da proposição P4 para o desenvolvimento comum de políticas de privacidade dos dados.

P4.v2. Uma linguagem comum de privacidade promove uma maior agilidade na definição de políticas de privacidade, no desenvolvimento de mecanismos de controlo de conformidade (P5), e na sua integração com situações similares em outras organizações.

[1] Analisar qual o contributo de uma linguagem comum sobre privacidade para a agilidade organizacional que se pretende para as questões da proteção e privacidade dos dados.

[2] Validar o contributo da proposição P4 para o desenvolvimento comum de políticas de privacidade dos dados.

Tabela 7: Estrutura da proposição P4

Proposição – descrição, enquadramento e fundamentação

P5.*"Accountability – responsabilidade e conformidade"*

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P5.v1. Um programa de responsabilidade sólido e transparente, que contemple medidas adequadas e eficazes para pôr em prática as obrigações e princípios da legislação em vigor sobre proteção de dados, constitui a ferramenta operacional necessária para as questões da privacidade.

[1] Compreender qual a importância atribuída aos programas de responsabilidade. Verificar se estes já se encontram institucionalizados, e nestas situações compreender o seu efeito prático.

[2] Analisar a relação e dependência da proposição P5 em relação ao princípio da responsabilidade e na consequente necessidade de um programa de responsabilidade da organização.

P5.v2. Um programa de conformidade constitui o meio de demonstração da vontade e da capacidade da organização em ser responsável e responsabilizada pelas práticas de gestão de dados. É essencial à salvaguarda da privacidade de dados, assim como à confiança do titular dos dados na organização, e entre esta e outras organizações. A eficácia e exigência das tarefas de conformidade dependem da sensibilidade dos dados, do volume dos dados processados e dos riscos específicos identificados.

[1] Compreender qual a importância atribuída à necessidade de programas (cultura) de conformidade e verificar se estes já se encontram institucionalizados. Verificar se é possível existir partilha de conhecimento e experiências que permitam o desenvolvimento de um programa de conformidade global para todas as organizações que partilham dados.

[2] Analisar a relação e dependência da proposição P5 em relação ao desenvolvimento de uma cultura de conformidade.

P5.v3. Os sistemas de *accountability* são essenciais à confidencialidade dos dados, ao disponibilizarem provas de evidência que permitem atribuir responsabilidade a comportamentos não esperados no domínio da privacidade dos dados.

[1] Verificar se os sistemas de registo das tarefas realizadas sobre os dados, quer por utilizadores quer por outros sistemas, e que permitem monitorizar se estas estão de acordo com o perfil de comportamento definido, são uma ferramenta indispensável à privacidade dos dados.

[2] Validar a proposição P5 em relação aos sistemas de *accountability*. Esta proposição permite cruzar resultados com a proposição P3.v3 sobre identidade.

P5.v4. O desenvolvimento de rótulos de qualidade (esquema de certificação) para as medidas adotadas para uma gestão eficiente da conformidade legal, proteção e segurança dos dados, são no futuro uma ferramenta essencial ao desenvolvimento de um ambiente de interoperabilidade confiável e seguro em matérias de privacidade dos dados.

[1] A certificação ou selo de qualidade é vital para o funcionamento dos sistemas de informação, como é o caso da segurança. Importa pois perceber qual a opinião sobre a criação de um selo de qualidade para o domínio global da privacidade e para o domínio específico da privacidade dos dados.

[2] Validar se é importante para a proposição P5 o desenvolvimento de selos de qualidade ou certificação.

Tabela 8: Estrutura da proposição P5

Proposição – descrição, enquadramento e fundamentação

P6. "Dados e manipulação de dados"

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P6.v1. À semelhança da proteção de dados, a privacidade de dados deve ser preocupação constante durante todo o ciclo de vida[74] dos dados em ambientes de interoperabilidade.

[1] A informação recolhida vai permitir esclarecer se a privacidade dos dados deve ser uma preocupação constante em todas as fases do ciclo de vida dos dados, ou se ao contrário, apenas algumas fases são problemáticas e necessitam de atenção especial.

[2] Validar a proposição P6 em relação à necessidade de a privacidade dos dados se apresentar como parte integrante do planeamento do ciclo de vida dos dados (principio *Privacy by Design*).

P6.v2. A existência de procedimentos para analisar o tipo e quantidade de dados pessoais recolhidos (a sua adequação e relevância) em relação ao (s) objetivo (s) definido (s), o seu período de retenção (não mais que o necessário), assim como a transparência, clarificação e publicação destes procedimentos são essenciais à compreensão e definição de medidas de proteção da privacidade dos dados

[1] Confirmar se existem procedimentos institucionalizados focados no estudo dos dados e qual a importância atribuída às questões da privacidade nesta fase.

[2] Validar a proposição P6 em relação à necessidade de procedimentos de análise dos dados nomeadamente se são adequados, pertinentes e não excessivos face às finalidades para que são recolhidos e para que serão posteriormente tratados (princípio da *qualidade dos dados*).

P6.v3. A classificação[75], dinâmica (durante todo o seu ciclo de vida), dos dados é essencial à definição dos níveis de proteção e privacidade pretendidos, assim como os domínios onde pode circular, isto é dentro da organização e entre organizações. Esta *classificação dos dados vai permitir definir os requisitos de proteção associados à informação de forma a restringir a circulação da informação com base nas componentes identidade e legalidade* (Jericho Forum, 2009c).

[1] Analisar se é condição fundamental as políticas de proteção de dados e consequentes políticas de privacidade terem por base uma classificação objetiva de dados.

[2] Validar se a proposição P6 depende de uma classificação dos dados quando relacionada com privacidade dos dados.

P6.v4. A privacidade dos dados depende diretamente (1) do âmbito, (2) das tecnologias aplicadas e (3) dos *standards* usados da/na proteção de dados, implementados localmente e em ambientes de interoperabilidade. Quanto mais granular melhor. Quanto mais interoperáveis melhor.

[1] Compreender se a privacidade dos dados depende do âmbito desenhado e implementado para a proteção de dados, ou seja, a privacidade fica facilitada quando a proteção de dados é especificada individualmente para cada elemento de dados em vez de ser especificada para um conjunto de dados ou uma classe de dados.

[2] Validar a associação e dependência da proposição P6 em relação à proteção de dados, ao seu âmbito e às tecnologias aplicadas a este nível.

Tabela 9: Estrutura da proposição P6

[74] KPMG Data Life Cycle – (1) generation; (2) use; (3) transfer; (4) transformation; (5) storage; (6) archival; (7) destruction.

[75] Exemplo - classificação da informação em quatro níveis: pública, atividade normal, sensível, altamente sensível (Jericho Forum, 2009a).

Proposição – descrição, enquadramento e fundamentação

P7. "Estratégia para a privacidade"

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P7.v1. Uma estratégia para a privacidade está associada ao reconhecimento da privacidade como fator estratégico para a organização, e da sua responsabilidade sobre este assunto.

[1] O ponto de partida para a existência de uma estratégia para a privacidade está dependente da importância da privacidade para a organização em causa. Neste sentido é importante compreender se o desenvolvimento de uma estratégia para a organização está diretamente associada ao reconhecimento da privacidade como fator estratégico.

[2] Validar a dependência da proposição P7 em relação ao reconhecimento por parte dos gestores executivos da privacidade como fator estratégico e qual o seu papel neste domínio.

P7.v2. Uma estratégia para a privacidade constitui uma ferramenta essencial ao planeamento e integração de mecanismos de proteção e controlo da privacidade.

[1] Compreender se a estratégia para a privacidade deve posicionar-se como a base de um programa integrado de proteção e controlo da privacidade, com outros existentes ao nível da segurança e da proteção de dados.

[2] Validar a influência da proposição P7 no desenvolvimento de um programa integrado de proteção, para toda a organização.

P7.v3. O conhecimento e consciência das práticas existentes de processamento de dados e a identificação do risco associado à ausência de políticas de proteção da privacidade e proteção de dados são impulsionadores de uma visão estratégica para a privacidade.

[1] Conhecer a experiência das organizações em análises do risco em assuntos de privacidade e qual a sua relação com o desenvolvimento de uma estratégia para o controlo deste risco.

[2] Validar a relação da proposição P7 com o reconhecimento e conhecimento do risco associado a possíveis quebras de privacidade.

P7.v4. Uma estratégia para a privacidade é promotora de uma cultura de privacidade. Uma cultura de privacidade emerge em cenários em que as questões associadas à privacidade e proteção dos dados têm por base uma estratégia de desenvolvimento em detrimento de auditorias pontuais de conformidade.

[1] Determinar se em ambientes de colaboração o primeiro passo para a existência de uma cultura de privacidade (P2) generalizada em todas as organizações passa pela existência de uma estratégia para a privacidade

[2] Validar a relação da proposição P7 com a proposição P2.

P7.v5. Em ambientes de interoperabilidade, a colaboração para o desenvolvimento de uma estratégia conjunta para a privacidade potenciaria o desenvolvimento de uma plataforma confiável para a recolha, partilha e utilização de dados pessoais.

[1] Compreender se a harmonização das estratégias de privacidade é preponderante ao desenvolvimento de uma plataforma confiável para a recolha, partilha e utilização de dados pessoais, ou se esta pode ser criada com a ausência de linhas orientadoras de desenvolvimento.

[2] Validar a relação da proposição P7 com a necessidade de unificar as árias estratégias de privacidade numa estratégia conjunta.

Tabela 10: Estrutura da proposição P7

Proposição – descrição, enquadramento e fundamentação

P8. "Confiança e gestão da confiança"

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P8.v1. A confiança constitui um dos pilares fundamentais aos processos de colaboração entre as organizações num ambiente de interoperabilidade.

[1] Compreender se a existência de relações de confiança entre os vários organismos da organização são fundamentais à interoperabilidade organizacional projetada.

[2] Validar a proposição P8 em relação aos contextos de interoperabilidade organizacional, e à necessidade de experiência nestes contextos (P1.v1).

P8.v2. O contexto de interoperabilidade influencia a atitude e a confiança de uma organização em relação às restantes, com implicação sobre a privacidade dos dados partilhados.

[1] Verificar se o nível de confiança dos utilizadores do sistema, num contexto de colaboração com outra ou outras organizações é afetado em relação à privacidade dos dados.

[2] Validar a proposição P8 em relação aos contextos de interoperabilidade organizacional e ao funcionamento da privacidade dos dados nestes.

P8.v3. A utilização de tecnologias inerentemente invasivas da privacidade, tecnologias novas que apresentam ameaças e que provocam demasiado interesse público representam um risco à confiança sobre o sistema.

[1] Verificar se o nível de confiança pode ser afetado com o contínuo recurso a tecnologias de informação que podem afetar a privacidade tanto de profissionais como do titular dos dados.

[2] Validar a proposição P8 em relação à cada vez maior utilização de tecnologias de informação, que podem ser invasivas da privacidade.

Tabela 11: Estrutura da proposição P8

Proposição – descrição, enquadramento e fundamentação

P9.*"Ética e cooperação humana"*

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P9.v1. A iniciativa (atitude) e falta de confiança do titular dos dados ao condicionar ou limitar o acesso e utilização dos seus dados têm influência direta sobre a sua disponibilidade entre sistemas.

[1] Analisar se a iniciativa do titular dos dados pode comprometer os objetivos que estão na base da colaboração entre organizações.

[2] Validar a proposição P9 em relação à iniciativa do titular dos dados.

P9.v2. A *transparência* para com o titular dos dados, sendo necessário assegurar que este está suficientemente informado sobre o ambiente de colaboração entre as organizações, devendo ter acesso à informação sobre como estão a ser usados os seus dados, quem acedeu, de onde, para que fins e quais os meios técnicos utilizados para o seu processamento.

[1] Compreender se é necessário fazer evoluir o conceito de transparência face ao ambiente de colaboração e partilha de dados pessoais entre as organizações. Analisar se devem ser disponibilizadas soluções alternativas que permitam ao titular dos dados uma maior compreensão sobre o funcionamento e a proteção de dados em ambientes colaborativos, melhorando assim o princípio da transparência.

[2] Validar a proposição P9 em relação à transparência do objetivo para o qual os dados pessoais estão a ser recolhidos e à partilha de dados entre vários sistemas.

P9.v3. A atitude dos profissionais face à mudança que decorre dos novos requisitos do ambiente de colaboração, assim como a sua atitude face à deterioração da sua privacidade profissional, podem apresentar efeitos negativos para o sucesso das políticas de privacidade para o contexto da colaboração.

[1] Compreender se as mudanças tecnológicas associadas à interoperabilidade condicionam a atitude dos profissionais e se esta pode contribuir para o sucesso do projeto no global e a privacidade dos dados em particular.

[2] Validar a proposição P9 em relação à resistência às mudanças tecnológicas inerentes a um ambiente de colaboração.

Tabela 12: Estrutura da proposição P9

Proposição – descrição, enquadramento e fundamentação

P10.*"Estrutura organizativa"*

Variáveis Dependentes – ID e descrição

[1] O que se pretende conhecer?

[2] O motivo da recolha da informação

P10.v1. A resolução das dificuldades em ambientes de colaboração em matéria de privacidade dos dados resultantes da heterogeneidade organizacional depende da compreensão comum da importância da interoperabilidade organizacional e de uma estratégia e acordos comuns para o seu desenvolvimento.

[1] Analisar se uma cultura em interoperabilidade, neste caso organizacional, é importante ao desenvolvimento de práticas de privacidade dos dados.

[2] Validar a proposição P2 em relação à necessidade de desenvolvimento de uma cultura em interoperabilidade organizacional.

Tabela 13: Estrutura da proposição P10

4. Entrevistas por perfil de participante

Entrevista semiestruturada - *Perfil 1*
Elenco de questões para a entrevista a responsáveis locais pela implementação e coordenação da PDS

	Item	Questão
1	P2.v1.1	*Muitas organizações utilizam o termo "cultura", quando de alguma forma querem evidenciar valores importantes para o seu sucesso. Por exemplo: "cultura da qualidade", "cultura de segurança", "cultura empreendedora".* De que forma o sucesso da partilha de dados pode ser influenciada pelo desenvolvimento de uma cultura de privacidade transversal a todas as organizações?
2	P2.v2.1	*Num sistema de informação podem existir várias situações (contextos) de privacidade, com base numa justificação e gestão diferenciadas.* Qual a importância de um cultura de privacidade para que uma organização consiga lidar em simultâneo com várias situações de privacidade que exigem por parte da organização atitudes diferenciadas?
3	P2.v3.1	A maioria dos profissionais consegue distinguir os vários tipos de privacidade com que é confrontado diariamente? De que forma a compreensão e distinção da privacidade dos dados, face aos outros tipos de privacidade dependem de uma maior ou menor cultura de privacidade?
4	P2.v3.2	A distinção entre privacidade, proteção e segurança dos dados está também dependente de uma cultura de privacidade, ou apenas do conhecimento das questões técnicas associadas?
5	P5.v1.1	*É cada vez mais exigido às organizações que estas apresentem programas de responsabilidade em relação aos dados que recolhem e processam. É necessário que as organizações conheçam perante que entidades devem ter uma atitude de responsabilidade, assim como o que deve estar na base do desenvolvimento de um programa de responsabilidade.* A elaboração de um programa de responsabilidade, que contemple medidas para pôr em prática as obrigações e princípios da legislação, pode contribuir para a passagem da teoria à prática no domínio da privacidade dos dados? Se sim, quais as partes que devem promover o seu enquadramento e desenvolvimento?
6	P5.v4.1	Qual o contributo espectável para o desenvolvimento de um esquema de certificação aplicável a uma organização em relação à sua preparação em matéria de privacidade dos dados para um ambiente de colaboração? Aumentaria a confiança entre as organizações participantes no ambiente de colaboração?
7	P8.v2.1	O facto de uma organização operar em múltiplos sistemas, concebidos de forma isolada e com práticas de privacidade diferentes, pode influenciar ou condicionar a confiança dos seus utilizadores sobre a proteção e privacidade dos dados?
8	P8.v1.1	*Nenhum sistema subsiste sem confiança entre as partes.* De que forma a interoperabilidade organizacional depende da gestão da confiança entre as organizações no geral e entre os serviços afetados em particular?
9	P8.v1.2	É importante identificar os níveis de confiança em relação à colaboração das restantes organizações no domínio da privacidade dos dados?
10	P8.v3.1	*Muitas das novas tecnologias apresentam sérios riscos para a privacidade no global e para a privacidade dos dados em particular, devendo atempadamente este impacto ser analisado e reduzido ao mínimo.* Esta análise é determinante para a confiança dos profissionais sobre o sistema?
11	P6.v1.1	Estão todas as organizações cientes das limitações relacionadas com a recolha, utilização, partilha e retenção de informação no ambiente de colaboração?
12	P6.v1.2	Quais são as fases do ciclo de vida dos dados - criação, utilização, *transferência [entre sistemas]*, armazenamento, arquivo e destruição - mais preocupantes em matérias de privacidade que justifiquem medidas adicionais de proteção?

