INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Desenvolvimento de um modelo de avaliação da ética digital

Caso de Estudo numa entidade do Setor da Saúde em Portugal

Inês Isabel Cardoso de Oliveira Casaleiro

Mestrado em Gestão de Sistemas de Informação

Orientadores:

Doutor Bráulio Alexandre Barreira Alturas, Professor Associado,
Iscte – Instituto Universitário de Lisboa

Doutor Nuno Alexandre Correia Martins Cavaco, Professor Auxiliar Convidado,
Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa

Novembro, 2020

TECNOLOGIAS
E ARQUITETURA

Departamento de Ciências e Tecnologias de Informação

Desenvolvimento de um modelo de avaliação da ética digital
Caso de Estudo numa entidade do Setor da Saúde em Portugal

Inês Isabel Cardoso de Oliveira Casaleiro

Mestrado em Gestão de Sistemas de Informação

Orientadores:

Doutor Bráulio Alexandre Barreira Alturas, Professor Associado,
Iscte – Instituto Universitário de Lisboa

Doutor Nuno Alexandre Correia Martins Cavaco, Professor Auxiliar Convidado,
Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa

Novembro, 2020

Agradecimentos

A todos os profissionais de Saúde dedico esta minha dissertação, que no ano de 2020 mostraram, uma vez mais, o seu extraordinário trabalho, na luta e superação no combate à pandemia, ao qual demonstro a minha profunda admiração e gratidão.

Agradeço, especialmente, aos profissionais que participaram no estudo desta investigação, através das entrevistas e questionário, pela sua disponibilidade e vontade de contribuir para um futuro mais próspero na Saúde.

Aos meus orientadores, Professor Bráulio Alturas e Professor Nuno Cavaco, o meu muito obrigada, pelo incentivo, apoio e palavras dadas, que me ajudaram a crescer ao longo desta jornada.

Por fim, e não menos importante, agradeço com o maior carinho à minha família e amigos, particularmente aos meus pais, irmão, namorado e colegas de Mestrado, que me acompanharam e depositaram em mim a confiança e o orgulho de que este percurso fosse realizado da melhor maneira possível.

Muito obrigada e até sempre, ISCTE!

Resumo

A rápida expansão da tecnologia e a relevância que apresenta atualmente no quotidiano dos indivíduos traz consigo uma preocupação quanto às questões éticas na utilização dos meios digitais. Torna-se assim cada vez mais urgente regular os aspetos relacionados com a ética digital, de modo a credibilizar toda a informação existente nas mais variadas plataformas. Para compreender o significado de ética digital foi necessário realizar uma fase de revisão de literatura, que permitiu analisar o Estado da Arte da ética digital, principalmente no que diz respeito à área da Saúde, visto que é o caso de estudo desta investigação. Com isto, foram identificadas dimensões fundamentais de análise da ética digital e, de seguida, uma fase de conceção do modelo de avaliação da ética digital, com a realização de entrevistas a profissionais do setor da saúde, que contribuiu para uma análise qualitativa do tema e para validar as dimensões e critérios específicos de avaliação da ética digital. Através do caso de estudo, foi aplicado um questionário a uma entidade do setor da Saúde, com o objetivo de validar o modelo criado e classificar a entidade quanto ao desempenho na ética digital. Revela-se assim a importância de avaliar o desempenho da ética digital no setor da Saúde e a necessidade de consciencializar as entidades para as preocupações relativas a esta temática, de modo a que possam instituir medidas internas de melhoria, através de boas práticas e procedimentos institucionais adequados.

Palavras-Chave: tecnologia, ética, digital, ciência de dados, critérios, avaliação, saúde

Abstract

The fast growth of technology and the relevance it currently presents in the daily lives of individuals brings with it a concern about ethical issues in the use of digital media. It is thus becoming more and more urgent to regulate aspects related to digital ethics, in order to make all existing information credible on the most varied platforms. To understand the meaning of digital ethics it was necessary to carry out a literature review phase, which allowed to analyze the state of the art of digital ethics, especially in the area of Health, since it is the case of this research. With this, fundamental dimensions of analysis of digital ethics were identified, followed by a design phase of the model of evaluation of digital ethics, with interviews to health professionals, which contributed to a qualitative analysis of the subject and to validate the specific dimensions and criteria of evaluation of digital ethics. Through the case study, a questionnaire was applied to an entity of the Health sector, with the objective of validating the model created and classify the entity regarding the performance in digital ethics. This shows the importance of evaluating the performance of digital ethics in the Health sector and the need to make the entities aware of the concerns related to this theme, so that they can institute internal measures of improvement, through good practices and appropriate institutional procedures.

Keywords: technology, ethics, digital, data science, criteria, evaluation, health

Índice

Índice de Tabelas

Índice de Figuras

Lista de Abreviaturas e Siglas

ARS - Administrações Regionais de Saúde

ACES - Agrupamentos de Centros de Saúde

CISO - *Chief Information Security Officer*

CNPD - Comissão Nacional de Proteção de Dados

DPO - *Data Protection Officer*

IA - Inteligência Artificial

INE - Instituto Nacional de Estatística

IP – *Internet Protocol*

ISO - *International Organization for Standardization*

OCDE - Organização para a Cooperação e Desenvolvimento Económico

RFID - *Radio-Frequency IDentification*

RGPD - Regulamento Geral sobre a Proteção de Dados

SNS - Serviço Nacional de Saúde

SPMS - Serviços Partilhados do Ministério da Saúde

UE - União Europeia

Capítulo 1 – Introdução

1.1. Enquadramento do tema

O tema desta dissertação de mestrado é a ética digital e a proposta de investigação é o desenvolvimento de um modelo de avaliação da ética digital, através de um caso de estudo numa entidade do setor da saúde, em Portugal.

Com a rápida expansão da tecnologia, cada vez mais as organizações estão a avaliar as suas oportunidades, desenvolvendo e fornecendo produtos e serviços, e interagindo digitalmente com os clientes e outros interessados. A tecnologia digital, devidamente aproveitada, pode permitir que indivíduos, empresas, cidades e governos se tornem mais inteligentes, de forma a expandir as suas capacidades e adaptar-se a condições novas e em mudança (Snow et al., 2017).

Um dos setores que tem vindo a dar largos passos na adoção de tecnologias digitais é a Saúde, ao explorar os dados para o suporte de tomada de decisões e ao considerar novas soluções para reforçar o sistema de saúde. Ao mesmo tempo, a coleção, armazenamento, utilização e partilha de grandes conjuntos de dados de saúde coloca muitas questões éticas relativas à governação, qualidade, segurança, normas, privacidade e propriedade de dados (Zandi et al., 2019). Desta forma, torna-se importante avaliar as organizações quanto ao desempenho que têm relativamente à ética digital.

Assim, o primeiro objetivo ao realizar esta dissertação é tentar perceber o que é a ética digital. Segundo vários autores, o termo "ética digital" é aplicado nas reflexões e análises dos problemas éticos que surgem com a expansão tecnológica digital, principalmente os que envolvem privacidade e proteção de dados (Mahieu et al., 2018) ou até mesmo todos aqueles relacionados com a ética dos dados, informação e computacional (Floridi & Taddeo, 2016).

De seguida vão ser identificadas as dimensões utilizadas para avaliar a mesma no setor da Saúde e, posteriormente, a construção de um modelo, constituído por critérios apropriados de avaliação, baseado no enquadramento teórico e na análise qualitativa das entrevistas a realizar a profissionais da área. Através do caso de estudo, será aplicado um questionário a uma entidade do setor, no qual será obtida uma classificação do desempenho da mesma quanto à ética digital.

1.2. Motivação e relevância do tema

O motivo de escolha do tema da dissertação de mestrado surge com a relevância da tecnologia nos dias de hoje, não só na sua utilização a nível de lazer como também a nível profissional, nomeadamente na área da Saúde, que é fundamental para melhorar a análise diagnóstica e, assim, promover ganhos potenciais de saúde.

Porém, com a rápida expansão da tecnologia, aparecem consequentemente alguns riscos associados à sua utilização, tais como, a falta de segurança na informação disponibilizada, por exemplo, na privacidade e proteção de dados; a falta de controlo no acesso a dados e informações relevantes; a ocorrência de crimes digitais, como o roubo de identidade; o *cyberbullying* nas redes sociais, entre outros.

Visto que a tecnologia é uma ferramenta do dia-a-dia, e é utilizada pela maior parte da população em geral e pelas empresas, a Ética digital torna-se assim cada vez mais urgente e necessária, não só para regular todos os aspetos relacionados com a área tecnológica, mas também para credibilizar toda a informação existente nas mais variadas plataformas.

Deste modo, com a criação de dimensões e critérios para avaliar a ética digital, as organizações poderão prestar mais atenção a esta temática e obter um maior rigor na utilização das suas tecnologias, que irá levar a uma maior segurança e confiança por parte dos seus clientes e outras partes interessadas.

Na área da Saúde, esta temática é ainda mais relevante, uma vez que trata de dados sensíveis em que a credibilidade dos sistemas e segurança da informação é ainda mais crítica. Neste sentido, através do caso de estudo no setor da Saúde, estes pressupostos poderão ser validados visto que a utilização de tecnologias de informação e comunicação na área da saúde é essencial na promoção de modos de relacionamento mais seguros, acessíveis e eficientes nos cuidados de saúde. Assim, a possibilidade de ter a informação digitalizada e estruturada que assegure a partilha atempada e fiável de informações clínicas pode melhorar os resultados de saúde e eficiência, e também criar um repositório de dados valiosos para investigadores e gestores de sistemas de informação (OECD & Union, 2018).

1.3. Questões e objetivos de investigação

A questão de investigação proposta para esta dissertação é a seguinte: "Quais os critérios adequados para avaliar a ética digital no setor da Saúde?"

Quanto à função de pesquisa, pretende-se analisar o Estado da Arte da ética digital e concluir quais são os critérios mais apropriados na avaliação da ética digital nos serviços de Saúde, através da análise das entrevistas e do caso de estudo.

Os objetivos estabelecidos são, deste modo:

- Analisar o Estado da Arte da ética digital;
- Estabelecer dimensões de análise da ética digital;
- Criar um modelo constituído por dimensões de análise e critérios específicos de avaliação da ética digital, aplicável ao setor da Saúde;
- Validar o modelo de avaliação da ética digital através de uma parceria com uma entidade do setor da Saúde, obtendo um índice de classificação.

1.4. Abordagem metodológica

A dissertação baseou-se numa metodologia que contemplou inicialmente uma fase de análise de revisão de literatura, onde foi possível analisar o Estado da Arte do termo "ética digital" e caracterizar as dimensões de avaliação da ética digital, quanto ao setor da saúde.

Para conseguir desenvolver o processo do estudo empírico e verificar a questão de investigação foi ainda necessária uma fase qualitativa, com a realização de entrevistas a profissionais da área da Saúde, que é o setor em estudo, pretendendo-se validar as dimensões e os critérios de avaliação identificados na fase anterior.

De seguida, construiu-se o modelo de avaliação da ética digital, proposto inicialmente, com uma lista de dimensões e critérios de análise do desempenho da ética digital, que teve por base todo o Estado da Arte e o resultado das entrevistas realizadas.

Para validar o modelo e concluir acerca da sua adequabilidade, realizou-se um caso de estudo numa entidade do setor da saúde, com a aplicação de um questionário acerca dos critérios de avaliação, e assim foi possível aferir uma classificação da entidade quanto ao desempenho que tem em relação à ética digital.

1.5. Estrutura e organização da dissertação

A presente dissertação está organizada em seis capítulos que pretendem refletir as diferentes fases de trabalho até à sua conclusão.

Neste caso, o primeiro capítulo introduz a questão da investigação, a função de pesquisa e os objetivos da mesma, bem como uma breve descrição da abordagem metodológica e a estrutura geral do trabalho.

O segundo capítulo reflete o enquadramento teórico, designado por Revisão da Literatura, na qual foram abordados temas fundamentais para a concretização da investigação.

O terceiro capítulo é dedicado à Metodologia, explicando o que foi realizado em cada fase e quais os procedimentos seguidos, bem como os métodos de análise utilizados, para a realização do caso de estudo.

O quarto capítulo apresenta a conceção do modelo de avaliação de ética digital, de acordo com a análise dos resultados obtidos com a realização das entrevistas aos profissionais do setor da saúde.

O quinto capítulo é a concretização do Caso de Estudo, em que foi aplicado o questionário a uma entidade do setor da saúde, de modo a obter uma classificação quanto ao desempenho da ética digital.

No sexto e último capítulo apresentam-se as conclusões principais deste estudo bem como os contributos, as limitações e as propostas de trabalhos futuros.

Capítulo 2 – Revisão da Literatura

2.1. Ética

2.1.1. Conceito

O termo "ética" surge do latim *ethica* e do grego *éthos*, que significa um costume ou hábito. Além disso, consiste num conjunto de regras de conduta de um determinado indivíduo ou grupo (Gontijo, 2006).

O estudo da ética centra-se principalmente na sociedade e no comportamento humano, tendo o conceito surgido na antiguidade, através de alguns filósofos, como Demócrito e Aristóteles, que identificavam a ética como um meio de alcançar a felicidade (Figueiredo, 2008).

Todavia, o estudo da ética não é apenas explorado pela filosofia, mas também por diversos profissionais nas mais variadas áreas, como por exemplo, a Sociologia, Antropologia, Psicologia, Biologia, Medicina, Jornalismo, Economia e Gestão, entre outros. Isto deve-se pelo facto de cada área ter um código de ética, com o objetivo de delimitar as ações da profissão em si e de quem as pratica (Figueiredo, 2008).

Deste modo, pode referir-se que a ética é a classificação de comportamentos específicos como certo ou errado, assim como de uma conduta boa ou má, dentro de uma determinada profissão (Wilson et al., 2010). O comportamento ético cria então respeito, fortalece a integridade e permite aos indivíduos mostrarem-se como honestos e confiáveis (Rice, 2006).

Além disso, cada pessoa possui um código de ética individual, ou seja baseado em valores, crenças, experiência, cultura e educação que adquirem ao longo da sua vida. Um código ético é assim uma fonte de valores e características que permite a cada indivíduo optar pelo que é certo ou errado, sendo a base do seu comportamento ético e da tomada de decisões (Reay & Hinings, 2009).

De certa forma, a decisão ética traz uma questão importante, isto é, de como esse resultado afetará os outros indivíduos, daí a necessidade de pensar sobre qual é a consequência e a maneira como os outros responderão à resolução (Godden et al., 2010).

2.1.2. Ética e Moral

Etimologicamente, moral tem um significado semelhante ao da ética, com a diferença de que é derivada da palavra latina *mores*. Porém, cada um dos termos considera algo mais específico dentro do mesmo tema (Gontijo, 2006).

A moral trata assim da consciência adquirida pelo ser humano a partir do momento histórico em que ele começa a viver em sociedade. É toda a aprendizagem das normas sociais que regulam o comportamento humano, e que são adquiridos pela tradição e educação do dia-a-dia. Além disso, é um conjunto de regras coletivas que facilitam o convívio, em que é mutuamente aceite e intrínseco ao indivíduo na sociedade. Já a ética trata do comportamento individual em relação à sociedade, o que garante o bem-estar social. Define ainda como o ser humano deve comportar-se diante do meio social (Figueiredo, 2008).

Tradicionalmente, a ética referia-se ao estudo filosófico da moralidade, sendo este último um conjunto de crenças mais ou menos sistemático, geralmente mantido em comum por um grupo, sobre como as pessoas deveriam viver. Mais tarde, o termo foi aplicado a códigos morais ou sistemas de valores particulares (e mais restritos), contudo o nome do estudo filosófico permanece como ética (Gontijo, 2006).

2.1.3. Ética nas Organizações

Como referido anteriormente, a ética considera o modo de agir de indivíduo numa determinada situação, não apenas para atingir um objetivo específico, mas também tendo em conta todos os aspetos ao seu redor (Dias, 2014).

Neste caso, a ética nos negócios das organizações refere-se a um conjunto de regras de ética profissional que estuda os princípios e problemas de conduta ou morais, que surgem num determinado ambiente de negócios. As questões relacionadas à ética nos negócios concentram-se nos fatores políticos, económicos, legais e outros fatores sociais. Outras questões podem ser relativas ao funcionamento de um determinado negócio ou empresa, ou até mesmo a questões individuais, ou seja, à conduta ou comportamento de indivíduos dentro de um negócio ou empresa (Almeida, 2007).

O objetivo final da ética individual é desenvolver um conjunto de padrões éticos que possam ser considerados aceitáveis depois de considerar tudo cuidadosamente numa situação específica. Esses padrões éticos aceites individualmente também podem ser aplicados a diferentes situações, como pessoal, social e até em um negócio. A maioria dos consumidores concorda que uma empresa deve seguir o mesmo padrão moral ao interagir com um cliente individual, bem como interagir com todos os clientes local, nacional ou globalmente (McKinney et al., 2010)

A ética acaba por se tornar num dilema para os gestores, uma vez que pode ser motivo de conflito entre as atividades económicas, o desempenho social e a integridade humana. As empresas e organizações devem resolver estas questões caso a caso, pelo facto de não haver um regulamento geral, ou seja, as predisposições dos gestores são direcionadas a determinadas escolhas devido aos seus próprios níveis de desenvolvimento moral (Webley & Werner, 2008)

Essas escolhas devem refletir valores e crenças organizacionais. Os governos, por meio de leis e regulamentos, podem ajudar a estabelecer o significado de ética. No entanto, uma solução eficaz para a questão deve conter um mecanismo no qual as considerações éticas se tornem uma parte central das operações. Um componente essencial para garantir o desempenho ético das empresas modernas é a integração do raciocínio moral em toda a organização (Webley & Werner, 2008).

É necessário um código de ética, de modo a evitar comportamentos antiéticos, bem como estabelecer um ambiente ético dentro da organização. Deve ter influência formal e informal para controlar o comportamento antiético e educar os colaboradores sobre comportamentos éticos (Tenbrunsel et al., 2003).

