Universidade de Evora - Escola de Ciências Sociais

Mestrado em Políticas Públicas e Projectos

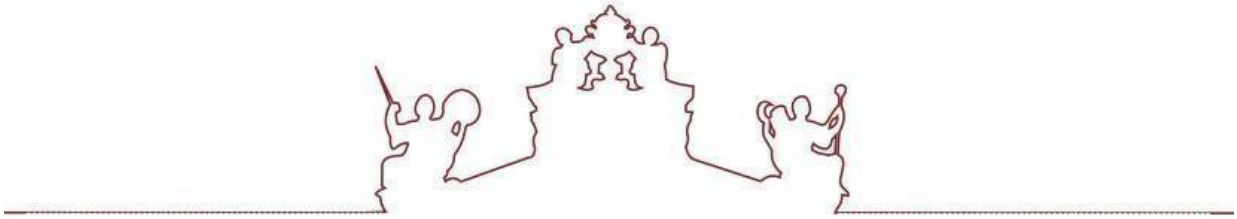
Dissertação

Telemedicina em Portugal: Uma realidade emergente com segurança insuficiente

Maria Helena Guerreiro Duarte

Orientador(es) | Marco Martins

Évora 2025



Universidade de Evora - Escola de Ciências Sociais

Mestrado em Políticas Públicas e Projectos

Dissertação

Telemedicina em Portugal: Uma realidade emergente com segurança insuficiente

Maria Helena Guerreiro Duarte

Orientador(es) | Marco Martins

Évora 2025

A dissertação foi objeto de apreciação e discussão pública pelo seguinte júri nomeado pelo Diretor da Escola de Ciências Sociais:

Presidente | Elsa Cristina Neves Janúario Vaz (Universidade de Evora)

Vogais | António Caleiro (Universidade de Evora) (Arguente)
Marco Martins (Universidade de Evora) (Orientador)

Évora 2025

Agradecimentos

Gostaria de expressar a minha profunda gratidão a todos que, de alguma forma, contribuíram para a realização deste trabalho.

Em primeiro lugar, agradeço aos meus pais, Telmo Duarte e Sandra Leal, pelo apoio incondicional, amor e paciência que me deram ao longo de toda a minha vida. Sem o vosso apoio e coragem, não teria chegado até aqui. Vocês sempre procuraram dar-me asas para seguir os meus magnânimos sonhos, e sou eternamente grata por me permitirem voar.

Aos meus amigos, que foram fundamentais nesta jornada. Agradeço-lhes por me mostrarem que não estava sozinha neste caminho e por me acompanharem sempre com alegria e confiança.

Um especial agradecimento ao meu orientador, Marco António Martins, que esteve sempre presente, atento às minhas necessidades e incansável até chegarmos ao nosso objetivo. A sua orientação, profissionalismo e sabedoria foram cruciais para a conclusão desta tese.

Agradeço também à Universidade de Évora, que me proporcionou um ambiente propício para o meu crescimento académico e pessoal. Agradeço a todos os professores que, ao longo deste percurso, partilharam os seus conhecimentos e contribuíram para a minha formação.

Por fim, um agradecimento a todas as pessoas que, de alguma forma, tocaram o meu caminho e trouxeram positividade. Agradeço a todos aqueles que me deram a palavra certa no momento certo, e que me permitiram crescer.

"A inovação é a capacidade de ver mudanças como uma oportunidade, não como uma ameaça." — Steve Jobs

Telemedicina em Portugal: Uma realidade emergente com segurança insuficiente

---

Resumo

A telemedicina, como subsecção da e-saúde, ganhou destaque no debate sobre segurança digital nas instituições de saúde, especialmente com a pandemia de Covid-19. Face à escassez de médicos e à sobrelotação dos serviços, tornou-se uma solução essencial para democratizar o acesso aos cuidados, permitindo consultas à distância. No entanto, a sua complexidade tecnológica expõe vulnerabilidades à cibercriminalidade. Esta dissertação analisa a evolução da telemedicina em Portugal, destacando a importância da cibersegurança na protecção da privacidade e da informação clínica. O trabalho inclui testemunhos médicos e identifica carências formativas na área. A pandemia forçou adaptações digitais no SNS, acelerando a aceitação popular e modernizando a comunicação médica. Conclui-se que a digitalização melhora a eficiência hospitalar, mas exige investimentos em infraestruturas e formação. A tecnologia digital foi determinante na gestão da pandemia, desde a compreensão do vírus à promoção de boas práticas. O reforço da cibersegurança é imperativo para garantir uma telemedicina segura e eficaz.

Palavras-Chave: Telemedicina, Telemedicina em Portugal, Cibersegurança, Plataformas Digitais, Pandemia Covid-19.

Telemedicine in Portugal: An emerging reality with insufficient security

---

Abstract

Telemedicine, as a subsection of e-health, has gained prominence in discussions on digital security within healthcare institutions, especially during the Covid-19 pandemic. In the face of physician shortages and overcrowded services, it became an essential solution for democratizing access to care, enabling remote consultations. However, its technological complexity exposes vulnerabilities to cybercrime. This dissertation analyses the evolution of telemedicine in Portugal, highlighting the importance of cybersecurity in protecting privacy and clinical information. The study includes medical testimonials and identifies training gaps in the field. The pandemic forced digital adaptations within the National Health Service (SNS), accelerating public acceptance and modernising medical communication. It concludes that digitalisation improves hospital efficiency but requires investment in infrastructure and education. Digital technologies were crucial in managing the pandemic, from understanding the virus to promoting good hygiene practices. Strengthening cybersecurity is imperative to ensure that telemedicine fully achieves its potential as a safe and effective means of delivering healthcare.

Keywords: Telemedicine, Telemedicine in Portugal, Cybersecurity, Digital Platforms, Covid-19 Pandemic.

Estrutura

Capítulo IV. Telemedicina e a Pandemia Covid-19

Conclusão

- **Introdução**

A prestação de cuidados de saúde encontra-se, desde há décadas, em processo de transformação, impulsionada pelo progresso tecnológico e pela necessidade de adaptação dos sistemas de saúde a novas exigências sociais, económicas e demográficas. Neste contexto, a telemedicina surge como uma das ferramentas mais promissoras na transição digital da saúde, permitindo a prestação de serviços clínicos à distância, através de tecnologias de informação e comunicação. A Organização Mundial da Saúde (WHO, 2010) reconhece a telemedicina como um instrumento estratégico para ampliar o acesso aos cuidados, reduzir desigualdades e melhorar a eficiência dos sistemas de saúde, especialmente em zonas remotas ou subatendidas.

Apesar de Portugal ter aderido à evolução da saúde digital e da prática médica remota, a implementação da telemedicina permanece assimétrica e fragmentada. Estudos como o de Dias (2014), centrado na cardiologia pediátrica na região Centro, demonstram o potencial da telemedicina, mas também revelam a disparidade no seu uso consoante as especialidades e as regiões. O relatório da Comissão de Acompanhamento da Intervenção Estratégica para o Desenvolvimento da Telemedicina (CIEDT, s.d.) evidencia avanços significativos em projetospiloto, embora saliente a falta de uniformidade nacional. A integração plena da telemedicina exige, por isso, um investimento continuado em infraestruturas, interoperabilidade de sistemas e uma abordagem centrada no utente, salvaguardando princípios éticos, deontológicos e legais.

A ausência de regulamentação específica, a carência de formação dos profissionais de saúde e a escassez de recursos técnicos são obstáculos que comprometem a sustentabilidade e a equidade da prática clínica digital. Pereira (2014) adverte para os riscos relacionados com a segurança do doente no contexto da telemedicina e da saúde eletrónica, apontando a necessidade de um quadro regulatório robusto e de mecanismos de responsabilização. Do ponto de vista ético e jurídico, autores como Stanberry (1998) alertam para a necessidade de clarificar os deveres profissionais, as responsabilidades clínicas e os limites legais da prática remota, sublinhando a importância de assegurar o consentimento informado, a confidencialidade e a proteção de dados.

Neste panorama, é fundamental refletir sobre o papel da Ordem dos Médicos, das administrações regionais de saúde e do próprio Ministério da Saúde na construção de um modelo funcional, seguro e integrado. A Ordem dos Médicos (s.d.), por exemplo, tem vindo a emitir pareceres sobre as condições jurídicas para o exercício da telemedicina, mas a ausência de normas específicas e detalhadas continua a criar zonas cinzentas na prática clínica diária. Monteiro (2008) argumenta que a telemedicina não deve ser vista apenas como uma extensão técnica do acto médico, mas como um vetor de transformação profunda no espaço da saúde e do bem-estar, exigindo novas lógicas organizacionais e uma visão estratégica de longo prazo.

Este trabalho adopta uma abordagem qualitativa, descritiva e exploratória, centrando-se numa revisão narrativa da literatura e análise documental normativa. Foram examinados documentos oficiais, legislação, despachos ministeriais, relatórios técnicos, artigos científicos e pareceres de entidades relevantes, com o objetivo de caracterizar a evolução e o estado atual da telemedicina em Portugal. A análise incidiu sobre três eixos fundamentais: (i) iniciativas institucionais e regionais no domínio da telemedicina, incluindo programas do Serviço Nacional de Saúde como o Projeto de Telemedicina no SNS (SNS, 2016); (ii) enquadramento normativo e ético-legal aplicável, onde se incluem contribuições fundamentais da WHO (1998), Pereira (2014) e Stanberry (1998); e (iii) cibersegurança em contexto de saúde digital, com ênfase na proteção da privacidade, na autenticação dos intervenientes e na responsabilidade clínica, conforme explorado por Santos (2015) no seu modelo de adoção tecnológica com base na reputação e privacidade do utilizador.

Ao abordar criticamente estas dimensões, pretende-se contribuir para uma compreensão aprofundada dos desafios e oportunidades associados à transformação digital da medicina em Portugal, oferecendo perspectivas para o desenho de políticas públicas mais eficazes, inclusivas e sustentáveis.

- Referências Bibliográficas

Comissão de Acompanhamento da Intervenção Estratégica para o Desenvolvimento da Telemedicina (CIEDT). (s.d.). Obtido de http://www.ciedt.org/

Dias, J. S. (2014). Telemedicina: Um estudo da cardiologia pediátrica na região centro.

Coimbra: Faculdade de Direito da Universidade de Coimbra.

Monteiro, M. H. (2008). A Telemedicina como um vetor de profunda transformação no espaço da saúde e do bem-estar. Obtido de https://www.repository.utl.pt/bitstream/10400.5/4859/1/210.pdf

Ordem dos Médicos. (s.d.). Informação jurídica – condições para exercício da telemedicina. Obtido a 5 de outubro de 2020, de https://ordemdosmedicos.pt/informacao-juridica-condicoes-para-exercicio-da-telemedicina/

Pereira, A. L. (2014). *Patient Safety in e-Health and Telemedicine*. Lex Medicinae – Revista Portuguesa de Direito da Medicina, 11, 95-106.

Pestana, O. (2009). Sistemas de informação de saúde em Portugal: Mito e realidade. Em L. F.

Santos, T. M. (2015). A reputação, a privacidade e o utilizador de telemedicina: Modelo de adoção de tecnologia. Coimbra; Oliveira do Hospital: Escola Superior de Educação de Coimbra; Escola Superior de Tecnologias e Gestão de Oliveira do Hospital.

Serviço Nacional de Saúde. (2016). Projeto de telemedicina no SNS. Obtido de https://www.sns.gov.pt/noticias/2016/12/12/projeto-de-telemedicina-no-sns/

Stanberry, *B.* (1998). *The Legal and Ethical Aspects of Telemedicine.* Royal Society Medicine Press.