	Item	Questão
13	P6.v2.1	Concorda que o conhecimento generalizado do objetivo da recolha e tratamento dos dados é o ponto de partida para uma compreensão das necessidades de privacidade dos dados pessoais?
14	P6.v3.1	A identidade digital dos profissionais permite-nos controlar quem, como e de onde se acede aos dados. Contudo os dados apresentam diferentes níveis de exigência quanto à situação de privacidade. Uma nomenclatura de classificação dos dados permite adaptar melhor as políticas de privacidade aos dados? Quais os principais desafios, no domínio da classificação dos dados, que é necessário considerar quando os dados são partilhados com outras organizações?
15	P3.v1.1	Quais as preocupações/questões enfrentadas pelas organizações pelo facto de que, cada vez mais, as organizações funcionam e dependerem do funcionamento em rede (integradas ou em colaboração com outras organizações)?
16	P3.v1.2	É possível e desejável uma interoperabilidade organizacional que suporte a partilha de experiência ao nível da segurança de infraestruturas e promova uma padronização das melhores práticas de segurança? Que efeitos práticos pode apresentar esta partilha de experiência?
17	P4.v1.1	*A falta de um vocabulário partilhado para discutir as questões da privacidade faz com que tanto responsáveis de sistemas como gestores executivos, muitas vezes, concordem com especificações para os sistemas que não conseguem lidar com a privacidade de forma satisfatória.* Quais as maiores dificuldades que poderiam ser resolvidas com a existência de uma linguagem de privacidade, uma taxonomia, neste caso focada na privacidade dos dados?
18	P4.v2.1	Que benefícios práticos pode apresentar uma linguagem consensual orientada para as questões da privacidade para os responsáveis dos sistemas de informação?
19	P10.v1.1	Na sua opinião, e tendo em conta a complexidade da questão da privacidade dos dados no contexto de colaboração entre várias organizações, qual a abordagem que melhor se adapta a esta complexidade? Uma abordagem conjunta e integrada, ou uma abordagem individual e isolada? O que é necessário para operacionalizar uma abordagem conjunta deste assunto?
20	P10.v1.2	Como lidar com as dificuldades de interoperabilidade e colaboração organizacional que tem origem na heterogeneidade organizacional caracterizada por diferentes níveis de competências, estratégias e culturas organizacionais, tecnologias e outros recursos disponíveis?
21	P1.v1.1	Podemos afirmar que o sucesso do planeamento de políticas de proteção e privacidade de dados está muito dependente de experiência em projetos de partilha de dados e interoperabilidade? Pode indicar alguns exemplos de projetos na sua organização?
22	P1.v2.1	Se nos focarmos no objetivo de desenvolver um ambiente seguro e confiável para a partilha de dados, que experiência é exigível aos responsáveis pelo desenvolvimento dos sistemas de informação?
23	P1.v2.2	Qual o resultado espectável de uma melhoria do conhecimento da legislação de proteção e privacidade dos dados?
24	P1.v3.1	Quais os recursos humanos que considera fundamentais ao suporte das questões da privacidade dos dados para o âmbito alargado do contexto de colaboração com outras organizações? Justifica-se uma estrutura organizativa de suporte às questões da privacidade dos dados para o âmbito alargado do contexto de colaboração?
25	P1.v4.1	Que tipo (s) de eventos, podem contribuir para uma melhoria da preparação da globalidade dos utilizadores do sistema informático (de informação), em relação à privacidade dos dados?

Entrevista semiestruturada - *Perfil 2*

Elenco de questões para a entrevista a técnicos e responsáveis pelos sistemas de informação

	Item	Questão
1	P3.v1.1	Quais as preocupações/questões enfrentadas pelas organizações pelo facto de que, cada vez mais, as organizações funcionam e dependerem do funcionamento em rede (integradas ou em colaboração com outras organizações)?
2	P3.v1.2	É possível e desejável uma interoperabilidade organizacional que suporte a partilha de experiência ao nível da segurança de infraestruturas e promova uma padronização das melhores práticas de segurança? Que efeitos práticos pode apresentar esta partilha de experiência?
3	P3.v2.1	Os procedimentos ou políticas de segurança existentes têm por base uma análise prévia do risco em segurança, dos sistemas e das tecnologias de informação? *Se sim*, quais as vantagens ou contributos para a definição das políticas de segurança? *Se não*, qual foi a base para a definição das políticas de segurança implementadas?
4	P3.v3.1	*A identidade digital e os sistemas tecnológicos para a sua gestão constituem um dos elementos de suporte ao funcionamento e à evolução do ambiente de colaboração e partilha de dados.* Qual a evolução desejável para estes sistemas tecnológicos face aos desafios do ambiente de colaboração com outras organizações?
5	P3.v4.1	Os problemas de privacidade dos dados que surgem na sua utilização primária[76] são diferentes da sua utilização secundária[77]? Qual a melhor forma de lidar com a exigência de privacidade nas situações de utilização secundária?
6	P3.v5.1	É possível elaborar planos de contingência para situações em que há uma violação da proteção de dados pessoais? Que tipo de medidas devem ser definidas?
7	P4.v1.1	*A falta de um vocabulário partilhado para discutir as questões da privacidade faz com que tanto responsáveis de sistemas como gestores executivos, muitas vezes, concordem com especificações para os sistemas que não conseguem lidar com a privacidade de forma satisfatória.* Quais as maiores dificuldades que poderiam ser resolvidas com a existência de uma linguagem de privacidade, uma taxonomia, neste caso focada na privacidade dos dados?
8	P4.v2.1	Que benefícios práticos pode apresentar uma linguagem consensual orientada para as questões da privacidade para os responsáveis dos sistemas de informação?
9	P6.v1.1	Estão todas as organizações cientes das limitações relacionadas com a recolha, utilização, partilha e retenção de informação no ambiente de colaboração?
10	P6.v1.2	Quais são as fases do ciclo de vida dos dados - criação, utilização, *transferência [entre sistemas]*, armazenamento, arquivo e destruição - mais preocupantes em matérias de privacidade que justifiquem medidas adicionais de proteção?
11	P6.v2.1	Concorda que o conhecimento generalizado do objetivo da recolha e tratamento dos dados é o ponto de partida para uma compreensão das necessidades de privacidade dos dados pessoais?
12	P6.v3.1	A identidade digital dos profissionais permite-nos controlar quem, como e de onde se acede aos dados. Contudo os dados apresentam diferentes níveis de exigência quanto à situação de privacidade. Uma nomenclatura de classificação dos dados permite adaptar melhor as políticas de privacidade aos dados? Quais os principais desafios, no domínio da classificação dos dados, que é necessário considerar quando os dados são partilhados com outras organizações?

[76] Interfaces ou aplicações que colaboram na manutenção de um conjunto de dados sobre um titular dos dados.

[77] Cruzamento com outros dados, utilização dos dados para objetivos secundários, retenção e destruição dos dados.

	Item	Questão
13	P6.v4.1	*Não faz sentido pensar em políticas de privacidade se estas não tiverem por suporte medidas de proteção dos dados. A privacidade dos dados depende em parte das decisões implementadas ao nível da proteção dos dados.* Para um ambiente de interoperabilidade e colaboração, desenvolvido sobre sistemas heterogéneos, o que é preponderante para otimizar esta dependência (*da privacidade dos dados em relação à proteção dos dados*)?
14	P5.v1.1	*É cada vez mais exigido às organizações que estas apresentem programas de responsabilidade em relação aos dados que recolhem e processam. É necessário que as organizações conheçam perante que entidades devem ter uma atitude de responsabilidade, assim como o que deve estar na base do desenvolvimento de um programa de responsabilidade.* A elaboração de um programa de responsabilidade, que contemple medidas para pôr em prática as obrigações e princípios da legislação, pode contribuir para a passagem da teoria à prática no domínio da privacidade dos dados? Se sim, quais as partes que devem promover o seu enquadramento e desenvolvimento?
15	P5.v2.1	*Na segurança informática, é prática regular a análise da sua conformidade face às políticas de segurança desenhadas, como garantia da sua eficácia e melhoria continua.* Como é que se pode avaliar, de uma forma contínua, se um determinado contexto de utilização dos dados está de acordo com os requisitos legais e políticas de privacidade existentes?
16	P5.v2.2	Quais os fatores determinantes para a definição do nível de exigência e periodicidade das tarefas de análise da conformidade?
17	P5.v2.3	Considera importante a publicação do resultado destes processos de análise de conformidade? Se sim, porquê e qual na sua opinião pode ser o resultado esperado com a publicação destes resultados?
18	P5.v3.1	*O registo de todas as tarefas e a sua origem local ou remota são uma das garantias da correta utilização destes dados face às políticas e legislação aplicáveis.* Qual o desempenho ou funções esperadas de um sistema de *accountability* para o contexto de partilha de dados entre sistemas e como se espera que estes evoluam no futuro?
19	P5.v4.1	Qual o contributo espectável para o desenvolvimento de um esquema de certificação aplicável a uma organização em relação à sua preparação em matéria de privacidade dos dados para um ambiente de colaboração? Aumentaria a confiança entre as organizações participantes no ambiente de colaboração?
20	P1.v1.1	Podemos afirmar que o sucesso do planeamento de políticas de proteção e privacidade de dados está muito dependente de experiência em projetos de partilha de dados e interoperabilidade? Pode indicar alguns exemplos de projetos na sua organização?
21	P1.v2.1	Se nos focarmos no objetivo de desenvolver um ambiente seguro e confiável para a partilha de dados, que experiência é exigível aos responsáveis pelo desenvolvimento dos sistemas de informação?
22	P1.v2.2	Qual o resultado espectável de uma melhoria do conhecimento da legislação de proteção e privacidade dos dados?
23	P1.v3.1	Quais os recursos humanos que considera fundamentais ao suporte das questões da privacidade dos dados para o âmbito alargado do contexto de colaboração com outras organizações? Justifica-se uma estrutura organizativa de suporte às questões da privacidade dos dados para o âmbito alargado do contexto de colaboração?
24	P1.v4.1	Que tipo (s) de eventos, podem contribuir para uma melhoria da preparação da globalidade dos utilizadores do sistema informático (de informação), em relação à privacidade dos dados?

Entrevista semiestruturada - *Perfil 3*
Elenco de questões para a entrevista a profissionais de saúde

	Item	Questão
1	P2.v2.1	*Num sistema de informação podem existir várias situações (contextos) de privacidade, com base numa justificação e gestão diferenciadas.* Qual a importância de um cultura de privacidade para que uma organização consiga lidar em simultâneo com várias situações de privacidade que exigem por parte da organização atitudes diferenciadas?
2	P2.v3.1	A maioria dos profissionais consegue distinguir os vários tipos de privacidade com que é confrontado diariamente? De que forma a compreensão e distinção da privacidade dos dados, face aos outros tipos de privacidade dependem de uma maior ou menor cultura de privacidade?
3	P2.v3.2	A distinção entre privacidade, proteção e segurança dos dados está também dependente de uma cultura de privacidade, ou apenas do conhecimento das questões técnicas associadas?
4	P9.v3.1	Sente que, nunca como hoje, é necessário tratar a informação da mesma forma como se trata um paciente?
5	P9.v3.2	A que níveis se pode manifestar a atitude dos vários profissionais face às mudanças e requisitos organizacionais decorrentes das iniciativas de colaboração entre organizações?
6	P9.v3.3	Existe a consciência de um aumento de práticas que degradam o direito e expectativas da privacidade profissional face ao crescimento de um "controlo tecnológico invisível"?
7	P9.v3.4	Qual a influência que este "controlo tecnológico invisível" do trabalho dos profissionais que afeta a sua privacidade profissional, pode ter sobre a sua atitude face à sua participação num ambiente de colaboração?
8	P9.v3.5	Enquanto profissional de saúde, concorda que a sua própria ação ou omissão[78] pode prejudicar outros profissionais (ética)?
9	P8.v1.1	*Nenhum sistema subsiste sem confiança entre as partes.* De que forma a interoperabilidade organizacional depende da gestão da confiança entre as organizações no geral e entre os serviços afetados em particular?
10	P8.v1.2	É importante identificar os níveis de confiança em relação à colaboração das restantes organizações no domínio da privacidade dos dados?
11	P8.v2.1	O facto de uma organização operar em múltiplos sistemas, concebidos de forma isolada e com práticas de privacidade diferentes, pode influenciar ou condicionar a confiança dos seus utilizadores sobre a proteção e privacidade dos dados?
12	P8.v3.1	Muitas das novas tecnologias apresentam sérios riscos para a privacidade no global e para a privacidade dos dados em particular, devendo atempadamente este impacto ser analisado e reduzido ao mínimo. Esta análise é determinante para a confiança dos profissionais sobre o sistema?
13	P1.v4.1	Que tipo (s) de eventos, podem contribuir para uma melhoria da preparação da globalidade dos utilizadores do sistema informático (de informação), em relação à privacidade dos dados?

[78] Neste caso a confidencialidade do médico – proteção do paciente.

Entrevista semiestruturada - *Perfil 4*

Elenco de questões para a entrevista a gestores e administradores

	Item	Questão
1	P2.v1.1	*Muitas organizações utilizam o termo "cultura", quando de alguma forma querem evidenciar valores importantes para o seu sucesso. Por exemplo: "cultura da qualidade", "cultura de segurança", "cultura empreendedora".* De que forma o sucesso da partilha de dados pode ser influenciada pelo desenvolvimento de uma cultura de privacidade transversal a todas as organizações?
2	P2.v2.1	*Num sistema de informação podem existir várias situações (contextos) de privacidade, com base numa justificação e gestão diferenciadas.* Qual a importância de um cultura de privacidade para que uma organização consiga lidar em simultâneo com várias situações de privacidade que exigem por parte da organização atitudes diferenciadas?
3	P5.v1.1	*É cada vez mais exigido às organizações que estas apresentem programas de responsabilidade em relação aos dados que recolhem e processam. É necessário que as organizações conheçam perante que entidades devem ter uma atitude de responsabilidade, assim como o que deve estar na base do desenvolvimento de um programa de responsabilidade.* A elaboração de um programa de responsabilidade, que contemple medidas para pôr em prática as obrigações e princípios da legislação, pode contribuir para a passagem da teoria à prática no domínio da privacidade dos dados? Se sim, quais as partes que devem promover o seu enquadramento e desenvolvimento?
4	P5.v2.1	*Na segurança informática, é prática regular a análise da sua conformidade face às políticas de segurança desenhadas, como garantia da sua eficácia e melhoria continua.* Como é que se pode avaliar, de uma forma contínua, se um determinado contexto de utilização dos dados está de acordo com os requisitos legais e políticas de privacidade existentes?
5	P5.v4.1	Qual o contributo espectável para o desenvolvimento de um esquema de certificação aplicável a uma organização em relação à sua preparação em matéria de privacidade dos dados para um ambiente de colaboração? Aumentaria a confiança entre as organizações participantes no ambiente de colaboração?
6	P4.v1.1	*A falta de um vocabulário partilhado para discutir as questões da privacidade faz com que tanto responsáveis de sistemas como gestores executivos, muitas vezes, concordem com especificações para os sistemas que não conseguem lidar com a privacidade de forma satisfatória.* Quais as maiores dificuldades que poderiam ser resolvidas com a existência de uma linguagem de privacidade, uma taxonomia, neste caso focada na privacidade dos dados?
7	P7.v1.1	Numa linguagem de gestão, qual o fator determinante, para que os gestores executivos assumam a necessidade de uma estratégia para a privacidade, não isolada, e integrada com a estratégia desenvolvida para o sistema de informação?
8	P7.v1.2	Qual a importância do reconhecimento por parte dos gestores executivos da responsabilidade da sua organização ou a sua própria responsabilidade em relação à proteção da privacidade dos dados e das pessoas?
9	P7.v2.1	De que forma ou qual será a ferramenta indicada para que todas as decisões relativas à privacidade dos dados possam ser integradas, proporcionando uma proteção mais eficiente?
10	P7.v3.1	Qual a influência que o risco, o seu conhecimento, a previsão do seu impacto pode ter sobre a necessidade de as organizações desenvolverem uma visão estratégia para a privacidade?
11	P7.v4.1	Considera que existe uma influência considerável entre a existência de uma estratégia de privacidade e uma cultura organizacional em privacidade? Qual a dependência entre estes dois conceitos (o que é que depende do quê?)