Um código de ética é assim uma declaração formal dos valores de uma organização em relação às questões sociais e éticas, comunicando aos seus colaboradores o que representa a empresa (Schwartz, 2002).

2.1.4. Ética e Responsabilidade Social

O termo "Responsabilidade Social" é cada vez mais utilizado nas organizações, visto que, se uma empresa pretende maximizar o lucro a longo prazo, necessita de reconhecer algumas obrigações sociais, como ser socialmente responsável. Deve então ser implementada uma abordagem de proteção do bem-estar da sociedade, preservando o meio ambiente e contribuindo positivamente como uma instituição socialmente responsável. Além disso, a maioria das empresas no mundo atual dá uma maior importância a ser eticamente responsável e, por essa razão, maximizar o lucro não é a principal prioridade (Queiroz et al., 2017).

Para uma melhor compreensão do seu significado, a Responsabilidade Social é vista como um conjunto de entendimentos comuns de relacionamentos, obrigações e deveres geralmente aceites entre as principais instituições e o povo, denominado por certos filósofos e teóricos políticos como "contrato social" (Steiner, 1972).

A Responsabilidade Social nos negócios das organizações é, em si, uma parte substancial deste contrato social, que se relaciona com o impacto da organização no bem-estar da sociedade. Alguns exemplos disso são o apoio às minorias, a satisfação do consumidor, a melhoria da comunidade e proteção ambiental, entre outros (Hill, 1982).

A Responsabilidade Social é assim uma consequência da ética que leva a uma determinada organização a ser responsabilizada pelos seus impactos na sociedade e no ambiente, tendo uma estratégia de gestão que visa incorporar essa conduta nas suas operações e atividades (Almeida, 2007)

Por essa razão foi criada a ISO 26000, uma norma internacional de responsabilidade social, referindo que "A característica essencial da responsabilidade social é a disponibilidade da organização para incorporar considerações sociais e ambientais no seu processo de tomar decisões e ser responsabilizável pelo impacto das suas decisões e atividades na sociedade e no ambiente. Isto implica uma conduta ética e transparente".

2.2. Ética Digital

2.2.1. Conceito

Após uma abordagem do significado de ética, no seu sentido mais lato, há que tentar perceber no que consiste a ética digital, de modo a compreender melhor os objetivos da dissertação.

Já desde a segunda metade do século XX, que o conceito de ética digital é abordado, no entanto, sem a atual designação, em que alguns cientistas da área da Informática, como por exemplo, Norbert Wiener (1989/1950) e Joseph Weizenbaum (1976), chamaram a atenção do público da época para os desafios éticos emergentes na tecnologia da computação, através da responsabilidade moral dos profissionais de Informática (Capurro, 2018).

Segundo vários autores, o termo "ética digital" é aplicado nas reflexões e análises dos problemas éticos que surgem com a expansão tecnológica digital, principalmente os que envolvem privacidade e proteção de dados (Mahieu et al., 2018) ou até mesmo todos aqueles relacionados com a ética dos dados, informação e computacional (Floridi & Taddeo, 2016). Além disso, pode ainda ser retratada na regulação e governança digital, através de uma relação de avaliação moral (Floridi, 2018a).

Com a rápida expansão da tecnologia, aparecem consequentemente alguns riscos associados, tais como, a falta de segurança na informação disponibilizada, por exemplo, na privacidade e proteção de dados; a falta de controlo no acesso a dados e informações relevantes; a ocorrência de crimes digitais, como o roubo de identidade; o *cyberbullying* nas redes sociais, entre outros (Maggiolini, 2014).

Visto que a tecnologia é uma ferramenta do dia-a-dia, e é utilizada pela maior parte da população em geral e pelas organizações em Portugal, a ética digital torna-se assim cada vez mais urgente e necessária, não só para regular todos os aspetos relacionados com a área tecnológica, mas também para credibilizar toda a informação existente nas mais variadas plataformas.

2.2.2. Relação da Ética Digital com a Governança Digital e Regulação Digital

A revolução digital, através de uma sociedade de informação mais amadurecida, transformou toda a visão quanto aos valores, às prioridades e aos comportamentos na utilização das tecnologias. Daí o desafio não ser apenas na inovação digital mas também na governança do digital e de que forma se pode regular (Floridi, 2018a).

A governança digital consiste então na prática de estabelecer e implementar políticas, procedimentos e padrões para o desenvolvimento, uso e gestão adequados da "esfera" da informação (Burr et al., 2020). Pode incluir diretrizes e recomendações que se sobrepõem, mas que não são idênticos, à regulação digital. Esta é pressuposta numa legislação relevante, através de um sistema de regras elaborado e aplicado por instituições sociais e governamentais, com o objetivo de regular o comportamento dos agentes relevantes na "esfera" da informação (Floridi, 2018b). Assim, nem todos os aspetos da regulação digital são uma questão de governança digital e nem todos os aspetos da governança digital são uma questão de regulação digital. Tudo isto é aplicado à ética digital, que, como abordado em capítulos anteriores, estuda e avalia problemas morais relacionados com dados e informação, algoritmos, práticas e infra-estruturas correspondentes, a fim de formular e apoiar soluções moralmente boas. Neste caso, a ética digital molda a regulação e a governação digitais através da relação de avaliação moral (Floridi, 2018a).

Deste modo, pode-se afirmar que a governança digital, a ética digital e a regulação digital são abordagens diferentes mas complementares, como se pode ver na Figura 1.

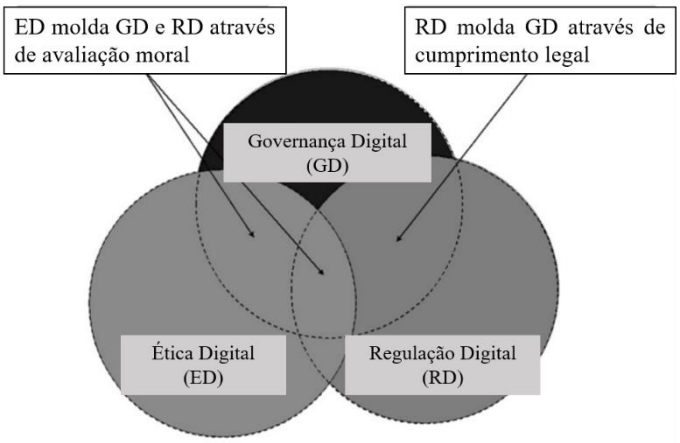


Figura 1 - Relação da Ética Digital com a Governança Digital e Regulação Digital. Fonte adaptada: (Floridi, 2018)

2.3. Ética Digital na Saúde

Como já foi dito anteriormente, as tecnologias de informação encontram-se bastante disseminadas em diversos setores da sociedade portuguesa e, nos últimos anos, começam a dar largos passos no setor da Saúde, nomeadamente, ao contribuir para a evolução e para a melhoria na prestação de cuidados (Morais Nunes & Matos, 2018).

Em Portugal, através do Serviço Nacional de Saúde (SNS), foram adotadas várias estratégias de implementação das tecnologias, como fator de inovação ao serviço da saúde, referentes a todos os cuidados integrados de saúde, que compreendem a sua promoção e vigilância, a prevenção da doença, o diagnóstico e tratamento dos pacientes, e a reabilitação clínica e social.

Assim, a inovação digital que tem vindo a ocorrer nos últimos anos traz para o setor da Saúde muitos avanços, neste caso, quanto à investigação e aos cuidados clínicos prestados. Esta inovação tem, por acréscimo, consequências éticas de grande amplitude, em particular na governança dos dados pessoais gerados a partir da investigação e através das práticas médicas de cuidados de saúde (Albinati, 2018).

Esses dados são denominados de "*Big Data*", ou em português "Grandes Dados", que consistem em grandes e complexos volumes de dados, transacionados a alta velocidade, que requerem tecnologias e técnicas avançadas para permitir a captura, armazenamento, distribuição, gestão e análise da informação e a sua transformação em conhecimento. Abrangem características tais como variedade, velocidade e, no que respeita especificamente aos cuidados de saúde, veracidade. As técnicas analíticas existentes podem ser aplicadas à vasta quantidade de dados clínicos e de saúde existentes relacionados com os pacientes para se chegar a uma compreensão mais profunda dos resultados, os quais podem então ser aplicados no ponto de tratamento (Raghupathi & Raghupathi, 2014).

Devido à elevada quantidade de dados que o setor da Saúde gera, impulsionados pela manutenção de registos, conformidade e requisitos regulamentares, e cuidados aos pacientes, a tendência atual é para uma rápida digitalização dos *Big Data*. A par da evolução tecnológica, pelos requisitos obrigatórios e pelo potencial para melhorar a qualidade da prestação de cuidados de saúde, reduzindo entretanto os custos, estas enormes quantidades de dados têm como objetivos apoiar uma vasta gama de funções

médicas e de cuidados de saúde, incluindo entre outros apoio à decisão clínica, vigilância de doenças, e gestão da saúde da população.

Os dados eletrónicos de saúde são tão grandes e complexos que são difíceis (ou impossíveis) de gerir com *software* e/ou *hardware* tradicional; nem podem ser facilmente geridos com ferramentas e métodos tradicionais ou comuns de gestão de dados, devido não só ao volume como também à diversidade de tipos de dados e à velocidade a que devem ser geridos (Frost & Sullivan, 2012).

O uso de grandes quantidades de dados nos cuidados de saúde aumenta significativamente as preocupações com a segurança dos dados e a privacidade dos pacientes, tornando-se necessário adotar medidas para mitigar riscos de quebras de informação, por exemplo, na garantia da segurança dos registos dos pacientes, através de políticas e procedimentos relacionados com a cibersegurança (Abouelmehdi et al., 2017).

Além disso, o facto de se introduzirem grandes conjuntos de dados de diversas fontes exige um esforço adicional no armazenamento, processamento e comunicação dos mesmos, sendo assim necessária uma efetiva governança, regulamentação e gestão dos dados relativos aos cuidados de saúde (Kupwade Patil & Seshadri, 2014). A Figura 2 retrata uma grande nuvem de dados que incorpora os dados clínicos, financeiros, sociais, genómicos, físicos e psicológicos relativos aos pacientes.

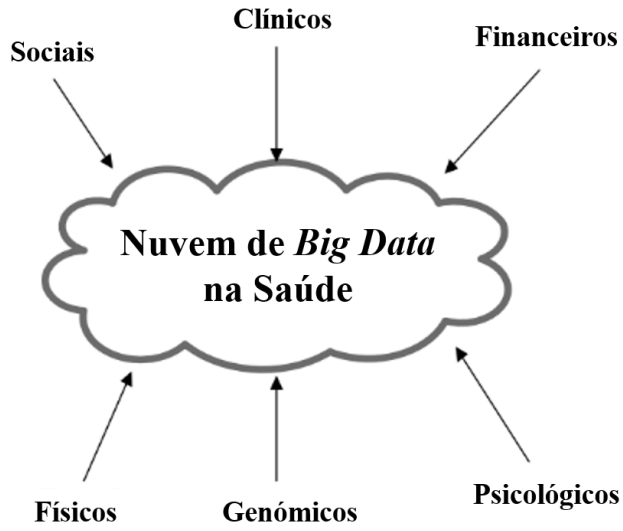


Figura 2 - Tipo de Big Data na Saúde. Fonte adaptada: (Kupwade Patil & Seshadri, 2014)

Por exemplo, a anonimização de dados antes da análise poderia proteger a identidade do paciente. Além disso, a privacidade - preservando esquemas de encriptação que permitem executar algoritmos de previsão em dados encriptados enquanto se protege a identidade de um paciente - é essencial para a obtenção de análises que determinam planos otimizados de cuidados de saúde.

Além disso, à medida que a análise da informação clínica agregada ganha popularidade, é necessário elaborar novas leis de privacidade para proteger a privacidade dos pacientes. Por exemplo, é necessário o "consentimento informado" dos pacientes antes de realizar qualquer análise dos seus dados e redigir novas normas para ilustrar claramente todos os processos envolvidos na realização de análises dos *Big Data* sobre os dados dos pacientes (Kupwade Patil & Seshadri, 2014).

Quanto à tradicional gestão de dados, os dados biológicos são recolhidos, armazenados, acedidos e analisados de acordo com meios analógicos de identificação, sendo os dados biológicos ligados através de autorização prévia, manutenção de registos e controlo ligados a sujeitos vivos reais, que são dotados de certos direitos à privacidade e proteção de dados. Num contexto digital, a tensão entre a ética dos cuidados e a ética da monitorização da informação torna-se mais pertinente.

As agências de saúde pública utilizam cada vez mais meios eletrónicos para adquirir, utilizar, manter e armazenar informações pessoais de saúde. Os formatos eletrónicos de dados podem melhorar o desempenho das principais funções de saúde pública, mas ameaçam potencialmente a privacidade porque podem ser facilmente duplicados e transmitidos a pessoas não autorizadas. Para isso, é necessário avaliar possíveis ameaças, implementar políticas atualizadas, formar pessoal, e desenvolver medidas de engenharia preventiva para proteger a informação (Myers et al., 2008).

Ao considerar a melhor forma de desenvolver um sistema eficaz que proporcione cuidados de qualidade e valor para os consumidores de saúde - e que seja capaz de satisfazer a procura de cuidados futuros – o papel que os pacientes desempenham tornou-se cada vez mais importante: devolver-lhes um papel de protagonista é hoje uma prioridade para as políticas de saúde, tanto a nível ético como pragmático (Graffigna, 2016).

2.4. Dimensões de Avaliação da Ética Digital na Saúde

2.4.1. Privacidade e Proteção de Dados

Com a evolução exponencial das tecnologias digitais surge cada vez mais uma preocupação com a proteção dos dados dos cidadãos. Para isso foi criada e adotada uma nova legislação que permite incorporar valores principais de privacidade, autonomia e integridade (Mahieu et al., 2018).

De acordo com a Constituição da República Portuguesa, no artigo 35.º, Utilização da Informática: "Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos previstos na lei." (*Constituição da República Portuguesa*, 1976).

De acordo com o artigo 6.º do Regulamento Geral sobre a Proteção de Dados (RGPD): "A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais." (*REGULAMENTO (UE) 2016/ 679 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016*)

A criação do RGPD permitiu assim que fossem definidos requisitos pormenorizados acerca da recolha, armazenamento e gestão de dados pessoais, que são aplicados tanto a empresas e organizações europeias que tratam dados pessoais na União Europeia (UE) como a empresas e organizações estabelecidas fora do território da UE que tratam dados pessoais de pessoas de vivem na UE.

Os dados pessoais consistem então em qualquer tipo de informações sobre uma determinada pessoa, identificada ou identificável, denominada titular dos dados. Alguns exemplos de dados pessoais são o nome, morada, número do documento de

identificação/passaporte, rendimento, perfil cultural, endereço IP (protocolo de internet), dados na posse de um hospital ou médico (que identifiquem de forma inequívoca uma pessoa para fins relacionados com a saúde), entre outros.

O RGPD prevê regras rigorosas em matéria de tratamento de dados tendo como base o consentimento dos titulares. O objetivo destas regras é assegurar que o titular dos dados percebe para que é que está a dar consentimento. Isto significa que o consentimento deve ser dado de forma livre, específica, informada e inequívoca, por meio de um pedido apresentado numa linguagem simples e clara. O consentimento do titular dos dados deve ser dado através de um ato positivo, por exemplo assinalando uma casa ou assinando um formulário. Sempre que um titular dê consentimento para o tratamento dos seus dados pessoais, só se pode tratar esses dados para as finalidades para as quais o consentimento foi dado. O titular tem de ter possibilidade de retirar o consentimento.

Quanto ao setor da Saúde, e de acordo com o artigo 35º. do (*REGULAMENTO (UE) 2016/ 679 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016*):

"Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*."

Quanto à questão da privacidade e proteção de dados, e de acordo com o artigo 63º. do mesmo regulamento:

“ Os titulares de dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude. Aqui se inclui o seu direito de acederem a dados sobre a sua saúde, por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados. Por conseguinte, cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências. Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. Esse direito não deverá prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o *software*. Todavia, essas considerações não deverão resultar na recusa de prestação de todas as informações ao titular dos dados. Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido.”

2.4.2. Cibersegurança

De modo a garantir a segurança das redes e sistemas de informação, com a proteção e defesa do ciberespaço a nível nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das organizações, nomeadamente, entidades públicas e privadas foi criada a Estratégia Nacional de Segurança do Ciberespaço, relativamente ao intervalo de tempo 2019-2023. Para perceber no que consiste é necessário reter alguns conceitos importantes.

O termo ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação (Monteiro, 2008). A cibersegurança consiste num conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e

correção que têm como objetivo manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem. Já a ciberdefesa prende-se na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço. Por cibercrime entendem-se os factos correspondentes a crimes previstos na lei praticados com recurso a meios tecnológicos, em que estes sejam essenciais à prática do crime em causa (*Resolução do Conselho de Ministros 92/2019, 2019-06-05*).

No plano organizacional, as organizações precisam de adotar metodologias de análise e gestão de risco, considerar a segurança das redes e da informação como um fator de vantagem competitiva e não como um custo, incutir nos seus funcionários os objetivos de uma política de segurança e tomar decisões informadas. No plano sociopolítico são essenciais legisladores informados que produzam boas leis, políticos conscientes do quadro de ameaças e, em caso de concretização, da dimensão do respetivo impacto.

No plano ético são precisos indivíduos e entidades moralizadas e sensibilizadas para as questões da cibersegurança, sendo para isso urgente um plano de educação institucional, com a integração destas temáticas nos vários graus de ensino e nas várias áreas (Santos, 2011).

Quanto à área da saúde, a crescente utilização de meios tecnológicos permite disponibilizar informação aos cidadãos e profissionais de saúde em tempo útil, todavia, aumenta a sua exposição ao risco. O atual nível de complexidade dos sistemas de informação e os riscos que lhes são inerentes exigem a criação e manutenção de meios que permitam a vigilância permanente da informação e da sua otimização, a fim de garantir a adequada segurança dos mesmos. Assim, torna-se fundamental prover a todo o envolvente da saúde de recursos técnicos e logísticos e de competências necessárias à melhor preservação dos meios tecnológicos ao serviço do cidadão, garantindo a proteção da informação e a preservação da qualidade dos recursos que contribuem para a prestação contínua dos serviços de cuidados de saúde. Deve então ser constante a proteção, a vigilância e as avaliações de segurança do sistema nacional de saúde, quer para a minimização do risco de perda de dados, quer como garantia da qualidade dos serviços prestados (*Despacho 8877/2017, 2017-10-09*).