World Health Organization Group Consultation on Health Telematics. (1998). *A Health Telematics Policy.* Geneva: World Health Organization.

World Health Organization. (2010). *Telemedicine in Member States - Opportunities and*

Developments. Report on the Second Global Survey on eHealth Global Observatory for eHealth

Series, Volume 2.

Capítulo I. Conceito Operacional da Telemedicina

1.1. O Início da Telemedicina: Fundamentação e Evolução

A Telemedicina, longe de ser um conceito recente fruto da imaginação contemporânea, possui raízes históricas profundas entrelaçando-se com o desenvolvimento tecnológico ao longo dos séculos. Conceptualmente, trata-se de uma técnica antiga que tem evoluído em paralelo com os avanços dos meios de telecomunicação disponíveis.

Uma das primeiras referências a cuidados de saúde à distância remonta ao século XIX, quando o correio era o principal canal comunicativo. Naquele tempo, os médicos compartilhavam informações com os seus pacientes ou com outros médicos por correspondência. Naturalmente, a velocidade de transmissão de informação era muito insuficiente, comprometendo, em certa medida, a eficácia do tratamento. Curiosamente, algumas perspectivas sugerem que a Telemedicina pode ter origens ainda mais remotas, considerando que a comunicação de surtos de peste em povoações por meio de fogueiras ou outros sinais pode também ser vista como uma forma primitiva de Telemedicina.

A Telemedicina é, em essência, uma consequência direta da revolução tecnológica. O seu desenvolvimento, ainda que não inicialmente projetado, teve início com a invenção do computador por *Charles Babbage* em 1834, e foi impulsionado pela revolução nas telecomunicações, particularmente através da criação de redes militares durante o período da Guerra Fria. As primeiras experiências concretas de Telemedicina ocorreram na década de 1960. Em 1960, o Instituto Psiquiátrico do *Nebraska*, nos Estados Unidos, foi interligado ao hospital de *Norfolk*, marcando um dos primeiros usos documentados da Telemedicina. Posteriormente, em 1967, a Universidade de *Harvard* estabeleceu uma linha de comunicação entre o *Massachusetts General Hospital* e o Aeroporto de *Boston* para responder a emergências médicas no aeroporto.

De acordo com Monteiro (2008), "a Telemedicina teve um desenvolvimento muito acentuado a partir de meados de 1990, com fortes investimentos em novos projetos, onde médicos informados destas novas potencialidades viram a oportunidade de desenvolver novos formatos

de prestação de cuidados de saúde" (p. 3). Este período foi crucial para a consolidação da Telemedicina como uma prática inovadora e indispensável no fornecimento de assistência à saúde, refletindo a interseção entre a medicina e as inovações nas tecnologias de informação e comunicação.

Este percurso histórico revela que a Telemedicina, embora moldada pelas inovações tecnológicas, está enraizada numa prática contínua de adaptação e evolução que tem como objetivo ampliar o acesso aos serviços de saúde, superando as barreiras geográficas e temporais.

1.1.1. O Conceito de Telemedicina: Fundamentação e Implicações

A Telemedicina é o conjunto de tecnologias e ferramentas que permite a realização de práticas médicas remotamente. Com o progresso dos meios de comunicação, tornou-se comum que o contato entre médico e paciente aconteça à distância, sem comprometer a qualidade do atendimento. As aplicações desta técnica têm demonstrado respostas positivas seja por parte dos especialistas da área de saúde, seja por parte dos indivíduos atendidos , evidenciando a sua eficácia e relevância no contexto atual mostrando adaptar-se á sistematização de conceitos, de Adriano Moreira, mais especificamente os conceitos operacionais que conjugam o “sentido das coisas de forma focada, das estruturas e das relações”, destinando-se a “sistematizar a realidade observável” e adaptar-se a “relações e necessidades do objeto do método”.

Segundo a definição da Organização Mundial da Saúde (OMS), Telemedicina é "a oferta de serviços relacionados aos cuidados com a saúde, nos casos em que a distância é um fator crítico; tais serviços são providos por profissionais da área da saúde, utilizando tecnologias de informação e comunicação para o intercâmbio de informações válidas para diagnósticos, prevenção e tratamento de doenças, e a educação contínua de prestadores de serviços em saúde, bem como para funções de pesquisa e avaliação; tudo no interesse de melhorar a saúde dos indivíduos e das comunidades".

Complementando esta visão, Monteiro (2008) afirma que “a Telemedicina é a designação mais longínqua que se relaciona prioritariamente com a possibilidade de realizar teleconsultas e telediagnósticos à distância, baseados em resultados provenientes de imagens, textos ou sons de observações e exames médicos, seja em tempo real ou em tempo diferido” (pág.3).

Este enquadramento conceptual sublinha a capacidade da Telemedicina de transcender as limitações geográficas, proporcionando a obtenção a serviços de saúde de alto padrão, independentemente da localização do paciente. Através da Telemedicina, as barreiras físicas são superadas, permitindo um intercâmbio eficaz de informações médicas e promovendo a melhoria contínua dos serviços de saúde.

1.1.2. Aplicabilidade da Telemedicina: Onde e Como É Utilizada

A Telemedicina tem sido progressivamente integrada em hospitais e organizações de saúde que, ao formar colaborações com outras instituições reconhecidas, procuram otimizar o

processo de consulta e troca de informações. Esta tecnologia revela-se abrangente e indiscriminatória, adaptando-se a diversas necessidades do setor da saúde e beneficiando todos os seus intervenientes.

Entre as suas principais aplicações, destaca-se a disseminação de estudos científicos e relatos clínicos, essenciais para a formação continuada dos profissionais e para a avaliação de novas abordagens terapêuticas.

Simultaneamente, a partilha de informação clínica entre especialistas e pacientes melhora a comunicação e permite uma tomada de decisão mais informada. No acompanhamento de doentes crónicos, idosos e grávidas de alto risco, esta tecnologia possibilita um seguimento personalizado, garantindo maior proximidade e intervenção atempada.

A acessibilidade é igualmente potenciada ao facilitar a assistência a pacientes com mobilidade reduzida, eliminando barreiras geográficas e assegurando a continuidade dos cuidados. Adicionalmente, a construção de bases de dados epidemiológicas permite a monitorização de tendências em saúde pública, favorecendo a prevenção e o controlo de doenças.

No âmbito do estudo de patologias graves, a Telemedicina facilita a partilha de casos clínicos complexos, promovendo o intercâmbio de conhecimento e o desenvolvimento de novas abordagens terapêuticas. Para os profissionais de saúde, proporciona a possibilidade de ensino remoto, facilitando a atualização contínua em diversas especialidades.

A promoção da saúde e a prevenção de complicações também são aspetos centrais, incentivando os pacientes a assumirem um papel ativo na gestão do seu estado clínico. Além disso, a realização de intervenções cirúrgicas assistidas por robôs operados remotamente representa uma das vertentes mais inovadoras, aumentando a precisão e a segurança dos procedimentos.

Desta forma, a Telemedicina consolida-se como um elemento essencial na evolução dos cuidados de saúde, potenciando a acessibilidade, a eficiência e a inovação na prestação de serviços médicos.

A evolução tecnológica tem impulsionado diferentes modalidades de Telemedicina, ampliando as possibilidades no setor da saúde. Entre as principais abordagens, a teleconsulta permite a interação remota entre pacientes e profissionais de saúde, viabilizando diagnósticos e

tratamentos através de ferramentas digitais que asseguram a transmissão segura de informações clínicas.

Paralelamente, a teleinterconsulta fortalece a colaboração entre especialistas, promovendo uma análise mais aprofundada dos casos e facilitando a obtenção de segundas opiniões, o que contribui para diagnósticos mais precisos e abordagens terapêuticas mais eficazes.

A telemonitorização por sua vez, assume um papel determinante no acompanhamento de doentes crónicos, possibilitando um seguimento contínuo e intervenção precoce. A integração de biossensores e softwares especializados permite a recolha de sinais vitais, enquanto equipas de saúde asseguram a monitorização regular e orientações adaptadas às necessidades clínicas.

Por fim, a telecirurgia representa uma das inovações mais disruptivas, combinando robótica e realidade virtual para a realização de intervenções à distância com elevado grau de precisão e segurança. Esta abordagem expande o acesso a cuidados cirúrgicos especializados, beneficiando regiões com limitações na oferta de serviços médicos.

Deste modo, a diversidade das aplicações da Telemedicina reforça o seu impacto na eficiência dos cuidados de saúde, consolidando-se como uma ferramenta essencial para a modernização do setor.

Em síntese, a Telemedicina está moldando uma nova era na prática médica, onde a tecnologia alinha-se às exigências dos doentes e dos especialistas de saúde, promovendo um atendimento mais acessível, eficiente e seguro. A contínua evolução destas modalidades tecnológicas reflete a capacidade de adaptação e integração da telemedicina aos desafios contemporâneos da saúde, proporcionando benefícios significativos para toda a sociedade.

1.2. A Urgência da Telemedicina: Necessidades e Justificação

A Telemedicina surge como uma tentativa significativa de democratizar o atendimento em sistemas de saúde. Em face do crescente congestionamento nos consultórios médicos e da escassez de profissionais disponíveis, que frequentemente leva a longas filas de espera e salas de atendimento sobrecarregadas, a Telemedicina configura-se como uma solução diferenciada.

Este avanço permite que a saúde se torne acessível a todos, independentemente do tempo e do local, oferecendo uma alternativa viável para o atendimento médico.

A implementação da Telemedicina beneficia não apenas os pacientes, que em muitos casos precisam percorrer distâncias consideráveis para uma consulta, mas também amplia as oportunidades para os profissionais de saúde. Estes, ao utilizarem novas ferramentas tecnológicas, têm a capacidade de alcançar novos círculos de pacientes e diversificar suas práticas de maneira significativa.

Neste contexto, plataformas emergentes como a Doctorino[1] destacam-se como pioneiras na oferta de serviços de Telemedicina no mercado português. Estas plataformas projetam construir uma realidade onde o atendimento em sistemas de saúde é otimizado e inovador, ampliando a oferta de serviços e proporcionando um acesso mais amplo e eficiente aos cuidados médicos.

A telemedicina tem vindo a ser progressivamente integrada nos sistemas de seguros de saúde, como evidenciado pela prática observada na França. Neste país, a telemedicina é atualmente contemplada pelos seguros de saúde com o objetivo de reconhecer as teleconsultas como uma alternativa tão viável quanto as consultas presenciais. O intuito é assegurar que as teleconsultas cumpram "os mesmos critérios e requisitos de qualidade estabelecidos para os atendimentos físicos, promovendo assim uma equidade no acesso e na eficácia dos cuidados médicos" (Vasconcelos da Cunha et al., 2004).

Neste contexto, a telemedicina configura-se não apenas como uma inovação tecnológica, mas como uma resposta a uma série de necessidades que se perpetuam por diferentes períodos históricos. Ela manifesta a capacidade de oferecer "cuidados médicos de alta qualidade em qualquer momento e lugar, demonstrando um compromisso contínuo com a excelência e a acessibilidade na saúde" (Monteiro, 2008). A evolução da telemedicina é, portanto, um reflexo da constante procura pelo melhoramento no atendimento em sistemas de saúde, evidenciando

[1] Doctorino é uma plataforma digital que facilita a marcação autónoma de consultas médicas para os utilizadores. Criada por Nuno Gonçalves, especialista em marketing, e José Cautela, médico, a iniciativa foi lançada em dezembro de 2019, com um investimento inicial de meio milhão de euros. A plataforma, que já inclui mais de mil profissionais em Lisboa e no Porto, ajuda a construir uma presença digital para os médicos e otimiza a gestão de agendas, uma tarefa de grande impacto nos recursos humanos.

a aplicação das melhores práticas disponíveis para atender para atender às demandas dos doentes e especialistas de saúde.