12	P7.v5.1	Sendo que o âmbito de uma estratégia organizativa para a privacidade deve refletir a natureza e missão da organização, qual a colaboração possível a este nível entre as organizações participantes no ambiente de colaboração?
13	P8.v1.1	*Nenhum sistema subsiste sem confiança entre as partes.* De que forma a interoperabilidade organizacional depende da gestão da confiança entre as organizações no geral e entre os serviços afetados em particular?
14	P8.v1.2	É importante identificar os níveis de confiança em relação à colaboração das restantes organizações no domínio da privacidade dos dados?
15	P8.v2.1	O facto de uma organização operar em múltiplos sistemas, concebidos de forma isolada e com práticas de privacidade diferentes, pode influenciar ou condicionar a confiança dos seus utilizadores sobre a proteção e privacidade dos dados?
16	P8.v3.1	Muitas das novas tecnologias apresentam sérios riscos para a privacidade no global e para a privacidade dos dados em particular, devendo atempadamente este impacto ser analisado e reduzido ao mínimo. Esta análise é determinante para a confiança dos profissionais sobre o sistema?
17	P9.v3.1	Sente que, nunca como hoje, é necessário tratar a informação da mesma forma como se trata um paciente?
18	P9.v3.2	A que níveis se pode manifestar a atitude dos vários profissionais face às mudanças e requisitos organizacionais decorrentes das iniciativas de colaboração entre organizações? *Padrão: a postura, avaliação, aceitação ou oposição manifestados pelos profissionais de uma organização em relação às mudanças que possam decorrer do facto da organização desenvolver iniciativas de interoperabilidade podem condicionar o seu sucesso.*
19	P9.v3.3	Existe a consciência de um aumento de práticas que degradam o direito e expectativas da privacidade profissional face ao crescimento de um "controlo tecnológico invisível"?
20	P9.v3.4	Qual a influência que este "controlo tecnológico invisível" do trabalho dos profissionais que afeta a sua privacidade profissional, pode ter sobre a sua atitude face à sua participação num ambiente de colaboração?
21	P1.v3.1	Quais os recursos humanos que considera fundamentais ao suporte das questões da privacidade dos dados para o âmbito alargado do contexto de colaboração com outras organizações? Justifica-se uma estrutura organizativa de suporte às questões da privacidade dos dados para o âmbito alargado do contexto de colaboração?
22	P10.v1.1	Na sua opinião, e tendo em conta a complexidade da questão da privacidade dos dados no contexto de colaboração entre várias organizações, qual a abordagem que melhor se adapta a esta complexidade? Uma abordagem conjunta e integrada, ou uma abordagem individual e isolada? O que é necessário para operacionalizar uma abordagem conjunta deste assunto?
23	P10.v1.2	Como lidar com as dificuldades de interoperabilidade e colaboração organizacional que tem origem na heterogeneidade organizacional caracterizada por diferentes níveis de competências, estratégias e culturas organizacionais, tecnologias e outros recursos disponíveis?
24	P1.v4.1	Que tipo (s) de eventos, podem contribuir para uma melhoria da preparação da globalidade dos utilizadores do sistema informático (de informação), em relação à privacidade dos dados?

Anexo II - Protocolo para o *estudo de caso* – acordo de colaboração, Perfil 1

Privacidade dos dados

em ambientes de interoperabilidade - a área da saúde

Acordo de colaboração

Apresentação

O presente documento tem como intuito apresentar o objetivo do projeto de investigação "*Privacidade dos dados em ambientes de interoperabilidade – a área da saúde*", as condições de participação e a estrutura da entrevista, aos participantes identificados, e que pela sua experiência profissional se enquadram no objetivo do estudo.

O projeto de investigação, na área dos sistemas de informação, apresenta como principal objetivo a identificação e o estudo dos fatores críticos à privacidade dos dados, em contextos de colaboração entre organizações, onde existe partilha de dados entre sistemas de informação heterogéneos - como é o caso da Plataforma de Dados da Saúde (PDS).

Estamos perante uma realidade complexa, subjetiva, para a qual é essencial o seu estudo em contexto real, onde a compreensão do contexto de ação e as experiências individuais são muito relevantes para a identificação dos fatores relacionados com a "atividade humana" que podem condicionar a privacidade dos dados em processos de colaboração inter-organizacional. A opinião, a experiência e o conhecimento dos vários atores num fenómeno com estas características constituem a principal, senão única, fonte primária de informação.

Após a autorização oficial para a realização do estudo, e com a colaboração de um interlocutor em cada uma das unidades de análise, foi possível identificar para cada um dos 4 perfis pré-definidos, o número de profissionais que se pretende integrar no estudo. Dada a sua experiência profissional e a perspetiva de que a sua participação pode ser uma mais-valia para este estudo, foi indicado o seu nome para a fase seguinte, que consiste na recolha de dados.

No sentido de otimizar o contributo individual expectável, nas páginas seguintes são apresentadas as questões a abordar na entrevista, que se pretende seja a mais aberta possível, assim como a agenda das entrevistas. Desta forma, é possível ao participante analisar as questões, refletir sobre as mesmas, e preparar a exposição que melhor transmite a sua experiência nesta temática.

Sendo inviável a cobertura total e de todas as instituições que integram a PDS, foram constituídas unidades de análise, as seguintes organizações:

a. *Projeto-piloto – Unidade Local de Saúde do Norte Alentejano, Portalegre (ULSNA);*
b. Hospital do Espírito Santo E.P.E, Évora (HES);
c. USF Saúde Mais, Santa Maria da Feira (USF);
d. Hospital Professor Doutor Fernando Fonseca E.P.E., Amadora (HFF);
e. *Instituto Nacional de Emergência Médica,* Lisboa (INEM);
f. Serviços Partilhados do Ministério da Saúde E.P.E. (SPMS);
g. Grupo de *beta-tester* de Utentes.

A recolha de dados será realizada através do recurso a entrevistas semiestruturadas, com as seguintes características:

a. De participação voluntária*;*
b. Uma duração de 30 a 40 minutos;
c. Será recolhida a opinião da pessoa sobre as questões em estudo, e em nenhuma situação será recolhida a opinião da pessoa sobre a instituição, nem sobre a forma como esta funciona;
d. Todos os dados serão tratados de forma confidencial e apenas no âmbito da investigação em curso, não sendo possível que outras pessoas ou entidades externas utilizem estes dados para outro fim.

Ficha técnica: este é um estudo de investigação realizado no âmbito do programa de doutoramento em gestão, especialidade em sistemas de informação, da Universidade de Évora, da autoria de Secundino Lopes (secundino.lopes@estgp.pt), docente do Instituto Politécnico de Portalegre, sob a orientação do Prof. Rui Quaresma (quaresma@uevora.pt), Professor auxiliar da Universidade de Évora.

Entrevista semiestruturada - *Perfil 1*

Elenco de questões para a entrevista a **responsáveis locais pela implementação e coordenação da PDS**

	Questão
1	*Muitas organizações utilizam o termo "cultura", quando de alguma forma querem evidenciar valores importantes para o seu sucesso. Por exemplo: "cultura da qualidade", "cultura de segurança", "cultura empreendedora".* De que forma o sucesso da partilha de dados pode ser influenciado pelo desenvolvimento de uma cultura de privacidade transversal a todas as organizações?
2	*Existem nas organizações várias situações (contextos) de privacidade, justificadas e geridas muitas vezes de formas diferenciadas.* Qual a importância de uma cultura de privacidade para que uma organização consiga lidar com as várias situações de privacidade que identificou?
3	A maioria dos profissionais consegue distinguir os vários tipos de privacidade[79] com que é confrontado diariamente? De que forma a compreensão e distinção da privacidade dos dados, face aos outros tipos de privacidade dependem de uma maior cultura de privacidade?
4	Por outro lado, a distinção entre privacidade[80], proteção e segurança dos dados está também dependente de uma cultura de privacidade, ou apenas do conhecimento das questões técnicas associadas?
5	*É cada vez mais exigido às organizações que estas apresentem um programa de responsabilidade[81] em relação à proteção de dados pessoais. Permite identificar perante que entidades devem ter uma atitude de responsabilidade, assim como o que deve estar na base do desenvolvimento de um programa de responsabilidade.* A elaboração de um programa de responsabilidade, que contemple medidas para pôr em prática as obrigações e princípios da legislação, pode contribuir para a passagem da teoria à prática no domínio da privacidade dos dados? Se sim, quais as partes que devem promover o seu enquadramento e desenvolvimento?
6	*No domínio da segurança de infraestruturas tecnológicas é muito comum os seus responsáveis recorrerem a esquemas de certificação reconhecidos publicamente, como forma de melhoria contínua das soluções implementadas e como garantia de qualidade tecnológica para os seus colaboradores.* Que benefícios pode apresentar a certificação de uma organização em matérias de proteção de dados? A certificação das organizações a este nível aumentaria a confiança entre as

[79] São os exemplos da privacidade da pessoa, por vezes referida como privacidade corporal, privacidade do comportamento e da esfera pessoal, privacidade das comunicações pessoais e privacidade dos dados pessoais.

[80] **A privacidade**, também conhecida por privacidade dos dados, é um valor e um direito à privacidade na recolha, utilização, armazenamento e partilha de dados pessoais de um indivíduo. A privacidade dos dados deve ser analisada sempre que dados identificáveis relativos a uma ou mais pessoais são recolhidos e armazenados em formato digital ou num outro suporte.

[81] Um **programa de responsabilidade** constitui o meio de demonstração da vontade e da capacidade da organização em ser responsável e responsabilizada pelas práticas de gestão de dados. É essencial à salvaguarda da privacidade de dados, assim como à confiança do titular dos dados na organização, e entre esta e outras organizações. Deve constituir-se como um programa sólido e transparente, que contemple medidas adequadas e eficazes para pôr em prática as obrigações e princípios da legislação em vigor sobre proteção de dados. Constitui a ferramenta operacional necessária para as questões da privacidade.

	organizações participantes no ambiente de partilha de dados como a PDS?
7	O facto de uma organização operar com múltiplos sistemas, concebidos de forma isolada e com práticas de privacidade e proteção de dados diferentes, pode influenciar ou condicionar a confiança dos seus utilizadores nestes sistemas?
8	*Existem vários fatores com influência sobre a colaboração e a interoperabilidade entre organizações, nomeadamente questões de cultura, estrutura e práticas organizacionais.* De que forma o desenvolvimento de iniciativas de interoperabilidade organizacional, por exemplo nos domínios da segurança e proteção de dados, depende da confiança estabelecida entre as organizações?
9	Uma análise atempada dos impactos (riscos) sobre a privacidade que podem surgir com o desenvolvimento ou aquisição de uma nova solução tecnológica ou serviço de informação, que utiliza dados pessoais, pode influenciar a confiança dos profissionais utilizadores destas soluções? Se sim, de que forma?
10	Estão as organizações cientes das limitações relacionadas com a recolha, utilização, partilha e retenção de informação no ambiente de colaboração?
11	Quais são as fases do ciclo de vida dos dados[82] - criação, utilização, *transferência [entre sistemas]*, armazenamento, arquivo e destruição - mais preocupantes em matérias de privacidade que justifiquem medidas adicionais de proteção?
12	Concorda que o conhecimento generalizado do objetivo da recolha e tratamento dos dados[83] é o ponto de partida para uma compreensão da necessidade de privacidade dos dados pessoais?
13	*Os dados apresentam diferentes níveis de exigência quanto à sua privacidade, pelo que a sua classificação é importante para a definição de requisitos e níveis de proteção da privacidade.* Uma nomenclatura de classificação dos dados permite adaptar melhor as políticas de privacidade dos dados? Quais os principais desafios, no domínio da classificação dos dados, que é necessário considerar quando os dados são partilhados com outras organizações?
14	Quais as maiores preocupações enfrentadas pelas organizações pelo facto de que, cada vez mais, as organizações funcionam e dependem do funcionamento em rede (integradas ou em colaboração com outras organizações)?
15	É possível e desejável uma interoperabilidade organizacional que suporte a partilha de experiência ao nível da segurança de infraestruturas e promova uma padronização das melhores práticas de segurança? Que efeitos práticos pode apresentar esta partilha de experiência?
16	*A falta de um vocabulário partilhado para discutir as questões da privacidade faz*

[82] Quer sejam, ***dados pessoais*** (qualquer informação relativa a uma pessoa singular identificada ou identificável), ***dados sensíveis*** (são um subconjunto dos dados pessoais, sobre o qual uma das partes acredita dever ser privado, nomeadamente dados que divulguem informações sobre a origem racial ou étnica, religiosa, política, bem como dados pessoais de saúde), ***dados de identificação pessoal*** (subconjunto dos dados pessoais que permitem uma identificação direta da pessoa em causa, ou qualquer outra informação que identifica ou pode ser usada para identificar, contactar, ou localizar a pessoa a quem se refere tal informação), ou ***dados anónimos*** (dados que não podem ser associados a qualquer titular de dados identificado ou identificável).

[83] Implementando desta forma o princípio da *especificação de objetivos* da Diretiva 95/46/CE de proteção de dados, que define que os dados pessoais devem ser recolhidos para finalidades determinadas, legais e legítimas, e não podem ser tratados de formas não compatíveis com estas finalidades.

	com que tanto responsáveis de sistemas como gestores executivos, muitas vezes, concordem com especificações para os sistemas que não conseguem lidar com a privacidade de forma satisfatória. Quais as maiores dificuldades que poderiam ser resolvidas com a existência de uma linguagem de privacidade, uma taxonomia[84], neste caso focada na privacidade dos dados?
17	Para o contexto da colaboração e partilha de dados entre organizações, que benefícios práticos pode apresentar uma taxonomia orientada para as questões da privacidade, utilizada por todos os responsáveis dos sistemas de informação?
18	Na sua opinião, e tendo em conta a complexidade da questão da privacidade dos dados no contexto de colaboração entre várias organizações, qual a abordagem que melhor se adapta a esta complexidade: uma abordagem conjunta e integrada, ou uma abordagem individual e isolada? O que é necessário para operacionalizar uma abordagem conjunta deste assunto?
19	*As organizações são diferentes em termos de disponibilidade e prontidão para a colaboração e interoperabilidade, nomeadamente devido à sua heterogeneidade tecnológica e organizativa.* Para garantir a privacidade e proteção dos dados, o que é necessário promover nas organizações para se atingir uma maior capacidade de colaboração?
20	Podemos afirmar que o sucesso do planeamento de políticas de proteção e privacidade de dados está muito dependente da experiência em projetos de partilha de dados e em interoperabilidade? Pode indicar alguns exemplos de projetos na sua organização?
21	Se nos focarmos no objetivo de desenvolver um ambiente seguro e confiável para a partilha de dados, que experiência é exigível aos responsáveis pelo desenvolvimento dos sistemas de informação?
22	Qual o resultado expectável de uma melhoria do conhecimento da legislação de proteção e privacidade dos dados?
23	Quais os recursos humanos que considera fundamentais ao suporte das questões da privacidade dos dados para o âmbito alargado do contexto de colaboração com outras organizações? Justifica-se uma estrutura organizativa de suporte às questões da privacidade dos dados para o âmbito alargado do contexto de colaboração?
24	Que tipo (s) de eventos pode (m) contribuir para uma melhoria da preparação da globalidade dos profissionais em relação à privacidade dos dados?

Agenda para as entrevistas

Nome Completo	Data	Hora	Local

84 Uma taxonomia de privacidade dos dados constitui "*um conjunto documentado e ordenado de tipos, classificações, categorizações e/ou princípios que são frequentemente alcançados por meio de mecanismos, incluindo a nomeação, definição e/ou o agrupamento de atributos, e que por sua vez ajudaram a descrever, diferenciar, identificar, organizar e fornecer relações contextuais entre entidades, tipos e itens de privacidades dos dados*".

Anexo III - Protocolo para o *estudo de caso* – acordo de colaboração, Perfil 2

Privacidade dos dados

em ambientes de interoperabilidade - a área da saúde

Acordo de colaboração

Apresentação

O presente documento tem como intuito apresentar o objetivo do projeto de investigação "*Privacidade dos dados em ambientes de interoperabilidade – a área da saúde*", as condições de participação e a estrutura da entrevista, aos participantes identificados, e que pela sua experiência profissional se enquadram no objetivo do estudo.

O projeto de investigação, na área dos sistemas de informação, apresenta como principal objetivo a identificação e o estudo dos fatores críticos à privacidade dos dados, em contextos de colaboração entre organizações, onde existe partilha de dados entre sistemas de informação heterogéneos - como é o caso da Plataforma de Dados da Saúde (PDS).

Estamos perante uma realidade complexa, subjetiva, para a qual é essencial o seu estudo em contexto real, onde a compreensão do contexto de ação e as experiências individuais são muito relevantes para a identificação dos fatores relacionados com a "atividade humana" que podem condicionar a privacidade dos dados em processos de colaboração inter-organizacional. A opinião, a experiência e o conhecimento dos vários atores num fenómeno com estas características constituem a principal, senão única, fonte primária de informação.

Após a autorização oficial para a realização do estudo, e com a colaboração de um interlocutor em cada uma das unidades de análise, foi possível identificar para cada um dos 4 perfis pré-definidos, o número de profissionais que se pretende integrar no estudo. Dada a sua experiência profissional e a perspetiva de que a sua participação pode ser uma mais-valia para este estudo, foi indicado o seu nome para a fase seguinte, que consiste na recolha de dados.

No sentido de otimizar o contributo individual expectável, nas páginas seguintes são apresentadas as questões a abordar na entrevista, que se pretende seja a mais aberta possível, assim como a agenda das entrevistas. Desta forma, é possível ao participante analisar as questões, refletir sobre as mesmas, e preparar a exposição que melhor transmite a sua experiência nesta temática.

