Fall 10-16-2021

Evaluation of the Digital Ethics Performance in the Health Sector, in Portugal

Inês Casaleiro
Instituto Universitário de Lisboa (ISCTE-IUL), ines_casaleiro@iscte-iul.pt

Bráulio Alturas
Instituto Universitário de Lisboa (ISCTE-IUL), braulio.alturas@iscte-iul.pt

Nuno Cavaco
Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa, namc@fct.unl.pt

Avaliação do Desempenho da Ética Digital no Setor da Saúde, em Portugal

Evaluation of the Digital Ethics Performance in the Health Sector, in Portugal

Inês Casaleiro, Instituto Universitário de Lisboa (ISCTE-IUL), Portugal,
ines_casaleiro@iscte-iul.pt

Bráulio Alturas, Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR-Iscte, Portugal,
braulio.alturas@iscte-iul.pt

Nuno Cavaco, Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa, Portugal,
namc@fct.unl.pt

Resumo

A rápida expansão da tecnologia e a sua relevância no quotidiano dos indivíduos traz consigo uma preocupação quanto às questões éticas na utilização dos meios digitais. Foi realizada uma revisão de literatura, que permitiu analisar o Estado da Arte da ética digital, principalmente no que diz respeito à área da Saúde, 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.

Palavras-chave: tecnologia da informação; ética digital; 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. A literature review was carry out, 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 in the Health sector, with the aim of validating the model created and classifying the entity as to the performance in digital ethics.

Keywords: *information technology; digital ethics; criteria; evaluation; health.*

1. INTRODUÇÃO

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

ISSN 2183-489X

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 este estudo 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.

2. ÉTICA DIGITAL

2.1. Conceito

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, 2018).

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. Aplicação na Saúde

Até 1999, alguns hospitais nacionais não dispunham nem de grandes meios informáticos nem do pessoal técnico de apoio necessário, quer em quantidade quer em qualidade. A quase totalidade dos equipamentos informáticos existentes na altura estava atribuída a tarefas administrativas. E, mesmo nestes casos, alguns equipamentos eram partilhados por mais do que um funcionário administrativo (Costa et al., 2012). A partir do início do século XXI, 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 (Matos & Nunes, 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 (Burgess et al., 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 utilização de 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, 2011). 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).

2.3. Dimensões de Avaliação

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 retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos previstos na lei." (República Portuguesa, 1976).

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, 2007). 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 (República Portuguesa, 2019).

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). O 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" (Oliveira et al., 2010). Nos últimos anos tem sido utilizado para explorar a inteligência coletiva 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).

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).

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. A IA passa por várias fases de planeamento, raciocínio, análise de dados, previsão dos resultados e atuação em conformidade. 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).

A IA é, mais do que nunca, uma área que tem preocupado, em termos de ética, funcionários e políticos. A maior preocupação é garantir uma utilização do que é definido como uma inteligência artificial responsável. Para isso, há que ter em conta, conceitos como privacidade, responsabilidade, proteção e segurança, justiça e não discriminação, controlo humano da tecnologia, responsabilidade profissional e, finalmente, a promoção dos valores humanos (Martins et al., 2021).

3. METODOLOGIA

A partir da análise e revisão da literatura, nomeadamente aos aspetos relacionados com a ética digital, foram definidas as dimensões e critérios mais adequados para avaliar a ética digital.

Com o objetivo de validar as dimensões e critérios, foram realizadas entrevistas a profissionais do setor da Saúde, que, por serem indivíduos especializados na área, possibilitaram enriquecer e tornar mais credível o estudo de investigação. Para isso, foram escolhidos cinco profissionais que trabalham em instituições distintas, na área da Saúde, e com tipos diferentes de funções, tais como, um profissional de gestão de sistemas de informação de Hospital, um profissional com função administrativa de Hospital, um médico de Centro de Saúde, um enfermeiro de Hospital e um docente universitário na área da Bioética.

Com as informações obtidas na análise das entrevistas, foram novamente revistas as dimensões de avaliação da ética digital e, de seguida, criado um modelo de avaliação da ética digital, com a elaboração de um questionário para ser 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.

4. CONCEÇÃO DO MODELO DE AVALIAÇÃO DA ÉTICA DIGITAL

As dimensões definidas na revisão de literatura foram a Privacidade e Proteção de Dados, a Cibersegurança, o Crowdsourcing e a Inteligência Artificial, na qual foi acrescentada a dimensão Qualidade dos Sistemas, através das análises das entrevistas realizadas.

A Tabela 1 apresenta as dimensões e os critérios associados enumerados, para a aplicação do questionário.