1.2.1 Metas e Propósitos da Telemedicina: Uma Visão Focada

O principal objetivo da telemedicina é fornecer cuidados de saúde a pacientes que enfrentam restrições na mobilidade, que estão em ambientes perigosos ou representam um risco para a equipa médica. Esta abordagem adequa-se a situações em que o tratamento não pode ser realizado pelos métodos tradicionais e exige a adaptação de regras e procedimentos para garantir um atendimento eficaz.

A telemedicina estabelece-se como uma abordagem moderna para acompanhar pacientes, partilhar dados clínicos e interpretar resultados de diagnósticos. Estes diagnósticos são analisados e transmitidos digitalmente, complementando a prática médica convencional. Atualmente, a telemedicina é amplamente aplicada a nível global, respeitando os regulamentos e normas médicas em vigor, de forma segura.

O uso de tecnologias de informação, que melhoram a rapidez e a qualidade na partilha de conhecimento, permite aos médicos tomar decisões com mais rapidez e exatidão. Com a telemedicina, os especialistas conseguem aceder a exames a partir de qualquer lugar, utilizando computadores e dispositivos móveis, como smartphones e tablets com ligação à internet.

A telemedicina representa uma superação das barreiras e limitações dos serviços de saúde, facilitando a conexão remota entre prestadores de serviços e especialistas, hospitais de referência e centros de saúde. O principal desafio está na integração da telemedicina nos serviços de saúde existentes, o que requer a organização adequada das consultas e a capacitação dos profissionais envolvidos.

1.2.2. As Vantagens da Telemedicina: Impactos Positivos na Saúde

Os benefícios proporcionados pela telemedicina são amplamente reconhecidos e incluem diversas vantagens operacionais e estratégicas, que contribuem para a qualidade e o desempenho dos serviços de saúde.

Entre as vantagens principais, destacam-se diversos aspetos fundamentais. A eliminação da necessidade de deslocação física traduz-se na redução de custos e do tempo despendido pelos pacientes, sendo particularmente vantajosa para populações em zonas remotas. Paralelamente, a rapidez no acesso a opiniões especializadas permite uma resposta imediata em situações de urgência, otimizando a assistência em casos críticos.

A Telemedicina também se revela essencial na gestão hospitalar, ao mitigar a sobrelotação e reduzir os riscos de infeções hospitalares, promovendo um uso mais eficiente das infraestruturas de saúde. A descentralização dos serviços permite que um maior número de pacientes beneficie de atendimento médico sem comprometer a capacidade dos estabelecimentos de saúde.

No âmbito académico e científico, a Telemedicina fomenta a cooperação entre investigadores, favorecendo a partilha de informação clínica e contribuindo para o avanço da investigação médica. Adicionalmente, possibilita a formação e capacitação contínua de profissionais de saúde, independentemente da sua localização, assegurando a atualização permanente dos conhecimentos e a melhoria global da qualidade assistencial.

Assim, a Telemedicina não só transforma a prestação de cuidados de saúde, mas também consolida uma abordagem inovadora e sustentável, alinhada com as exigências contemporâneas do setor.

A primeira grande vantagem da telemedicina foi notoriamente percebida na atenção básica a grupos reduzidos situados em áreas geográficas e/ou socioculturais isolados dos principais centros urbanos. Estas áreas frequentemente apresentam altas taxas de mortalidade devido à escassez de profissionais qualificados e à falta de recursos de apoio ao diagnóstico local. O isolamento intelectual e a falta de recursos especializados são desafios significativos que a telemedicina pode ajudar a superar.

Como destacado pela Associação Médica Americana:

"A telemedicina é uma ferramenta poderosa que pode fornecer acesso a cuidados de saúde para transações anteriormente inacessíveis e melhorar a eficiência e a qualidade dos serviços de saúde."

Anteveem-se que a telemedicina alargue as funções dos técnicos de saúde, conectando-os aos serviços prestados por hospitais e centros especializados. Esta articulação garante um sistema de atendimento contínuo que inclui prevenção, diagnóstico e terapêutica, favorecendo uma abordagem mais completa e eficiente na prestação de cuidados de saúde.

1.3. Obstáculos Críticos da Telemedicina: Análise dos Desafios

Embora a telemedicina ofereça vastas possibilidades e benefícios para o âmbito da saúde, a sua introdução em larga escala ainda enfrenta uma série de desafios significativos. Estes obstáculos impedem que os recursos disponíveis sejam amplamente utilizados, limitando assim o potencial da telemedicina em diversas regiões.

Entre as principais barreiras encontram-se questões de infraestrutura, como a baixa conectividade à internet e o fornecimento irregular de eletricidade em áreas remotas. Adicionalmente, muitos dos equipamentos de comunicação utilizados não são adequados para operar em diferentes condições climáticas, o que compromete a sua funcionalidade em certas regiões. Fatores culturais também desempenham um papel crucial, visto que existe uma relutância por parte de certos profissionais de saúde em aceitar modelos de atendimento que se afastam das práticas convencionais. Esta resistência cultural é reforçada por questões legais, incluindo a ausência de uma regulamentação internacional padronizada que suporte a prática da telemedicina de maneira consistente e segura.

Adicionalmente, a ausência de pesquisas abrangentes sobre a relação custo-eficácia e a eficácia da telemedicina restringe a sua implementação em nível mundial. Embora a telessaúde tenha demonstrado seu valor em várias situações, a implementação dessas tecnologias é frequentemente restringida pelos elevados custos associados aos equipamentos, transporte, manutenção e formação de profissionais de saúde. A capacitação desses profissionais exige investimentos significativos, não só em termos de recursos monetários, mas igualmente em relação ao tempo e empenho para assegurar que a formação seja pertinente e eficiente. A conectividade à internet é atualmente um dos obstáculos mais visíveis em várias realidades. Muitas localidades, e até mesmo regiões inteiras, enfrentam sérias limitações na ligação á web, o que compromete a implementação generalizada da telemedicina. Para que essa prática possa ser verdadeiramente eficaz, é necessário que ocorra uma modernização do setor, permitindo que o acesso à informação seja facilitado e que a formação dos profissionais de saúde seja sólida e contínua. No entanto, esta modernização apresenta-se como um desafio, estando dispersa e abstrata em muitos contextos, embora já demonstre um efeito benéfico no processo de cuidados de bem-estar da população.

Outro ponto crítico que requer atenção é a necessidade de estabelecer políticas sólidas de privacidade e confidencialidade no uso da telemedicina. As informações dos pacientes, quando

são transferidas e armazenadas digitalmente, devem ser protegidas contra acessos não autorizados. Além disso, a troca de informações entre técnicos de saúde e entre diferentes jurisdições precisa ser regulada de forma a garantir que a privacidade dos pacientes seja respeitada. A verificação da identidade dos profissionais de saúde durante a comunicação eletrónica, especialmente por *e-mail*, é também uma preocupação crucial, uma vez que a segurança das informações trocadas depende dessa confirmação.

No panorama internacional, todas as nações enfrentam dilemas éticos relacionados com a ética profissional, a proteção da informação, o respeito à integridade e a salvaguarda da privacidade de dados no domínio das Tecnologias de Informação e Comunicação (TIC). Uma das discussões mais fervorosas concentra-se na aplicação da telemedicina por parte de profissionais de saúde de várias regiões, onde a falta de regulamentação internacional clara levanta dúvidas sobre a responsabilidade pelos serviços prestados.

Para além disso, a falta de pesquisas consistentes sobre a eficácia e a relação custo-eficácia da telessaúde dificulta a tarefa de persuadir os decisores políticos e investidores a apoiarem uma implementação mais abrangente. Este é um entrave significativo que impede o avanço da telemedicina, especialmente em contextos onde a alocação de recursos é limitada e decisões precisam ser justificadas por dados concretos.

Outro desafio a ser superado está relacionado à dependência dos recursos locais para o tratamento dos pacientes, mesmo quando o diagnóstico é facilitado pela telemedicina. A eficácia da telessaúde pode ser afetada pela escassez de medicamentos, pela insuficiência e pela má qualidade dos recursos médicos, bem como pela falta de profissionais competentes nas áreas atendidas. Sem um conhecimento aprofundado da realidade local, é complicado implementar a telemedicina de modo a satisfazer as verdadeiras necessidades da comunidade.

Contudo, apesar desses desafios, várias nações têm obtido resultados favoráveis com a adoção da telessaúde. Um dos principais incentivos para o uso dessas tecnologias tem sido o potencial para reduzir a necessidade de transporte e encaminhamento de pacientes a grandes centros urbanos. Adicionalmente, a telemedicina ajuda a estabelecer os profissionais de saúde em áreas rurais, proporcionando apoio constante e possibilidades de crescimento profissional, o que, em última análise, promove uma prática médica mais sustentável e abrangente.

1.3.1. Panorama Internacional da Telemedicina: Adoção e Impactos

A telemedicina, um campo em constante evolução, teve as suas primeiras experiências bemsucedidas na década de 1970, em Itália, quando a Universidade de Roma implementou o Tele- ECG em cerca de 50 hospitais em todo o país. Este marco não apenas impulsionou a inovação no setor, mas também levou, em 1989, à criação de uma associação que envolveu várias universidades e centros de pesquisa, resultando no surgimento de diversas empresas de telemedicina na Itália.

O reconhecimento oficial da consulta médica à distância pela Organização Mundial da Saúde (OMS) ocorreu no princípio da década de 90. Na nação norte-americana, no mesmo período, a criação da *American Telemedicine Association* (ATA) consolidou a prática, disseminando-se rapidamente por países da Europa e da Ásia, refletindo uma visão compartilhada sobre o potencial da telemedicina.

Nos Estados Unidos, a telemedicina é utilizada há mais de 30 anos em diversas especialidades médicas e em diferentes etapas do tratamento dos pacientes. Esta prática foi inicialmente adotada para facilitar o acesso aos serviços de saúde, especialmente para indivíduos em localidades distantes, ao mesmo tempo em que contribuía para a redução de custos logísticos e humanos. Um exemplo notável é o uso da telemedicina para atender pacientes idosos e veteranos de guerra, cuja mobilidade é frequentemente limitada. Ao reduzir a necessidade de deslocamentos frequentes, a telemedicina não só diminui os custos associados ao transporte, mas também minimiza o stress dos pacientes.

Na América Latina, apesar dos debates contínuos sobre a viabilidade e eficácia da telemedicina, a pandemia Covid-19 acelerou a sua adoção. A Ordem dos Médicos e a Secretaria de Saúde em vários países latino-americanos autorizaram a prática, refletindo uma necessidade urgente de adaptação às novas circunstâncias impostas pela crise pandémica.

A experiência dos centros de referência nos Estados Unidos, Europa e Ásia demonstra o potencial da telemedicina em áreas como dermatologia e cirurgia. Através de videoconferências e do uso de braços robóticos controlados à distância, estes centros têm explorado novas fronteiras na prática médica. Além disso, a telemedicina foi adaptada para situações sensíveis, como o “teleaborto”, implementado em clínicas de ginecologia nos

Estados Unidos, refletindo a crescente necessidade de soluções inovadoras para problemas complexos durante a pandemia.
Em França, a telemedicina, que antes encontrava resistência entre os profissionais de saúde, experimentou um crescimento exponencial durante a pandemia. O número de teleconsultas aumentou de 10 mil por semana para mais de 1,1 milhão, demonstrando uma mudança significativa na perceção e na utilização desses serviços. De maneira semelhante, no território britânico, o Serviço Público de Saúde (SPS) viu um aumento substancial no número de consultas online, com a maioria dos atendimentos sendo realizados à distância.