Sendo inviável a cobertura total e de todas as instituições que integram a PDS, foram constituídas unidades de análise, as seguintes organizações:

a. *Projeto-piloto – Unidade Local de Saúde do Norte Alentejano, Portalegre (ULSNA);*
b. Hospital do Espírito Santo E.P.E, Évora (HES);
c. USF Saúde Mais, Santa Maria da Feira (USF);
d. Hospital Professor Doutor Fernando Fonseca E.P.E., Amadora (HFF);
e. *Instituto Nacional de Emergência Médica,* Lisboa (INEM);
f. Serviços Partilhados do Ministério da Saúde E.P.E. (SPMS);
g. Grupo de *beta-tester* de Utentes.

A recolha de dados será realizada através do recurso a entrevistas semiestruturadas, com as seguintes características:

a. De participação voluntária*;*
b. Uma duração de 30 a 40 minutos;
c. Será recolhida a opinião da pessoa sobre as questões em estudo, e em nenhuma situação será recolhida a opinião da pessoa sobre a instituição, nem sobre a forma como esta funciona;
d. Todos os dados serão tratados de forma confidencial e apenas no âmbito da investigação em curso, não sendo possível que outras pessoas ou entidades externas utilizem estes dados para outro fim.

Ficha técnica: este é um estudo de investigação realizado no âmbito do programa de doutoramento em gestão, especialidade em sistemas de informação, da Universidade de Évora, da autoria de Secundino Lopes (secundino.lopes@estgp.pt), docente do Instituto Politécnico de Portalegre, sob a orientação do Prof. Rui Quaresma (quaresma@uevora.pt), Professor auxiliar da Universidade de Évora.

Entrevista semiestruturada - *Perfil 2*

Elenco de questões para a entrevista a **técnicos e responsáveis pelos sistemas de informação**

	Questão
1	Quais as maiores preocupações enfrentadas pelas organizações pelo facto de que, cada vez mais, as organizações funcionam e dependem do funcionamento em rede (integradas ou em colaboração com outras organizações)?
2	É possível e desejável uma interoperabilidade[85] organizacional que suporte a partilha de experiência ao nível da segurança de infraestruturas e promova uma padronização das melhores práticas de segurança? Que efeitos práticos pode apresentar esta partilha de experiência?
3	Os procedimentos ou políticas de segurança existentes têm por base uma análise prévia do risco em segurança, dos sistemas e das tecnologias de informação? *Se sim*, quais as vantagens ou contributos para a definição das políticas de segurança? *Se não*, qual foi a base para a definição das políticas de segurança implementadas?
4	*A identidade digital[86] e os sistemas tecnológicos para a sua gestão constituem um dos elementos de suporte ao funcionamento e à evolução do ambiente de colaboração e partilha de dados.* Qual a evolução desejável para estes sistemas tecnológicos face aos desafios do ambiente de colaboração com outras organizações?
5	Os problemas de privacidade dos dados[87] que surgem na sua utilização primária[88] são diferentes dos problemas que surgem na sua utilização secundária[89]? Qual a melhor forma de lidar com a exigência de privacidade nas situações de utilização secundária?
6	É possível elaborar planos de contingência para situações em que há uma violação da proteção de dados pessoais? Que tipo de medidas devem ser definidas?
7	*A falta de um vocabulário partilhado para discutir as questões da privacidade faz com que tanto responsáveis de sistemas como gestores executivos, muitas vezes, concordem com especificações para os sistemas que não conseguem lidar com a privacidade de forma satisfatória.* Quais as maiores dificuldades que poderiam ser resolvidas com a existência de uma linguagem de privacidade, uma taxonomia, neste caso focada na privacidade dos dados?
8	Para o contexto da colaboração e partilha de dados entre organizações, que benefícios práticos pode apresentar uma taxonomia orientada para as questões da privacidade, utilizada por todos os responsáveis dos sistemas de informação?
9	Estão as organizações cientes das limitações relacionadas com a recolha, utilização, partilha e retenção de informação no ambiente de colaboração?

[85] **Interoperabilidade** é a capacidade de dois ou mais sistemas heterogéneos e independentes trocarem e utilizarem informação e serviços, independente das aplicações informáticas utilizadas.

[86] A **identidade digital** constitui a representação digital dos dados relacionados com uma pessoa, empresa, sistema, máquina, acessível por meios técnicos computacionais.

[87] **A privacidade**, também conhecida por privacidade dos dados, é um valor e um direito à privacidade na recolha, utilização, armazenamento e partilha de dados pessoais de um indivíduo. A privacidade dos dados deve ser analisada sempre que dados identificáveis relativos a uma ou mais pessoais são recolhidos e armazenados em formato digital ou num outro suporte.

[88] Interfaces ou aplicações que colaboram na manutenção de um conjunto de dados sobre um titular dos dados.

[89] Cruzamento com outros dados, utilização dos dados para objetivos secundários, retenção e destruição dos dados.

10	Quais são as fases do ciclo de vida dos dados[90] - criação, utilização, *transferência [entre sistemas]*, armazenamento, arquivo e destruição - mais preocupantes em matérias de privacidade que justifiquem medidas adicionais de proteção?
11	Concorda que o conhecimento generalizado do objetivo da recolha e tratamento dos dados[91] é o ponto de partida para uma compreensão da necessidade de privacidade dos dados pessoais?
12	*Os dados apresentam diferentes níveis de exigência quanto à sua privacidade, pelo que a sua classificação é importante para a definição de requisitos e níveis de proteção da privacidade.* Uma nomenclatura de classificação dos dados permite adaptar melhor as políticas de privacidade dos dados? Quais os principais desafios, no domínio da classificação dos dados, que é necessário considerar quando os dados são partilhados com outras organizações?
13	*Não faz sentido pensar em políticas de privacidade se estas não tiverem por suporte medidas de proteção dos dados[92]. A privacidade dos dados depende em parte das decisões implementadas ao nível da proteção dos dados.* Para um ambiente de interoperabilidade e colaboração, desenvolvido sobre sistemas heterogéneos, o que é preponderante para otimizar esta dependência (*da privacidade dos dados em relação à proteção dos dados*)?
14	*É cada vez mais exigido às organizações que estas apresentem um programa de responsabilidade[93] em relação à proteção de dados pessoais. Permite identificar perante que entidades devem ter uma atitude de responsabilidade, assim como o que deve estar na base do desenvolvimento de um programa de responsabilidade.* A elaboração de um programa de responsabilidade, que contemple medidas para pôr em prática as obrigações e princípios da legislação, pode contribuir para a passagem da teoria à prática no domínio da privacidade dos dados? Se sim, quais as partes que devem promover o seu enquadramento e desenvolvimento?
15	*Na segurança informática, é prática corrente a análise regular da sua conformidade face às políticas de segurança desenhadas, como garantia da sua eficácia e melhoria*

[90] Quer sejam, ***dados pessoais*** (qualquer informação relativa a uma pessoa singular identificada ou identificável), ***dados sensíveis*** (são um subconjunto dos dados pessoais, sobre o qual uma das partes acredita dever ser privado, nomeadamente dados que divulguem informações sobre a origem racial ou étnica, religiosa, política, bem como dados pessoais de saúde), ***dados de identificação pessoal*** (subconjunto dos dados pessoais que permitem uma identificação direta da pessoa em causa, ou qualquer outra informação que identifica ou pode ser usada para identificar, contactar, ou localizar a pessoa a quem se refere tal informação), ou ***dados anónimos*** (dados que não podem ser associados a qualquer titular de dados identificado ou identificável).

[91] Implementando desta forma o princípio da *especificação de objetivos* da Diretiva 95/46/CE de proteção de dados, que define que os dados pessoais devem ser recolhidos para finalidades determinadas, legais e legítimas, e não podem ser tratados de formas não compatíveis com estas finalidades.

[92] Enquanto a privacidade é um valor e um direito e está mais focada em dados pessoais identificáveis com especial atenção nos dados sensíveis, a **proteção de dados** engloba todos os tipos de dados, e é a garantia de que os dados não são corrompidos, e são utilizados apenas para fins autorizados e em conformidade com as políticas de privacidade em vigor.

[93] Um **programa de responsabilidade** constitui o meio de demonstração da vontade e da capacidade da organização em ser responsável e responsabilizada pelas práticas de gestão de dados. É essencial à salvaguarda da privacidade de dados, assim como à confiança do titular dos dados na organização, e entre esta e outras organizações. Deve constituir-se como um programa sólido e transparente, que contemple medidas adequadas e eficazes para pôr em prática as obrigações e princípios da legislação em vigor sobre proteção de dados. Constitui a ferramenta operacional necessária para as questões da privacidade.

	continua. Que ferramenta é necessária para que se possa avaliar, de uma forma contínua, se um determinado contexto de utilização dos dados está de acordo com os requisitos legais e políticas de privacidade existentes?
16	Quais os fatores determinantes para a definição do nível de exigência e periodicidade das tarefas de análise da conformidade em relação à privacidade e proteção dos dados?
17	Considera importante a publicação do resultado destes processos de análise de conformidade? Se sim, porquê e qual na sua opinião pode ser o resultado esperado com a publicação destes resultados?
18	*O registo de todas as tarefas e a sua origem local ou remota são uma das garantias da correta utilização destes dados face às políticas e legislação aplicáveis.* Qual o desempenho ou funções esperadas de um sistema de *accountability* para o contexto de partilha de dados entre sistemas e como se espera que estes evoluam no futuro?
19	*No domínio da segurança de infraestruturas tecnológicas é muito comum os seus responsáveis recorrerem a esquemas de certificação reconhecidos publicamente, como forma de melhoria contínua das soluções implementadas e como garantia de qualidade tecnológica para os seus colaboradores.* Que benefícios pode apresentar a certificação de uma organização em matérias de proteção de dados? A certificação das organizações a este nível aumentaria a confiança entre as organizações participantes no ambiente de partilha de dados como a PDS?
20	Podemos afirmar que o sucesso do planeamento de políticas de proteção e privacidade de dados está muito dependente da experiência em projetos de partilha de dados e em interoperabilidade? Pode indicar alguns exemplos de projetos na sua organização?
21	Se nos focarmos no objetivo de desenvolver um ambiente seguro e confiável para a partilha de dados, que experiência é exigível aos responsáveis pelo desenvolvimento dos sistemas de informação?
22	Qual o resultado expectável de uma melhoria do conhecimento da legislação de proteção e privacidade dos dados?
23	Quais os recursos humanos que considera fundamentais ao suporte das questões da privacidade dos dados para o âmbito alargado do contexto de colaboração com outras organizações? Justifica-se uma estrutura organizativa de suporte às questões da privacidade dos dados para o âmbito alargado do contexto de colaboração?
24	Que tipo (s) de eventos pode (m) contribuir para uma melhoria da preparação da globalidade dos profissionais em relação à privacidade dos dados?

Agenda para as entrevistas

Nome Completo	Data	Hora	Local

Anexo IV - Protocolo para o *estudo de caso* – acordo de colaboração, Perfil 3

Privacidade dos dados

em ambientes de interoperabilidade - a área da saúde

Acordo de colaboração

Apresentação

O presente documento tem como intuito apresentar o objetivo do projeto de investigação "*Privacidade dos dados em ambientes de interoperabilidade – a área da saúde*", as condições de participação e a estrutura da entrevista, aos participantes identificados, e que pela sua experiência profissional se enquadram no objetivo do estudo.

O projeto de investigação, na área dos sistemas de informação, apresenta como principal objetivo a identificação e o estudo dos fatores críticos à privacidade dos dados, em contextos de colaboração entre organizações, onde existe partilha de dados entre sistemas de informação heterogéneos - como é o caso da Plataforma de Dados da Saúde (PDS).

Estamos perante uma realidade complexa, subjetiva, para a qual é essencial o seu estudo em contexto real, onde a compreensão do contexto de ação e as experiências individuais são muito relevantes para a identificação dos fatores relacionados com a "atividade humana" que podem condicionar a privacidade dos dados em processos de colaboração inter-organizacional. A opinião, a experiência e o conhecimento dos vários atores num fenómeno com estas características constituem a principal, senão única, fonte primária de informação.

Após a autorização oficial para a realização do estudo, e com a colaboração de um interlocutor em cada uma das unidades de análise, foi possível identificar para cada um dos 4 perfis pré-definidos, o número de profissionais que se pretende integrar no estudo. Dada a sua experiência profissional e a perspetiva de que a sua participação pode ser uma mais-valia para este estudo, foi indicado o seu nome para a fase seguinte, que consiste na recolha de dados.

No sentido de otimizar o contributo individual expectável, nas páginas seguintes são apresentadas as questões a abordar na entrevista, que se pretende seja a mais aberta possível, assim como a agenda das entrevistas. Desta forma, é possível ao participante analisar as questões, refletir sobre as mesmas, e preparar a exposição que melhor transmite a sua experiência nesta temática.

Sendo inviável a cobertura total e de todas as instituições que integram a PDS, foram constituídas unidades de análise, as seguintes organizações:

a. *Projeto-piloto – Unidade Local de Saúde do Norte Alentejano, Portalegre (ULSNA);*
b. Hospital do Espírito Santo E.P.E, Évora (HES);
c. USF Saúde Mais, Santa Maria da Feira (USF);
d. Hospital Professor Doutor Fernando Fonseca E.P.E., Amadora (HFF);
e. *Instituto Nacional de Emergência Médica,* Lisboa (INEM);
f. Serviços Partilhados do Ministério da Saúde E.P.E. (SPMS);
g. Grupo de *beta-tester* de Utentes.

A recolha de dados será realizada através do recurso a entrevistas semiestruturadas, com as seguintes características:

a. De participação voluntária*;*
b. Uma duração de 30 a 40 minutos;
c. Será recolhida a opinião da pessoa sobre as questões em estudo, e em nenhuma situação será recolhida a opinião da pessoa sobre a instituição, nem sobre a forma como esta funciona;
d. Todos os dados serão tratados de forma confidencial e apenas no âmbito da investigação em curso, não sendo possível que outras pessoas ou entidades externas utilizem estes dados para outro fim.

Ficha técnica: este é um estudo de investigação realizado no âmbito do programa de doutoramento em gestão, especialidade em sistemas de informação, da Universidade de Évora, da autoria de Secundino Lopes (secundino.lopes@estgp.pt), docente do Instituto Politécnico de Portalegre, sob a orientação do Prof. Rui Quaresma (quaresma@uevora.pt), Professor auxiliar da Universidade de Évora.

Entrevista semiestruturada - *Perfil 3*

Elenco de questões para a entrevista a **profissionais de saúde**

	Questão
1	*Existem nas organizações várias situações (contextos) de privacidade, justificadas e geridas muitas vezes de formas diferenciadas.* Qual a importância de uma cultura de privacidade para que uma organização consiga lidar com as várias situações de privacidade que identificou?
2	A maioria dos profissionais consegue distinguir os vários tipos de privacidade com que é confrontado diariamente? De que forma a compreensão e distinção da privacidade dos dados, face aos outros tipos de privacidade dependem de uma maior cultura de privacidade?
3	Por outro lado, a distinção entre privacidade[94], proteção[95] e segurança[96] dos dados está também dependente de uma cultura de privacidade, ou apenas do conhecimento das questões técnicas associadas?
4	A que níveis se pode manifestar a atitude dos vários profissionais face às mudanças e requisitos organizacionais decorrentes das iniciativas de colaboração entre organizações?
5	Existe a consciência de um aumento de práticas que degradam o direito e expectativas da privacidade profissional face ao crescimento de um "controlo tecnológico invisível"?
6	Qual a influência que este "controlo tecnológico invisível" do trabalho dos profissionais que afeta a sua privacidade profissional, pode ter sobre a sua atitude face à sua participação num ambiente de colaboração?
7	Enquanto profissional de saúde, concorda que a sua própria ação ou omissão[97] pode prejudicar outros profissionais (ética)?
8	Estão as organizações cientes das limitações relacionadas com a recolha, utilização, partilha e retenção de informação no ambiente de colaboração?
9	Quais são as fases do ciclo de vida dos dados[98] - criação, utilização, *transferência [entre sistemas]*, armazenamento, arquivo e destruição - mais preocupantes em matérias de privacidade que justifiquem medidas adicionais de proteção?

[94] **A privacidade**, também conhecida por privacidade dos dados, é um valor e um direito à privacidade na recolha, utilização, armazenamento e partilha de dados pessoais de um indivíduo. A privacidade dos dados deve ser analisada sempre que dados identificáveis relativos a uma ou mais pessoais são recolhidos e armazenados em formato digital ou num outro suporte.

[95] Enquanto a privacidade é um valor e um direito e está mais focada em dados pessoais identificáveis com especial atenção nos dados sensíveis, a **proteção de dados** engloba todos os tipos de dados, e é a garantia de que os dados não são corrompidos, e são utilizados apenas para fins autorizados e em conformidade com as políticas de privacidade em vigor.