De seguida, apresenta-se 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.

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.
	1.7. Anonimizar informação que passa para os parceiros.
2. Cibersegurança	2.1. Cumprir os *standards* de segurança;
	2.2. Utilizar tecnologia de virtualização e máquina virtual;
	2.3. Cumprir os critérios de autenticação multifator: 2.3.1. Autenticação de *logins* únicos para cada sessão; 2.3.2. Criação de terminais com leitores de *RFID;* 2.3.3. Criar mais passos de verificação da identidade;
	2.4. Fazer *logoff* para terminar sessão;
	2.5. Implementar *shut down timer* após longo tempo de sessão aberta e não utilizada;
	2.6. Manutenção e atualizações de *softwares* de segurança;
	2.7. Receber alertas e *lock down* quando há acesso indevido;
	2.8. Realizar auditorias;
	2.9. 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;
5. Qualidade dos Sistemas	5.1. Garantir que o sistema de informação de raiz possui uma arquitetura de modelo de dados que inclua todos os intervenientes na sua conceção e 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.

Tabela 1 – Modelo de Avaliação da Ética Digital

5. CASO DE ESTUDO

Foi aplicado um questionário a um profissional da área de Saúde, com o objetivo de ser testado o modelo de avaliação da ética digital, em que para cada pergunta foi contemplado o respetivo critério.

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 1.

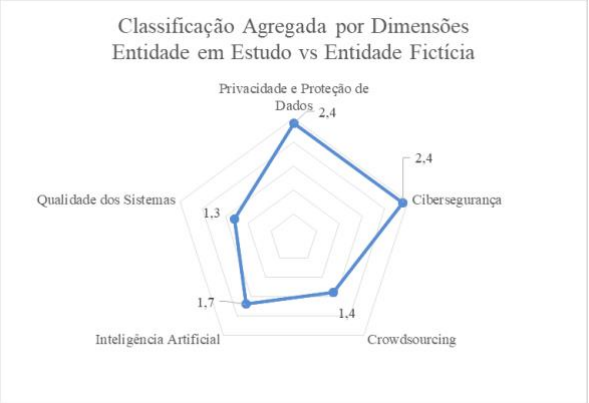

Figura 1 – Classificação Agregada por Dimensões

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 (1,7) 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 as dimensões com melhores classificações são a Privacidade e Proteção de Dados e a Cibersegurança, ambas 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.

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.	
	1.7. Anonimizar informação que passa para os parceiros.	
2. Cibersegurança	2.1. Cumprir os *standards* de segurança;	
	2.2. Utilizar tecnologia de virtualização e máquina virtual;	
	2.3. Cumprir os critérios de autenticação multifator:	
	2.3.1. Autenticação de logins únicos para cada sessão;	
	2.3.2. Criação de terminais com leitores de RFID;	
	2.3.3. Criar mais passos de verificação da identidade;	
	2.4. Fazer *logoff* para terminar sessão;	
	2.5. Implementar *shut down timer* após longo tempo de sessão aberta e não utilizada;	
	2.6. Manutenção e atualizações de *softwares* de segurança;	
	2.7. Receber alertas e *lock down* quando há acesso indevido;	
	2.8. Realizar auditorias;	
	2.9. 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;	
5. Qualidade dos Sistemas	5.1. Garantir que o sistema de informação de raiz possui uma arquitetura de modelo de dados que inclua todos os intervenientes na sua conceção e 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.	

Tabela 2 – Classificação por Critérios

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 também verificar-se um critério com melhor classificação (4), que é "2.3.1 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 2 e Tabela 3.

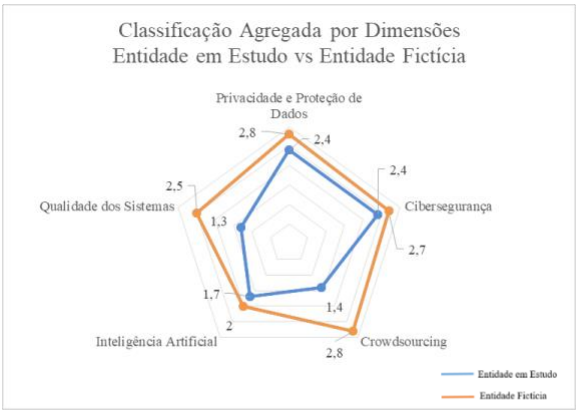

Figura 2 – Classificação Agregada por Dimensões: Entidade em Estudo vs Entidade Fictícia