Taiwan, um território que se destacou pela sua resposta eficaz à pandemia Covid-19, rapidamente legalizou temporariamente a telemedicina no início do surto. Esta medida foi crucial para garantir o distanciamento social e para desocupar hospitais e centros de saúde para atendimento dos casos mais graves, ao mesmo tempo que assegurava atendimento médico para pacientes com quadros leves.

Apesar do avanço global da telemedicina, as abordagens ainda variam significativamente de país para país, refletindo diferenças nas regulamentações, infraestrutura de saúde, cultura e disponibilidade de tecnologia. A colaboração internacional e a troca de melhores práticas são essenciais para uma expansão bem-sucedida da telemedicina a nível global, garantindo que as inovações neste campo sejam amplamente acessíveis e eficazes, independentemente do contexto local.

Assim, a telemedicina não só democratiza o ingresso aos serviços de saúde, assim como enfrenta o desafio de assegurar que todos os intervenientes tenham acesso aos recursos tecnológicos e às plataformas necessárias para uma transição digital harmoniosa e inclusiva.

1.3.2. Países Pioneiros em Telemedicina: Modelos de Sucesso Global

O recurso às tecnologias de comunicação no setor médico iniciou-se no princípio do século XX, inaugurando uma fase de avanços que iriam modificar de forma significativa o exercício da medicina. Em 1906, *Willem Einthoven*, laureado com o Prémio Nobel e inventor do eletrocardiograma, deu início a experiências pioneiras ao realizar consultas à distância utilizando a rede telefónica. *Einthoven* não apenas descreveu o procedimento para a realização do eletrocardiograma (ECG) por telefone, como também estabeleceu as bases para a telemedicina moderna.

Em 1910, na Inglaterra, foi criado o primeiro estetoscópio elétrico, operado por meio de uma chamada telefónica, o que representou um avanço significativo na capacidade de monitorização remota dos pacientes. Durante a Primeira Guerra Mundial, a partir de 1916, a utilização do rádio permitiu uma comunicação crucial entre médicos posicionados em zonas costeiras e na frente de batalha, ligando-os a hospitais móveis e embarcações para oferecer suporte médico e dados logísticos fundamentais.

Outro marco significativo ocorreu em 1948, quando foram transmitidas pela primeira vez imagens radiológicas por telefone entre *West Chester* e Filadélfia, demonstrando o potencial das telecomunicações para o diagnóstico médico à distância. Nos anos 50, especialistas em radiologia do Hospital Jean-Talon, em Montreal, no Canadá, avançaram ainda mais ao desenvolver a teleradiologia, um campo que permitiria a análise de imagens médicas a partir de locais remotos, expandindo as fronteiras do atendimento especializado.

Estas inovações pioneiras não abriram apenas caminho para uma ampla gama de possibilidades na aplicação das tecnologias emergentes na área da saúde, mas também inspiraram o surgimento de diversos projetos e instituições dedicadas a explorar estas novas fronteiras. Estes esforços iniciais estabeleceram as bases para o desenvolvimento contínuo da telemedicina, que continua a evoluir e a expandir o seu alcance, proporcionando novas possibilidades para a oferta de serviços de saúde de excelência a comunidades cada vez mais vastas e variadas.

Instituição Médica de Nebraska

Em 1955, o Hospital Psiquiátrico de Nebraska tornou-se uma das primeiras instituições nos EUA a implementar um sistema interno de televisão. Em 1964, com apoio do Instituto Nacional de Saúde Mental, foi criada uma ligação bidirecional entre o Hospital Psiquiátrico e o Hospital Estadual de Norfolk, localizado a 180 quilómetros de distância. Esta conexão era empregada tanto para propósitos educacionais quanto para consultas entre especialistas e médicos de família. Em 1971, a Instituição Médica de Nebraska foi interligada ao Hospital de Veteranos de Omaha, e o mesmo processo foi aplicado em mais duas localidades.

STARPAHC (*Space Technology Applied to Rural Papago Advanced Health Care*)

Este programa, desenvolvido entre 1972 e 1975, ofereceu assistência médica à reserva indígena Papago, no Arizona. Idealizado pela NASA (National Aeronautics and Space Administration) e executado em colaboração com a Lockheed, o projeto foi criado e avaliado pela comunidade de Papago, pelo Serviço de Saúde Indígena e pelo Departamento de Saúde, Educação e Bem-Estar dos EUA. As metas fundamentais consistiam em oferecer assistência médica tanto aos astronautas no espaço como aos habitantes da reserva Papago. Para estes últimos, uma viatura equipada com vários aparelhos médicos, operada por dois paramédicos nativos, foi ligada a especialistas hospitalares através de uma conexão bidirecional por microondas, que possibilitava a transmissão de som.

Hospital Geral de Massachusetts/Centro de Saúde do Aeroporto Internacional Logan (Boston)

Esta unidade foi estabelecida em 1967 para oferecer assistência médica tanto aos funcionários do aeroporto como aos passageiros. Os profissionais de saúde do hospital atendiam os doentes na unidade de saúde através de uma conexão audiovisual bidirecional. O centro dispunha de técnicos de enfermagem disponíveis a todo o momento, encarregues de avaliar e identificar os doentes que precisavam de cuidados.

Demonstração Biomédica ATS-6 do Alasca:

No ano de 1971, a Biblioteca Nacional de Medicina, através do Centro de Comunicação Biomédica, escolheu 26 locais no Alasca para investigar de que forma a utilização de transmissão de vídeo via satélite poderia aprimorar a excelência dos serviços de saúde na região. Foi empregado o ATS-1, o satélite inaugural da série da NASA, lançado em 1966, e que funcionou de 1971 a 1975. Em quatro desses pontos, foram montadas estações de receção de satélite que possibilitavam a transmissão e receção de vídeo em tonalidades monocromáticas, enquanto um quinto ponto permitia apenas a receção do vídeo. Todas as localidades estavam dotadas de conexões bidirecionais de som.

Exigências de Vídeo para Telediagnóstico:

Em 1974, a NASA e a SCI Systems de Houston realizaram um estudo para identificar os critérios mínimos necessários para a execução de telediagnósticos. A experiência foi realizada utilizando um sistema de simulação, onde uma fita de alta qualidade, contendo exames clínicos feitos por uma enfermeira sob a supervisão de um médico através de um circuito de televisão fechado, serviu como referência. Esta fita foi eletronicamente comprometida para simular sistemas de baixa qualidade de transmissão. A gravação comprometida, manipulada por um procedimento estatístico não determinístico, foi então apresentada a um vasto conjunto de profissionais de saúde. Estes tentaram chegar a um diagnóstico preciso e identificar sinais físicos nos doentes. Foram analisados seis sistemas de transmissão distintos.

Universidade Memorial de Newfoundland (MUN):

A MUN (Memorial University of Newfoundland) foi uma das instituições pioneiras no

Programa Espacial do Canadá. O satélite Hermes, resultado de uma parceria entre o Canadá e os Estados Unidos, ofereceu ao Canadá a oportunidade de empregar tecnologia de satélite para formação à distância e assistência médica.

Desde 1977, o Centro de Telemedicina da MUN dedicou-se à criação de redes de som interativas para iniciativas educativas e partilha de informações médicas. A plataforma de videoconferência da MUN, uma rede constituída por cinco conexões especializadas, iniciou operações em 1977. A MUN também esteve envolvida em teleconferências internacionais e, em 1985, integrou o projeto do satélite internacional Intelsat, demonstrando a utilização eficaz e económica da tecnologia de telemedicina.

Telemedicina no Norte-Oeste:

Lançado em 1984 na Austrália, esta iniciativa visava testar uma inovadora infraestrutura de transmissão via satélite, chamada Q-network. Um dos objetivos centrais da iniciativa era garantir assistência médica ás comunidades de cinco localidades isoladas no sul da Carpentária. A Q-network era composta por 20 pontos de transmissão com ligações bidirecionais e apenas 20 para receção. Todas as localidades foram equipadas com equipamentos de comunicação e envio de documentos. A análise realizada indicou que a tecnologia utilizada teve melhorias na qualidade dos cuidados médicos prestados aos residentes da área coberta pela rede.

Conexão Espacial NASA para Arménia/Ufa

Em 1989, a NASA lançou o primeiro projeto global de telemedicina, conhecido como “ponte espacial” que conectava a Arménia a Ufa. No mês de Dezembro de 1988, um poderoso sismo afetou a República Soviética da Arménia, resultando na oferta de assistência dos Estados Unidos á União Soviética para a realização de atendimentos médicos na área da tragédia. Com a colaboração e a fiscalização de uma equipa conjunta EUA/URSS em biologia espacial, foram efetuadas sessões de telemedicina utilizando vídeo, áudio e fac-simile entre a unidade de saúde em Yerevan, Arménia, e quatro instituições de saúde nos EUA. Esta iniciativa que atendimentos de saúde podiam ser efetuados por meio de uma rede de satélites, ultrapassando barreiras governamentais, culturais e comunitárias.

O desenvolvimento da telemedicina na Europa teve os seus primeiros marcos significativos durante a década de 1970. No entanto, foi somente no final do ano de 1980 que se observou um investimento substancial na área, impulsionado pela Comunidade Europeia por meio da iniciativa focada em tecnologias de comunicação à distância na medicina, designada como AIM (Advanced Informatics in Medicine). Entre 1989 e 1990, a fase inicial do programa AIM foi realizada através da execução de 42 iniciativas, das quais se sobressaem o ADAM (Advanced Architecture in Medicine), o AEMI (Advanced Environment for Medical Image Interpretation) e o KISS (Knowledge-based Interactive Signal Monitoring System). O principal êxito desta fase inicial foi a criação de uma comunidade AIM, composta por aproximadamente 3.000 indivíduos, incluindo profissionais de saúde e investidores, que se dedicaram a estabelecer objetivos e especificações para a telemedicina.

Entre 1991 e 1994, a iniciativa AIM prosseguiu sob a denominação "*Telematics Applications in Areas of General Interest"*, período em que existiu um aumento substancial no investimento comparado à fase anterior. Durante essa etapa, o foco principal foi o desenvolvimento de protótipos e a realização de aplicações de base, testando e avaliando a aceitação por parte dos pacientes. Entre os projetos mais significativos dessa fase destacam-se o FEST (*Framework for European Services in Telemedicine*) e o EPIC (*European Prototype for Integrated Care*). A

iniciativa FEST destacou-se por criar uma solução de telemedicina que possibilitava a formulação de decisões em conjunto entre vários hospitais locais e um centro de especialização. Por sua vez, a iniciativa EPIC foi orientada para a criação de uma rede de teleassistência voltada para seniores e indivíduos com limitações.

Ao longo do intervalo de 1995 a 1998, com a etapa de progresso do "*Framework Programme IV*"[2] , a União Europeia intensificou ainda mais o financiamento nas soluções de dados e interação direcionadas ao setor da saúde. Esta iniciativa foi fundamental para reconhecer as necessidades dos pacientes e possibilitar a criação de modelos experimentais e ferramentas que validassem opções tecnológicas e analisassem a receção destas inovações pelos pacientes.

Com o progresso das comunicações, englobando infraestruturas digitais e antenas espaciais, a medicina à distância na Europa continuou a desenvolver-se de maneira progressiva. Um marco histórico neste contexto ocorreu a setembro de 2001, com a realização da primeira operação transatlântica, viabilizada por uma chamada telefónica de qualidade constante e pelo uso de

um robô, demonstrando assim o potencial revolucionário da telemedicina e a sua capacidade de transcender barreiras geográficas.