Os Serviços Partilhados do Ministério da Saúde (SPMS), no âmbito dos serviços partilhados de sistemas e tecnologias de informação, tem por missão a cooperação, a partilha de conhecimentos e informação e o desenvolvimento de atividades de prestação

de serviços nas áreas dos sistemas e tecnologias de informação e de comunicação, garantindo a operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde e promovendo a definição e utilização de normas, metodologias e requisitos que garantam a interoperabilidade e interconexão dos sistemas de informação da saúde, entre si e com os sistemas de informação transversais à Administração Pública. Apesar dos SPMS não terem tutela sobre o setor privado e social da saúde, as *guidelines* emitidas são, em grande parte, implementadas por estes setores (Sebastião & Nunes, 2019).

Segundo o modelo de governação estabelecido, relativo à implementação da política de cibersegurança da saúde, foram criadas medidas por forma a promover a articulação entre e nas instituições, com vista a garantir a cibersegurança das redes e dos sistemas de informação de saúde, independentemente da sua localização, em função da conectividade existente. É também necessário acompanhar, apoiar e monitorizar as medidas de proteção, deteção, resposta e recuperação dos recursos críticos do SNS; definir o modelo de avaliação para a gestão e monitorização das medidas de cibersegurança; desenvolver ações de formação, campanhas de sensibilização e desenvolvimento de planos e ações de comunicação para os riscos de cibersegurança. Quanto aos ativos, é crucial fomentar uma gestão segura de *hardware*, *software*, redes e comunicações, promovendo a cooperação entre instituições de saúde, a nível regional e local; promover uma cultura de gestão de risco em matéria de *software* ou do *hardware* e redes e comunicações, designadamente através da incorporação de requisitos de gestão de risco nas aquisições a realizar; definir estratégias de combate à fraude no âmbito da cibersegurança; monitorizar e demonstrar com regularidade os resultados das medidas adotadas (*Despacho 8877/2017, 2017-10-09*).

2.4.3. *Crowdsourcing*

Crowdsourcing é uma combinação de duas palavras: "*crowd*" que significa um grupo de pessoas e "*sourcing*" que significa fonte, ou seja, a origem de algo (Świeszczak & Świeszczak, 2016).

Segundo (Oliveira et al., 2010) *crowdsourcing* é "uma forma de externalizar para um conjunto de pessoas tarefas de criação de ativos intelectuais, muitas vezes colaborativo,

com o objetivo de ter um acesso mais fácil a uma grande variedade de competências e experiências".

Nos últimos anos tem sido utilizado para explorar a inteligência colectiva de trabalhadores qualificados, por exemplo, no crescimento no mercado dos dispositivos móveis, com a expansão das redes sem fios através de organizações públicas e privadas, e na investigação científica, dada a sua capacidade de permitir a captura de dados em custos reduzidos.

No caso do setor da Saúde, a rápida evolução da medicina alarga o fosso entre conhecimento e prática, as tecnologias que permitem o *crowdsourcing* entre pares têm-se tornado cada vez mais comuns. O *crowdsourcing* tem o potencial de ajudar os prestadores de cuidados a colaborarem para resolverem problemas específicos dos pacientes em tempo real (Khare et al., 2016).

Contudo, é necessário explorar as implicações legais e éticas inerentes ao crowdsourcing na área da saúde e para aumentar a consciencialização entre os vários intervenientes antes que a adoção de tecnologias baseadas em multidões se torne mais generalizada. Algumas preocupações são a proteção dos pacientes, a responsabilidade do prestador de cuidados de saúde, recolha dos dados, retenção de dados e publicação anónima multidirecional (Świeszczak & Świeszczak, 2016).

Quanto à privacidade esta pode ser relativa aos dados, ou seja, é necessário perceber se certos dados recebem proteção legal ou se, por exemplo, são classificados como "informações de saúde protegidas"; à relação paciente-prestador que requer confiança, que respeite a confidencialidade de informação que um paciente pode divulgar com segurança a sua história médica, pensamentos e sentimentos privados, e outras informações necessárias para que o prestador possa compreender, diagnosticar, tratar, e ainda consultar os colegas para fornecer o melhor cuidado possível (Sims et al., 2019).

Quanto à segurança é necessário garantir a confiança na segurança da rede de *crowdsourcing*, de modo a proteger e ter a oportunidade de ter discussões intelectuais abertas numa plataforma segura. Para isso devem existir processos institucionais claros para a identificação dos conjuntos dos registos designados na aplicação de crowdsourcing, bem como meios para fornecer acesso ou negação do paciente e revisão institucional destas decisões, dando a oportunidade de refletir sobre quais os aspetos da tomada de decisões clínicas que devem fazer parte do processo de decisão clínica do

paciente registado. Os prestadores estão eticamente empenhados em proteger a informação de saúde, pessoalmente identificável dos pacientes e não arriscarão expô-los mesmo com o custo de inibir o avanço tecnológico (Sims et al., 2019).

Para além das questões sobre a privacidade, anonimato, responsabilidade e retenção de dados, é possível identificar preocupações sobre como esta tecnologia pode ter impacto na segurança dos pacientes e na capacidade dos prestadores de garantirem uma maior qualidade nos cuidados de saúde. Por exemplo, como e quando utilizar a tecnologia e se é apropriado na presença do paciente, se a utilização de aplicações de *crowdsourcing* é vista como uma admissão de incompetência em oposição a um esforço conjunto de especialistas para prestar os melhores cuidados possíveis. Algumas destas interações podem fornecer informação adicional sobre o paciente, aumentar as observações clínicas, informar as recomendações de tratamento, e melhorar os cuidados ao paciente. Os fornecedores necessitam de orientação sobre a melhor forma de gerir a informação, incluindo como incorporar eficazmente a tecnologia nos cuidados ao paciente (Juusola et al., 2016).

2.4.4. Inteligência Artificial

A Inteligência Artificial (IA) caracteriza-se por ser um ramo da ciência da computação, capaz de criar máquinas inteligentes que se podem comportar como um ser humano, pensar como humanos, processar informação, agir por si só ou através de palavras simples e ainda capazes de tomar decisões por si próprios. Com o objetivo final de criar consciência, a IA passa por várias fases de planeamento, raciocínio, análise de dados, previsão dos resultados e atuação em conformidade. Também envolve a utilização de estatísticas, probabilidades e outras ferramentas matemáticas (Kumar, 2020, p. 105).

Algumas tarefas que a IA pode executar são, por exemplo, jogar um jogo de tabuleiro, traduzir línguas, ouvir e responder a instruções humanas, ou identificar padrões específicos em dados visuais, como reconhecimento de rostos a partir de imagens de videovigilância, ou áreas suspeitas em mamografias. Estes algoritmos são construídos através de abordagens e técnicas como o *machine learning, deep learning* e *neural networks* (Carter et al., 2020).

O desenvolvimento da IA tem sofrido algumas mudanças ao longo dos anos, nomeadamente na área da Saúde, conforme o constatado na Figura 3.

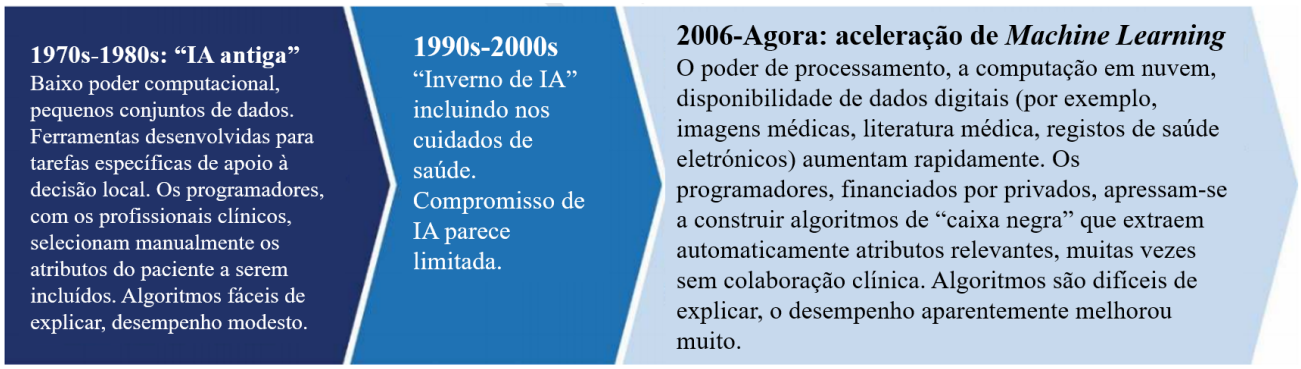


Figura 3 - Mudança entre "IA antiga" e "IA atual". Fonte adaptada: (Carter et al., 2020)

Os primeiros sistemas de apoio à decisão clínica, ou seja, "IA antiga", utilizavam técnicas de sistemas especializados, em que os seres humanos eram necessários para fornecer regras ao sistema e selecionar quais os atributos a incluir no mesmo, daí ser fácil prever o que um algoritmo definido pelo ser humano estava a fazer.

Já a "IA atual" caracteriza-se pela utilização de novas técnicas de aprendizagem de máquinas (especialmente *deep learning*) que permitem um algoritmo para classificar e agrupar dados de forma independente. Ao invés de serem explicitamente programados para prestar atenção a atributos ou variáveis específicas, estes algoritmos têm a capacidade de desenvolver, pela exposição a dados, a capacidade de reconhecer padrões nesses dados. Um objetivo é estabelecido e o algoritmo é exposto a grandes volumes de dados de informação que podem ser mais ou menos heterogéneos: por exemplo, apenas dados de imagem, ou dados de imagem com diagnósticos clínicos.

Ao longo do tempo, o algoritmo, independentemente de instrução humana explícita, aprende a identificar e extrair atributos relevantes dos dados para alcançar o objetivo. A aprendizagem não supervisionada permite graus de liberdade ao algoritmo para agrupar dados com base na semelhança e reduzir a sua dimensão para suportar a decisão. Este processo de redução de dimensão simplifica os dados, por exemplo, selecionar um subconjunto dos dados a processar, ou construir um novo conjunto de características a partir dos dados originais.

A crescente disponibilidade de dados de saúde e o rápido desenvolvimento de grandes métodos analíticos de dados tornou possíveis as recentes aplicações bem-sucedidas da IA

nos cuidados de saúde (Jiang et al., 2017). A utilização da IA na Saúde tem particular relevância no cálculo do risco, na fase diagnóstica, no suporte à decisão clínica, no planeamento de gestão e no incremento da precisão na medicina. Um exemplo relevante é o tratamento do cancro da mama, que é uma área líder para o desenvolvimento da IA.

Com a natureza comercial do mercado de IA na Saúde é importante considerar as implicações éticas, legais e sociais, considerando os valores codificados em algoritmos, a necessidade de avaliar resultados, e questões de enviesamento e transferibilidade, propriedade de dados, confidencialidade e consentimento, e responsabilidade legal, moral e profissional. A Figura 4 resume os condutores para resultados não desejados, os potenciais riscos que requerem mitigação, as possíveis soluções e os resultados desejados.

Figura 4 - Condutores, Riscos, Soluções e Resultados Desejados. Fonte adaptada: (Carter et al., 2020)

Capítulo 3 – Metodologia

3.1. Desenho de investigação

A metodologia de investigação refere-se aos princípios e procedimentos dos processos lógicos de pensamento que são aplicados a uma investigação científica. Assim, a metodologia de investigação é o meio através do qual se alcançam os objetivos de investigação e se obtêm as respostas às questões da investigação. Dentro de uma metodologia de investigação, podem ser utilizados diferentes ferramentas para atingir a questão e os objetivos da investigação (Sutrisna, 2009).

Face ao exposto, a metodologia da investigação foi estruturada em 5 fases principais, como mostra Figura 5.

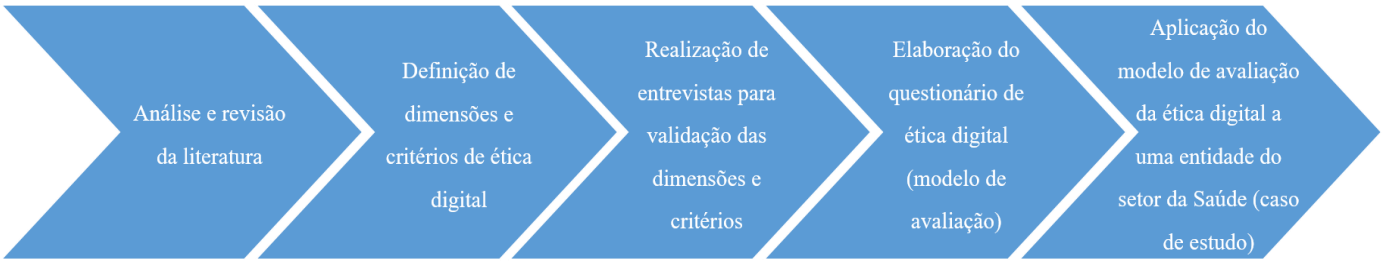


Figura 5 - Fases da investigação

Primeiramente, foi feita uma análise e revisão da literatura, nomeadamente aos aspetos relacionados com a ética digital. Com base na fase anterior, foram definidas as dimensões e critérios mais adequados de ética digital.

Para validar as dimensões e critérios, foram realizadas entrevistas a profissionais do setor da Saúde, que, por serem indivíduos especializados na área, deram o seu contributo com informações que enriqueceram e tornaram mais credível o trabalho realizado.

Com as informações obtidas na análise das entrevistas, foram novamente revistas as dimensões de avaliação da ética digital e proposta uma criação de um modelo de avaliação da ética digital, com a elaboração de um questionário que foi testado posteriormente.

O modelo de avaliação da ética digital foi então aplicado, através do questionário elaborado, a uma entidade do setor da Saúde. Este caso de estudo permitiu aferir uma classificação à entidade quanto ao desempenho da ética digital.

3.2. Objetivos de investigação

Antes de serem definidos os objetivos gerais para uma dissertação é pertinente identificar uma questão ou um problema dentro de uma determinada área de atuação. A questão da investigação é um passo particularmente significativo na investigação, uma vez que reduz o objetivo e a finalidade da investigação a áreas específicas que o estudo irá abordar. Além disso, é vital na orientação da escolha da metodologia, métodos, amostra, tamanho da amostra, instrumento de recolha de dados e técnicas de análise de dados (Doody & Bailey, 2016).

Deste modo, e como já se referiu anteriormente, a questão de investigação proposta para esta dissertação foi a seguinte: "Quais os critérios adequados para avaliar a ética digital no setor da Saúde?"

Para isso os objetivos estabelecidos foram:

- Analisar o Estado da Arte da ética digital;
    - Definir o seu significado e como pode ser aplicado.
- Estabelecer dimensões de análise da ética digital;
    - Identificar as dimensões principais antes da análise qualitativa.
- Criar um modelo constituído por dimensões de análise e critérios específicos de avaliação da ética digital, aplicável ao setor da Saúde;
    - Verificar se as dimensões são apropriadas para o caso de estudo em específico.
    - Definir os critérios necessários para a construção do modelo.
- Validar o modelo de avaliação da ética digital através de uma parceria com uma entidade do setor da Saúde, obtendo um índice de classificação.
    - Verificar se os critérios definidos são adequados para avaliar o desempenho da entidade quanto à ética digital.

Capítulo 4 – Conceção do Modelo de Avaliação da Ética Digital

4.1. Estruturação da informação

O capítulo 4 tem como principal foco a conceção do modelo de avaliação da ética digital, através da análise dos resultados da fase qualitativa da investigação.

Com o objetivo de verificar as dimensões da ética digital, através do caso de estudo na área da Saúde, foi necessário realizar entrevistas a profissionais do setor, de modo a validar e confirmar a adequabilidade das dimensões e critérios de avaliação.

Para isso, foram escolhidos cinco profissionais que trabalham em instituições distintas, na área da Saúde, e com tipos diferentes de funções:

- 1 profissional de gestão de sistemas de informação de Hospital
- 1 profissional com função administrativa de Hospital
- 1 médico de Centro de Saúde
- 1 enfermeiro de Hospital
- 1 docente universitário na área da Bioética

4.2. Validação das dimensões e critérios

4.2.1. Guião da Entrevista

As entrevistas foram realizadas em reunião *online*, através da aplicação *Zoom*, com a duração média de 50 minutos, e tiveram como base o seguinte guião:

1. Saudações iniciais.

2. Apresentar o tema de Investigação "Analisar o Estado da Arte da ética digital e concluir quais são os critérios mais apropriados na avaliação da ética digital nos serviços de Saúde".

3. Explicar os objetivos da Entrevista:

- Estabelecer dimensões de análise da ética digital;
- Criar e validar um modelo constituído por dimensões de análise e critérios específicos de avaliação da ética digital, aplicável ao setor da Saúde;

4. Identificar as funções que o entrevistado executa no seu local de trabalho.

- Que profissão e que tipo de funções executa no seu local de trabalho?

5. Relacionar a função do entrevistado com a utilização de plataformas digitais/sistemas de informação no quotidiano da sua profissão.

- De acordo com o tipo de função que executa no dia-a-dia da sua profissão, que tipo de tecnologia utiliza e para que utiliza?

6. Perceber se o entrevistado consegue identificar o desempenho da ética digital na utilização de plataformas digitais/sistemas de informação nas suas funções.

- Ao utilizar a tecnologia consegue identificar ou tem alguma preocupação com o desempenho da ética digital?

7. Questionar acerca das dimensões da ética digital no setor da Saúde.

- Quanto às dimensões da ética digital na área da Saúde, quais os aspetos principais que tem em conta ao utilizar a tecnologia na sua profissão?