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.	
	1.7. Anonimizar informação que passa para os parceiros.	
2. Cibersegurança	2.1. Cumprir os *standards* de segurança;	
	2.2. Utilizar tecnologia de virtualização e máquina virtual;	
	2.3. Cumprir os critérios de autenticação multifator:	
	2.3.1. Autenticação de logins únicos para cada sessão;	
	2.3.2. Criação de terminais com leitores de RFID;	
	2.3.3. Criar mais passos de verificação da identidade;	
	2.4. Fazer *logoff* para terminar sessão;	
	2.5. Implementar *shut down timer* após longo tempo de sessão aberta e não utilizada;	
	2.6. Manutenção e atualizações de *softwares* de segurança;	
	2.7. Receber alertas e *lock down* quando há acesso indevido;	
	2.8. Realizar auditorias;	
	2.9. 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;	
5. Qualidade dos Sistemas	5.1. Garantir que o sistema de informação de raiz possui uma arquitetura de modelo de dados que inclua todos os intervenientes na sua conceção e 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

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

6. CONCLUSÕES

6.1. Principais Conclusões

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. Limitações e dificuldades

As limitações e dificuldades que ocorreram na realização deste estudo 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.

6.3. 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.

AGRADECIMENTOS

Este trabalho foi realizado no ISTAR - Information Sciences and Technologies and Architecture Research Center do ISCTE - Instituto Universitário de Lisboa, Portugal, e foi parcialmente financiado pela Fundação para a Ciência e a Tecnologia (Projeto "FCT UIDB / 04466/2020").

REFERÊNCIAS

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

Burgess, J. P., Floridi, L., Pols, A. & van den Hoven, J. (2018). *Ethics Advisory Group Report 2018*.

Capurro, R. (2018). Why Information Ethics? *International Journal of Applied Research on Information Technology and Computing*, *9*(1), 50–52. 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. *Breast*, *49*, 25–32. https://doi.org/10.1016/j.breast.2019.10.001

Costa, L. P., Alturas, B. & Lapão, L. V. (2012). Análise da Qualidade do Suporte Informático aos Profissionais de Saúde em Unidades Hospitalares [Analysis of the Quality of Computer Support to Health Professionals in Hospital Units]. *7th Iberian Conference on Information Systems and Technologies, CISTI 2012*, Madrid, Spain, 1380–1383.

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

Floridi, L. & Taddeo, M. (2016). What Is Data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*. https://doi.org/10.4324/9780429061219-2

Frost, D. & Sullivan, S. (2011). Drowning in Big Data? Reducing Information Technology Complexities and Costs for Healthcare Organizations. In *Frost & Sullivan White Paper*. www.frost.com

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

Maggiolini, P. (2014). Um Aprofundamento Para o Conceito de Ética Digital. *Revista de Administração de Empresas*, *54*(5), 585–591.

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

Martins, R. V., Alturas, B. & Alexandre, I. M. (2021). Perspective for the Use of Adoption Theories in Artificial Intelligence. *16th Iberian Conference on Information Systems and Technologies, CISTI 2021*, Chaves, Portugal, 1-4. https://doi.org/10.23919/CISTI52073.2021.9476340

Matos, A. A. de & Nunes, A. M. (2018). Tecnologias da informação e comunicação no sistema de saúde Português Tecnologías de la información y comunicación en el sistema de salud portugués. *Journal of Health Informatics*, *10*(1), 30–34.

Monteiro, S. (2007). O Ciberespaço: o termo, a definição e o conceito. *DataGramaZero: Revista de Ciência Da Informação*, *8*(3), Não paginado. https://brapci.inf.br/index.php/article/download/7547

Oliveira, F., Ramos, I. & Santos, L. (2010). Definition of a crowdsourcing innovation service for the European SMEs. In *Current Trends in Web Engineering: Vol. 6385 LNCS* (pp. 412–416). https://doi.org/10.1007/978-3-642-16985-4_37

Raghupathi, W. & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. *Health Information Science and Systems*, *2*(1), 1–10. https://doi.org/10.1186/2047-2501-2-3

República Portuguesa. (1976). Constituição da República Portuguesa Decreto de aprovação da Constituição - Diário da República n . º 86 / 1976 , Série I de 1976-04-10 Princípios fundamentais. *Diário Da República*, *I*(86), 1–97.

República Portuguesa. (2019). Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho. *Diário Da República*, *1*(108), 2888–2895. https://dre.pt/application/file/a/122498847

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), 7–8. https://doi.org/10.1186/s41469-017-0017-y

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

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. https://doi.org/10.2471/BLT.18.227686