Estas iniciativas evidenciaram o papel central da Europa no avanço da telemedicina, criando um modelo que combina inovação tecnológica com o foco nas necessidades dos pacientes, abrindo caminho para a evolução contínua desta área no mundo inteiro.

O papel desempenhado pelos países pioneiros no desenvolvimento da telemedicina tem sido crucial para demonstrar os benefícios e a viabilidade desta prática inovadora. A contribuição destes países foi essencial para estabelecer as bases técnicas, legais e éticas que permitiram à telemedicina converter-se num recurso eficiente na oferta de serviços de saúde. Através de

[2] Os Programas-Quadro (FP) da União Europeia, lançados pela Comissão Europeia, têm como objetivo promover a investigação no Espaço Europeu de Investigação (ERA). Ao longo de oito edições, de FP1 a FP8, as prioridades evoluíram: do enfoque inicial em pesquisa tecnológica nos FP6 e FP7, até o foco em inovação no Horizon 2020 (FP8), visando crescimento económico e soluções para utilizadores finais, principalmente entidades governamentais.

iniciativas pioneiras, como as que foram realizadas nos Estados Unidos, Canadá, e países europeus, foi possível testar, implementar e refinar tecnologias que hoje são indispensáveis para o atendimento médico à distância.

Estes esforços iniciais não demonstraram apenas a eficácia da telemedicina em contextos específicos, como também inspiraram outras nações a adotarem práticas semelhantes, promovendo assim uma expansão global da acessibilidade aos serviços de saúde. Nos Estados Unidos, a aplicação da telemedicina em áreas remotas e em grupos de pacientes com mobilidade reduzida evidenciou o potencial desta tecnologia para superar barreiras geográficas e logísticas, oferecendo uma solução prática e eficiente para problemas de acesso.

Com a evolução da telemedicina, observa-se uma adoção crescente desta prática em diversos países ao redor do mundo. Países em desenvolvimento e desenvolvidos têm reconhecido as vantagens de integrar a telemedicina nos seus sistemas de saúde, procurando melhorar o acesso aos cuidados médicos, reduzindo custos e otimizando a utilização dos recursos disponíveis.

Em suma, o desenvolvimento e a expansão da telemedicina demonstram um compromisso internacional com o desenvolvimento progressivo e contínuo dos cuidados de saúde. A adoção de práticas de telemedicina numa escala global não amplia apenas o acesso ao atendimento médico, mas também representa um avanço significativo na procura por uma rede de saúde mais justa e eficaz, que possa atender às necessidades de todas as populações, independentemente da sua localização ou circunstâncias.

1.3.4. Telemedicina no Mundo: Adaptação e Implementação Global

No campo da telemedicina, têm surgido diversas *startups* que fornecem soluções inovadoras, não apenas para a área em geral, mas também com foco em objetivos específicos, como a telemonitorização e a teleassistência de doenças ou situações particulares. Em Portugal, empresas emergentes estão a integrar-se rapidamente nesta realidade, alinhando-se com as tendências globais do setor.

A nível internacional, empresas como a norte-americana *Teladoc Health* já implementaram soluções em vários hospitais ao redor do mundo. Esta multinacional, considerada a primeira e maior empresa de telemedicina nos Estados Unidos, foi fundada em 2002 e atualmente mantém atividade em 130 países, atendendo 27 milhões de membros e pacientes. A *Teladoc Health*

oferece uma vasta gama de serviços, incluindo consultas médicas à distância, opiniões médicas especializadas, e uma plataforma certificada que utiliza inteligência artificial e dados analíticos para telemonitorização. Além disso, a empresa está a colaborar com a Organização Portuguesa de Gestores de Hospitais para fornecer formação a profissionais de saúde e pacientes, dotando-os de conhecimentos e ferramentas essenciais para o uso eficaz da telemedicina.

Outra empresa que se destaca é a *Babylon Health,* que está integrada em partes do sistema nacional de saúde do Reino Unido. A *Babylon* oferece uma aplicação inovadora que utiliza sistemas de inteligência artificial para triagem de sintomas, realiza teleconsultas, e facilita o fornecimento de medicamentos por correspondência imediatamente após a consulta, tudo dentro de um ecossistema de saúde digital. A empresa já expandiu os seus serviços para países como Canadá, Ruanda, Arábia Saudita e Estados Unidos, consolidando-se como uma importante peça no mercado global de telemedicina.

No contexto português, a *Sword Health* tem-se destacado como a primeira fisioterapeuta digital focada em problemas de costas, uma condição que afeta aproximadamente 2 mil milhões de pessoas no mundo inteiro. Combinando inteligência artificial com equipas clínicas especializadas, a *Sword Health* tem obtido reconhecimento internacional, conquistando prémios e financiamento significativo. A sua plataforma digital de terapia, que promove a recuperação de pacientes nas suas próprias casas, sem a necessidade de cirurgias ou opioides, já se expandiu para a Europa, Austrália e Estados Unidos, com o seu principal centro tecnológico localizado no Porto.

Outra empresa portuguesa relevante é a *Knok*, uma aplicação que conecta médicos e pacientes em tempo real, ajudando a evitar filas e otimizando o atendimento médico. Com operações em Lisboa e no Porto, a *Knok* permite aos utilizadores selecionar médicos com base nas suas qualificações e nas avaliações de outros pacientes, funcionando de forma semelhante ao modelo de mobilidade da *Uber*.

Adicionalmente, a *startup* portuguesa *B2Quant* desenvolveu um software inovador voltado para o diagnóstico de perturbações do sistema neurológico central. Este software quantifica com exatidão os marcadores biológicos de imagens cerebrais, possibilitando analisar a magnitude de lesões e atrofias, atenuando assim a diminuição das capacidades mentais e de movimento. O trabalho da *B2Quant* demonstra especialmente a aplicação de tecnologias

avançadas no campo da telemedicina, com um impacto direto na melhoria dos cuidados de saúde.

Estas iniciativas destacam a contribuição crescente das *startups* no desenvolvimento da telemedicina, tanto em Portugal quanto no cenário internacional. Ao proporcionarem soluções tecnológicas inovadoras, estas empresas não apenas melhoram a acessibilidade aos serviços de saúde, mas também transformam a maneira como esses serviços são prestados, promovendo uma maior eficiência e eficácia nos sistemas de saúde globalmente.

1.3.5. Cibersegurança e legislação Internacional referente à Telemedicina

Num cenário contemporâneo, em que os serviços de saúde adaptados estão amplamente incorporados, a salvaguarda dos dados reveste-se de uma importância crucial, exigindo a execução minuciosa de condições essenciais como: Confidencialidade, Integridade, Disponibilidade e Conformidade legal e normativa, com especial ênfase na Privacidade.

A segurança da informação na saúde assenta em princípios essenciais que garantem a proteção e fiabilidade dos dados clínicos. A confidencialidade preserva a privacidade dos pacientes, assegurando que apenas indivíduos autorizados acedem a informações sensíveis e que esse acesso ocorre estritamente para fins justificados. Num contexto onde a circulação de dados clínicos é intensa, esta salvaguarda torna-se indispensável para manter a confiança no sistema.

A integridade dos dados assegura a sua exatidão e completude, garantindo que qualquer alteração é rigorosamente controlada. A fiabilidade da informação disponível aos profissionais de saúde é determinante para a precisão dos diagnósticos e a segurança dos tratamentos, sendo qualquer comprometimento neste aspeto um risco potencial para a qualidade da assistência prestada.

A disponibilidade da informação clínica permite que os dados sejam acessíveis quando necessário, assegurando a continuidade dos cuidados. Em ambientes dinâmicos, onde decisões médicas dependem de um fluxo eficiente de dados, garantir a acessibilidade torna-se essencial. Desde os Registos Médicos Eletrónicos à telemonitorização e ao apoio remoto, a gestão eficaz da disponibilidade de informação traduz-se em maior eficiência assistencial.

A conformidade legal e normativa constitui outro pilar fundamental, assegurando que o tratamento dos dados clínicos está alinhado com as diretrizes regulatórias. A privacidade dos pacientes é protegida por normativas rigorosas que estabelecem padrões para a recolha, armazenamento e utilização da informação de saúde, garantindo que os direitos individuais são salvaguardados e que a gestão dos dados ocorre de forma ética e segura.

Neste cenário, a nova legislação europeia sobre a proteção de informações, que se tornou efetiva em maio de 2018, transformou significativamente a forma como as organizações europeias devem responder aos requisitos de conformidade. Este regulamento não só atualizou a legislação para alinhá-la com os avanços tecnológicos como também estabeleceu uma única legislação pan-europeia para a proteção de informações, substituindo as normativas locais em vigor na área comunitária. Além disso, o regulamento introduziu a noção de ponto de contacto único, possibilitando que as entidades se relacionem com uma única entidade de fiscalização, facilitando a conformidade e reforçando a proteção dos dados em toda a União Europeia.

Este conjunto de requisitos e regulamentações representa um passo decisivo na modernização do sistema de saúde, assegurando que as integrações de tecnologias avançadas nos cuidados personalizados sejam acompanhadas por estruturas robustas de salvaguarda de informações, fundamentais para assegurar a proteção e a credibilidade dos pacientes e especialistas de saúde.

Capítulo II. O Uso da Telemedicina em Território Português

2.1. O Progresso da Telemedicina em Portugal

Em Portugal, a atenção pela saúde digital surgiu em 1999, ano em que foi formada a Comissão de Acompanhamento da Iniciativa Estratégica para o Desenvolvimento da Saúde Digital (CIEDT). Desde então, a intenção de atribuir um posicionamento central na reestruturação dos serviços de saúde tem sido reiterada em diversos registos governamentais. No entanto, a regulamentação da prática no contexto do Sistema Público de Saúde só começou a tomar forma com a divulgação do regulamento n.º 567/2006, que estabeleceu pela primeira vez os quadros de tarifas para as intervenções e atendimentos de telemedicina.

Conforme o regulamento a n.º 567/2006, a teleconsulta é definida como:

"Utilização de comunicações interativas, audiovisuais e de dados em consulta médica com a presença do doente, a qual utiliza estes meios para obter parecer à distância de, pelo menos, outro médico e com registo obrigatório no equipamento e no processo clínico do doente" (Ministério da Saúde, Portaria n.º 567/2006, anexo I, art.º 3.º, let. c).

O regulamento destaca a necessidade de anotar o atendimento no ficheiro clinico do paciente, um passo crucial para consolidar a estrutura tecnológica da partilha de dados de saúde de forma conectada. Além disso, estabeleceu que as consultas à distância fossem cobradas com o mesmo custo das consultas de saúde tradicionais, com a opção de adicionar o custo dos métodos auxiliares empregados.

Atualmente, o Despacho do Secretário de Estado Adjunto do Ministro da Saúde, n.º 3571/2013, é o principal regulamento voltado para a medicina à distância, tentando pavimentar uma estratégia para a execução dos serviços remotos. Esta determinação define a medicina à distância como uma "ferramenta" disponível para os especialistas em saúde, que oferece vários benefícios, como a redução da distância geográfica entre as unidades de saúde e os doentes, prevenindo viagens evitáveis e proporcionando maior agilidade na assistência em algumas especialidades. O despacho destaca ainda que a consulta à distância ″aumenta a acessibilidade às consultas de Especialidades Médicas, aumenta a equidade, proporcionando a possibilidade de todos os pacientes receberem melhor qualidade nos cuidados de saúde, reduzindo os custos associados″ (Despacho n.º 3571/2013: 8325).
A telemonitorização igualmente é considerada essencial para um controlo mais eficaz das doenças persistentes. Nesta abordagem, recomenda-se a criação de uma rede conectada ao serviço público de saúde, objetivando alcançar ″a monitorização remota, praticada por uma equipa de profissionais de saúde, a partir de uma Instituição sobre um grupo de doentes crónicos que seguem um protocolo a partir dos seus domicílios″ (Despacho n.º 3571/2013: 8326).