8. Verificar quais os critérios mais apropriados para avaliar o desempenho da ética digital na prestação dos serviços de Saúde, mais concretamente, na função do entrevistado.

- De acordo com as dimensões identificadas anteriormente, quais os critérios que considera apropriados para avaliar o desempenho da ética digital na área da Saúde, no seu tipo de funções?

9. Agradecimentos finais.

4.2.2. Técnica de análise das Entrevistas

A análise das entrevistas tiveram em conta o tipo de entrevista que as classificam. Neste caso optou-se por uma entrevista semiestruturada, ou seja, que combina perguntas fechadas e abertas, no qual o entrevistado tem a liberdade de se posicionar favorável ou não sobre o tema, sem se prender à pergunta formulada (Nunes, 2007).

Nas questões abertas pretende-se dar mais profundidade às reflexões, deixando o entrevistado falar livremente sobre o tema. É uma forma de poder explorar mais amplamente uma questão, atendendo principalmente a finalidades exploratórias, utilizado detalhar e formular com mais precisão os conceitos relacionados (Boni & Quaresma, 2005).

Depois de feitas e transcritas as entrevistas, foi necessário analisá-las recorrendo visualmente aos mapas conceituais, através do *software* Leximancer. É uma ferramenta analítica de texto que tem como objetivo analisar o conteúdo de um conjunto de documentos textuais e exibir visualmente a informação extraída. A visualização da informação é apresentada através de um mapa conceptual que representa os principais conceitos que se encontram no texto, bem como informações sobre a forma como estão

relacionados. É também um meio de resumir, indexar, quantificar e exibir a estrutura conceptual do texto, e um meio de utilizar esta informação para explorar ideias e relações interessantes (Leximancer Pty Ltd, 2019).

4.2.3. Conclusões das entrevistas

Foram então identificados os pontos-chave e agrupados os temas mais preponderantes por questão, de modo a poder identificar as dimensões e critérios de avaliação da Ética digital. De referir, que se encontram no Anexo 1 mapas conceptuais complementares às questões apresentadas.

1. Que profissão e que tipo de funções executa no seu local de trabalho?

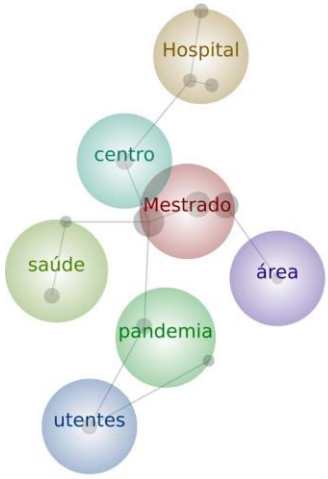


Figura 6 – Mapa Conceptual da Questão 1

De acordo com as necessidades identificadas anteriormente foram escolhidos profissionais relacionados com a **área** de **Saúde** com diferentes tipos de funções, como as áreas de **gestão** de sistemas de **informação**, **apoio** administrativo, medicina, enfermagem e educação. Além disso, foram também escolhidos profissionais diferentes locais de **trabalho**, como é o caso de **Hospital** (público e privado), **Centro** de **Saúde** e Faculdade. É importante referir algumas palavras que sobressaem no mapa conceptual da Figura 6, como é o caso de "**Mestrado**", visto que para alguns tipos de funções os profissionais têm especialidades nas suas áreas; de "**pandemia**" pelo facto de, no momento das entrevistas, os profissionais lidarem diariamente com uma pandemia,

derivado ao novo coronavírus SARS-CoV-2; de "**utentes**" por ser maioritariamente o foco da profissão dos entrevistados.

2. De acordo com o tipo de função que executa no dia-a-dia da sua profissão, que tecnologia utiliza e para que utiliza?

Figura 7 – Mapa Conceptual da Questão 2

Como se pode visualizar no mapa conceptual da Figura 7, a utilização da **tecnologia** no quotidiano das funções dos entrevistados é maioritariamente feita através dos **sistemas** de informação de **saúde** próprios das **instituições** onde exercem a sua função. Na maior parte das respostas concluem que o digital é relevante em vários aspetos no **âmbito** dos **serviços** e prestação de **cuidados**, nomeadamente na relação com o cliente/utente; na recolha, identificação, registo, **acesso** e tratamento dos **dados** dos pacientes; na extração de indicadores para auxílio do diagnóstico e gestão da terapêutica; no agendamento das consultas; na otimização do trabalho e das tarefas, e no aumento dos conhecimentos.

Outras atividades nas quais a tecnologia é fundamental são a implementação de sistemas, equipamentos e dispositivos de diagnóstico médico (ex: ressonância magnética, sistemas de monitorização, robotização das cirurgias, entre outros), com o objetivo de mudança para tecnologias mais avançadas; o planeamento dos investimentos e nos contratos com fornecedores; a simulação do comportamento administrativo, técnico e médico; a definição de *workflows*, utilizando aplicações *web*, para otimizar o atendimento multicanal, de modo a transmitir informação transversal e centralizada; e a gestão otimizada do *stock* de produtos hospitalares.

Adicionalmente, a utilização da tecnologia está também associada ao trabalho não assistencial, ou seja, na visualização e extração de indicadores; na verificação do cumprimento dos objetivos atribuídos a cada utente, por exemplo, em indicadores de controlo da diabetes, adesão à terapêutica, realização de rastreios, etc; na gestão do processo do utente, quando é necessária a articulação com outras instituições da saúde, com a partilha de informações pessoais e clínicas; na utilização de ferramentas de apoio à decisão clínica; no acesso à informação atualizada com origem na comunidade científica, com a partilha de *guidelines*, protocolos e estudos, que permitem tomar decisões informadas e com a evidência científica recente.

3. Ao utilizar a tecnologia consegue identificar ou tem alguma preocupação com o desempenho da ética digital?

Figura 8 – Mapa Conceptual da Questão 3

Ao analisar as respostas, foram agrupados vários tipos de preocupações relativas ao desempenho da ética digital na área da **saúde**, em relação à utilização dos **dados**, dos **sistemas**, da **segurança**, da **partilha** de informação e da **formação** (ver Figura 8).

Quanto à utilização dos **dados**, foi abordada a importância do cumprimento do **RGPD**, com o **consentimento informado** na **cedência de dados** para atos médicos, de modo a ser possível obter um plano terapêutico, para que a equipa de profissionais de saúde possa identificar os factos, estabelecer associações e causalidades, determinar o diagnóstico e,

de acordo com o mesmo, estabelecer um plano de intervenção, que confere ao paciente a informação necessária e os factos relevantes que lhe permita fazer uma escolha livre e esclarecida, sem coação externa. Para isto é necessário o **respeito pela autonomia**, ou seja, quem confere o acesso é o titular dos dados e, neste âmbito, quem tem a **custódia dos dados** são as instituições. Os processos clínicos são propriedade de quem tem a custódia da informação, mas os dados dos processos clínicos são do titular dos dados, o cidadão, e portanto, do ponto de vista **ético**, ninguém pode aceder aos dados sem a sua autorização, com a exceção da possibilidade de a lei definir limites ao direito de acesso.

Outras preocupações relativas aos dados são a alimentação/introdução dos mesmos nos diversos pontos de cuidados; a garantia de que os dados que foram inseridos nas fichas dos utentes estão corretos; se os utentes são alertados para disponibilizar os seus contactos telefónicos e eletrónicos para futuras interações; a utilização de *benchmarking* de dados clínicos, ao nível da imagiologia/radiologia (exames com base na radiação), na qual se coloca a questão do nível de **anonimização** de dados que se tem no *benchmarking*, ou seja, é verificada uma anonimização a nível do **paciente** mas a nível institucional consegue ter vários níveis de segmentação de passagem de informação; a questão do nível de **privacidade** com que se vai fornecer para a plataforma os dados, pois quanto mais agregados forem menos *outcomes* se conseguem obter, dificultando a análise e a estatística sobre múltiplas variáveis; ao introduzir os dados dos utentes, o facto de poder surgir um erro de **identificação**, tendo sempre que se garantir a identidade da pessoa, não só pelo nome mas também por outro tipo de atributos, daí o nome não pode ser um campo de registo único; na **gestão** da **qualidade** dos dados, ao realizar **auditorias** aos processos, com o objetivo de perceber quem teve **acesso** ao processo de determinados pacientes; a transversalidade de passagem de informação do processo clínico do paciente a todos os profissionais de saúde, que pode ser importante nalgumas situações críticas de saúde (urgências, internamento, exames complementares de diagnóstico), mas que tem como risco a fuga de informação.

Relativamente aos **sistemas** de informação em si, existem preocupações a nível da capacidade que os mesmos têm em estar minimamente preparados para obrigar a **reduzir o erro**; no caso dos fabricantes que, ao desenvolverem o sistema, não conseguem identificar os aspetos necessários para aquele sistema, continuando a sair para o mercado sem **integrações** feitas; as **certificações** têm custos elevados e, em alguns casos, não

cumprem os *standards* universais; a informação não é passada corretamente, logo causa problemas na gestão da mesma.

No que respeita à **segurança** nos sistemas de informação questiona-se o âmbito da robustez técnica do sistema, no ponto de vista da tecnologia, da forma como o sistema está desenhado para impedir os ***hackers*** de poderem ter acesso; as questões da salvaguarda da privacidade e confidencialidade do próprio sistema, na conceção dos ambientes do *software*, que deveriam garantir várias camadas de segurança e que os dados armazenados são protegidos de forma a oferecer segurança ao profissional e ao utente.

Quanto à **partilha de informação** entre várias entidades do setor da Saúde, em particular entre os cuidados primários e hospitalares, bem como entre centros hospitalares de diferentes regiões e hospitais públicos e privados, a falta de interoperabilidade entre as diversas plataformas dificulta o acesso a informação clínica relevante para a continuidade de prestação de cuidados de saúde, nomeadamente o acesso ao histórico de registos clínicos de episódios anteriores

Por outro lado, a partilha desta informação sensível de um utente/agregado familiar pode ser indevidamente utilizada, extraviada, roubada ou acedida por motivos que não sejam os melhores ou os mais corretos, e nesse aspeto, é importante a implementação de regras, controlos e mecanismos de segurança na transmissão da informação, bem como a obrigatoriedade da utilização de ***passwords*** no acesso.

Por fim, quanto à **formação** na utilização da tecnologia de informação é imperativo consciencializar o utilizador para o cumprimento dos princípios da ética e dos valores que estão subjacentes ao sistema e aos próprios cuidados de saúde, de modo a que os profissionais adquiram maior **literacia informática** e estejam capacitados para otimizar os sistemas na potenciação da tecnologia, para obter resultados no ponto de vista técnico e científico e no melhor uso de programar e ter resultados que permitem planear e replanear novas medidas de acordo com aquilo que são os cuidados prestados.

4. Quanto às dimensões da ética digital na área da Saúde, quais os aspetos principais que tem em conta ao utilizar a tecnologia na sua profissão?

Figura 9 – Mapa Conceptual da Questão 4

As dimensões principais da ética digital identificadas na análise de resposta, que estão destacadas no mapa conceptual da Figura 9, foram: a **Inteligência Artificial**, a **Privacidade** e Proteção de **Dados**, com o **RGPD**, e Segurança.

Quanto à **Inteligência Artificial**, o facto de permitir mediar um processo de **tomada de decisão clínica**, com base em toda a **informação** relevante, conduz à tomada de decisão mas não substitui a decisão clínica do profissional, o que é fundamental para que todas as variáveis sejam equacionadas, com segurança. Traz investigação em si para poder decidir, na construção de **algoritmos de decisão**, de modo a otimizar os processos de tomada de decisão clínica, de chegada ao diagnóstico, à escolha e à seleção das intervenções mais adequadas e de acordo com a prática baseada na evidência, o que existe e pode ser mobilizado naquela situação específica. Dão segurança ao utilizador e aos beneficiários de cuidados, em que o raciocínio é mediado não só pelo profissional ou na equipa, mas também por algo mais **racional**, onde estão espelhadas as mais recentes **inovações**.

No caso dos **cuidados** de saúde primários não existe ainda propriamente o que se pode considerar de Inteligência Artificial, visto que são apenas utilizados *scores* (pontuações), algoritmos básicos e *websites* que conseguem **aceder** e ir através de dados de sintomatologia obter seguimento ou o passo mais correto, mas que acabam por ser processos que não são propriamente autónomos, ou seja, em que obrigam o profissional

a **inserir** manualmente os dados e, de acordo com esses dados (e com os algoritmos que estão na base), a máquina sugere qual o próximo passo mais lógico.

Quanto à **Privacidade e Proteção de Dados**, são referidos os aspetos relacionados com o **RGPD;** a **finalidade** e **custódia** dos dados; a **confidencialidade**, privacidade e **respeito pela autonomia** do titular dos dados, ou seja, do cidadão e do que o profissional de saúde é capaz de explicar no âmbito daquilo que é o consentimento informado para a partilha dos dados em saúde; o saber no sistema de informação, **quem tem acesso à informação, para que é que vai ser utilizada, como vai ser guardada**, e se alguém tiver acesso, o titular é informado de que tal indivíduo acedeu e por que razão é que teve acesso se não houve autorização. Daí ser necessária a capacitação dos utilizadores saberem quem, como, quando, porquê, que utilizam os dados, de modo a colher dados no âmbito do processo de cuidados assistenciais, prestação de cuidados de saúde, acompanhamento do plano terapêutico, instituição de medidas profiláticas, preventivas, curativas ou mitigação de efeitos secundários, ou seja, aos vários níveis de intervenção de saúde, mas que são exclusivos unicamente para este âmbito.

Também é importante referir a **privacidade** na utilização dos dados no processo clínico, na **investigação**, como por exemplo na extração de indicadores de produtividade mobilizados para as plataformas de gestão, pelo cidadão, de acordo com a sua viabilidade. Além disso, foram aboradadas as questões de intimidade, participação ativa, transição segura de dados e partilha de informação, através de ferramentas otimizadas, e a segurança na informação do *background* do paciente, à situação atual, aos pendentes e ao que está planeado.

5. De acordo com as dimensões identificadas anteriormente, quais os critérios que considera apropriados para avaliar o desempenho da ética digital na área da Saúde, no seu tipo de funções?

Figura 10 – Mapa Conceptual da Questão 5

Para identificar os critérios apropriados para avaliar o desempenho da ética digital na área da Saúde, foram tidos em conta os conceitos que se encontram na Figura 10 e agrupadas as dimensões descritas anteriormente.

Quanto à **Privacidade e Proteção de Dados**, os critérios principais identificados são o cumprimento da **legislação** que está em vigor, que regula os sistemas que utilizem **dados** clínicos e que está de acordo com as normas da Comissão Nacional de Proteção de Dados (CNPD); a realização de **auditorias** para determinar se há o cumprimento das normas; a criação de ***Data Protection Officer*** (DPO) nas instituições, que é um profissional capacitado (idealmente com formação em ética) em formar, aos vários níveis da decisão de uma instituição, para as questões éticas, quer seja no âmbito de uma decisão mais política, seja no âmbito da decisão mais operacional dos sistemas de informação em saúde ou da ética assistencial, tendo em conta o cumprimento legal dos princípios de confidencialidade e privacidade, e também os princípios de guarda, titularidade, custódia e destruição de dados. Além disso deve-se considerar todos os aspetos relacionados com os processos de **anonimização** e pseudo anonimização no acesso aos dados, em que uma solução passa pelos **utentes estarem codificados por número de utentes**, para que quando o profissional aceda aos dados do utente não tenha toda a informação visível (nome, data de nascimento, morada, telefones, NIF, número da Segurança Social, etc.), em que toda a informação que está descrita (doença, medicação, exames, etc.) está

unicamente relacionado com aquele número de utente. Daí a necessidade de separar os dados pessoais do utente dos dados de saúde, identificando o paciente apenas pelo número de utente/número do processo hospitalar/número da ficha do utente, em que para aceder tem que ter *password*, senão bloqueia. Além disso, no quadro de identificação dos pacientes deveria haver uma opção para ser colocada a **autorização para fornecer os dados**.

Relativamente à **Segurança**, considera-se importante ter ***standards*** de segurança de rede claros no armazenamento e custódia de dados; utilizar tecnologia de máquina virtual, ou seja, ***VMware,*** em maior parte dos consultórios, através da virtualização do *desktop*, que permite a manutenção dos terminais, **atualizações** mais rápidas, por exemplo, na última versão de segurança do *Windows*, e que permite ainda às áreas administrativa e de suporte trabalhar remotamente, de forma segura; a entrada com **autenticação de *logins*, ou seja, utilizador e *passwords* únicos** para cada utilizador (domínio de privacidade); fazer ***logoff*** cada vez que se acaba de utilizar a sessão e desligar o computador; ter leitores de RFID (identificação por radiofrequência), através de terminais que abrem na sessão e no ecrã que está a ser utilizado, trazendo ganhos de produtividade e *engagement*; os servidores têm que estar blindados, para não sofrerem ataques, senão há perda de credibilidade.

Existem ainda algumas normas que se referem à **Cibersegurança**, ou seja, que tentam proteger os dados dos profissionais para que pessoas alheias à saúde não consigam entrar nos sistemas, e através disso roubar os seus dados e os dados dos utentes. No caso de necessidade de trabalho de investigação ou de aceder à informação de um utente para divulgar para um tribunal ou assistente social, as comissões de ética possuem uma série de protocolos que têm de seguir e autorizações que têm de solicitar para que seja autorizada, cedida e consultada a informação para esses fins. É necessário um maior controlo de quem acede à informação dos utentes nas plataformas, em que, a **entidade reguladora**, que supervisiona os Agrupamentos de Centros de Saúde (ACES), as Administrações Regionais de Saúde (ARS), os SPMS, entre outros, possa facilmente verificar, por exemplo, e escolhendo aleatoriamente "x" número de pessoas, quem nos últimos tempos acedeu à informação daquele utente e identificar se todos os acessos foram a partir de um centro de saúde, com o *login* de um profissional de saúde. Se o utente tem a possibilidade de receber uma **mensagem de alerta** de quem está a aceder aos seus dados, eventualmente, a entidade reguladora tem a capacidade de controlar quem é que

acede aos dados, de onde, e criar avisos/alertas automáticos para que, se esse acesso for feito fora do sistema de saúde, despolete um alerta e ative um ***lock down*** dessa informação. Ou seja, tentar controlar de melhor forma quem é que consegue aceder à informação, através de um reforço de *passwords* e procedimentos, em que, por exemplo, para aceder ou para fazer o link entre o sistema do centro de saúde e a plataforma hospitalar faria sentido nesse procedimento o profissional inserir a *password* de verificação, para que não haja um acesso externo indevido ao sistema. Portanto, criar um passo intermédio que requeira **autenticação, identificação de quem acede ou não**, e **auditorias** por técnicos especializados na área que controlem e testem frequentemente o acesso às informações para detetar eventuais falhas. Por exemplo, auditorias num centro de saúde, uma vez por ano ou de seis em seis meses, em que se avalie os acessos a informações de utentes, de forma a detetar se há acessos indevidos e, caso ocorram fora do horário normal de trabalho, identificar as razões que originaram esses acessos.