[96] A **segurança** dos dados está relacionada com as questões técnicas de segurança das infraestruturas de armazenamento e comunicação. É um elemento crítico de qualquer sistema informático, devendo fornecer as garantias necessárias à proteção e integridade dos dados. Capacidade de um sistema resistir a eventos acidentais ou a acessos maliciosos ou ilícitos que comprometem a disponibilidade, a autenticidade, a integridade, a confidencialidade dos dados.

[97] Neste caso a confidencialidade do médico – proteção do paciente

[98] Quer sejam, ***dados pessoais*** (qualquer informação relativa a uma pessoa singular identificada ou identificável), ***dados sensíveis*** (são um subconjunto dos dados pessoais, sobre o qual uma das partes acredita dever ser privado, nomeadamente dados que divulguem informações sobre a origem racial ou étnica, religiosa, política, bem como dados pessoais de saúde), ***dados de identificação pessoal*** (subconjunto dos dados pessoais que permitem uma identificação direta da pessoa em causa, ou qualquer outra informação que identifica ou pode ser usada para identificar, contactar, ou

10	Concorda que o conhecimento generalizado do objetivo da recolha e tratamento dos dados[99] é o ponto de partida para uma compreensão da necessidade de privacidade dos dados pessoais?
11	Uma análise atempada dos impactos (riscos) sobre a privacidade que podem surgir com o desenvolvimento ou aquisição de uma nova solução tecnológica ou serviço de informação, que utiliza dados pessoais, pode influenciar a confiança dos profissionais utilizadores destas soluções? Se sim, de que forma?
12	Que tipo (s) de eventos pode (m) contribuir para uma melhoria da preparação da globalidade dos profissionais em relação à privacidade dos dados?

Agenda para as entrevistas

Nome Completo	Data	Hora	Local

localizar a pessoa a quem se refere tal informação), ou ***dados anónimos*** (dados que não podem ser associados a qualquer titular de dados identificado ou identificável).

[99] Implementando desta forma o princípio da *especificação de objetivos* da Diretiva 95/46/CE de proteção de dados, que define que os dados pessoais devem ser recolhidos para finalidades determinadas, legais e legítimas, e não podem ser tratados de formas não compatíveis com estas finalidades.

Anexo V - Protocolo para o *estudo de caso* – acordo de colaboração, Perfil 4

Privacidade dos dados

em ambientes de interoperabilidade - a área da saúde

Acordo de colaboração

Apresentação

O presente documento tem como intuito apresentar o objetivo do projeto de investigação "*Privacidade dos dados em ambientes de interoperabilidade – a área da saúde*", as condições de participação e a estrutura da entrevista, aos participantes identificados, e que pela sua experiência profissional se enquadram no objetivo do estudo.

O projeto de investigação, na área dos sistemas de informação, apresenta como principal objetivo a identificação e o estudo dos fatores críticos à privacidade dos dados, em contextos de colaboração entre organizações, onde existe partilha de dados entre sistemas de informação heterogéneos - como é o caso da Plataforma de Dados da Saúde (PDS).

Estamos perante uma realidade complexa, subjetiva, para a qual é essencial o seu estudo em contexto real, onde a compreensão do contexto de ação e as experiências individuais são muito relevantes para a identificação dos fatores relacionados com a "atividade humana" que podem condicionar a privacidade dos dados em processos de colaboração inter-organizacional. A opinião, a experiência e o conhecimento dos vários atores num fenómeno com estas características constituem a principal, senão única, fonte primária de informação.

Após a autorização oficial para a realização do estudo, e com a colaboração de um interlocutor em cada uma das unidades de análise, foi possível identificar para cada um dos 4 perfis pré-definidos, o número de profissionais que se pretende integrar no estudo. Dada a sua experiência profissional e a perspetiva de que a sua participação pode ser uma mais-valia para este estudo, foi indicado o seu nome para a fase seguinte, que consiste na recolha de dados.

No sentido de otimizar o contributo individual expectável, nas páginas seguintes são apresentadas as questões a abordar na entrevista, que se pretende seja a mais aberta possível, assim como a agenda das entrevistas. Desta forma, é possível ao participante analisar as questões, refletir sobre as mesmas, e preparar a exposição que melhor transmite a sua experiência nesta temática.

Sendo inviável a cobertura total e de todas as instituições que integram a PDS, foram constituídas unidades de análise, as seguintes organizações:

h. *Projeto-piloto – Unidade Local de Saúde do Norte Alentejano, Portalegre (ULSNA);*
i. Hospital do Espírito Santo E.P.E, Évora (HES);
j. USF Saúde Mais, Santa Maria da Feira (USF);
k. Hospital Professor Doutor Fernando Fonseca E.P.E., Amadora (HFF);
l. *Instituto Nacional de Emergência Médica,* Lisboa (INEM);
m. Serviços Partilhados do Ministério da Saúde E.P.E. (SPMS);
n. Grupo de *beta-tester* de Utentes.

A recolha de dados será realizada através do recurso a entrevistas semiestruturadas, com as seguintes características:

e. De participação voluntária*;*
f. Uma duração de 30 a 40 minutos;
g. Será recolhida a opinião da pessoa sobre as questões em estudo, e em nenhuma situação será recolhida a opinião da pessoa sobre a instituição, nem sobre a forma como esta funciona;
h. Todos os dados serão tratados de forma confidencial e apenas no âmbito da investigação em curso, não sendo possível que outras pessoas ou entidades externas utilizem estes dados para outro fim.

Ficha técnica: este é um estudo de investigação realizado no âmbito do programa de doutoramento em gestão, especialidade em sistemas de informação, da Universidade de Évora, da autoria de Secundino Lopes (secundino.lopes@estgp.pt), docente do Instituto Politécnico de Portalegre, sob a orientação do Prof. Rui Quaresma (quaresma@uevora.pt), Professor auxiliar da Universidade de Évora.

Entrevista semiestruturada - *Perfil 4*

Elenco de questões para a entrevista a **gestores e administradores**

	Questão
1	*Muitas organizações utilizam o termo "cultura", quando de alguma forma querem evidenciar valores importantes para o seu sucesso. Por exemplo: "cultura da qualidade", "cultura de segurança", "cultura empreendedora".* De que forma o sucesso da partilha de dados[100] pode ser influenciado pelo desenvolvimento de uma cultura de privacidade transversal a todas as organizações?
2	*Existem nas organizações várias situações (contextos) de privacidade, justificadas e geridas muitas vezes de formas diferenciadas.* Qual a importância de uma cultura de privacidade para que uma organização consiga lidar com as várias situações de privacidade[101] que identificou?
3	*É cada vez mais exigido às organizações que estas apresentem um programa de responsabilidade[102] em relação à proteção de dados pessoais. Permite identificar perante que entidades devem ter uma atitude de responsabilidade, assim como o que deve estar na base do desenvolvimento de um programa de responsabilidade.* A elaboração de um programa de responsabilidade, que contemple medidas para pôr em prática as obrigações e princípios da legislação, pode contribuir para a passagem da teoria à prática no domínio da privacidade dos dados[103]? Se sim, quais as partes que devem promover o seu enquadramento e desenvolvimento?
4	*Na segurança informática, é prática corrente a análise regular da sua conformidade face às políticas de segurança desenhadas, como garantia da sua eficácia e melhoria continua.* Que ferramenta é necessária para que se possa avaliar, de uma forma contínua, se um determinado contexto de utilização dos dados está de acordo com os requisitos legais e políticas de privacidade existentes?
5	*No domínio da segurança de infraestruturas tecnológicas é muito comum os seus responsáveis recorrerem a esquemas de certificação reconhecidos publicamente, como*

[100] Quer sejam, ***dados pessoais*** (qualquer informação relativa a uma pessoa singular identificada ou identificável), ***dados sensíveis*** (são um subconjunto dos dados pessoais, sobre o qual uma das partes acredita dever ser privado, nomeadamente dados que divulguem informações sobre a origem racial ou étnica, religiosa, política, bem como dados pessoais de saúde), ***dados de identificação pessoal*** (subconjunto dos dados pessoais que permitem uma identificação direta da pessoa em causa, ou qualquer outra informação que identifica ou pode ser usada para identificar, contactar, ou localizar a pessoa a quem se refere tal informação), ou ***dados anónimos*** (dados que não podem ser associados a qualquer titular de dados identificado ou identificável).

[101] São os exemplos da privacidade da pessoa, por vezes referida como privacidade corporal, privacidade do comportamento e da esfera pessoal, privacidade das comunicações pessoais e privacidade dos dados pessoais.

[102] Um **programa de responsabilidade** constitui o meio de demonstração da vontade e da capacidade da organização em ser responsável e responsabilizada pelas práticas de gestão de dados. É essencial à salvaguarda da privacidade de dados, assim como à confiança do titular dos dados na organização, e entre esta e outras organizações. Deve constituir-se como um programa sólido e transparente, que contemple medidas adequadas e eficazes para pôr em prática as obrigações e princípios da legislação em vigor sobre proteção de dados. Constitui a ferramenta operacional necessária para as questões da privacidade.

[103] **A privacidade**, também conhecida por privacidade dos dados, é um valor e um direito à privacidade na recolha, utilização, armazenamento e partilha de dados pessoais de um indivíduo. A privacidade dos dados deve ser analisada sempre que dados identificáveis relativos a uma ou mais pessoais são recolhidos e armazenados em formato digital ou num outro suporte.

	forma de melhoria contínua das soluções implementadas e como garantia de qualidade tecnológica para os seus colaboradores. Que benefícios pode apresentar a certificação de uma organização em matérias de proteção de dados? A certificação das organizações a este nível aumentaria a confiança entre as organizações participantes no ambiente de partilha de dados como a PDS?
6	*A falta de um vocabulário partilhado para discutir as questões da privacidade faz com que tanto responsáveis de sistemas como gestores executivos, muitas vezes, concordem com especificações para os sistemas que não conseguem lidar com a privacidade de forma satisfatória.* Quais as maiores dificuldades que poderiam ser resolvidas com a existência de uma linguagem de privacidade, uma taxonomia[104], neste caso focada na privacidade dos dados?
7	Numa linguagem de gestão, qual o fator determinante, para que os gestores executivos assumam a necessidade de uma estratégia para a privacidade, não isolada, e integrada com a estratégia desenvolvida para o sistema de informação?
8	Qual a importância do reconhecimento por parte dos gestores executivos da responsabilidade da sua organização ou a sua própria responsabilidade em relação à proteção da privacidade dos dados e das pessoas?
9	De que forma ou qual será a ferramenta indicada para que todas as decisões relativas à privacidade dos dados possam ser integradas, proporcionando uma proteção mais eficiente?
10	Qual a influência que o risco, o seu conhecimento, e a previsão do seu impacto, podem ter sobre a necessidade de as organizações desenvolverem uma visão estratégica para a privacidade?
11	Considera que existe uma influência considerável entre a existência de uma estratégia de privacidade e uma cultura organizacional em privacidade? Qual a dependência entre estes dois conceitos (o que é que depende do quê?)
12	Sendo que o âmbito de uma estratégia organizativa para a privacidade deve refletir a natureza e missão da organização, qual a colaboração possível a este nível entre as organizações participantes no ambiente de colaboração?
13	*Existem vários fatores com influência sobre a colaboração e a interoperabilidade organizacional entre organizações, nomeadamente questões de cultura, estrutura e práticas organizacionais.* De que forma o desenvolvimento de iniciativas de interoperabilidade organizacional, por exemplo nos domínios da segurança e proteção de dados, depende da confiança estabelecida entre as organizações?
14	O facto de uma organização operar com múltiplos sistemas, concebidos de forma isolada e com práticas de privacidade e proteção de dados diferentes, pode influenciar ou condicionar a confiança dos seus utilizadores nestes sistemas?
15	Uma análise atempada dos impactos (riscos) sobre a privacidade que podem surgir com o desenvolvimento ou aquisição de uma nova solução tecnológica ou serviço de informação, que utiliza dados pessoais, pode influenciar a confiança dos profissionais

[104] Uma taxonomia de privacidade dos dados constitui "*um conjunto documentado e ordenado de tipos, classificações, categorizações e/ou princípios que são frequentemente alcançados por meio de mecanismos, incluindo a nomeação, definição e/ou o agrupamento de atributos, e que por sua vez ajudaram a descrever, diferenciar, identificar, organizar e fornecer relações contextuais entre entidades, tipos e itens de privacidades dos dados*".

	utilizadores destas soluções? Se sim, de que forma?
16	A que níveis se pode manifestar a atitude dos vários profissionais face às mudanças e requisitos organizacionais decorrentes das iniciativas de colaboração entre organizações?
17	Existe a consciência de um aumento de práticas que degradam o direito e expectativas da privacidade profissional face ao crescimento de um "controlo tecnológico invisível"?
18	Qual a influência que este "controlo tecnológico invisível" do trabalho dos profissionais, que afeta a sua privacidade profissional, pode ter sobre a sua atitude face à sua participação num ambiente de colaboração?
19	Quais os recursos humanos que considera fundamentais ao suporte das questões da privacidade dos dados para o âmbito alargado do contexto de colaboração com outras organizações? Justifica-se uma estrutura organizativa de suporte às questões da privacidade dos dados para o âmbito alargado do contexto de colaboração?
20	Na sua opinião, e tendo em conta a complexidade da questão da privacidade dos dados no contexto de colaboração entre várias organizações, qual a abordagem que melhor se adapta a esta complexidade: uma abordagem conjunta e integrada, ou uma abordagem individual e isolada? O que é necessário para operacionalizar uma abordagem conjunta deste assunto?
21	*As organizações são diferentes em termos de disponibilidade e prontidão para a colaboração e interoperabilidade*[105]*, nomeadamente devido à sua heterogeneidade tecnológica e organizativa.* Para garantir a privacidade e proteção dos dados, o que é necessário promover nas organizações para se atingir uma maior capacidade de colaboração?
22	Que tipo (s) de eventos pode (m) contribuir para uma melhoria da preparação da globalidade dos profissionais em relação à privacidade dos dados?

Agenda para as entrevistas

Nome Completo	Data	Hora	Local

[105] **Interoperabilidade** é a capacidade de dois ou mais sistemas trocarem e utilizarem informação, independente das aplicações informáticas utilizadas.

Anexo VI - Convite à participação das instituições no *estudo de caso*

Assunto: Solicitação de colaboração com projeto de investigação no âmbito do programa de doutoramento em gestão - sistemas de informação da Universidade de Évora

No âmbito do programa de doutoramento em gestão - sistemas de informação da Universidade de Évora, e em colaboração com os Serviços Partilhados do Ministério da Saúde (SPMS) - responsáveis pelo desenvolvimento da Plataforma de Dados da Saúde (PDS) – está em curso o projeto de investigação intitulado "Privacidade dos dados em ambientes de interoperabilidade – a área da saúde".

Este estudo tem por objetivo a identificação e o estudo dos fatores críticos para a privacidade dos dados em contextos de colaboração entre organizações, onde existe partilha de dados e serviços, como é o caso da PDS. Dada a natureza e o objetivo deste estudo, o seu sucesso e os contributos que dele poderão resultar dependem, fortemente, da qualidade da informação e do conhecimento detidos pelos vários profissionais intervenientes na PDS.

Assim, pretende-se que o HFF constitua uma das sete unidades de análise nacionais selecionadas para a fase de recolha de dados, que se pretende iniciar com a maior brevidade possível. Face ao exposto, solicita-se a autorização necessária para a recolha de dados de acordo com o "protocolo de estudo de caso" que se anexa, assim como a indicação de um interlocutor local de apoio à operacionalização do estudo.