Reconhecendo a ausência de uma abordagem eficaz para a expansão da saúde digital, o

Ministério da Saúde considerou essencial traçar iniciativas sólidas para implementar uma rede de serviços de telemonitorização no Serviço Público de Saúde. O despacho determinou que as instituições hospitalares do Serviço Público de Saúde devem promover a implementação destes serviços em colaboração com os Agrupamentos de Centros de Saúde (ACES) da sua área de

abrangência. Adicionalmente, identificou as especialidades médicas prioritárias para a implementação dos serviços de telemedicina, nomeadamente ″dermatologia, fisiatria, neurologia, cardiologia, cardiologia pediátrica, pneumologia″ (Despacho n.º 3571/2013: 8326).

O despacho recomenda ainda que as teleconsultas sejam realizadas, sempre que possível, em tempo real, sugerindo que o primeiro contacto entre o profissional de saúde e o doente ocorra de forma presencial. A recomendação em questão, encontra-se em consonância com a literatura cientifica, que defende ″uma combinação de encontros ao vivo com encontros virtuais ou, pelo menos, um primeiro contacto ao vivo, de modo a conciliar as vantagens proporcionadas pela utilização das TIC com a necessidade de proteger a qualidade da comunicação entre médico e doente″ (Bhalla e Rudd, 2010).

O regulamento n.º 3571/2013 aborda o ajuste dos dispositivos tecnológicos utilizados para a prestação de cuidados de saúde à distância, estabelecendo que a contratação deve ser efetuada pelas instituições hospitalares que possuam os recursos tecnológicos indispensáveis.

Finalmente, com o intuito de adaptar as diretrizes do Ministério da Saúde numa política de execução eficaz, o Despacho n.º 3571/2013 estipula que as ″Administrações Regionais de Saúde (ARS) apresentem planos regionais para o desenvolvimento da telemedicina em articulação com as entidades hospitalares e com a Comissão para a Informatização Clínica" (Despacho n.º 3571/2013: 8326).

Assim, a telemedicina em Portugal, progressivamente institucionalizada através de portarias e despachos, é uma ferramenta indispensável para a modernização e a eficiência do sistema de bem-estar, prometendo melhorar o acesso, a equidade e o padrão dos cuidados fornecidos aos pacientes.

As inovações tecnológicas nas áreas da informática e das telecomunicações introduziram melhorias notáveis na prática da saúde, a ponto de alterar profundamente as interações entre os pacientes e os profissionais deste setor. Não se trata de redefinir a Medicina e áreas relacionadas, mas sim de praticar estas disciplinas de uma maneira inovadora, aproveitando os benefícios trazidos pelo progresso científico. As características dos intervenientes são cruciais para a difusão e a implementação das inovações tecnológicas na área clínica, o que realça a

importância de examinar a problemática da incorporação de novas soluções de comunicação e informação no contexto organizacional com uma perspetiva progressista.

A telemedicina, atualmente, transcende a mera consulta e assistência médica à distância, entre hospitais, centros de saúde em zonas rurais e médicos itinerantes. Ela implica, necessariamente, a realização de ações de formação e a transferência de tecnologias, contribuindo para o domínio das ferramentas e a plena integração das TIC nas organizações de saúde e no quotidiano dos profissionais de área.

Em Portugal, apesar da crescente disseminação da telemedicina, fortemente impulsionada pela pandemia Covid-19, ainda há procedimentos que necessitam de uma estrutura de ação sólida. Um exemplo claro é o adiamento da obrigatoriedade de os médicos emitirem as prescrições eletronicamente, onde "poderá haver prolongamento até ao final do ano de 2021, caso se verifique que há muitos médicos ainda sem capacidade para passarem receitas digitais" (Ministério da Saúde).

Inicialmente, o limite para a conclusão da utilização das receitas tradicionais estava previsto para junho de 2021, mas o Ministério da Saúde reconheceu a necessidade de flexibilidade, afirmando que "estamos atentos às necessidades das pessoas" e "não somos indiferentes às dificuldades". Tal flexibilização foi essencial, dado que "há médicos que não têm hábitos informáticos e nem sequer usam telemóvel", e o fim das receitas tradicionais poderia impactar que "milhares e milhares de portugueses vão ficar sem acesso a medicamentos" (Miguel Guimarães, Bastonário da Ordem dos Médicos).

A data prevista para a eliminação das receitas tradicionais tinha sido previamente adiada, de

31 de março para 31 de dezembro de 2020, devido ao contexto pandémico e às limitações dos Serviços Partilhados do Ministério da Saúde em avançar com a formação para médicos sem práticas informáticas. Para contornar este obstáculo, a Ordem dos Médicos cedeu os seus espaços, facilitando a realização das formações num ambiente mais acessível para os profissionais menos familiarizados com as tecnologias.

A pandemia Covid-19 exigiu que o setor da saúde tivesse de adaptar-se rapidamente às novas circunstâncias e possibilidades, permitindo que a telemedicina demonstrasse o seu valor num momento de crise extrema. Esta situação impulsionou a aceleração do processo de digitalização das organizações de saúde. As consultas à distância e a partilha de exames online

têm promovido o acesso à medicina, mas é crucial garantir que esta troca de informações seja realizada de forma segura.

Com esta transformação, exames que antes eram imprimidos e entregues aos pacientes passaram a ser partilhados virtualmente. Apesar das diferenças práticas, a responsabilidade de manter a privacidade do paciente recai sobre a instituição e deve ser uma prioridade em ambos os modelos. Por isso, é essencial investir em cibersegurança para proteger a troca de informações e assegurar que as plataformas utilizadas garantam a segurança dos dados dos indivíduos que confiam as suas informações à proteção institucional.

A anulação de consultas, intervenções cirúrgicas e outros exames diagnósticos, juntamente com o medo da população em procurar os serviços de saúde em unidades hospitalares e centros de atendimento, levou á inevitável deterioração das condições de saúde e até de situações agudas urgentes "não-COVID".[3]

A perceção, por parte dos profissionais e instituições de saúde, da importância de manter um acompanhamento regular dos seus pacientes desencadeou uma verdadeira proliferação de

sistemas para consultas à distância, em várias modalidades (chamadas telefónicas, videoconferência, mensagens de texto, correio eletrónico, entre outras) e de soluções para monitorização remota de pacientes nas suas residências.

Várias entidades de cuidados de saúde – públicas, privadas e do setor social – e até instituições de outros setores, como seguradoras, rapidamente adotaram estes sistemas, respondendo à exigência urgente de manter o contacto com os seus pacientes e de assegurar atendimento, ainda que à distância.

A análise das diversas dimensões da telemedicina revela que as suas principais vantagens estão intrinsecamente associadas ao aumento da acessibilidade aos cuidados de saúde, além de atenuar os efeitos adversos da demora e da separação geográfica na entrega dos serviços. A telemedicina, portanto, não apenas amplia o acesso aos cuidados, como também encurta

[3] A COVID-19 é uma doença respiratória causada por um agente infeccioso pertencente a uma família de microrganismos que atacam o sistema respiratório. O nome dessa família tem origem na sua forma, que se assemelha a uma coroa sob o microscópio.

distâncias, facilitando a aproximação dos pacientes aos serviços de saúde e melhorando a comunicação entre os prestadores desses cuidados.

Além disso, a telemedicina é amplamente reconhecida como uma ferramenta que melhora o acesso a conteúdos relacionados com a saúde, contribuindo significativamente para a racionalização de recursos humanos e materiais. Um exemplo de sucesso da implementação da telemedicina em Portugal é observado na região do Alentejo, onde esta prática tem sido desenvolvida de forma sistemática desde 1998, cobrindo uma vasta gama de serviços e integrando diversos provedores de assistência médica e especialidades médicas.

No Alentejo, uma região caracterizada por uma população maioritariamente envelhecida, com um alto índice de dependência e geograficamente dispersa, a telemedicina tem-se mostrado crucial para adequar a oferta de assistência médica às necessidades específicas da população. Ao aproximar pacientes e prestadores, a telemedicina não só evita os custos diretos e indiretos relacionados com deslocações e acompanhamento familiar, como também reduz significativamente os tempos de espera para consultas.

Desta forma, a prática da telemedicina no Alentejo constitui um exemplo notável de como os serviços de saúde podem ser adaptados às necessidades da comunidade, demonstrando a sua eficácia em otimizar a assistência médica fornecida.

Porém, é evidente que, em muitas organizações de saúde, ainda não há um reconhecimento pleno da importância da telemedicina dentro da estrutura organizacional dessas entidades. Tal é comprovado pela reduzida percentagem de instituições que dispõem de uma unidade orgânica dedicada à organização das atividades de telemedicina. A criação de uma unidade específica poderia permitir um planeamento harmonioso e sistemático destas atividades, possibilitando uma gestão estratégica e operacional mais eficaz das ferramentas da telemedicina, adaptadas aos contextos em que as entidades de saúde se inserem.
Uma das principais lacunas na difusão da telemedicina em Portugal, e em muitos outros países, é a falta de interesse e motivação dos especialistas em saúde em integrar esta prática. Dado que a adesão dos clínicos é um elemento fundamental para o êxito da telemedicina, é essencial que sejam identificadas e implementadas medidas específicas que incentivem a inclusão dos profissionais no processo.

A disseminação do uso dos sistemas de interação e dados em diversas áreas profissionais, especialmente entre as gerações mais jovens, assim como a capacidade de explorar as suas potencialidades, são fatores que podem aumentar a aceitação e o estímulo aos próximos especialistas em saúde. Um dos fatores de sucesso nos contextos onde são aplicadas as soluções de telemedicina é a abordagem coletiva à sua prática. A implementação da telemedicina com o envolvimento de uma equipa de trabalho tende a ser mais motivada e eficaz do que em projetos impulsionados pelo individualismo. As experiências de telemedicina realizadas em Portugal demonstraram uma tendência predominante para a utilização interna e para a ligação com países menos desenvolvidos de língua oficial portuguesa. Até ao momento, não foi comunicada nenhuma experiência em que as unidades de saúde em Portugal tenham sido recetoras externas de informação.

A conexão com outros países mais desenvolvidos representa uma oportunidade ainda inexplorada. Com a aplicação da norma comunitária que regula a circulação de pacientes no espaço europeu, prevê-se um aumento da mobilidade destes pacientes, o que exigirá a criação de condições para a circulação de informações entre diferentes sistemas de saúde.

Neste contexto, a telemedicina emerge como uma solução privilegiada para responder aos novos desafios enfrentados pelos agentes do setor da saúde na União Europeia, oferecendo uma plataforma sólida para a integração e troca de informações essenciais à prestação de cuidados de saúde transnacionais.

2.2. Iniciativas de Referência: Projetos de Telemedicina em Portugal

A rápida transformação do sistema de saúde e a consequente adaptação dos profissionais e pacientes a uma nova realidade, que apesar de não inédita, revolucionou a maneira como se relacionam, é um marco na evolução da assistência médica. O desenvolvimento da plataforma *RSE Live*[4] , pelas Unidades Partilhadas de Saúde, foi possível realizar consultas remotas instantâneas, conectando pacientes e especialistas de saúde de modo virtual, através das novas

[4] A RSE Live é uma solução digital da SPMS que possibilita consultas remotas em tempo real entre pacientes e profissionais de saúde, permitindo também interações diretas entre estes profissionais.

soluções de interação e dados. Este avanço possibilitou que as consultas fossem realizadas à distância, desde que o médico considerasse apropriado e o paciente estivesse de acordo.
Nos últimos anos, diversas unidades hospitalares do Serviço Público de Saúde intensificaram a utilização da Telessaúde, particularmente no contexto da pandemia, com a finalidade de garantir a continuidade e o padrão dos cuidados durante o acompanhamento dos indivíduos em cuidados. A Telessaúde provou ser uma ferramenta essencial para a entrega de atendimento, assegurando a equidade no acesso, a proximidade e a eficiência no uso dos recursos disponíveis.