Outro exemplo é haver um ***shut down timer***, ou seja, se o programa estiver aberto mais de "x" tempo sem ser utilizado, ele grava e fecha automaticamente, para prevenir que outra pessoa aceda à sessão e ao *login* que estava aberto. Tentar impedir que não profissionais de saúde consigam aceder a esta informação, ou seja, criar mais **passos de verificação ou mais regras**, para que apenas os profissionais de saúde que tenham as suas *passwords* e os seus códigos consigam aceder a esta informação, dentro do horário de funcionamento das suas unidades e dentro daquilo que lhes diz respeito (ex: utentes que não estão registados num determinado centro de saúde, fora situações esporádicas).

Para isto resultar, é necessário ser dada **formação relacionada com a Cibersegurança** aos profissionais de saúde, de modo a prevenir situações de *hacking* ou roubo de informação, com a construção de *passwords* fortes, não colocar *passwords* em papel em objetos ou sítios públicos, com mais passos de verificação para garantir que só os profissionais conseguem aceder aos dados efetivamente, nas alturas e nos utentes adequados a que dizem respeito.

Quanto ao ***Crowdsourcing***, devem existir critérios específicos de **divulgar de forma anonimizada** exames clínicos com outros profissionais de saúde fora da instituição, especialistas da área "x" (ex: partilha de imagens através dos sistemas dos próprios hospitais, através de um link, com registo do médico). A sua utilização traz benefício para o utente mas tem que ser feito de **forma auditável, com consentimento do utente.** No caso dos estudos clínicos de investigação, têm que ser autorizados pela cedência de dados.

Em relação à **Inteligência Artificial**, é necessário haver **certificações** na implementação de dispositivos médicos, plataformas e *softwares*; escolher **parceiros tecnológicos idóneos**, que estejam devidamente certificados e regulados no mercado europeu; a não transição de dados para fora das instituições; a passagem de informação ser feita de forma **anonimizada** e identificada para um parceiro referenciado.

Outros critérios importantes, realtivos à qualidade dos sistemas de informação, são a criação de um sistema de raiz através da **construção de uma arquitetura de modelo de dados por parte de todos os intervenientes na sua utilização** (profissionais de saúde); conseguir demonstrar ou evidenciar que internamente as organizações fazem **auditorias**, em que haja cumprimentos dos códigos deontológicos, rigor da informação, bom comportamento humano dos profissionais na passagem da informação para fora das instituições; antes do *software* ser desenvolvido deve respeitar e garantir a qualidade no âmbito da ética digital (antes de ser comercializado na prestação direta de cuidados); quando há uma **atualização de *software* ou um novo programa**, a entidade local dinamiza formações para auxiliar no funcionamento dos sistemas.

Deste modo, às dimensões definidas na revisão de literatura, tais como, a Privacidade e Proteção de Dados, a Cibersegurança, o *Crowdsourcing* e a Inteligência Artificial, foi acrescentada a dimensão Qualidade dos Sistemas, através das análises das entrevistas realizadas.

4.3. Construção do Modelo de Avaliação da Ética Digital

As dimensões definidas anteriormente (Privacidade e Proteção de Dados, Cibersegurança, Crowdsourcing, Inteligência Artificial e Qualidade dos Sistemas) serviram de suporte para a criação do modelo de avaliação da ética digital, o qual foi complementado com a revisão da literatura e as entrevistas realizadas. A Tabela 1 apresenta as dimensões e os critérios associados enumerados, para a aplicação do questionário.

Tabela 1 - Modelo de Avaliação da Ética Digital

DIMENSÕES	CRITÉRIOS
1. Privacidade e Proteção de Dados	1.1. Cumprir a legislação relativa ao RGPD;
	1.2. Realizar auditorias;
	1.3. Criação de um DPO;
	1.4. Codificação por número de utente;
	1.5. Autorização dos utentes para fornecer dados;
	1.6. Facultar o acesso e possibilitar ao titular aceder diretamente aos seus dados pessoais e clínicos.
2. Cibersegurança	2.1. Cumprir os *standards* de segurança;
	2.2. Utilizar tecnologia *Vmware;*
	2.3. Autenticação de *logins* únicos para cada sessão;
	2.4. Fazer *logoff* para terminar sessão;
	2.5. Implementar *shut down timer* após longo tempo de sessão aberta e não utilizada;
	2.6. Criação de terminais com leitores de *RFID;*
	2.7. Manutenção e atualizações de *softwares* de segurança;
	2.8. Receber alertas e *lock down* quando há acesso indevido;
	2.9. Criar mais passos de verificação da identidade;
	2.10. Realizar auditorias;
	2.11. Dar formação de cibersegurança a profissionais de saúde.
3. *Crowdsourcing*	3.1. Ter processos institucionais claros para a identificação dos conjuntos de registos designados na aplicação de *crowdsourcing*;
	3.2. Anonimizar dados/informação na divulgação dos mesmos;
	3.3. Consentimento do utente para ceder os dados;
	3.4. Autenticação dos profissionais na partilha de registos;
	3.5. Realizar auditorias.
4. Inteligência Artificial	4.1. Cumprir os regulamentos e legislação;
	4.2. Certificações na implementação de dispositivos médicos, plataformas e *softwares;*
	4.3. Escolher parceiros tecnológicos idóneos, que estejam devidamente certificados e regulados no mercado europeu;

	4.4. Anonimizar informação que passa para os parceiros.
5. Qualidade dos Sistemas	5.1. Criar um sistema de informação de raiz através da construção de uma arquitetura de modelo de dados por parte de todos os intervenientes na sua utilização;
	5.2. Demonstrar ou evidenciar que internamente as organizações fazem auditorias, em que haja cumprimentos dos códigos deontológicos, rigor da informação, bom comportamento humano dos profissionais na passagem da informação para fora das instituições;
	5.3. Antes do *software* ser desenvolvido deve respeitar e garantir a qualidade no âmbito da ética digital;
	5.4. Quando há uma atualização de *software* ou um novo programa, a entidade local fornecer formação para ajudar no funcionamento dos sistemas.

De seguida, irá ser feita a avaliação de cada critério, através do caso de estudo numa entidade do setor da Saúde. A classificação dos critérios vai ser realizada segundo a seguinte escala, em que quanto maior a pontuação maior o empenho quanto à ética digital:

0 – Nenhum

1 – Débil

2 – Suficiente

3 – Abrangente

4 – Total

O facto de ser atribuída uma classificação para os critérios permite avaliar o critério, por média aritmética, bem como a dimensão e estabelecer um índice global de ética digital, que é um índice final de todas as dimensões. Isto permite fazer estudos comparativos com outras entidades, avaliar onde existem oportunidades de melhoria, através de boas práticas, e definir recomendações para progredir quanto à ética digital. Salienta-se que, devido ao modelo ainda não ter sido testado com várias entidades, não é possível fazer ponderação, ou seja, definir se um determinado critério é comparativamente mais importante que outro.

Capítulo 5 – Caso de Estudo

5.1. Aplicação do modelo

Foi aplicado o seguinte questionário a um profissional da área de Saúde, com o objetivo de ser testado o modelo de avaliação da ética digital criado no ponto anterior, em que para cada pergunta é contemplado o respetivo critério.

1) Aspetos gerais

a. Qual o tipo de instituição de Saúde em que trabalha?

R: Um hospital público com 277 camas de internamento, 6 blocos operatórios, 35 gabinetes de consulta e 10 salas de parto.

b. Em que área da Saúde se inclui a sua profissão?

R: Área da gestão.

2) Privacidade e Proteção de Dados

a. Quanto ao RGPD, são cumpridas, a nível institucional, as regras relativas ao mesmo, no âmbito da Saúde?

				X
0 – Nenhum	1 – Débil	2 – Suficiente	3 – Abrangente	4 – Total

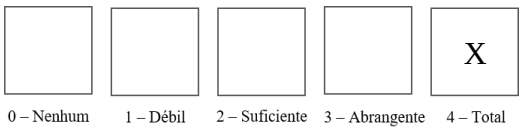
Observações: _____

b. São realizadas auditorias no âmbito da privacidade e da proteção de dados? Se sim, de que tipo e com que frequência?

			X	
0 – Nenhum	1 – Débil	2 – Suficiente	3 – Abrangente	4 – Total

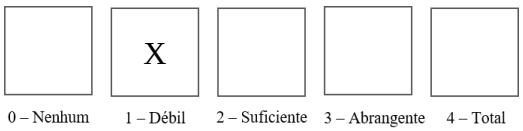
Observações: Tanto internas como externas. Anualmente.

c. A instituição tem implementado um DPO (Data Protection Officer)?



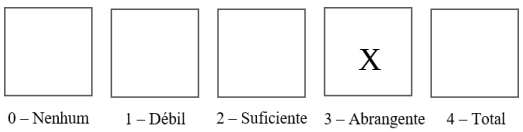
Observações: Existe uma equipa dedicada à área legal e outra à área operacional de sistemas de informação, sendo nesta designada um CISO (Chief Information Security Officer).

d. Existe uma codificação dos dados do utente por número de utente?



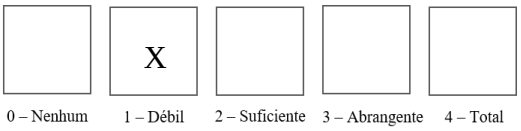
Observações: A informação do utente tem níveis de acesso, administrativo e clínico, sendo atribuídos vários perfis (médico, enfermeiro, pessoal administrativo e outros profissionais de saúde de várias áreas, como por exemplo, farmacêutico, psicólogo, nutricionista, etc.). Há controlos de acesso em função da necessidade de cada profissional.

e. É pedido aos utentes uma autorização para fornecer os seus dados?



Observações: Na admissão e em atos programados (informação genérica). No caso da informação clínica para outras entidades é autorizada caso a caso pelo utente (por exemplo, as seguradoras).

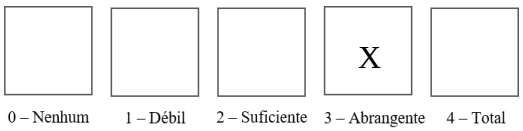
f. É facultado o acesso e possibilitado ao titular aceder diretamente aos seus dados pessoais e/ou clínicos?



Observações: O acesso à informação é sempre por pedido do próprio utente e a informação é cedida consoante o tipo de dados. Os dados pessoais são cedidos por pessoal administrativo e os clínicos por pessoal médico.

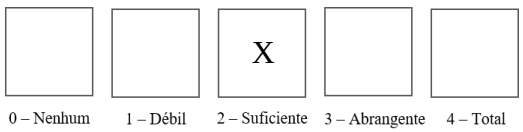
3) Cibersegurança

a. São cumpridos os *standards* de segurança?



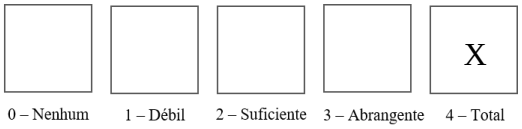
Observações: Através da segurança física no acesso ao *data center* e da segurança dos sistemas de informação pelos *firewalls*, sistemas de *data protection*, entre outros.

b. É utilizada a tecnologia *Vmware*? Se sim, em quê?



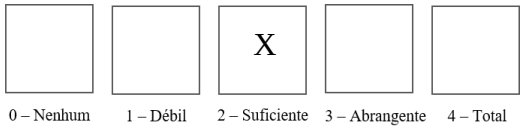
Observações: Na manutenção dos postos de trabalho, com o acesso ao *desktop* pela equipa de *helpdesk* de informática.

c. Existe autenticação de *logins* únicos para cada sessão/utilizador?



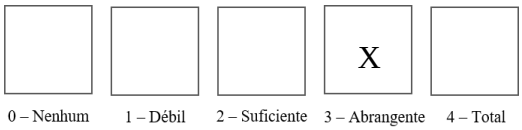
Observações: Cada funcionário tem um *login* único, em que a *password* é alterada mensalmente. Os médicos têm ainda uma utilização obrigatória do cartão da Ordem dos Médicos e *passwords* para validação de prescrições.

d. É utilizado o *logoff* para terminar sessão?



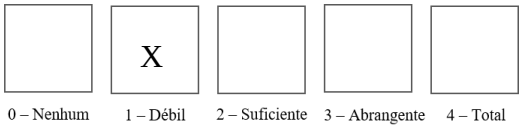
Observações: É incentivada a implementação das medidas de segurança, tais como *logoff* das sessões e a não partilha de *passwords*.

e. É implementado um *shut down timer* após longo tempo de sessão aberta e não utilizada?



Observações: Existem imagens padronizadas de *desktop*, em que há um limite de tempo para fechos das sessões sem atividade.

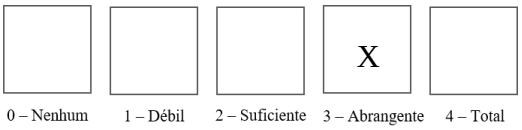
f. Existem terminais com leitores de *RFID*?



Observações: Apenas no caso dos dispositivos móveis como os PDA (Personal Digital Assistants), em que a sessão é aberta com a leitura de *QR Code*, que está no cartão de

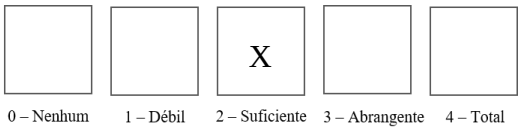
identificação do profissional, que identifica o utilizador automaticamente e obriga a colocar a sua *password*.

g. Existe manutenção e atualização dos *softwares* de segurança?



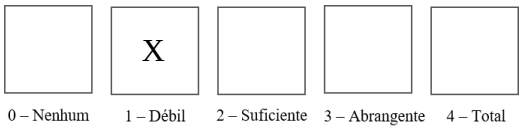
Observações: Existem rotinas diárias e mecanismos de deteção de riscos que geram alertas automáticos.

h. São recebidos alertas e é feito um *lock down* dos sistemas quando há acesso indevido?



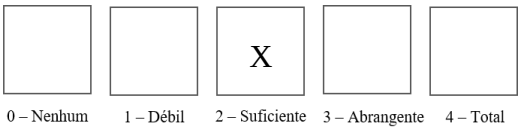
Observações: Quando há deteções existe uma plataforma de segurança que alerta a equipa responsável dos riscos tipificados. A alguns fatores de risco estão associadas ações de acesso à informação e de colocação da informação em quarentena, portanto é variável.

i. São implementados mais passos de verificação da identidade?



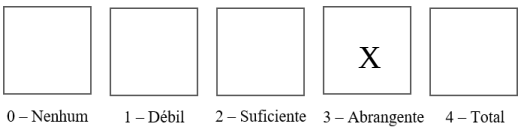
Observações: Está em desenvolvimento a criação de regras que impeçam o acesso furtuito à informação. Por exemplo, só se o utente tiver um ato marcado é que o médico da respetiva especialidade pode, dentro de um limite temporal, aceder a essa informação. Outro exemplo significativo é o reforço de proteção de acesso de informação a figuras públicas ou casos mediáticos.

j. São realizadas auditorias no âmbito da segurança? Se sim, de que tipo e com que frequência?



Observações: Internas permanentemente e externas anualmente.

k. É dada formação de cibersegurança aos profissionais de saúde? Se sim, em que altura e com que frequência?



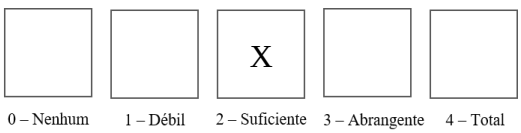
Observações: Há um programa de *e-learning* com módulo obrigatório de cibersegurança para todos os utilizadores dos sistemas de informação. É dada na admissão do funcionário e com revisão anual.

4) *Crowdsourcing*

a. É utilizado o *Crowdsourcing*?

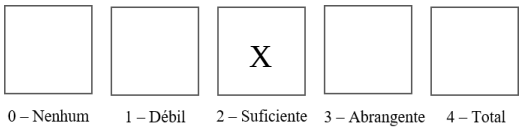
R: Sim, existem sessões clínicas presenciais com a abordagem de temas específicos com interesses transversais e está em preparação uma plataforma de partilha de conhecimento e desenvolvimento, tanto ao nível individual como ao nível da interação em equipa.

b. Têm processos institucionais claros para o funcionamento do *crowdsourcing* na instituição?



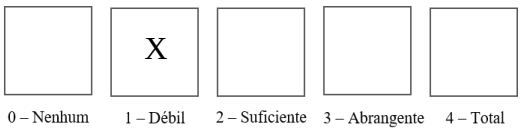
Observações: Existe uma comissão de ética que avalia e dá parecer sobre os estudos observacionais, os ensaios clínicos e os ensaios estatísticos.

c. É garantida a anonimização dos dados/informação dos utentes na divulgação dos mesmos?



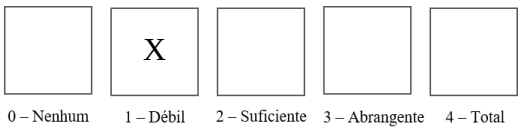
Observações: Existem regras que impõem a anonimização dos dados referentes a um utente com uma determinada patologia, com interesse na investigação/divulgação.

d. Existe consentimento do utente para ceder os seus dados?