Fico a aguardar uma resposta positiva e apresento os melhores cumprimentos,
Secundino Domingos Marques Lopes

Anexo VII - Participantes por unidade de estudo

Unidade Local de Saúde do Norte Alentejano, Portalegre (ULSNA)	
Relação dos participantes no estudo.	
Perfil	**Nome**
1	Eng.º Bruno Silva
2	Ricardo Cortes
2	Manuel Sardinha
3	Dr. José Romeira Martires
3	Dr. Eduardo Soeiro
4	Dr. Joaquim Araújo

- Interlocutor local para o estudo: Eng.º Bruno Silva
- As entrevistas tiveram lugar nas instalações da ULSNA nos dias 11 e 12 de dezembro de 2013

USF Saúde Mais, Santa Maria da Feira (USF)	
Relação dos participantes no estudo.	
Perfil	**Nome**
1	António Manuel Silva, ARS Norte
2	Sónia Camelo, ARS Norte
3	Patrícia Maria Duarte Soares
3	Márcio Rafael Oliveira Silva
4	Maria Dulce Sousa Campos;
3	Sílvia Ferreira Dias

- Interlocutor local para o estudo: *Enf. Sílvia Dias*
- As entrevistas tiveram lugar nas instalações da USF nos dias 23 e 24 de janeiro de 2014

Instituto Nacional de Emergência Médica, Lisboa (INEM)	
Relação dos participantes no estudo.	
Perfil	**Nome**
1	Dr. José ferreira
2	Filipe Botas
2	José Sousa
3	João Reis (TAE)
3	João Lourenço (Enfermeiro)
3	Francisco Marcão (Médico)
4	Dr. Júlio Pedro

- Interlocutor local para o estudo: *Dr. José Ferreira*

- As entrevistas tiveram lugar nas instalações do INEM nos dias 30 e 31 de janeiro de 2014

Hospital Professor Doutor Fernando Fonseca (HFF)	
Relação dos participantes no estudo.	
Perfil	**Nome**
1	Eng.º Rui Gomes
2	Tomé Vardasca
2	Eng.º Carlos Sousa
3	Dr.ª. Lucília (Diretora Clínica)
4	Dr. Luís Gouveia (Vogal CA)

- Interlocutor local para o estudo: *Eng.º Rui Gomes*
- As entrevistas tiveram lugar nas instalações do HFF nos dias 13 e 14 de fevereiro de 2014

Serviços Partilhados do Ministério da Saúde (SPMS)	
Relação dos participantes no estudo.	
Perfil	**Nome**
1	Paulo Jorge Sá
2	Maria João Campos
2	Cristina Carvalho
4	Prof. Henrique Martins

- Interlocutor local para o estudo: *Paulo Jorge Sá*
- As entrevistas tiveram lugar nas instalações da SPMS no Porto e em Lisboa entre os dias 18 de abril e 23 de maio de 2014

Hospital do Espírito Santo E.P.E, Évora (HES)	
Relação dos participantes no estudo.	
Perfil	**Nome**
1	Sónia Piedade Martins
2	Ricardo Cabecinha
2	Fernando Silva
3	Conceição Barata
4	Manuel Carvalho

- Interlocutor local para o estudo: Sónia Piedade Martins
- As entrevistas tiveram lugar nas instalações do HES entre os dias 16 de julho e 19 de novembro de 2014

Anexo VIII - **Convite à participação dos profissionais no *estudo de caso***

Assunto: Participação no estudo de investigação sobre a Privacidade dos dados

Ex. M (ª). Senhor (a)

No âmbito do programa de doutoramento em gestão - sistemas de informação da Universidade de Évora, e em colaboração com os Serviços Partilhados do Ministério da Saúde (SPMS) - responsáveis pelo desenvolvimento da Plataforma de Dados da Saúde (PDS) – estou a desenvolver o projeto de investigação intitulado "Privacidade dos dados em ambientes de interoperabilidade – a área da saúde".

Neste sentido, e com a colaboração do Eng.º Rui Gomes, foi possível identificar para o HFF, os participantes que dada a sua experiência e perfil profissional, o seu contributo pode ser uma mais-valia para o estudo.

Assim, envio em anexo um documento que (1) descreve de forma sucinta o estudo, (2) contem o elenco de questões a desenvolver na entrevista, e (3) apresenta uma agenda para as entrevistas aos participantes. É importante a leitura deste documento antes da entrevista de trabalho.

Solicito-lhe assim, que me confirme a sua participação, assim como a sua disponibilidade de acordo com as indicações na agenda das entrevistas.

Fico a aguardar uma resposta positiva e apresento os melhores cumprimentos,

Nota: alguma questão sobre o estudo e sobre a sua operacionalização podem contactar-me pelo 96xxxxxxx.

Anexo IX - Estrutura do inquérito, Perfil 5

Inquérito para a recolha de dados - *Perfil 5*
Elenco de questões para o inquérito ao Titular dos dados/UTENTE

Texto inicial de apresentação

Este inquérito, de resposta anónima e livre, faz parte do projeto de investigação intitulado "Privacidade dos dados em ambientes de interoperabilidade – a área da saúde", desenvolvido no âmbito do programa de doutoramento em Gestão da Universidade de Évora, e com a colaboração dos Serviços Partilhados do Ministério da Saúde (SPMS), organização responsável pelo desenvolvimento da Plataforma de Dados da Saúde (PDS). Pretende-se compreender a perceção dos Utentes sobre os conceitos da privacidade dos dados, assim como a sua opinião sobre a informação e as ferramentas que lhe são disponibilizadas para gestão e monitorização da privacidade dos seus dados pessoais.

Questões

1 Qual a situação que mais o(a) preocupa quanto à sua privacidade (escolha apenas uma opção)?
   a. A violação da privacidade das suas comunicações pessoais.
   b. A perda de privacidade em espaços públicos (face às tecnologias de vigilância e localização).
   c. A violação da privacidade dos seus dados pessoais.

2 Qual a situação de utilização e partilha dos seus dados, que lhe suscita mais preocupações quanto à sua proteção e privacidade (escolha apenas uma opção)?
   a. No apoio aos tratamentos de saúde, em que os seus dados de saúde podem ser partilhados entre profissionais de saúde.
   b. No funcionamento da organização hospitalar, em que os seus dados podem ser utilizados e partilhados internamente, para melhorar o apoio médico, melhorar o atendimento e se necessário contactá-lo pessoalmente.
   c. No contacto com outras instituições do setor da saúde, em que os seus dados podem ser partilhados para faturação dos serviços de saúde a outras entidades.

3 Sempre que os seus dados forem suscetíveis de serem legitimamente partilhados com outros destinatários, que informação considera importante que lhe seja enviada. Atribua um grau de importância entre 1 (nada importante) e 5 (muito importante).

	1	2	3	4	5
a. Os tipos de dados partilhados					
b. A identificação do utilizador/organização que vai receber os dados					
c. O propósito da partilha dos dados					
d. As medidas adotadas para a proteção dos dados					

4 Com base na informação que lhe é disponibilizada na PDS, consegue distinguir entre situações (a) em que existe uma base legal que permite que os seus dados sejam partilhados e (b) situações em que os seus dados nunca serão partilhados?
   a. Sim
   b. Não

5 Determinadas situações de partilha de dados exigem um consentimento por parte do seu titular, permitindo-lhe restringir o acesso aos seus dados a determinadas pessoas ou serviços. Em sua opinião (escolha apenas uma opção):

c. As situações que exigem consentimento não são claras nem compreensíveis.
d. As situações que exigem consentimento são claras e compreensíveis.
e. É um direito bem compreendido, mas de difícil gestão e controlo.

6 A confiança do titular dos dados (utente) na organização a quem facultou os seus dados pessoais é determinante para a gestão da privacidade.
Atribua um grau de importância (1-5) aos seguintes conjuntos de informação, que sendo públicos, podem influenciar a confiança do titular dos dados na organização:

	1	2	3	4	5
a. A publicação das políticas de privacidade e proteção de dados.					
b. A publicação dos direitos que o titular dos dados (utente) tem sobre os seus dados pessoais.					
c. A demonstração da conformidade da globalidade da organização para com os requisitos legais no domínio da proteção e privacidade dos dados.					
d. A publicação dos contextos e finalidades de utilização dos dados.					

7 A legislação sobre proteção de dados exige às organizações que utilizam os seus dados pessoais, determinadas obrigações (responsabilidades). Qual a sua opinião sobre estas obrigações (escolha apenas uma opção):

a. Não são do conhecimento generalizado dos utentes.
b. Existem mas não são claras para a maioria dos utentes.
c. Existem e permitem compreender as medidas de proteção implementadas.
d. Existem, são compreensíveis, mas a organização em causa não apresenta provas quanto ao seu cumprimento.

8 Como classifica a informação que lhe é disponibilizada sobre os seus direitos em termos de privacidade e proteção dos seus dados (escolha apenas uma opção):

a. Não foi possível encontrar qualquer informação.
b. A informação existente é mínima, e não permite compreender quais os direitos que assistem o titular dos dados.
c. A informação existente é suficiente, é de fácil acesso e compreensão, formulada numa linguagem clara e simples, para um conhecimento detalhado dos direitos do titular dos dados.

9 Confrontado com uma situação que lhe suscite preocupações em relação à utilização dos seus dados pessoais, consegue com base na informação que lhe é disponibilizada:

a. Identificar com facilidade os meios disponíveis para apresentar as dúvidas existentes? (sim/não)
b. Identificar a pessoa responsável pela utilização dos seus dados dentro da organização? (sim/não)
c. Contactar com facilidade o responsável na organização pela utilização dos seus dados? (sim/não)

10 Que funcionalidades são fundamentais à sua participação na gestão e controlo da privacidade dos seus dados pessoais (pode escolher várias opções)?

a. O consentimento – no sentido de limitar a utilização dos seus dados.
b. O controlo e a monitorização da utilização dos seus dados – indicação clara sobre quais os utilizadores e porque utilizaram os seus dados.
c. A possibilidade de atualização e correção dos seus dados.
d. A possibilidade de portabilidade dos seus dados num formato digital comum.

11 Considera que a sua atitude/ação pode ter uma influência significativa na gestão da privacidade dos seus dados?

a. Sim
b. Não

12 Considera a PDS como uma oportunidade para melhor compreender as questões da privacidade dos dados pessoais no domínio dos sistemas de gestão de saúde?
   a. Sim
   b. Não

Ficha técnica: Este inquérito, realizado no âmbito do projeto de investigação intitulado "Privacidade dos dados em ambientes de interoperabilidade - a área da saúde", é da autoria de Secundino Lopes (secundino.lopes@estgp.pt), docente do Instituto Politécnico de Portalegre, sob a orientação do Prof. Rui Quaresma (quaresma@uevora.pt), Professor auxiliar da Universidade de Évora.

Anexo X - Convite à participação no inquérito, Perfil 5

Gmail by Google

Secundino Lopes <secundino.lopes@gmail.com>

Participação no questionário académico - "Privacidade dos dados "

nao_responder@spms.min-saude.pt <nao_responder@spms.min-saude.pt> Fri, Oct 17, 2014 at 2:50 PM
To: secundino.lopes@gmail.com

Exmos. Srs.

No âmbito do programa de doutoramento em Gestão da Universidade de Évora, o Dr. Secundino Lopes, encontra-se a desenvolver um projeto de investigação intitulado "Privacidade dos dados em ambientes de interoperabilidade – a área da saúde", em colaboração com os Serviços Partilhados do Ministério da Saúde, que é a organização responsável pelo desenvolvimento da Plataforma de Dados da Saúde (PDS).

Este projeto visa obter informação fidedigna da percepção que os utentes têm sobre os conceitos da privacidade dos dados, bem como recolher opiniões sobre a informação e as ferramentas que lhe são disponibilizadas para a gestão e monitorização da privacidade dos seus dados pessoais no âmbito do Portal do Utente - Plataforma de Dados da Saúde.

Pelo acima exposto e considerando que é fundamental para a SPMS a realização de um questionário que permita avaliar a opinião dos utentes em relação ao Portal do Utente - PDS, solicito a vossa colaboração para preenchimento do questionário, que se encontra disponível no seguinte link:
https://docs.google.com/forms/d/1ymjgh-xYXq-EmCk5vLmSLLgAIOhn207wLaDLjY65-7E/viewform

Este projeto reveste-se de grande importância para o SNS e para o sucesso do projeto de investigação, pelo que solicito, mais uma vez a vossa colaboração.

Antecipadamente gratos pela participação, subscrevo-me com consideração.

Com os melhores cumprimentos,
Ana Maurício d´Avó
Diretora de Comunicação e Relações Públicas

Referências

Al-Fedaghi, S. (2012). Engineering privacy revisited. *Journal of Computer Science*, *8*(1), 107–120. doi:10.3844/jcssp.2012.107.120

Allen, A. L. (2007). Face to Face with "It": And Other Neglected Contexts of Health Privacy. In *PROCEEDINGS OF THE AMERICAN PHILOSOPHICAL SOCIETY* (Vol. 151, pp. 300–308).

AMA. (2008). *Plano de actividades 2008*. Retrieved from http://www.ama.pt/

Amicelle, A. (2012). D1.1. Report on Theoretical Frameworks and Previous Empirical Research. In *The Privacy & Security Research Paper. Series Summary of PACT deliverables* (pp. 1–19). Centre for Science, Society & Citizenship.

Antón, A. I., & Earp, J. B. (2003). A requirements taxonomy for reducing Web site privacy vulnerabilities. *Requirements Eng*. doi:10.1007/s00766-003-0183-z

APDSI. (2013). *Interoperabilidade na Saúde*. Retrieved from http://www.apdsi.pt/

APDSI. (2014). *O Tratamento de Dados Pessoais em Portugal. Breve Guia Prático*. Retrieved from http://www.apdsi.pt

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279. doi:10.1504/IJIEM.2010.035624

Aquilina, K. (2010). Public security versus privacy in technology law: A balancing act? *Computer Law & Security Review*, *26*(2), 130–143. doi:10.1016/j.clsr.2010.01.002

AR. Lei n.º 67/98 de 26 de Outubro. Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.o 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995) (1998).

Art. 29 WP. (2007a). *Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (RSE)*. Retrieved from http://ec.europa.eu/justice/policies/privacy/index_en.htm

Art. 29 WP. (2007b). *Parecer 4/2007 sobre o conceito de dados pessoais, 01248/07/PT WP 136*. Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Art. 29 WP. (2009). *The Future of Privacy. Joint contribution to the Consultation of*

the European Commission on the legal framework for the fundamental right to protection of personal data. Adopted on 01 December 2009. Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Art. 29 WP. (2010a). *Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169*. Retrieved from http://ec.europa.eu/justice/policies/privacy/index_en.htm

Art. 29 WP. (2010b). *Opinion 3/2010 on the principle of accountability, 00062/10/PT WP 173*. Retrieved from http://ec.europa.eu/justice/policies/privacy/index_en.htm

ATHENA. (2010). ATHENA Interoperability Framework (AIF). *The ATHENA Consortium*. Retrieved from http://athena.modelbased.net/index.html

Athreya, J. R. (2010). *Data Masking Best Practices*. Retrieved from http://www.oracle.com/us/products/database/data-masking-best-practices-161213.pdf

Baird, S. A. (2007). Government Role in Developing an Interoperability Ecosystem. *ICEGOV2007, December 10-13, 2007, Macao*, 65–68.

Bamberger, K. A., & Mulligan, D. K. (2011). Catalyzing Privacy: New Governance , Information Practices , and the Business Organization. *LAW &POLICY*, *33*.

Barker, K., Askari, M., Banerjee, M., Ghazinour, K., Mackas, B., Majedi, M., … Williams, A. (2009). A Data Privacy Taxonomy. In *BNCOD 26 Proceedings of the 26th British National Conference on Databases: Dataspace: The Final Frontier* (pp. 42–54). ACM Digital Library. doi:10.1007/978-3-642-02843-4_7

Benbasat, I., David, & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. doi:10.2307/248684

Berg, M., Langenberg, C., Berg, I. V. D., & Kwakkernaat, J. (1998). Considerations for sociotechnical design: Experiences with an electronic patient record in a clinical context. *International Journal of Medical Informatics*, *52*(1-3), 243–251. doi:10.1016/S1386-5056(98)00143-9

Berger, D. W. (2014). *What Healthcare CEO's Need to Know about IT Security Risk*. Retrieved from http://www.redspin.com/healthcare

Bertino, E., Bhargav-Spantzel, a., & Squicciarini, a. C. (2006). Policy Languages for

Digital Identity Management in Federation Systems. *Seventh IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'06)*, 54–66. doi:10.1109/POLICY.2006.22

Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2005). Establishing and protecting digital identity in federation systems. *Proceedings of the 2005 Workshop on Digital Identity Management - DIM '05*, 11. doi:10.1145/1102486.1102489

Biesdorf, S., & Niedermann, F. (2014). *Healthcare's digital future. health care systems and services*. Retrieved from http://www.mckinsey.com/insights/health_systems_and_services/healthcares_digital_future

Bolan, C., & Mende, D. (2004). Computer Security Research: Approaches and Assumptions Researchers. In *2nd Australian Information Security Management Conference* (pp. 115–124). Retrieved from http://igneous.scis.ecu.edu.au/proceedings/2004/aism/InfoSec Conference Complete Proceedings.pdf

Breaux, T. D., & Antón, A. I. (2008). Analyzing Regulatory Rules for Privacy and Security Requirements. *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING*, *34*(1), 5–20. doi:10.1109/TSE.2007.70746.

Brownsword, L. L., Carney, D. J., Fisher, D., Lewis, G., Meyers, C., Morris, E. J., … Wrage, L. (2004). *Current Perspectives on Interoperability*. Carnegie Mellon University - Software Engineering Institute Pittsburgh, PA 15213-3890.

C4ISR. (1998). *Levels of Information Systems Interoperability (LISI)*. AWG Architectures Working Group; Department of Defense (DoD); United States of America.

Caldeira, M. M., & Romão, M. J. B. (2002). Estratégias de investigação em sistemas de informação organizacionais - a utilização de métodos qualitativos. *Portuguese Journal of Management Studies*, *0*(1), 77–97. Retrieved from http://ideas.repec.org/a/pjm/journl/vviiy2002i1p77-97.html

CALLIOPE. (2009). *EHEALTH INTEROPERABILITY: STATE OF PLAY AND FUTURE PERSPECTIVES. AN ASSESSMENT OF EUROPEAN COUNTRIES' RESPONSES TO QUESTIONNAIRE ON RECOMMENDATION*

(COM(2008)594). Retrieved from http://ec.europa.eu/information_society/activities/health/policy/interoperability

CALLIOPE. (2010). *Developing an European eHealth Interoperability Roadmap - intermediate report – Specification of the Roadmap & Validation by the High Level Governance Group (Secretary of State)*. Retrieved from http://ec.europa.eu/information_society/activities/health/policy/interoperability

Campos, D. (2012). Sistemas de Gestão da Segurança da Informação nas Organizações de Saúde. *Tecno Hospital nº53. Revista de Engenharia E Gestão Da Saúde*, 12–14.