As vantagens da Telemedicina são inegáveis e evidentes. Destaca-se, entre outros benefícios, a promoção de equidade no fornecimento de serviços de saúde, a aproximação dos serviços aos pacientes e a otimização dos recursos existentes. Esta ferramenta, que responde diretamente às necessidades dos pacientes, apresenta-se como um instrumento facilitador na integração dos cuidados, com potencial para melhorar significativamente os impactos clínicos.

Em 2019, os impactos do "Barómetro da Adoção da Telessaúde e de Inteligência Artificial", um programa supervisionado pela Associação Portuguesa de Administradores Hospitalares em parceria com a *Glintt-Global Intelligent Technologies, S.A.*, e com apoio científico da Escola Nacional de Saúde Pública e institucional da SPMS, revelaram um amplo consenso em relação à partilha de dados clínicos por meio da Telemedicina. Os participantes do estudo reconheceram a Telemedicina como promotora de uma orientação adequada e de uma maior adesão à terapia pelos doentes, confirmando assim o seu papel crucial no fortalecimento da eficácia dos tratamentos e na melhoria geral do sistema de saúde.

Deste modo, a Telemedicina afirmou-se como uma resposta eficiente às necessidades emergentes durante a pandemia, mas também como um componente vital para a evolução dos cuidados de saúde em Portugal, com impacto positivo na equidade, proximidade e eficiência dos serviços de saúde. As novas tecnologias, ao impulsionarem a Telemedicina, abriram um vasto leque de oportunidades, não apenas para a realização de teleconsultas entre médicos e pacientes, mas também para a interconectividade entre especialistas em saúde e a promoção da educação à distância. Este cenário perspetiva o potencial revolucionário das soluções de interação e dados

na esfera da saúde, vislumbrando um futuro em que a medicina se irá tornar cada vez mais acessível e integrada.
No entanto, a implementação da telemedicina apresenta diversos desafios para as instituições de saúde, exigindo uma reorganização estrutural e um significativo reforço do investimento.
Em diferentes instituições do serviço público de saúde, o Instituto Português de Oncologia de Coimbra (IPO de Coimbra) reconheceu a relevância estratégica da medicina á distância, integrando-a na qualidade de prioritária no seu modelo de atividades e planeamento orçamental para 2019-2021. Entre as áreas destacadas, a teledermatologia surge como um componente central desta estratégia.

A teledermatologia, em particular, demonstra um enorme potencial no processo de referenciação de pacientes com condições cutâneas para unidades especializadas, permitindo uma triagem mais eficaz, assim como a realização de consultas remotas. ATeledermatologia contribui para uma melhor gestão dos casos, evitando deslocações desnecessárias e flexibilizando o encaminhamento para cuidados especializados. Este compromisso foi reforçado a 19 de julho de 2019, com a celebração de um acordo de cooperação entre o IPO de Coimbra e os Serviços Partilhados do Ministério da Saúde (SPMS).

Além disso, a SPMS, em parceria com a Associação *Fraunhofer* Portugal, está a desenvolver o projeto DERM.AI, que integra a Inteligência Artificial no Rastreio Teledermatológico. O IPO de Coimbra tem participado ativamente neste projeto, que visa facilitar o processo de indicação pelos profissionais de Clínica Geral e Familiar. O DERM.AI tem dois objetivos principais: a avaliação de uma plataforma digital que possibilita retirar imagens de alterações cutâneas em alta resolução e a construção de uma aplicação de IA para avaliar o potencial risco dessas alterações. Este sistema processa igualmente as representações visuais retiradas quanto as informações clínicas, baseando-se em dados retrospetivos, para fornecer uma ferramenta de apoio à decisão aos enfermeiros responsáveis.

A crescente importância da Telemedicina torna evidente a necessidade de uma maior normalização e regulamentação no setor. Existe um consenso generalizado sobre os benefícios que esta prática traz aos cidadãos, reforçando a ideia de que a participação ativa de todos os envolvidos, especialmente dos pacientes, é fundamental para o sucesso e o desenvolvimento contínuo da Telemedicina.

Esta abordagem integrada, combina inovação tecnológica com uma visão estratégica e regulamentação adequada, é essencial para garantir que a Telemedicina continue a evoluir de forma sustentável, trazendo benefícios tanto aos especialistas em saúde como para os pacientes, e fortalecendo um sistema de assistência médica mais eficaz e acessível em Portugal.

2.3. Cibersegurança na Telemedicina: Desafios e Estratégias em Portugal

A implementação da telemedicina, embora traga incontestáveis benefícios, apresenta desafios significativos, especialmente no que diz respeito à cibersegurança. A própria natureza da telemedicina, que depende da interconexão entre *softwares*, aplicações e dispositivos físicos para conectar pacientes aos profissionais de saúde à distância, expõe as redes de saúde a potenciais ciberataques.
O valor dos dados transmitidos nas redes de telemedicina torna-se um alvo atrativo para cibercriminosos, que procuram explorar vulnerabilidades para aceder a informações sensíveis. Caso tais dados sejam comprometidos, não apenas o desempenho das instituições de saúde pode ser afetado, mas a própria segurança do paciente pode ser colocada em risco.

A prática da telemedicina implica uma confiança inevitável na comunicação à distância, o 0que significa que as instituições de saúde não possuem controlo total sobre as redes utilizadas pelos pacientes. Cibercriminosos estão cientes destas limitações e exploram a incapacidade momentânea das instituições médicas para gerir o fluxo de informações de forma completa. Ao explorar essas vulnerabilidades, podem conseguir acesso não autorizado às redes das instituições e aos dados armazenados.

Embora seja impossível garantir totalmente a segurança das redes dos pacientes, o setor de saúde deve medidas sólidas para proteger as suas próprias redes contra ciberataques. É fundamental que, na interação com dados médicos, haja uma atenção redobrada à segurança destes dados. Implementar sistemas de acesso reservado, que requerem certificação válida para o acesso às informações, é uma medida crucial para garantir a proteção dos dados.

Os ciberataques têm aumentado de forma alarmante, como evidenciado pelo crescimento de 101% no número de incidentes reportados ao Centro Nacional de Cibersegurança (CNCS) durante o primeiro semestre de 2020, comparado ao mesmo período de 2019. Este aumento é particularmente preocupante devido à situação pandémica do Covid-19, onde a intensificação do uso da telemedicina coincidiu com um aumento dos ciberataques.

Pedro Mendonça, consultor do CNCS, sublinha que, no contexto do comércio eletrónico, “os portugueses revelam ter comportamentos preventivos, mas a solução não pode passar por deixar de usar, mas sim ter mais cuidado quando se usa”. No entanto, a adesão dos portugueses a práticas de cibersegurança continua a ser insuficiente. Dados do *Eurostat* revelam que 23%

dos portugueses evitam compras online por receio, contrastando com a média da União Europeia (UE) de apenas 6%. Além disso, indica que uma parte significativa dos cidadãos portugueses expressa preocupações em relação ao cibercrime, superando a média observada na União Europeia. Contudo, apenas uma fração dos portugueses fez alterações às suas palavras- passe no último ano, enquanto o restante da Europa apresenta uma taxa de atualização mais elevada.

O *phishing*, continua a ser um método predominante de ciberataque em Portugal, especialmente intensificado durante a pandemia. Este tipo de incidente, que consiste no envio de mensagens fraudulentas por *hackers* que se fazem passar por entidades fidedignas para obter informações sensíveis, representou 36% dos incidentes registados até agosto de 2020, comparado a 31% no final de 2019, conforme relatado pelo Observatório de Cibersegurança.

Com a eclosão da pandemia Covid-19, surgiram novos métodos de ataque, que incluem *phishing* com o nome de organizações de saúde para capturar dados pessoais, distribuição de *malware* via e-mail ou redirecionamento de *Domain Name System* (DNS), e aplicações maliciosas disfarçadas como ferramentas relacionadas à Covid-19, muitas vezes disseminando *ransomware*. Além disso, houve um aumento de fraudes digitais que solicitam doações falsas para a compra de materiais médicos, *websites* fraudulentos para a venda de produtos médicos, e a comercialização de kits Covid-19 na *darkweb*.

Campanhas de desinformação e *ransomware* direcionado a serviços essenciais intensificaram-se durante este período.

Portanto, a crescente dependência da telemedicina e das TIC no setor da saúde exige uma resposta igualmente construtiva em termos de cibersegurança. O fortalecimento da regulamentação, aliado a uma conscientização maior e à adoção de melhores práticas de segurança por parte de todos os intervenientes, é essencial para garantir que os benefícios da telemedicina sejam plenamente atingidos, sem comprometer a segurança e a privacidade dos pacientes.

2.4. Regulamentação e Proteção: A Evolução da Legislação em Cibersegurança na Telemedicina

A digitalização do setor da saúde em Portugal apresenta diversos desafios no que diz respeito à salvaguarda de informações pessoais, os quais devem ser cuidadosamente monitorizados para

assegurar a aderência ao Regulamento Geral sobre a Proteção de Dados (RGPD). Este regulamento define dados pessoais como qualquer informação que, identifique um ser humano específico, de maneira direta ou indireta, incluindo dados como identidade, endereço habitacional, contacto de e-mail, além de informações sobre o histórico de saúde e as condições médicas dos pacientes, juntamente com os perfis de clientes.

As instituições que integram o sistema de saúde pública e que realizam atividades de tratamento de dados pessoais incluem o registo, organização, pesquisa, proteção e transmissão de informações, que estão sujeitas a uma série de obrigações conforme o RGPD. Além das obrigações gerais estabelecidas por este regulamento, estas entidades devem assegurar a observância de normas particulares do setor da saúde que regulam a titularidade, o acesso e a validade no processamento das informações dos pacientes."

Normas Fundamentais para a Gestão de Informações Pessoais

A administração dos dados no Serviço Nacional de Saúde deve pautar-se por princípios rigorosos que assegurem uma gestão eficiente e transparente. A definição de finalidades legítimas impõe que as informações pessoais sejam recolhidas para propósitos claros e previamente estabelecidos, evitando desvios que comprometam a sua utilização ética.
O princípio da minimização determina que apenas os dados estritamente necessários sejam armazenados, prevenindo excessos que possam comprometer a privacidade dos indivíduos. Simultaneamente, a precisão e atualização contínua da informação garantem que os registos refletem a realidade clínica dos pacientes, reduzindo o risco de erros.

A gestão responsável dos prazos de armazenamento exige que os dados sejam conservados apenas pelo tempo indispensável à sua finalidade, em conformidade com as diretrizes da Comissão Nacional de Proteção de Dados (CNPD). Além disso, assegura-se que os titulares dos dados têm pleno conhecimento sobre a forma como as suas informações são utilizadas, bem como o direito de consulta e retificação.

O consentimento do titular é um requisito fundamental para o tratamento de dados, salvo nas exceções previstas legalmente, como nos casos em que a sua gestão é indispensável para a proteção de interesses vitais. Paralelamente, a implementação de medidas de segurança

robustas assegura a proteção contra acessos indevidos, perdas ou modificações não autorizadas, particularmente em ambientes digitais.