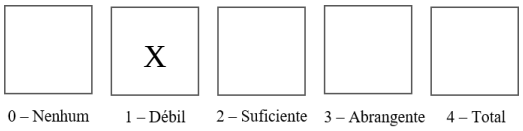
Observações: No caso dos ensaios clínicos é obrigatório o consentimento. Para outros estudos ainda não está implementada essa obrigatoriedade.

e. É garantida a autenticação dos profissionais de saúde na partilha de registos?



Observações: No momento atual o acesso é através dos processos clínicos. Na futura plataforma é através de acessos específicos, com dados clínicos anonimizados.

f. São realizadas auditorias no âmbito do *Crowdsourcing*?



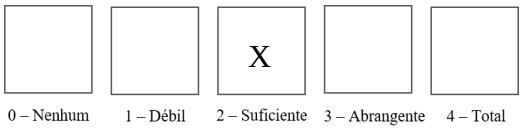
Observações: Só existem para os ensaios clínicos.

5) Inteligência Artificial

a. É utilizada a Inteligência Artificial?

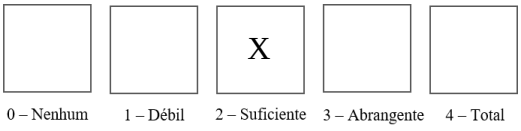
R: Sim, neste momento está na imagem médica e estão em desenvolvimento a implementação de um conjunto de algoritmos sobre os diagnósticos, para suporte à decisão clínica. Na triagem dos pacientes urgentes existe um algoritmo relativo à gravidade da doença e que determina tempos de resposta da intervenção de médicos/enfermeiros.

b. São cumpridos os regulamentos e legislação aplicados neste âmbito?



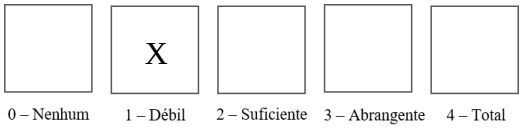
Observações: Existem ainda auditorias anuais.

c. Existem certificações na implementação de dispositivos médicos, plataformas e *softwares*?



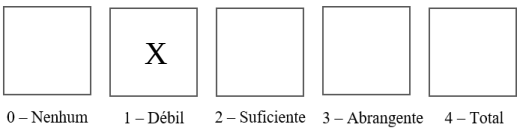
Observações: É certificada a tecnologia e os processos.

d. São escolhidos parceiros tecnológicos idóneos, que estejam devidamente certificados e regulados no mercado europeu?



Observações: Não existia e, neste momento, para os fornecedores de sistemas e tecnologias de informação estão em preparação os requisitos de certificação a exigir, aos que já existem e aos futuros parceiros.

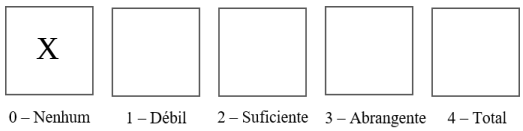
e. É garantida a anonimização da informação que passa para os parceiros?



Observações: Tem-se a preocupação em anonimizar mas há situações, em que para se resolverem problemas tecnológicos, tem de ser dado acessos aos parceiros.

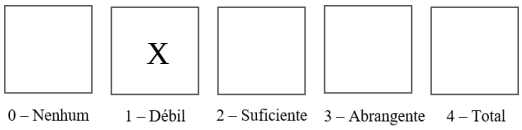
6) Qualidade dos sistemas

a. É possível criar um sistema de informação de raiz através da construção de uma arquitetura de modelo de dados por parte de todos os intervenientes na sua utilização?



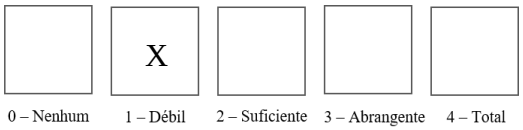
Observações: É desejável mas é impossível na instituição atual, devido ao histórico muito elevado de informação que já possui.

b. É possível demonstrar ou evidenciar que internamente a instituição realiza auditorias, em que haja cumprimentos dos códigos deontológicos, rigor da informação, bom comportamento humano dos profissionais e na passagem da informação para fora?



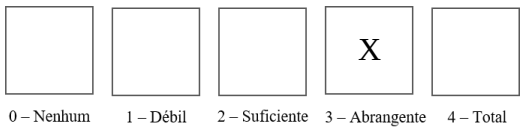
Observações: Apesar de ser concretizável e desejável, todavia ainda existem um conjunto de barreiras culturais cuja mudança não é automática, pelo que este processo tem que ser gradual.

c. Antes do *software* ser desenvolvido é garantida a qualidade no âmbito da ética digital?



Observações: Embora não seja uma prioridade existem, nos ambientes de qualidade, controlos que se introduzem para garantir a ética digital.

d. Quando há uma atualização de *software* ou um novo programa, é fornecida formação para auxiliar no funcionamento dos sistemas?



Observações: Dá-se a formação nas novas funcionalidades e avaliam-se potenciais erros resultantes da implementação do *upgrade*.

5.2. Conclusões do Caso de Estudo

A aplicação do modelo de avaliação da ética digital, através do questionário, permitiu obter um índice que classifica a entidade quanto ao desempenho da ética digital, numa escala de 0 a 4. Através do cálculo da média aritmética (soma total dos valores/número total de perguntas) obteve-se uma classificação de **2**, significando que a entidade em questão cumpre apenas suficientemente os critérios de avaliação da ética digital, pelo que tem ainda muitos aspetos a melhorar.

As dimensões foram também classificadas, de acordo com os critérios referentes às mesmas, como se pode ver na Figura 11.

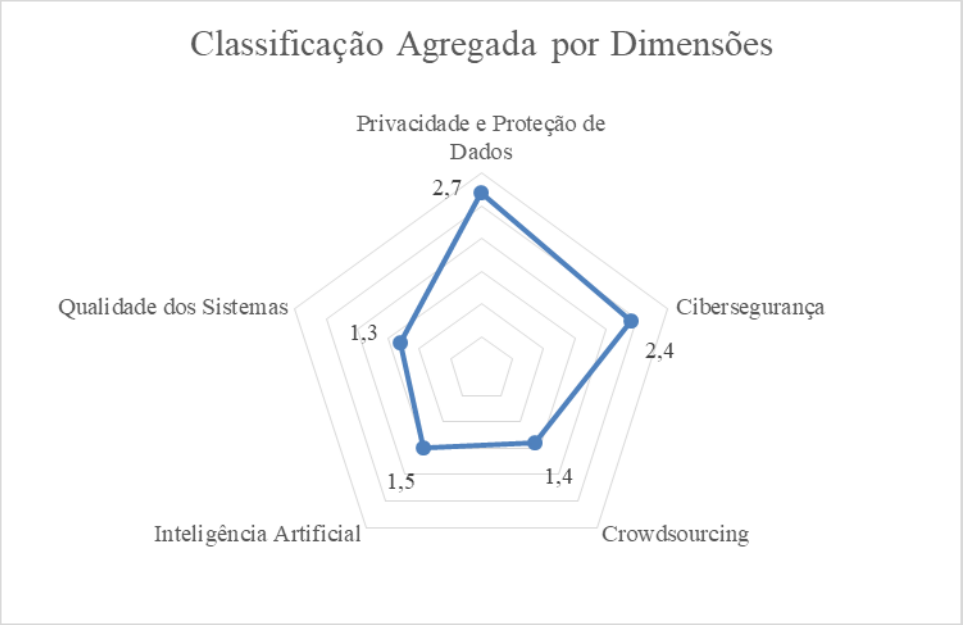


Figura 11 - Classificação Agregada por Dimensões

A dimensão que apresenta, em média, pior classificação é a Qualidade dos Sistemas, com o valor de 1,3, querendo dizer que o desempenho da ética digital neste aspeto é débil, portanto é necessário tomar medidas com vista à melhoria dos sistemas. Além disso, as dimensões da Inteligência Artificial (1,5) e do *Crowdsourcing* (1,4) têm também pontuações muito reduzidas, devido ao facto da entidade estudada ainda estar em fase de desenvolvimento das tecnologias relativas a estas áreas.

Já a dimensão com melhor classificação é a Privacidade e Proteção de Dados, com 2,7, e de seguida a dimensão de Cibersegurança, com 2,4. Contudo, ainda apresentam bastantes lacunas, visto que o desempenho é apenas suficiente.

Foram também organizados os critérios quanto à sua classificação, de forma ilustrativa, como se pode ver na Tabela 2.

Tabela 2 - Classificação por Critérios

DIMENSÕES	CRITÉRIOS	CLASSIFICAÇÃO 0	1	2	3	4
1. Privacidade e Proteção de Dados	1.1. Cumprir a legislação relativa ao RGPD;					●
	1.2. Realizar auditorias;				●	
	1.3. Criação de um DPO;					●
	1.4. Codificação por número de utente;		●			
	1.5. Autorização dos utentes para fornecer dados;				●	
	1.6. Facultar o acesso e possibilitar ao titular aceder diretamente aos seus dados pessoais e clínicos.		●			
2. Cibersegurança	2.1. Cumprir os *standards* de segurança;				●	
	2.2. Utilizar tecnologia *Vmware;*			●		
	2.3. Autenticação de *logins* únicos para cada sessão;					●
	2.4. Fazer *logoff* para terminar sessão;			●		
	2.5. Implementar *shut down timer* após longo tempo de sessão aberta e não utilizada;				●	
	2.6. Criação de terminais com leitores de *RFID;*		●			
	2.7. Manutenção e atualizações de *softwares* de segurança;				●	
	2.8. Receber alertas e *lock down* quando há acesso indevido;			●		
	2.9. Criar mais passos de verificação da identidade;		●			
	2.10. Realizar auditorias;			●		
	2.11. Dar formação de cibersegurança a profissionais de saúde.				●	
3. *Crowdsourcing*	3.1. Ter processos institucionais claros para a identificação dos conjuntos de registos designados na aplicação de *crowdsourcing* ;			●		
	3.2. Anonimizar dados/informação na divulgação dos mesmos;			●		
	3.3. Consentimento do utente para ceder os dados;		●			
	3.4. Autenticação dos profissionais na partilha de registos;		●			
	3.5. Realizar auditorias.		●			
4. Inteligência Artificial	4.1. Cumprir os regulamentos e legislação;			●		
	4.2. Certificações na implementação de dispositivos médicos, plataformas e *softwares;*			●		
	4.3. Escolher parceiros tecnológicos idóneos, que estejam devidamente certificados e regulados no mercado europeu;		●			
	4.4. Anonimizar informação que passa para os parceiros.		●			
5. Qualidade dos Sistemas	5.1. Criar um sistema de informação de raiz através da construção de uma arquitetura de modelo de dados por parte de todos os intervenientes na sua utilização;	●				
	5.2. Demonstrar ou evidenciar que internamente as organizações fazem auditorias, em que haja cumprimentos dos códigos deontológicos, rigor da informação, bom comportamento humano dos profissionais na passagem da informação para fora das instituições;		●			
	5.3. Antes do *software* ser desenvolvido deve respeitar e garantir a qualidade no âmbito da ética digital;		●			
	5.4. Quando há uma atualização de *software* ou um novo programa, a entidade local fornecer formação para ajudar no funcionamento dos sistemas.				●	

A dimensão acerca da qualidade dos sistemas apresenta a pior classificação (0) no critério "5.1. É possível criar um sistema de informação de raiz através da construção do modelo de dados por parte de todos os intervenientes na sua utilização?", visto que a instituição já tem um sistema implementado com vários anos e, por essa razão, tem um histórico muito elevado de informação, que impossibilita a criação de um sistema de raiz.

A dimensão da Privacidade e Proteção de Dados tem os critérios com classificação mais elevada, de 4, tais como, o critério "1.1. Quanto ao RGPD, são cumpridas, a nível institucional, as regras relativas ao mesmo, no âmbito da Saúde?", em que cumpre totalmente, e "1.3. A instituição tem implementado um DPO (Data Protection Officer)?", em que possuem uma equipa dedicada à área legal e outra à área operacional de sistemas de informação, sendo nesta designada um CISO (Chief Information Security Officer).

Na dimensão Cibersegurança, pode-se também verificar um critério com melhor classificação (4), que é "2.3. Existe autenticação de *logins* únicos para cada sessão/utilizador?", no qual a entidade fornece ao funcionário um *login* único, em que a *password* é alterada mensalmente. Além disso, os médicos têm ainda uma utilização obrigatória do cartão da Ordem dos Médicos e *passwords* para validação de prescrições, o que permite um nível mais elevado de segurança na utilização dos sistemas.

As duas formas de visualização anteriores são simples e diretas, permitindo fazer análises comparativas. A título ilustrativo apresenta-se um exemplo que compara a entidade em estudo com uma entidade fictícia, como se pode ver na Figura 12 e Tabela 3.

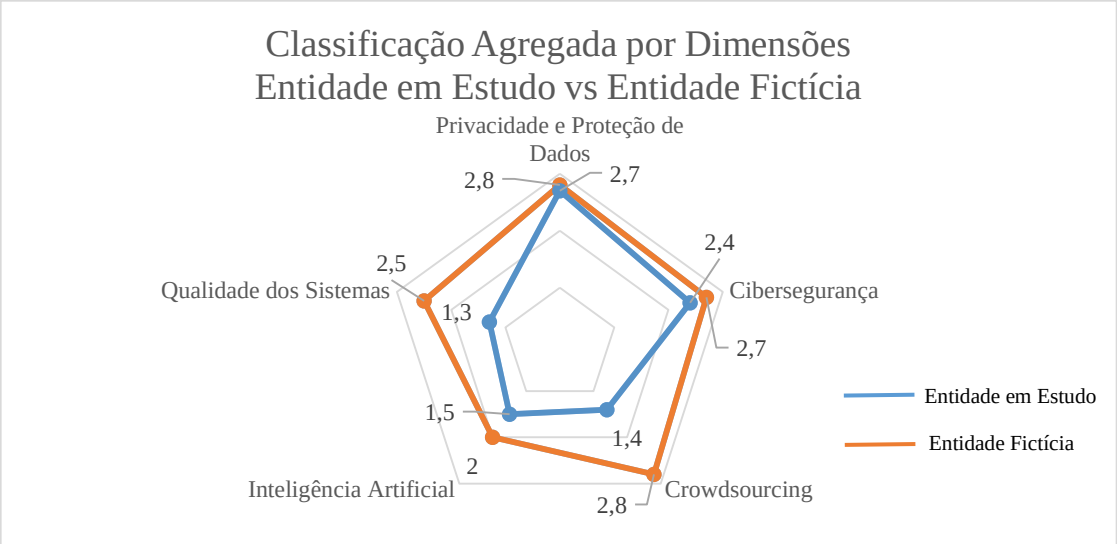


Figura 12 - Classificação Agregada por Dimensões: Entidade em Estudo vs Entidade Fictícia

Tabela 3 - Classificação por Critérios: Entidade em Estudo vs Entidade Fictícia

DIMENSÕES	CRITÉRIOS	CLASSIFICAÇÃO 0 1 2 3 4
1. Privacidade e Proteção de Dados	1.1. Cumprir a legislação relativa ao RGPD;	
	1.2. Realizar auditorias;	
	1.3. Criação de um DPO;	
	1.4. Codificação por número de utente;	
	1.5. Autorização dos utentes para fornecer dados;	
	1.6. Facultar o acesso e possibilitar ao titular aceder diretamente aos seus dados pessoais e clínicos.	
2. Cibersegurança	2.1. Cumprir os *standards* de segurança;	
	2.2. Utilizar tecnologia *Vmware;*	
	2.3. Autenticação de *logins* únicos para cada sessão;	
	2.4. Fazer *logoff* para terminar sessão;	
	2.5. Implementar *shut down timer* após longo tempo de sessão aberta e não utilizada;	
	2.6. Criação de terminais com leitores de *RFID;*	
	2.7. Manutenção e atualizações de *softwares* de segurança;	
	2.8. Receber alertas e *lock down* quando há acesso indevido;	
	2.9. Criar mais passos de verificação da identidade;	
	2.10. Realizar auditorias;	
	2.11. Dar formação de cibersegurança a profissionais de saúde.	
3. *Crowdsourcing*	3.1. Ter processos institucionais claros para a identificação dos conjuntos de registos designados na aplicação de *crowdsourcing* ;	
	3.2. Anonimizar dados/informação na divulgação dos mesmos;	
	3.3. Consentimento do utente para ceder os dados;	
	3.4. Autenticação dos profissionais na partilha de registos;	
	3.5. Realizar auditorias.	
4. Inteligência Artificial	4.1. Cumprir os regulamentos e legislação;	
	4.2. Certificações na implementação de dispositivos médicos, plataformas e *softwares;*	
	4.3. Escolher parceiros tecnológicos idóneos, que estejam devidamente certificados e regulados no mercado europeu;	
	4.4. Anonimizar informação que passa para os parceiros.	
5. Qualidade dos Sistemas	5.1. Criar um sistema de informação de raiz através da construção de uma arquitetura de modelo de dados por parte de todos os intervenientes na sua utilização;	
	5.2. Demonstrar ou evidenciar que internamente as organizações fazem auditorias, em que haja cumprimentos dos códigos deontológicos, rigor da informação, bom comportamento humano dos profissionais na passagem da informação para fora das instituições;	
	5.3. Antes do *software* ser desenvolvido deve respeitar e garantir a qualidade no âmbito da ética digital;	
	5.4. Quando há uma atualização de *software* ou um novo programa, a entidade local fornecer formação para ajudar no funcionamento dos sistemas.	

Entidade em Estudo — Entidade Fictícia

Por fim, é possível verificar que o modelo e índice da ética digital pode ser aplicado nas mais variadas entidades do setor da Saúde, sendo importante para avaliar o desempenho da ética digital nos procedimentos e políticas a tomar pelas instituições.