Canfora, G., Costante, E., Pennino, I., & Visaggio, C. A. (2008). A three-layered model to implement data privacy policies. *Computer Standards & Interfaces*, *30*(6), 398–409. doi:10.1016/j.csi.2008.03.008

Cavaye, A. L. M. (1996). Case study research: a multifaceted research approach for IS. *Lnformation Systems Journal*, (6), 227–242.

Cavoukian, A. (2003). *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age*. *Technology*. Retrieved from http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=470

Cavoukian, A. (2009). *PRIVACY BY DESIGN … TAKE THE CHALLENGE*. Information and Privacy Commissioner of Ontario, Canada. Retrieved from http://privacybydesign.ca/publications/pbd-the-book/

Cavoukian, A. (2011). *Privacy by Design: From Policy to Practice*. Retrieved from http://www.ipc.on.ca/

Cavoukian, A. (2012). *Privacy by Design and the Emerging Personal Data Ecosystem*. Retrieved from http://privacybydesign.ca/publications/

CE. (1995). DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Jornal Oficial Das Comunidades Europeias Nº L 281/31*.

CE. (2002). Directiva 2002/58/CE DO PARLAMENTO EUROPEU E DO

CONSELHO de 12 de Julho de 2002 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). *Jornal Oficial Das Comunidades Europeias*, 37–47.

Cecez-kecmanovic, D. (2001). Doing Critical IS Research: The Question of Methodology. In *Qualitative Research in IS: issues and trends* (pp. 142–163). Idea Group Publishing, Hershey. Retrieved from http://wwwdocs.fce.unsw.edu.au/sistm/staff/2001Cecez-KecmanovicchapteronCISresinTrauth_ed_corrected.pdf

Cechich, A., Gibbons, J., & Kesan, J. (2008). Interoperability Frameworks for Electronic Governance. In *ICEGOV2008* (pp. 5–6). Retrieved from http://www.icegov2008.icegov.org/

Chen, D. (2008). *Framework for Enterprise Interoperability*. Retrieved from http://chen33.free.fr/M2/Elearning/CIGI2009.Chen.final.pdf

Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry*, *59*(7), 647–659. doi:10.1016/j.compind.2007.12.016

Clark, T., & Jones, R. (1999). *Organisational Interoperability Maturity Model for C2*. Retrieved from http://www.sei.cmu.edu/library/assets/orginteroper.pdf

Clark, T., & Moon, T. (2001). Interoperability for Joint and Coalition Operations. *Australian Defence Force Journal*, (151), 23–36.

Clarke, R. (2000). Appropriate Research Methods for Electronic Commerce. *Department of Computer Science, Australian National University*. Retrieved May 2, 2012, from http://www.rogerclarke.com/EC/ResMeth.html

Clarke, R. (2004). *Identity Management*. Xamax Consultancy Pty Ltd. Retrieved from http://www.xamax.com.au/

Clarke, R. (2006). What's "Privacy"? Retrieved September 15, 2013, from http://www.rogerclarke.com/DV/Privacy.html

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law & Security Review*, *25*(2), 123–135. doi:10.1016/j.clsr.2009.02.002

Cleff, B. E. (2007). Privacy Issues in Mobile Advertising. *International Review of Law, Computers & Technology*, *21*(3), 225–236. doi:10.1080/13600860701701421

CNPD. (2004). *RELATÓRIO DE AUDITORIA AO TRATAMENTO DE INFORMAÇÃO DE SAÚDE NOS HOSPITAIS*. Retrieved from http://www.cnpd.pt/bin/relacoes/comunicados/7-12-04.htm

CNPD. (2012a). *AUTORIZAÇÃO n.º 3742/2012*. Retrieved from http://www.cnpd.pt

CNPD. (2012b). *Parecer 18/2012*. Retrieved from http://www.cnpd.pt

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. doi:10.1016/j.istr.2010.04.004

Conselho da Europa. Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais (1950). Retrieved from http://www.echr.coe.int

Costa, L., & Poullet, Y. (2012). Privacy and the regulation of 2012. *Computer Law & Security Review*, *28*(3), 254–262. doi:10.1016/j.clsr.2012.03.015

Culnan, M. J. (2011). *Accountability as the Basis for Regulating Privacy: Can Information Security Regulations Inform Privacy Policy?*

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. *Information Systems Journal*, *8*(4), 142–163. doi:10.1046/j.1365-2575.1998.00040.x

Dayarathna, R. (2011). Taxonomy for information privacy metrics. *Journal of International Commercial Law and Technology*, *6*(4), 194–206.

DoD JP1-02. (2010). *Department of Defense Dictionary of Military and Associated Terms (As Amended Through 15 August 2012)* (Vol. 2010). Joint Publication 1-02. Retrieved from http://www.dtic.mil/doctrine/dod_dictionary/index.html

Dutch, M. (2010). *A Data Protection Taxonomy*. *International immunology* (Vol. 25). San Francisco, California. Retrieved from http://snia.org/sites/default/files/A_Data_Protection_Taxonomy_V51.pdf

Earp, J. B., Antón, A. I., & Jarvinen, O. P. (2002). A Social , Technical and Legal Framework for Privacy Management and Policies. *Americas Conference on Information Systems (AMCIS)*, 605–612.

EC. (2011). *PIAF, A Privacy Impact Assessment Framework for data protection and privacy rights*. Retrieved from http://www.piafproject.eu

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550. doi:10.5465/AMR.1989.4308385

El Eman, K., & Arbuckle, L. (2014). *Anonymizer health data*. (A. Oram & A. MacDonald, Eds.). O'Reilly Media. Retrieved from http://oreilly.com

ENISA. (2010). *Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments*. Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/library/deliverables/survey-pat

ENISA. (2011). *Privacy, Accountability and Trust – Challenges and Opportunities*. Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/library/deliverables/pat-study

ENISA. (2012). *Study on data collection and storage in the EU*. Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection

EPG. (2008). *Privacy by Design. An Overview of Privacy Enhancing Technologies* (Vol. 44). Old Bank House 59, High Street Odiham. Retrieved from http://www.privacygroup.org

epSOS. (2010). *Smart Open Services for European Patients, Open eHealth initiative for a European large scale pilot of Patient Summary and electronic Prescription, D3.3.3 epSOS, epSOS Interoperability Framework*. Retrieved from http://www.epsos.eu/

Ernst & Young. (2012a). *Global Information Security Survey*. Retrieved from http://www.ey.com/

Ernst & Young. (2012b). *Privacy trends 2012. The case for growing accountability*. Retrieved from http://www.ey.com/

Ernst & Young. (2013). *Privacy trends 2013. The uphill climb continues*. Retrieved from http://www.ey.com/

Eurobarometer. (2011). *SPECIAL EUROBAROMETER 359 Attitudes on Data Protection and Electronic Identity in the European Union Special*

Eurobarometer 359. Retrieved from http://ec.europa.eu/public_opinion/index_en.htm

Fedorowicz, J., Gogan, J. L., & Williams, C. B. (2007). A collaborative network for first responders: Lessons from the CapWIN case. *Government Information Quarterly*, *24*(4), 785–807. doi:10.1016/j.giq.2007.06.001

Fewell, S., & Clark, T. (2003). *Organisational Interoperability: Evaluation and Further Development of the OIM Model*. Retrieved from http://www.researchgate.net/publication/27254919_Organisational_interoperability__evaluation_and_further_development_of_the_OIM_model

Fewell, S., Clark, T., Kingston, G., Richer, W., & Warne, L. (2004). *Evaluation of Organisational Interoperability in a Network Centric Warfare Environment*. *9th International Command and Control Research and Technology Symposium. Coalition Transformation: An Evolution of People, Processes and Technology to Enhance Interoperability. Topic: Coalition Interoperability*.

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, *12*(2), 219–245. doi:10.1177/1077800405284363

Ford, T. C., Colombi, J. M., Graham, S. R., & Jacques, D. R. (2007). A Survey on Interoperability Measurement. In *12th ICCRTS "Adapting C2 to the 21st Century."*

Frissen, V., Millard, J., Huijboom, N., Iversen, J. S., Kool, L., & Kotterink, B. (2007). *The Future of eGovernment. An exploration of ICT-driven models of eGovernment for the EU in 2020*. (D. Osimo, D. Zinnbauer, & A. Bianchi, Eds.). Retrieved from http://www.jrc.ec.europa.eu

Fugini, M., & Mezzanzanica, M. (2003). *Development of a Security Methodology for Cooperative Information Systems: the CooPSIS Project*. Retrieved from http://is2.lse.ac.uk/asp/aspecis/20030054.pdf

Gantz, S. (2010). Privacy and Security Considerations for EHR Incentives and Meaningful Use. *ISACA JOURNAL*, *5*, 1–7. Retrieved from http://www.isaca.org

Gasser, U., & Palfrey, J. (2007). BREAKING DOWN DIGITAL BARRIERS. When and How ICT Interoperability Drives Innovation. *Berkman Center for Internet & Society at Harvard University*, (November). Retrieved from http://cyber.law.harvard.edu/interop

GDPR. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2012). Retrieved from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Gonzalez, R., & Dahanayake, A. (2007). A Concept Map of Information Systems Research Approaches. In *IRMA International Conference* (pp. 845–849).

Gottschalk, P. (2009a). E-Government Interoperability: Frameworks for Aligned Development. In I. Global (Ed.), *E-Government Interoperability* (pp. 23–33). Norwegian School of Management, Norway: IGI Global.

Gottschalk, P. (2009b). Maturity levels for interoperability in digital government. *Government Information Quarterly*, *26*(1), 75–81. doi:10.1016/j.giq.2008.03.003

Gregor, S. (2006). THE NATURE OF THEORY IN INFORMATION SYSTEMS. *MIS Quarterly*, *30*(3), 611–642.

Guarda, P., & Zannone, N. (2009). Towards the development of privacy-aware systems. *Information and Software Technology*, *51*(2), 337–350. doi:10.1016/j.infsof.2008.04.004

Guba, E., & Lincoln, Y. (1994). Competing Paradigms in Qualitative Research. In Sage Publications (Ed.), *Handbook of Qualitative Research* (pp. 105–117). Thousand Island. Retrieved from http://ctl.iupui.edu/common/uploads/library/CTL/IDD443360.pdf

Guédria, W., Naudet, Y., & Chen, D. (2008). Interoperability Maturity Models – Survey and Comparison –. In *OTM 2008 Workshops, LNCS 5333* (pp. 273–282). Springer-Verlag Berlin Heidelberg 2008.

Gupta, M., & Sharman, R. (2008). Dimensions of Identity Federation: A Case Study in Financial Services. *Journal of Information Assurance and Security*, *3*, 244–256.

Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. *International Journal of Medical Informatics*, *80*(2), e26–e31. doi:10.1016/j.ijmedinf.2010.10.001

Hamidovic, H. (2010). An Introduction to the Privacy Impact Assessment Based on

ISO 22307. *ISACA JOURNAL*, *4*(Toolbox for IT Auditors), 1–6. Retrieved from http://www.isaca.org

Hansen, M., Schwartz, A., & Cooper, A. (2008). Privacy and Identity Management. *IEEE Security & Privacy March/April*, 38–45.

Haux, R. (2006). Health information systems - Past, present, future. *International Journal of Medical Informatics*, *75*(3-4 SPEC. ISS.), 268–281. doi:10.1016/j.ijmedinf.2005.08.002

HIQA. (2010). *Guidance on Privacy Impact Assessment in Health and Social Care*. Retrieved from http://www.hiqa.ie/

Hunton & Williams. (2009). *Data Protection Accountability: The Essential Elements A Document for Discussion*. Paris, France. Retrieved from http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

Hunton & Williams. (2010). *Demonstrating and Measuring Accountability. A Discussion Document. Accountability Phase II – The Paris Project*. Paris, France. Retrieved from http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

IBM. (2014). *IBM Security Services 2014, Cyber Security Intelligence Index, Analysis of cyber attack and incident data from IBM's worldwide security operations*. Retrieved from http://www-935.ibm.com/services/us/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic/

ICO. (2008). *Privacy by Design. UK Information Commissioner's Office*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

ICO. (2009). *Privacy Impact Assessment Handbook version 2*. Retrieved from http://www.adls.ac.uk/wp-content/uploads/2011/08/PIA-handbook.pdf

ICO. (2011). *Promoting openness by public bodies and data privacy for individuals - An information rights strategy for the Information Commissioner's Office (ICO)*. Retrieved from http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Corporate/Detailed_specialist_guides/ico_information_r

ights_strategy.ashx

IDABC. (2004). *EUROPEAN INTEROPERABILITY FRAMEWORK FOR PAN-EUROPEAN eGOVERNMENT SERVICES version 1.0*. Retrieved from http://europa.eu.int/idabc

IDABC. (2010). *European Interoperability Framework for European Public Services (EIF)*. Retrieved from http://europa.eu.int/idabc

IEEE. (1990). IEEE Standard Glossary of Software Engineering Terminology. *Office*. doi:10.1109/IEEESTD.1990.101064

IEEE. (2007). *IEEE Recommended Practice for Verification, Validation, and Accreditation of a Federation— An Overlay to the High Level Architecture Federation Development and Execution Process*. (IEEE Computer Society, Ed.). IEEE Computer Society.

Introna, L. D. (1997). Privacy and the computer: why we need privacy in the information society. *Metaphilosophy*, *28*(July), 259–275.

Introna, L. D., & Pouloudi, A. (1999). Privacy in the information age: stakeholders, interest and values. *Journal of Business Ethics JBE*, *22*(1), 27–38. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/11660716

IPC. (2009). *The New Federated Privacy Impact Assessment (F-PIA), Building Privacy and Trust-enabled*. Retrieved from http://www.ipc.on.ca

Iqbal, J. (2007). Learning from a Doctoral Research Project: Structure and Content of a Research Proposal. *Electronic Journal of Business Research Methods*, *5*(1), 11–20. Retrieved from http://www.ejbrm.com/main.html

ISO. (2008). ISO 27799:2008(E) Health informatics — Information security management in health using ISO/IEC 27002. ISO (International Organization for Standardization). Retrieved from http://www.iso.org

ISO 14258. (1999). *Industrial Automation Systems—Concepts and Rules for Enterprise Models. ISO TC184/SC5/WG1*. Retrieved from http://www.mel.nist.gov/sc5wg1/std-dft.htm

ISO/IEC. (2005). ISO/IEC 27002:2005(E) Information technology — Security techniques — Code of practice for information security management. ISO (International Organization for Standardization) and IEC (International

Electrotechnical Commission). Retrieved from http://www.iso.org

ISO/IEC. (2008). ISO/IEC 27005:2008(E) Information technology — Security techniques — Information security risk management. ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Retrieved from http://www.iso.org

ISO/IEC. (2009). ISO/IEC 27000:2009(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Retrieved from http://www.iso.org

Jericho Forum. (2006). *Trust and Co-operation*. Retrieved from http://www.opengroup.org/getinvolved/forums/jericho

Jericho Forum. (2007a). *Information Access Policy Management*. Retrieved from http://www.opengroup.org/getinvolved/forums/jericho

Jericho Forum. (2007b). *Principles for Managing Data Privacy*. Retrieved from http://www.opengroup.org/getinvolved/forums/jericho

Jericho Forum. (2009a). *Information Classification*. Retrieved from http://www.opengroup.org/getinvolved/forums/jericho

Jericho Forum. (2009b). *Trust Management - A Brief Overview*. Retrieved from http://www.opengroup.org/getinvolved/forums/jericho

Jericho Forum. (2009c). *Trust Management: Impact Sensitivity Categorization*. Retrieved from http://www.opengroup.org/getinvolved/forums/jericho

Jericho Forum. (2012). *Data Protection. Problem Statement and Requirements for Future Solutions* (No. W12C). Retrieved from http://www.opengroup.org/getinvolved/forums/jericho

Jhingran, A. D., Mattos, N., & Pirahesh, H. (2002). Information integration: A research agenda. *IBM Systems Journal*, *41*(4), 555–562. doi:10.1147/sj.414.0555

Ji, Z., Chen, J., & Wu, G. (2011). Secure interoperation of identity managements among different circles of trust. *Computer Standards & Interfaces*, *33*(6), 533–540. doi:10.1016/j.csi.2011.02.008

Johnson, J. L. (1989). Privacy and the judgment of others. *The Journal of Value Inquiry*, (23), 157–168. Retrieved from

http://link.springer.com/article/10.1007/BF00137284

Jóri, A. (2007). Data Protection in Europe. Retrieved September 25, 2013, from http://www.dataprotection.eu/

Kahn, S., & Sheshadri, V. (2008). Medical record privacy and security in a digital environment. *IT Professional*, *10*(2), 46–52. doi:10.1109/MITP.2008.34

Kalish, B. M. (2015). ONC Privacy Head Outlines Goals, Priorities for Her Office. *Health Data Management*. Retrieved April 17, 2015, from http://www.healthdatamanagement.com/news/ONC-Privacy-Head-Outlines-Goals-Priorities-for-Her-Office-50279-1.html?utm_campaign=mobile_technology_final-apr 16 2015&utm_medium=email&utm_source=newsletter&ET=healthdatamanagement%3Ae4201425%3A3697864a%3A&st=ema

Kasunic, M., & Anderson, W. (2004). *Measuring Systems Interoperability: Challenges and Opportunities. Software Engineering Measurement and Analysis Initiative.*

Kingston, G., Fewell, S., & Richer, W. (2005). An Organisational Interoperability Agility Model. In *10th ICCRTS.*

Koshutanski, H., Ion, M., & Telesca, L. (2007). Distributed Identity Management Model for Digital Ecosystems. In *International Conference on Emerging Security Information, Systems and Technologies* (pp. 132–138). IEEE Computer Society. doi:10.1109/SECURWARE.2007.15

Lahlou, S., Langheinrich, M., & Röcker, C. (2005). Privacy and trust issues with invisible computers, *48*(3), 59–60. doi:10.1145/1047671.1047705

Liberty Alliance. (2003). Privacy and Security Best Practices. Retrieved from http://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf

Lilien, L., & Bhargava, B. (2006). A Scheme for Privacy-Preserving Data Dissemination. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, *36*(3), 502–506. Retrieved from www.cs.purdue.edu/homes/bb/01632285.pdf

Lips, M. (2008). *IDENTITY MANAGEMENT IN INFORMATION AGE GOVERNMENT EXPLORING CONCEPTS, DEFINITIONS, APPROACHES AND SOLUTIONS*. Retrieved from http://www.egov.vic.gov.au/pdfs/idm-govt-08.pdf

Liu, L., & Gao, J. (2008). An Organization-Oriented Model for Federated Identity Management and Its Application. *The IEEE Internacional Conference on Industrial Informatics (INDIN 2008) DCC, Daejeon, Korea July 13-16, 2008*.