Capítulo 6 – Conclusões e recomendações

6.1. Principais conclusões

A ética é um termo presente no dia-a-dia das pessoas e das organizações, principalmente quando se refere a questões relacionadas com fatores políticos, económicos, legais e sociais, ou até mesmo a questões individuais, isto é, à conduta ou comportamento de indivíduos dentro de um negócio ou empresa.

Porém, a rápida expansão da tecnologia e a relevância que apresenta atualmente, não só na sua utilização a nível de lazer como também a nível profissional, traz consigo uma preocupação quanto às questões éticas na utilização dos meios digitais. Assim surge o termo "ética digital".

As consequências que a utilização da tecnologia pode trazer medem-se pelos riscos associados, tais como, a falta de segurança na informação disponibilizada, por exemplo, na privacidade e proteção de dados; a falta de controlo no acesso a dados e informações relevantes; a ocorrência de crimes digitais, como o roubo de identidade; o *cyberbullying* nas redes sociais, entre outros.

Visto que a tecnologia é uma ferramenta do dia-a-dia, e é utilizada pela maior parte da população em geral e pelas empresas e organizações em Portugal, a ética digital torna-se assim cada vez mais urgente e necessária, não só para regular todos os aspetos relacionados com a área tecnológica, mas também para credibilizar toda a informação existente nas mais variadas plataformas.

Deste modo, foi iniciada esta investigação com a questão de partida: "Quais os critérios adequados para avaliar a ética digital no setor da Saúde?". Através do caso de estudo no setor da Saúde, estes aspetos permitiram ser validados, visto que a utilização de tecnologias de informação e comunicação na área da saúde é essencial na promoção de modos de relacionamento mais seguros, acessíveis e eficientes na prestação de cuidados de saúde.

Para responder a esta questão foi necessário, inicialmente, realizar uma fase de revisão de literatura, que permitiu avaliar o Estado da Arte da ética digital, destacando os aspetos relacionados com a área da Saúde, e a identificação das dimensões fundamentais de análise da ética digital. De seguida, uma fase de conceção do modelo de avaliação da ética

digital, em que foi fundamental a realização de entrevistas a profissionais do setor da saúde, que contribuiu para uma análise qualitativa do tema e a possibilidade de criar um modelo constituído por dimensões de análise e critérios específicos de avaliação da ética digital, no setor da Saúde em Portugal. Foram destacadas cinco dimensões principais no desempenho da ética digital no setor da Saúde: a Privacidade e Proteção de Dados, Cibersegurança, o *Crowdsourcing*, a Inteligência Artificial e a Qualidade dos Sistemas.

Por fim, este modelo foi aplicado no caso de estudo, através de um questionário, que permitiu classificar os critérios quanto ao seu desempenho. Desta forma, foi possível criar um índice da ética digital no setor da Saúde, que permitiu validar a questão de partida e os objetivos da investigação. Além disso, pode-se também concluir que a criação de um modelo e índice da ética digital permite às organizações aprofundar as questões relacionadas com este tema, possibilitando as mesmas a tomar medidas internas de melhoria, através de boas práticas e procedimentos institucionais adequados.

6.2. Contributos para a comunidade científica e empresarial

A atual massificação da utilização da tecnologia e a facilidade de acesso às plataformas e à informação tem de garantir um futuro digital sustentável, que só pode ser construído baseado numa relação de confiança e na partilha de valores como o respeito pela privacidade digital dos cidadãos, em que os seus dados sejam tratados de forma responsável e segura e de formas transparentes por todos os participantes do ecossistema, nomeadamente na oportunidade de exercer a escolha e o controlo sobre os seus dados, permitindo a inovação e outros benefícios sociais.

É neste enquadramento que este trabalho académico pretende desafiar a comunidade científica e empresarial, ao reforçar uma abordagem a um tema como a ética digital, com a discussão de temáticas relevantes para a avaliação do desempenho nas várias organizações da sociedade.

Tendo por base a sensibilidade dos pessoais clínicos e o risco da sua utilização indevida por terceiros, realizou-se uma análise que permitiu levar à identificação das dimensões e dos critérios apropriados para avaliar o desempenho da ética digital no setor da saúde, em Portugal.

6.3. Limitações e dificuldades

As limitações e dificuldades que ocorreram na realização desta dissertação foram principalmente devido à pandemia (COVID-19) que assolou todo o mundo e que atrasou durante largos meses alguns objetivos pendentes. Neste caso, impossibilitou a realização de questionários a uma amostra considerável de profissionais de Saúde, que iriam suportar a validação das dimensões e critérios identificados no modelo e índice de avaliação da ética digital.

6.4. Propostas de investigação futura

Para futuras investigações, propõe-se então a aplicação do questionário testado a um nível considerado de amostras adequadas, o desenvolvimento aprofundado do modelo e índice de avaliação da ética digital e a criação de um *ranking* de classificação da ética digital, para ser testado nas mais variadas entidades da Saúde. De referir, que este índice pode ser extrapolado para outros setores da sociedade, de acordo com os critérios específicos de cada um, sistematizando práticas, que satisfaçam os critérios, com o objetivo de criar um manual de boas práticas e assim, poder surgir, idealmente, um selo institucional da ética digital nas organizações.

Bibliografia

Abouelmehdi, K., beni hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. Procedia Computer Science, 113, 73–80. https://doi.org/10.1016/j.procs.2017.08.292

Albinati, F. (2018, Janeiro 25). Ethics Advisory Group Report 2018 [Text]. European Data Protection Supervisor - European Data Protection Supervisor. https://edps.europa.eu/data-protection/our-work/publications/ethical-framework/ethics-advisory-group-report-2018_en

Almeida, F. J. R. de. (2007). Ética e desempenho social das organizações: Um modelo teórico de análise dos fatores culturais e contextuais. Revista de Administração Contemporânea, 11(3), 105–125. https://doi.org/10.1590/S1415-65552007000300006

Boni, V., & Quaresma, S. J. (2005). Aprendendo a entrevistar: Como fazer entrevistas em ciências sociais. Em Tese, 2(1), 68–80. https://doi.org/10.5007/%x

Burr, C., Taddeo, M., & Floridi, L. (2020). The Ethics of Digital Well-Being: A Thematic Review. Science and Engineering Ethics, 26(4), 2313–2343. https://doi.org/10.1007/s11948-020-00175-8

Capurro, R. (2018). Why Information Ethics? 1. International Journal of Applied Research on Information Technology and Computing, 9(1), 50. https://doi.org/10.5958/0975-8089.2018.00005.2

Carter, S. M., Rogers, W., Win, K. T., Frazer, H., Richards, B., & Houssami, N. (2020). The ethical, legal and social implications of using artificial intelligence systems in breast cancer care. The Breast, 49, 25–32. https://doi.org/10.1016/j.breast.2019.10.001

Constituição da República Portuguesa. (1976). Diário da República Eletrónico. Obtido 28 de Outubro de 2020, de https://dre.pt/legislacao-consolidada/-/lc/337/202006140751/127994/diploma/indice

Despacho 8877/2017, 2017-10-09. (sem data). Diário da República Eletrónico. Obtido 15 de Outubro de 2020, de https://dre.pt/web/guest/home/-/dre/108269312/details/3/maximized?serie=II&parte_filter=31&day=2017-10-09&date=2017-10-01&dreId=108253554

Dias, M. O. (2014). Ética, organização e valores ético-morais em contexto organizacional. Gestão e Desenvolvimento, 22, 89–113. https://doi.org/10.7559/gestaoedesenvolvimento.2014.259

Doody, O., & Bailey, M. (2016). Setting a research question, aim and objective. Nurse researcher, 23 4, 19–23.

Figueiredo, A. M. (2008). Ética: Origens e distinção da moral. Saúde, Ética & Justiça (e-ISSN 2317-2770), 13(1), 1–9. https://doi.org/10.11606/issn.2317-2770.v13i1p1-9

Floridi, L. (2018a). Soft Ethics and the Governance of the Digital. Philosophy & Technology, 31(1), 1–8. https://doi.org/10.1007/s13347-018-0303-9

Floridi, L. (2018b). Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage. Philosophy & Technology, 31(2), 163–167. https://doi.org/10.1007/s13347-018-0315-5

Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160360. https://doi.org/10.1098/rsta.2016.0360

Frost & Sullivan. (2012). A Frost & Sullivan White Paper Drowning in Big Data? Reducing Information Technology Complexities and Costs For Healthcare Organizations CONTENTS. https://www.academia.edu/6563567/A_Frost_and_Sullivan_White_Paper_Drowning_in_Big_Data_Reducing_Information_Technology_Complexities_and_Costs_For_Healthcare_Organizations_CONTENTS

Godden, S., Ambler, G., & Pollock, A. M. (2010). Recruitment of minority ethnic groups into clinical cancer research trials to assess adherence to the principles of the Department of Health Research Governance Framework: National sources of data and general issues arising from a study in one hospital trust in England. Journal of Medical Ethics, 36(6), 358–362. https://doi.org/10.1136/jme.2009.033845

Gontijo, E. D. (2006). Os termos «Ética» e «Moral». Mental, IV(7), 127–135.

Graffigna, G. (Ed.). (2016). Promoting Patient Engagement and Participation for Effective Healthcare Reform: IGI Global. https://doi.org/10.4018/978-1-4666-9992-2

Hill, G. W. (1982). Group versus individual performance: Are N + 1 heads better than one? Psychological Bulletin, 91(3), 517–539. https://doi.org/10.1037/0033-2909.91.3.517

Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017). Artificial intelligence in healthcare: Past, present and future. Stroke and Vascular Neurology, 2(4). https://doi.org/10.1136/svn-2017-000101

Juusola, J. L., Quisel, T. R., Foschini, L., & Ladapo, J. A. (2016). The Impact of an Online Crowdsourcing Diagnostic Tool on Health Care Utilization: A Case Study Using a Novel Approach to Retrospective Claims Analysis. J Med Internet Res, 18(6), e127. https://doi.org/10.2196/jmir.5644

Khare, R., Good, B. M., Leaman, R., Su, A. I., & Lu, Z. (2016). Crowdsourcing in biomedicine: Challenges and opportunities. Briefings in Bioinformatics, 17(1), 23–32. https://doi.org/10.1093/bib/bbv021

Kumar, M. M. (sem data). Emerging Trends in Big Data, IoT and Cyber Security. 258.

Kupwade Patil, H., & Seshadri, R. (2014). Big Data Security and Privacy Issues in Healthcare. Proceedings - 2014 IEEE International Congress on Big Data, BigData Congress 2014, 762–765. https://doi.org/10.1109/BigData.Congress.2014.112

Leximancer Pty Ltd. (2019). Leximancer User Guide. 149.

Maggiolini, P. (2014). UM APROFUNDAMENTO PARA O CONCEITO DE ÉTICA DIGITAL. Revista de Administração de Empresas, 54(5), 585–591. https://doi.org/10.1590/S0034-759020140511

Mahieu, R., van Eck, N. J., van Putten, D., & van den Hoven, J. (2018). From dignity to security protocols: A scientometric analysis of digital ethics. Ethics and Information Technology, 20(3), 175–187. https://doi.org/10.1007/s10676-018-9457-5

McKinney, J. A., Emerson, T. L., & Neubert, M. J. (2010). The Effects of Ethical Codes on Ethical Perceptions of Actions Toward Stakeholders. Journal of Business Ethics, 97(4), 505–516. https://doi.org/10.1007/s10551-010-0521-2

Monteiro, S. (2008). O Ciberespaço: O termo, a definição e o conceito | Pesquisa Brasileira em Ciência da Informação e Biblioteconomia. https://periodicos.ufpb.br/ojs/index.php/pbcib/article/view/6989

Morais Nunes, A., & Matos, A. (2018). Tecnologias da informação e comunicação no sistema de saúde Português. Electronic Journal of Health Informatics, 10, 30–34.

Myers, J., Frieden, T. R., Bherwani, K. M., & Henning, K. J. (2008). Ethics in Public Health Research. American Journal of Public Health, 98(5), 9.

Nunes, E. D. (2007). O desafio do conhecimento: Pesquisa qualitativa em saúde. Ciência & Saúde Coletiva, 12(4), 1087–1088. https://doi.org/10.1590/S1413-81232007000400030

OECD, & Union, E. (2018). Health at a Glance: Europe 2018. https://doi.org/10.1787/health_glance_eur-2018-en

Oliveira, F., Ramos, I., & Santos, L. (2010). Definition of a Crowdsourcing Innovation Service for the European SMEs. Em F. Daniel & F. M. Facca (Eds.), Current Trends in Web Engineering (pp. 412–416). Springer Berlin Heidelberg.

Queiroz, A., Cardoso, A. J. G., Souza, A. A. D., Teodosio, A. D. S. D. S., Ventura, E. C. F., Veloso, L. H. M., Ashley, P. A., Ferreira, R. D. N., Lima, P. R. D. S., Aligleri, L. M., Chaves, J. B. L., Borinelli, B., & Alves, A. R. (2017). Ética E Responsabilidade Social Nos Negócios. Saraiva Educação S.A.

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. Health Information Science and Systems, 2. https://doi.org/10.1186/2047-2501-2-3

Reay, T., & Hinings, C. R. (2009). Managing the Rivalry of Competing Institutional Logics. Organization Studies, 30(6), 629–652. https://doi.org/10.1177/0170840609104803

Regulamento (UE) 2016/ 679 Do Parlamento Europeu E Do Conselho - de 27 de abril de 2016—Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/ 46/ CE (Regulamento Geral sobre a Proteção de Dados). 88.

Resolução do Conselho de Ministros 92/2019, 2019-06-05. (sem data). Diário da República Eletrónico. Obtido 15 de Outubro de 2020, de https://dre.pt/home/-/dre/122498962/details/maximized

Rice, K. (2006). Ethical Issues In Linguistic Fieldwork: An Overview. Journal of Academic Ethics, 4(1), 123–155. https://doi.org/10.1007/s10805-006-9016-2

Santos, J. L. A. dos. (2011). Contributos para uma melhor governação da cibersegurança em Portugal. https://run.unl.pt/handle/10362/7341

Schwartz, M. S. (sem data). A Code of Ethics for CorporateCode of Ethics. 17.

Sebastião, Y., & Nunes, S. (2019). A Maturidade e Eficiência dos Processos da Governação de TI Baseadas no Cobit 5: Um Caso de Uma Organização do Setor da Saúde em Portugal.

Sims, M. H., Hodges Shaw, M., Gilbertson, S., Storch, J., & Halterman, M. W. (2019). Legal and ethical issues surrounding the use of crowdsourcing among healthcare providers. Health Informatics Journal, 25(4), 1618–1630. https://doi.org/10.1177/1460458218796599

Snow, C. C., Fjeldstad, Ø. D., & Langer, A. M. (2017). Designing the digital organization. Journal of Organization Design, 6(1), 7. https://doi.org/10.1186/s41469-017-0017-y

Steiner, G. A. (1972). Social Policies for Business. California Management Review, 15(2), 17–24. https://doi.org/10.2307/41164414

Sutrisna, M. (2009). Research Methodology in Doctoral Research: Understanding the Meaning of Conducting Qualitative Research.

Świeszczak, M., & Świeszczak, K. (2016). Crowdsourcing – what it is, works and why it involves so many people? World Scientific News, 48, 32–40.

Tenbrunsel, A. E., Smith-Crowe, K., & Umphress, E. E. (2003). Building Houses on Rocks: The Role of the Ethical Infrastructure in Organizations. Social Justice Research, 16(3), 285–307. https://doi.org/10.1023/A:1025992813613

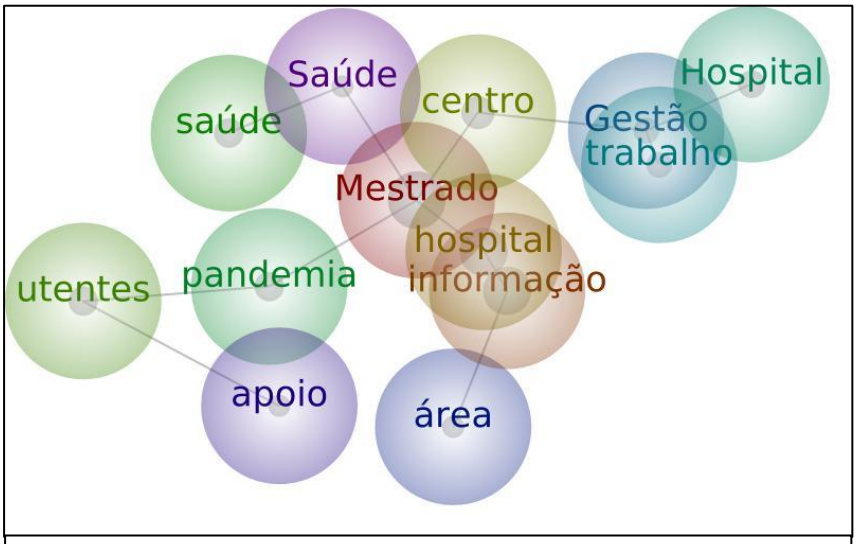
Webley, S., & Werner, A. (2008). Corporate codes of ethics: Necessary but not sufficient. Business Ethics: A European Review, 17(4), 405–415. https://doi.org/10.1111/j.1467-8608.2008.00543.x

Wilson, E., Pollock, K., & Aubeeluck, A. (2010). Gaining and maintaining consent when capacity can be an issue: A research study with people with Huntington's disease. Clinical Ethics, 5(3), 142–147. https://doi.org/10.1258/ce.2010.010024