Malhene, N., Trentini, A., Marques, G., & Burlat, P. (2012). Freight consolidation centers for urban logistics solutions: The key role of interoperability. *IEEE International Conference on Digital Ecosystems and Technologies*. doi:10.1109/DEST.2012.6227939

Marsh, S., Brown, I., & Khaki, F. (2008). *Privacy Engineering Whitepaper - A Report from a Special Interest Group of the Cyber Security KTN*.

Massey, A. K., & Antón, A. I. (2008). A Requirements-based Comparison of Privacy Taxonomies. *2008 Requirements Engineering and Law*, 1–5. doi:10.1109/RELAW.2008.1

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis. An Expanded Sourcebook*. (I. SAGE Publications, Ed.) (Second Edi.). SAGE Publications, Inc.

Moen, P., Ruohomaa, S., Viljanen, L., & Kutvonen, L. (2010). *Safeguarding against new privacy threats in inter-enterprise collaboration environments. Technical report, Series of Publications C, Report C-2010-56*. Retrieved from http://www.cs.helsinki.fi/group/cinco/publications/public_pdfs/moen10safeguarding.pdf

Moon, T., Fewell, S., & Reynolds, H. (2008). The What , Why , When and How of Interoperability. *Defense & Security Analysis*, *24*(1), 5–17. doi:10.1080/14751790801903178

Moor, J. H. (1997). Towards a Theory of Privacy in the Information Age. *Computers and Society Magazine*, (September), 27–32.

Morris, E., Levine, L., Meyers, C., Place, P., & Plakosh, D. (2004). *System of Systems Interoperability (SOSI): Final Report*. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA455619

Moss, L., & Adelman, S. (2015). The Role of Chief Data Officer in the 21st Century. *Data Integration, BI & Collaboration*. Retrieved March 10, 2015, from http://www.cutter.com/content-and-analysis/resource-centers/business-intelligence/sample-our-research/biar1302.html

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*,

21(2)(June). Retrieved from http://www.qual.auckland.ac.nz/

Navarrete, C., Gil-Garcia, J. R., Mellouli, S., Pardo, T. a., & Scholl, J. (2010). Multinational E-Government Collaboration, Information Sharing, and Interoperability: An Integrative Model. *2010 43rd Hawaii International Conference on System Sciences*, 1–10. doi:10.1109/HICSS.2010.282

NETHA. (2005). *Towards an Interoperability Framework Version 1.8*. Retrieved from www.nehta.gov.au

NETHA. (2006). *NEHTA's Approach to Privacy Version 1.0* (Vol. 77). Retrieved from www.nehta.gov.au

NETHA. (2007a). *Interoperability Framework*. Retrieved from www.nehta.gov.au

NETHA. (2007b). *Interoperability Maturity Model*. Retrieved from www.nehta.gov.au

NETHA. (2008). *Privacy Blueprint for the Individual Electronic Health Record - Report on Feedback*. Retrieved from http://www.nehta.gov.au

NETHA. (2009). *HI Service Security and Access Framework Version 1.0 – 13/11/09*. Retrieved from www.nehta.gov.au

OCDE. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *Internet economy*.

OCDE. (2007). *AT A CROSSROADS: "PERSONHOOD" AND DIGITAL IDENTITY IN THE INFORMATION SOCIETY*. Retrieved from www.oecd.org/dataoecd/31/6/40204773.doc

OCDE. (2013). *THE OECD PRIVACY FRAMEWORK*. Retrieved from http://www.oecd.org/sti/ieconomy/privacy.htm

Otjacques, B., Hitzelberger, P., & Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems*, *23*(4), 29–51. doi:10.2753/MIS0742-1222230403

Parker, C. M., Wafula, E. N., Swatman, P. M. C., & Swatman, P. A. (1994). Information Systems Research Methods: The Technology Transfer Problem1. In *ACIS'94 - 5th Australian Conference on Information Systems* (pp. 197–208).

Patrício, L., & Brito, A. (2012). O desenho da Plataforma de Dados da Saúde (PDS) ao

serviço dos cuidados e dos profissionais de saúde. *Tecno Hospital nº53. Revista de Engenharia E Gestão Da Saúde*, 16–19.

Peleg, M., Beimel, D., Dori, D., & Denekamp, Y. (2008). Situation-Based Access Control: privacy management via modeling of patient data access scenarios. *Journal of Biomedical Informatics*, *41*(6), 1028–40. doi:10.1016/j.jbi.2008.03.014

Peyton, L., Hu, J., Doshi, C., & Seguin, P. (2007). Addressing privacy in a federated identity management network for E-health. *8th World Congress on the Management of E-Business, WCMeB 2007 - Conference Proceedings*, (WCMeB). doi:10.1109/WCMEB.2007.34

Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization : Pseudonymity , and Identity Management*. Retrieved from http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Pham, Q., Mccullagh, A., & Dawson, E. (2007). Consistency of User Attribute in Federated Systems. *TrustBus 2007*, 165–177.

Plummer, A. A. (2001). Information Systems Methodology for Building Theory in Health Informatics: The Argument for a Structured Approach to Case Study Research. In *34th Hawaii International Conference on System Sciences* (Vol. 00, pp. 1–10). IEEE Computer Society.

Poursalidis, V., & Nikolaou, C. (2006). A New User-Centric Identity Management Infrastructure for Federated Systems. *TrustBus 2006*, 11–20.

Ramesh, V., Glass, R. L., & Vessey, I. (2004). Research in computer science: an empirical study. *Journal of Systems and Software*, *70*(1-2), 165–176. doi:10.1016/S0164-1212(03)00015-3

Ray, D., Gulla, U., & Dash, S. S. (2007). *Interoperability of e-Government Information Systems : A Survey*. Retrieved from http://csi-sigegov.orgwww.csi-sigegov.org/2/2_398_2.pdf

Reis, D. (2012). Plataforma de Dados da Saúde: i.desafios. *Tecno Hospital nº53. Revista de Engenharia E Gestão Da Saúde*, 27–30. Retrieved from www.tecnohospital.pt

Rohatgi, M., & Friedman, G. (2010). A structured approach for assessing & analyzing technical & nontechnical interoperability in socio-technical systems. *2010 IEEE*

International Systems Conference, 581–586. doi:10.1109/SYSTEMS.2010.5482337

Scholl, H. J., & Klischewski, R. (2007). E-Government Integration and Interoperability: Framing the Research Agenda. *International Journal of Public Administration*, *30*(8-9), 889–920. doi:10.1080/01900690701402668

Sensmeier, J. (2013). Interoperability-the Next Phase of Healthcare Transformation. *HIMSS Interoperability & Standards Committee*. Retrieved May 13, 2013, from http://blog.himss.org/2013/05/06/interoperability-the-next-phase-of-healthcare-transformation/

Shanks, G., & Parr, A. (2001). *Positivist, Single Case Study Research in Information Systems: a Critical Analysis*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.8766&rep=rep1&type=pdf

Shin, D., Ahn, G., & Shenoy, P. (2004). Ensuring Information Assurance in Federated Identity Management. *IEEE*, 821–826. Retrieved from http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1395193&abstractAccess=no&userType=inst

Skinner, G., Han, S., & Chang, E. (2006). An Introduction to a Taxonomy of Information Privacy in Collaborative Environments. In *5th WSEAS International Conference on Applied Computer Science* (Vol. 2006, pp. 981–986). Retrieved from http://www.fit.cbs.curtin.edu.au/

Soares, D. (2009). *Interoperabilidade entre Sistemas de Informação na Administração Pública*. Universidade do Minho.

Solove, D. (2006). A TAXONOMY OF PRIVACY. *University of Pennsylvania Law Review*, *154*(3), 477–560.

Solove, D. (2008). *Understanding Privacy. The George Washington University Law School; Public Law And Legal Theory Working Paper No. 420; Legal Studies Research Paper No. 420* (No. PUBLIC LAW AND LEGAL THEORY WORKING PAPER NO. 420). Retrieved from http://www.usdrinc.com/downloads/Privacy.pdf

Stelzer, D., Fischer, D., & Nirsberger, I. (2006). A Framework for Assessing Inter-organizational Integration of Business Information Systems. *International*

Journal of Interoperability in Business Information Systems (IBIS), *2*(2), 9–20. Retrieved from http://www.ibis-journal.net/

Stieger, S., Burger, C., Bohn, M., & Voracek, M. (2013). Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between facebook users and quitters. *Cyberpsychology, Behavior and Social Networking*, *16*(9), 629–34. doi:10.1089/cyber.2012.0323

Suess, J., & Morooney, K. (2009). Identity Management and Trust Services: Foundations for Cloud Computing. *Educause Review September/October 2009*, (October), 25–42.

Tavani, H. T. (2007). Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. *Metaphilosophy*, *38*(1), 1–22. doi:10.1111/j.1467-9973.2006.00474.x

Tavani, H. T. (2008). Informational Privacy: Concepts, Theories, and Controversies. In K. E. Himma & H. T. Tavani (Eds.), *THE HANDBOOK OF INFORMATION AND COMPUTER ETHICS* (pp. 131–164). WILEY.

Tavani, H. T., & Moor, J. H. (2001). Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. *Computers and Society Magazine*, (March), 6–11. Retrieved from http://dl.acm.org/citation.cfm?id=572278

The Internet Society. (2000). RFC 2828 - Internet Security Glossary. *Internet FAQ Archives*. Retrieved from http://www.faqs.org/rfcs/rfc2828.html

Tolk, A. (2003). Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability. In *8 th International Command and Control Research and Technology* (Vol. 5).

Tolk, A. (2006). What comes after the Semantic Web - PADS Implications for the Dynamic Web. In *Proceedings of the 20th Workshop on Principles of Advanced and Distributed Simulation (PADS'06)*.

Tolk, A., & Aaron, R. D. (2010). Addressing Challenges of Transferring Explicit Knowledge, Information, and Data in Large Heterogeneous Organizations: A Case Example from a Data-Rich Integration Project at the U.S. Army Test and Evaluation Command. *Engineering Management Journal*, *22*(2).

Tolk, A., & Diallo, S. Y. (2005). Model-Based Data Engineering for Web Services. *IEEE INTERNET COMPUTING*, (July/August), 65–70.

Tolk, A., & Muguira, J. A. (2003). The Levels of Conceptual Interoperability Model. In *Fall Simulation Interoperability Workshop* (pp. 25–42).

Turnitsa, C. (2005). Extending the Levels of Conceptual Interoperability Model. *Summer Computer Simulation Conference*.

UE. CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2010/C 83/02). , Pub. L. No. C 83/389 (2010). Jornal Oficial da União Europeia. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:pt:PDF

US Federal Trade Commission. (2010). *Protecting Consumer Privacy in an Era of Rapid Change: Preliminary Staff Report*. Washington. Retrieved from http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

Vernadat, F. B. (2010). Technical, semantic and organizational issues of enterprise interoperability and networking. *Annual Reviews in Control*, *34*(1), 139–144. doi:10.1016/j.arcontrol.2010.02.009

Vessey, I., Ramesh, V., & Glass, R. L. (2002). Research in Information Systems: An Empirical Study of Diversity in the Discipline and Its Journals. *Joumal of Management Information System*, *19*(2), 129–174.

Villiers, M. R. D. E. (2005). Three approaches as pillars for interpretive Information Systems research: development research, action research and grounded theory. In *SAICSIT 2005*. Retrieved from http://dl.acm.org/citation.cfm?id=1145675.1145691

Waldo, J., Lin, H. S., & Millett, L. I. (2007). Engaging Privacy and Information Technology in a Digital Age: Executive Summary. *Journal of Privacy and Confidentiality*, *2*(1), 5–18. Retrieved from http://repository.cmu.edu/jpc/vol2/iss1/

Waldo, J., Lin, H. S., & Millett, L. I. (2010a). Thinking About Privacy : Chapter 1 of " Engaging Privacy and Information Technology in a Digital Age ." *Journal of Privacy and Confidentiality*, *2*(1), 19–50. Retrieved from http://repository.cmu.edu/jpc/vol2/iss1/

Waldo, J., Lin, H. S., & Millett, L. I. (2010b). Thinking About Privacy: Chapter 1 of " Engaging Privacy and Information Technology in a Digital Age ." *Journal of*

Privacy and Confidentiality, *2*(1), 19–50. Retrieved from http://repository.cmu.edu/jpc/vol2/iss1/

Wang, W., Tolk, A., & Wang, W. (2009). The Levels of Conceptual Interoperability Model : Applying Systems Engineering Principles to M&S. In *Spring Simulation Multiconference (SpringSim'09). San Diego, CA, USA*.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Communications of the ACM*, *51*(6), 82–87. doi:10.1145/1349026.1349043

Windley, P. J. (2005). *Digital Identity*. (A. Randal & T. Apandi, Eds.) (First Edit.). O'Reilly Media.

Winters, L. S., Gorman, M. M., & Tolk, A. (2006). Next Generation Data Interoperability: It ' s all About the Metadata. In *Fall Simulation Interoperability Workshop*.

Wong, R. (2011). Data protection: The future of privacy. *Computer Law & Security Review*, *27*(1), 53–57. doi:10.1016/j.clsr.2010.11.004

WPISP. (2011). TERMS OF REFERENCE FOR THE REVIEW OF THE OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER DATA FLOWS OF PERSONAL DATA. Organisation for Economic Co-operation and Development.

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law & Security Review*, *28*(1), 54–61. doi:10.1016/j.clsr.2011.11.007

Wright, D., Gutwirth, S., Friedewald, M., De Hert, P., Langheinrich, M., & Moscibroda, A. (2009). Privacy, trust and policy-making: Challenges and responses. *Computer Law & Security Review*, *25*(1), 69–83. doi:10.1016/j.clsr.2008.11.004

Wuyts, K., Scandariato, R., De Decker, B., & Joosen, W. (2009). Linking Privacy Solutions to Developer Goals. *2009 International Conference on Availability, Reliability and Security*, 847–852. doi:10.1109/ARES.2009.51

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. In *International Conference on Information Systems (ICIS)*. AIS Electronic Library (AISeL). Retrieved from

http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1210&context=icis2008

Yeonjung, K., Hyangjin, L., Kilsoo, C., & Junghwan, S. (2007). Classification of privacy enhancing technologies on life-cycle of information. *Proceedings - The International Conference on Emerging Security Information, Systems, and Technologies, SECURWARE 2007*, 66–70. doi:10.1109/SECUREWARE.2007.4385312

Yin, R. K. (2009). *Case Study Research: Design and Methods, 4rd Edition (Applied Social Research Methods, Vol. 5)*.

Yuhanna, N. (2009). Test Data Privacy Is Critical To Meet Compliances for Application Development & Program Management Professionals. *Forrester Research*. Retrieved from http://www.forrester.com