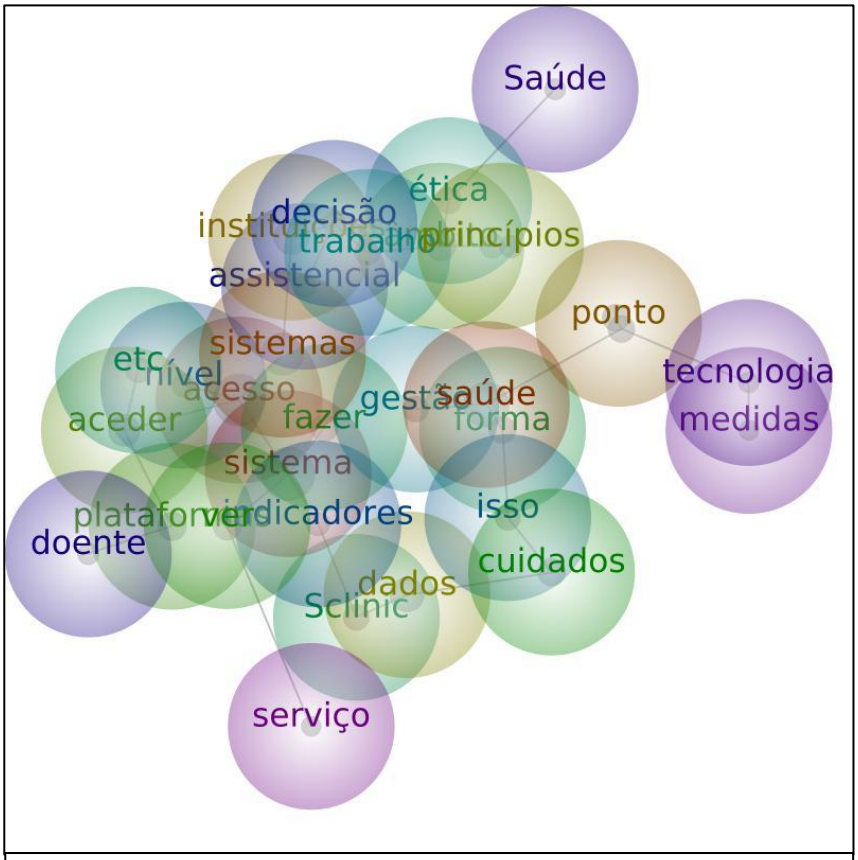
Zandi, D., Reis, A., Vayena, E., & Goodman, K. (2019). New ethical challenges of digital technologies, machine learning and artificial intelligence in public health: A call for papers. Bulletin of the World Health Organization, 97(1), 2–2. https://doi.org/10.2471/BLT.18.227686

Anexos e Apêndices

Anexo 1 – Mapas Conceptuais



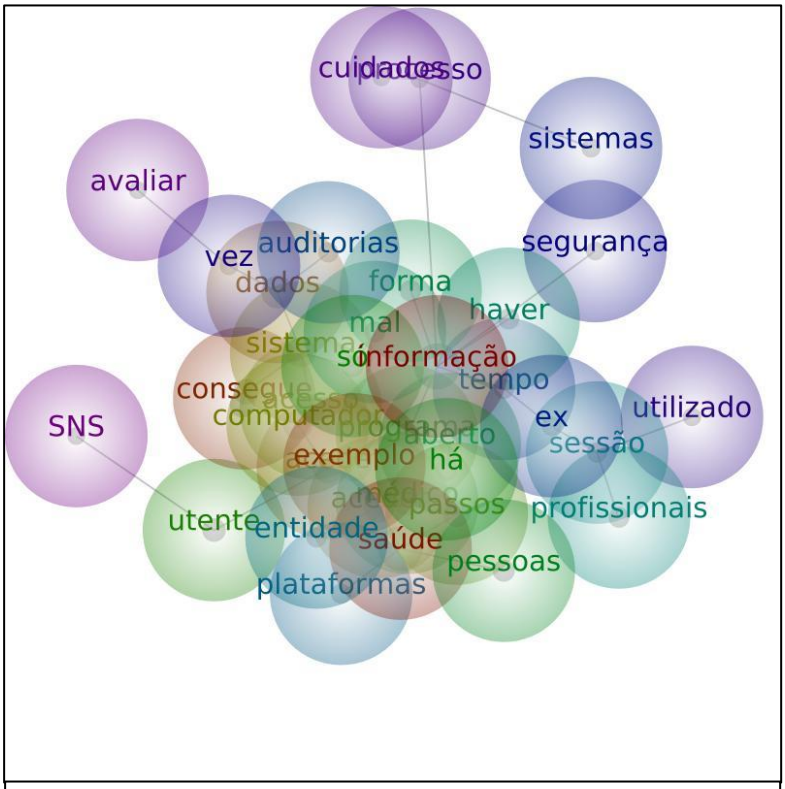
Mapa conceptual complementar da Questão 1



Mapa conceptual complementar da Questão 2

Mapa conceptual complementar da Questão 3

Mapa conceptual complementar da Questão 4



Mapa conceptual complementar da Questão 5

Apêndice A

CONSENTIMENTO INFORMADO DA ENTREVISTA

O presente estudo surge no âmbito de uma dissertação de mestrado em Gestão de Sistemas de Informação, a decorrer no ISCTE – Instituto Universitário de Lisboa.
O tema de investigação é a Ética Digital, na qual se pretende entender quais as dimensões utilizadas para avaliar a mesma, no âmbito da prestação dos serviços do setor da Saúde, em Portugal, e posteriormente criar um índice que vai permitir classificar os desempenhos nesta área.

O estudo é realizado por Inês Casaleiro (iicoc@iscte-iul.pt/iicasaleiro@gmail.com), sob a orientação dos Professores Bráulio Alturas (braulio.alturas@iscte-iul.pt) e Nuno Cavaco (namc@fct.unl.pt), que poderá contactar caso deseje colocar alguma dúvida ou partilhar algum comentário.

O seu contributo consiste na participação de uma entrevista que irá ser gravada e que durará cerca de 45 minutos a 1 hora. Não existem riscos associados à participação no estudo. As suas respostas ao estudo em questão vão contribuir para a formulação dos principais indicadores de investigação, juntamente com outros dados, que de igual modo serão analisados e apresentados à *posteriori* no relatório final da dissertação.

A participação neste estudo é estritamente voluntária. Ao participar, pode interromper a participação em qualquer momento sem ter de prestar qualquer justificação. Para além de voluntária, a participação é também anónima e confidencial. Em nenhum momento do estudo precisa de se identificar. A entrevista, como acima mencionado, será gravada para posterior transcrição das respostas. Porém, caso não aceite gravação, queira por favor indicar nas observações.

Face a estas informações, por favor indique se aceita participar no estudo:

☐ ACEITO ☐ NÃO ACEITO

Nome:_____
Data:_____
Assinatura
Entrevistado:_____
Observações:_____
____

Assinatura
Entrevistador:_____

O preenchimento deste consentimento informado presume que compreendeu e que aceita as condições do presente estudo, consentindo participar no mesmo.

Apêndice B

Guião da Entrevista:

1. Saudações iniciais.

2. O tema de Investigação é a ética digital e pretendo "Analisar o Estado da Arte da ética digital e concluir quais são os critérios mais apropriados na avaliação da ética digital nos serviços de Saúde".

3. Os objetivos da Entrevista são:
   - Estabelecer dimensões de análise da ética digital;
   - Criar e validar um modelo constituído por dimensões de análise e critérios específicos de avaliação da ética digital, aplicável ao setor da Saúde;

4. Para contexto, a primeira questão é: Que profissão e que tipo de funções executa no seu local de trabalho?

5. De acordo com o tipo de função que executa no dia-a-dia da sua profissão, que tipo de tecnologia utiliza e para que utiliza?

6. Ao utilizar a tecnologia consegue identificar ou tem alguma preocupação com o desempenho da ética digital?

7. Quanto às dimensões da ética digital na área da Saúde, quais os aspetos principais que tem em conta ao utilizar a tecnologia na sua profissão?

8. De acordo com as dimensões identificadas anteriormente, quais os critérios que considera apropriados para avaliar o desempenho da ética digital na área da Saúde, no seu tipo de funções?

9. Agradecimentos finais.

Apêndice C

Questionário:

1) Aspetos gerais

a. Qual o tipo de instituição de Saúde em que trabalha?

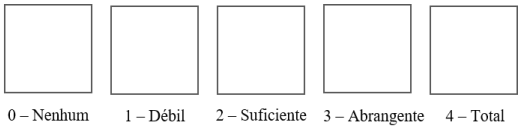
R: _____

b. Em que área da Saúde se inclui a sua profissão?

R: _____

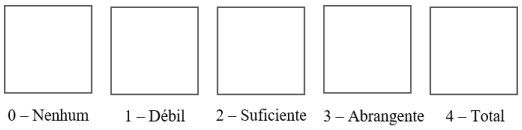
2) Privacidade e Proteção de Dados

a. Quanto ao RGPD, são cumpridas, a nível institucional, as regras relativas ao mesmo, no âmbito da Saúde?



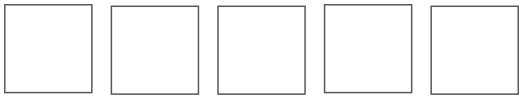
Observações: _____

b. São realizadas auditorias no âmbito da privacidade e da proteção de dados? Se sim, de que tipo e com que frequência?



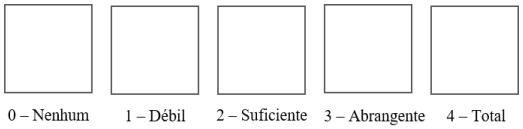
Observações: _____

c. A instituição tem implementado um DPO (Data Protection Officer)?



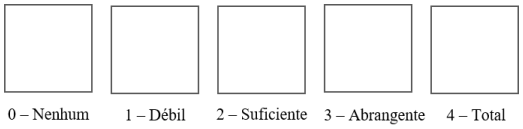
Observações: _____

d. Existe uma codificação dos dados do utente por número de utente?



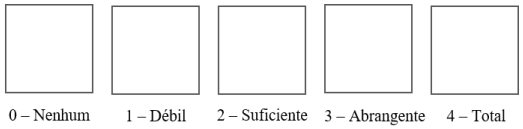
Observações: _____

e. É pedido aos utentes uma autorização para fornecer os seus dados?



Observações: _____

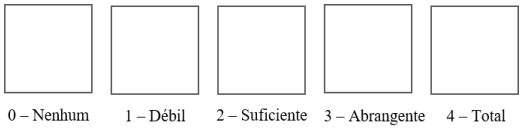
f. É facultado o acesso e possibilitado ao titular aceder diretamente aos seus dados pessoais e/ou clínicos?



Observações: _____

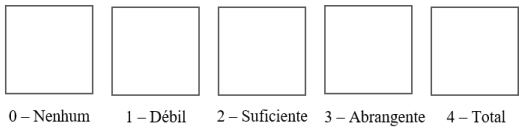
3) Cibersegurança

a. São cumpridos os *standards* de segurança?



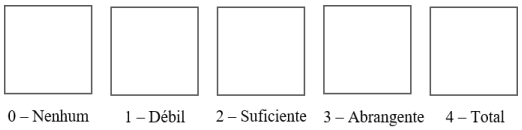
Observações: _____

b. É utilizada a tecnologia *Vmware*? Se sim, em quê?



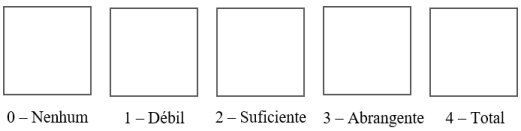
Observações: _____

c. Existe autenticação de *logins* únicos para cada sessão/utilizador?



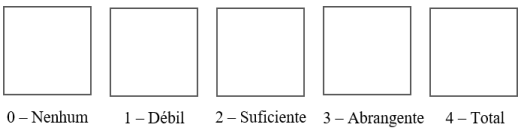
Observações: _____

d. É utilizado o *logoff* para terminar sessão?



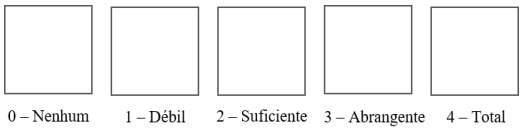
Observações: _____

e. É implementado um *shut down timer* após longo tempo de sessão aberta e não utilizada?



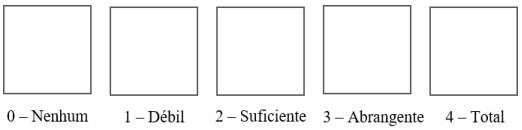
Observações: _____

f. Existem terminais com leitores de *RFID*?



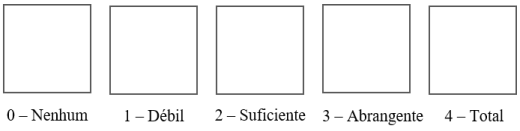
Observações: _____

g. Existe manutenção e atualização dos *softwares* de segurança?



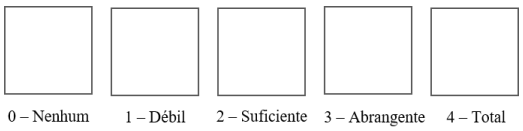
Observações: _____

h. São recebidos alertas e é feito um *lock down* dos sistemas quando há acesso indevido?



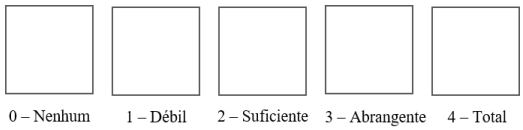
Observações: _____

i. São implementados mais passos de verificação da identidade?



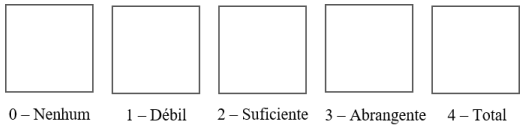
Observações: _____

j. São realizadas auditorias no âmbito da segurança? Se sim, de que tipo e com que frequência?



Observações: _____

k. É dada formação de cibersegurança aos profissionais de saúde? Se sim, em que altura e com que frequência?



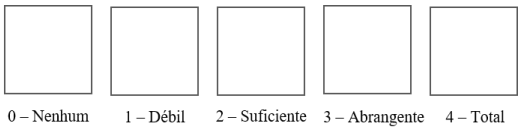
Observações: _____

4) Crowdsourcing

a. É utilizado o *Crowdsourcing*?

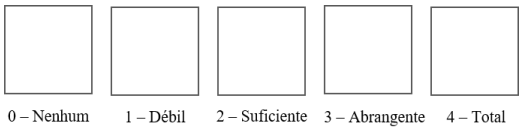
R: _____

b. Têm processos institucionais claros para o funcionamento do *crowdsourcing* na instituição?



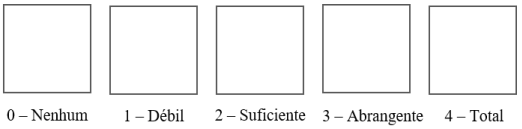
Observações: _____

c. É garantida a anonimização dos dados/informação dos utentes na divulgação dos mesmos?



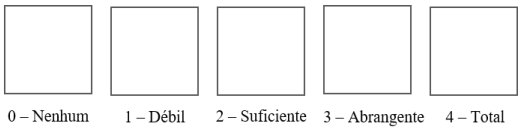
Observações: _____

d. Existe consentimento do utente para ceder os seus dados?



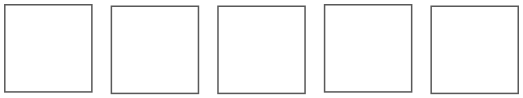
Observações: _____

e. É garantida a autenticação dos profissionais de saúde na partilha de registos?



Observações: _____

f. São realizadas auditorias no âmbito do *Crowdsourcing*?



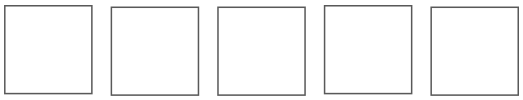
Observações: _____

5) Inteligência Artificial

a. É utilizada a Inteligência Artificial?

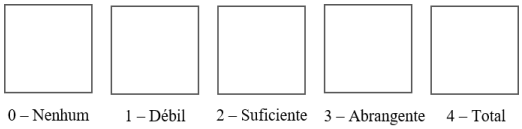
R: _____

b. São cumpridos os regulamentos e legislação aplicados neste âmbito?



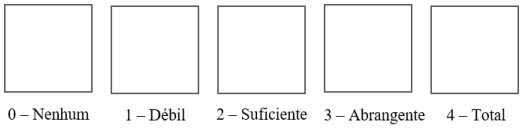
Observações: _____

c. Existem certificações na implementação de dispositivos médicos, plataformas e *softwares*?



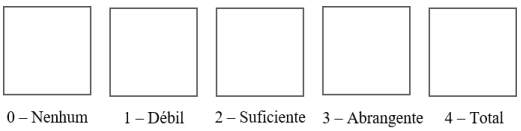
Observações: _____

d. São escolhidos parceiros tecnológicos idóneos, que estejam devidamente certificados e regulados no mercado europeu?



Observações: _____

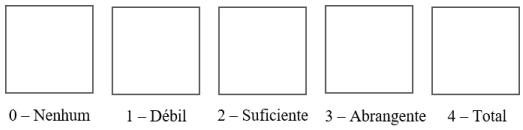
e. É garantida a anonimização da informação que passa para os parceiros?



Observações: _____

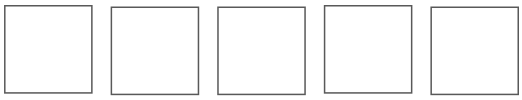
6) Qualidade dos sistemas

a. É possível criar um sistema de informação de raiz através da construção de uma arquitetura de modelo de dados por parte de todos os intervenientes na sua utilização?



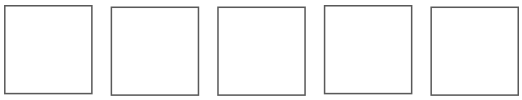
Observações: _____

b. É possível demonstrar ou evidenciar que internamente a instituição realiza auditorias, em que haja cumprimentos dos códigos deontológicos, rigor da informação, bom comportamento humano dos profissionais e na passagem da informação para fora?



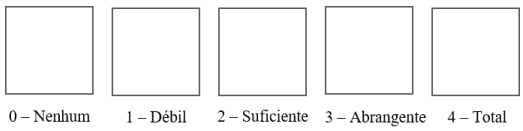
Observações: _____

c. Antes do *software* ser desenvolvido é garantida a qualidade no âmbito da ética digital?



Observações: _____

d. Quando há uma atualização de *software* ou um novo programa, é fornecida formação para auxiliar no funcionamento dos sistemas?



Observações: _____