Por fim, a conformidade com a CNPD impõe a notificação das práticas de tratamento de dados e, quando aplicável, a obtenção de autorização prévia, garantindo que a gestão da informação decorre dentro dos parâmetros regulatórios e em conformidade com as melhores práticas de proteção de dados.

Notificação e Controlo Prévio pela Comissão Nacional de Proteção de Dados (CNPD)

De acordo com a legislação, qualquer entidade do SNS que pretenda tratar dados pessoais deve notificar previamente a CNPD. Em certos casos, como o processamento de informação sensível, é fundamental obter autorização prévia da CNPD. Dados sensíveis incluem dados de saúde, informações genéticas, dados sobre a vida pessoal e origem cultural ou étnica. O processamento de informações de saúde, imprescindível para propósitos de saúde preventiva, diagnóstico clínico, fornecimento de cuidados ou administração de serviços de saúde, está sujeito a notificação simples à CNPD, desde que efetuado por profissionais ou pessoas sujeitas a confidencialidade profissional. No entanto, Caso as informações sejam empregues para objetivos distintos, como a pesquisa científica, ou se incluírem dados sobre raça, religião, ou comportamentos sociais, a autorização prévia da CNPD é obrigatória.

Autorização para o Processamento de Informações Pessoais

O processamento de informações pessoais geralmente requer autorização dos titulares, exceto em situações previstas no RGPD, como a execução de um contrato, a execução de deveres legais ou a procura por interesses justificados. Em situação de informações confidenciais, a regra é a proibição do tratamento, salvo exceções, como o consentimento do titular ou autorização da CNPD, ou quando se torna essencial para a proteção dos interesses fundamentais do indivíduo em causa.

Direito de Conhecimento e Acesso a Informações de Saúde

Quando as informações pessoais são recolhidas, mesmo sem consentimento, as entidades do SNS devem comunicar de forma transparente aos respetivos proprietários, incluindo a identificação da entidade gestora, os objetivos do processamento, eventuais partilhas dos dados, e os direitos de acesso, correção e remoção das informações. Esses elementos devem constar em todos os formulários de obtenção de dados e podem ser fornecidas verbalmente em

inquéritos. O acesso a informações de saúde é realizado por intermédio de um especialista em saúde.

Aplicação de Informações de Saúde para Pesquisa Científica

As informações de saúde obtidas no contexto da prestação de cuidados podem ser utilizadas para pesquisa científica, desde que os proprietários tenham sido informados e dado o seu consentimento. As pesquisas devem ser conduzidas de maneira a assegurar a ocultação da identidade dos pacientes.

Comunicação de Dados e Subcontratação

As entidades do SNS comunicam dados a diversas entidades, como a Direção Geral da Saúde e a Administração Central do Sistema de Saúde, para cumprir obrigações legais, e contratam prestadores de serviços que tratam os dados pessoais em seu nome. Ao subcontratar serviços, as entidades devem garantir que o subcontratante oferece garantias suficientes e que um contrato escrito formaliza as responsabilidades de salvaguarda de informações.

Ações Especiais de Segurança

Para o processamento de informações confidenciais, as organizações do SNS devem implementar ações de segurança específicas que assegurem a proteção contra acessos não autorizados e a distinção clara entre dados de saúde e dados administrativos. As ações de proteção devem ser proporcionais aos riscos e à natureza dos dados a proteger, com uma avaliação contínua das vulnerabilidades e impactos potenciais.

Consequências do Incumprimento

O incumprimento das regras do RGPD[5] pode resultar em contraordenações puníveis com coimas até 29.927,88 euros, além de penalidades adicionais, como bloqueio ou eliminação de dados e restrição ao processamento. A violação das normas pode acarretar responsabilidade civil e criminal, com penas de prisão ou multas. Além dos custos legais e financeiros, o incumprimento pode afetar gravemente a imagem e reputação das entidades do SNS. Multas de até 50 mil euros podem ser aplicadas a entidades da função pública e administradores de infraestruturas essenciais que não implementem planos de segurança adequados contra ciberataques e não reportem riscos e incidentes ao Centro Nacional de Cibersegurança (CNCS).

Em suma, a digitalização na área da saúde deve ser acompanhada por uma rigorosa observância das diretrizes de salvaguarda de dados e cibersegurança. A implementação de medidas adequadas e a constante vigilância são cruciais para resguardar as informações pessoais e garantir a integridade das operações do SNS.

[5] O Regulamento (UE) 2016/679, conhecido como RGPD, adotado a 27 de abril de 2016 pelo Parlamento Europeu e pelo Conselho, estabelece um conjunto harmonizado de normas para proteger a privacidade e os dados pessoais de indivíduos, assim como garantir o fluxo seguro de dados entre países dentro da União Europeia.

Capítulo III. Cibersegurança na Telemedicina

3.1. Segurança nas Interações: Garantindo a Privacidade nas Consultas à Distância

A proteção e a confidencialidade nas interações entre médicos e pacientes são fundamentais para assegurar a credibilidade e a legitimidade dos tratamentos disponibilizados pelo Sistema Público de Saúde. Estas dimensões são cruciais para manter a confiança necessária à harmonia e funcionalidade de um sistema comunicacional que desempenha um papel vital na vida humana. Qualquer falha ou ameaça a essas comunicações pode resultar em consequências de magnitude significativa, comprometendo a excelência e a segurança dos serviços.

Relação Médico-Paciente

No contexto da Telemedicina, a relação entre médico e paciente deve preservar os princípios essenciais que sustentam a prática clínica. A confiança mútua e a confidencialidade mantêm-se fundamentais, assegurando que a interação remota respeita os direitos dos pacientes e garante condições equivalentes às consultas presenciais.

A avaliação clínica exige que o médico tenha uma compreensão fundamentada da situação do paciente antes de recorrer à teleconsulta. A qualidade da informação recebida deve ser suficiente para sustentar um diagnóstico ou acompanhamento responsável.

A responsabilidade médica permanece inalterada na prática remota, impondo uma análise rigorosa dos dados disponíveis. O profissional de saúde apenas deve emitir pareceres ou tomar decisões clínicas quando dispõe de informação adequada e fidedigna. Em qualquer circunstância, a integridade dos cuidados prestados deve ser plenamente assegurada.

Margem de Influência e Responsabilidade do Médico

A atuação do médico na Telemedicina rege-se por princípios que garantem a qualidade e segurança da prática clínica. A liberdade de decisão assegura que o profissional avalia a adequação da medicina à distância para cada caso, podendo optar ou não pela sua utilização conforme o contexto clínico.

A responsabilidade pelo tratamento mantém-se com o médico que solicita opiniões a colegas, devendo este ponderar as recomendações recebidas e integrá-las no plano assistencial de forma fundamentada.

A emissão de pareceres na Telemedicina exige que o profissional disponha de conhecimento suficiente sobre o caso. Sempre que emite uma opinião, assume total responsabilidade pelas implicações clínicas, mesmo em cenários de urgência, garantindo que a prática remota respeita os princípios éticos e legais da profissão.

Levantamento de Informações sobre Segurança e Privacidade

Para avaliar a segurança e a privacidade nas comunicações entre médico e paciente, foi realizada uma sequência de diálogos com especialistas em saúde em exercício, com foco nas práticas e mecanismos de proteção utilizados no quotidiano.

Os resultados indicam que, no Hospital Espírito Santo de Évora, o principal mecanismo de segurança contra ameaças externas é o *software* antivírus integrado no programa *ALERT*[6]. Esta informação foi confirmada por três auxiliares de saúde em funções no hospital: Marco Santos, Mafalda Mendes e Bruna Guerreiro.

Adicionalmente, na entrevista com Emanuel Gouveia do Instituto Português de Oncologia de Lisboa Francisco Gentil (IPO), foi destacado que "Atualmente, existem vários problemas a nível de cibersegurança que se intensificaram com a chegada da pandemia. Os ataques

[6] O software clínico *ALERT*, global e de tecnologia tátil, é um Processo Clínico Eletrónico (PCE) com Partilha de Informação Clínica (HIE), Processo Clínico Eletrónico Pessoal (PHR), Sistema de Gestão de Dados do Paciente (PDMS), Sistema de Planeamento (PS) para a saúde e um sistema clínico de *Business Intelligence* (BI). Apto para *web* e *cloud*, adotado em vários países e implementado no âmbito de projetos nacionais, estaduais e empresariais, o software *ALERT c*umpre requisitos e certificações de produto locais e internacionais.

informáticos para acesso a dados de saúde aumentaram exponencialmente.” Esta observação sublinha a crescente preocupação com a cibersegurança e a necessidade de medidas mais robustas para proteger os dados de saúde no contexto da telemedicina.

Em suma, a integração da telemedicina no SNS exige uma abordagem meticulosa para assegurar que a segurança e a privacidade das comunicações entre médicos e pacientes sejam mantidas. A preservação da confiança mútua e o cumprimento rigoroso das responsabilidades médicas são essenciais para assegurar a eficiência e a proteção dos cuidados prestados através deste novo paradigma tecnológico.

Apesar de ainda serem necessários extensos melhoramentos e adaptações, está-se a criar uma base sólida para o futuro da segurança e privacidade no contexto da telemedicina. Conforme apontado por Emanuel Gouveia, especialista em oncologia no Instituto Português de Oncologia de Lisboa Francisco Gentil (IPO), "Hoje em dia utilizamos um sistema operativo aberto (com limitações) que nos permite diminuir a exposição e vulnerabilidade a ataques informáticos. Possuímos também um departamento de informática com uma secção dedicada à proteção dos dados de saúde produzidos diariamente na instituição e no grupo para o qual desempenho funções."

Esta preocupação é evidenciada pela implementação de medidas básicas de segurança, como o backup dos dados produzidos nos últimos dez anos, conforme exigido por lei. Emanuel Gouveia reforça esta observação ao afirmar: "Sim, existe atualmente um backup de todos os dados produzidos nos últimos 10 anos, como a lei exige."

Contudo, a ausência de uma plataforma nacional de informações que viabilize o conhecimento, caracterização e análise automática dos recursos tecnológicos disponíveis nas entidades fornecedoras de serviços de saúde em Portugal revela uma necessidade urgente. A base em questão permitiria não só o levantamento das soluções tecnológicas disponíveis, incluindo as relacionadas com a prática de telemedicina, mas também a implementação de um índice composto do desenvolvimento tecnológico das organizações de saúde. Este índice representaria, de forma sintética e quantitativa, a distribuição tecnológica existente, seja em termos das estruturas de base para a telemedicina, dos equipamentos em uso, ou da sua aplicação concreta.

A criação de um plano específico de desenvolvimento tecnológico surge como uma opção válida para responder a esta carência, permitindo discriminar os níveis evolutivos das organizações de saúde em Portugal. Este plano poderia ainda compartimentar as tecnologias por categorias distintas, incluindo os recursos de telemedicina e o nível de obsolescência dos equipamentos, possibilitando uma informação clara e exata da estrutura da oferta dos cuidados de saúde em diferentes áreas geográficas.

Perspetivas do meio envolvente:

Com a pandemia COVID-19, o trabalho remoto tornou-se uma necessidade, ampliando significativamente o perímetro de segurança das organizações. No entanto, nem todas estavam preparadas para esta realidade, e o investimento inicial não foi necessariamente direcionado para a cibersegurança.

Rui Barata Ribeiro, *Security Sales Leader* da IBM, comunicou que "não tem absolutamente claro que a cibersegurança tenha sido descurada numa primeira fase" da crise sanitária provocada pelo COVID-19. Observa que, embora tenha havido um aumento no investimento em cibersegurança proporcional aos gastos em IT durante 2020, "a área da segurança da informação foi uma área claramente negligenciada durante 2020 e tenho a perceção que alguns dos incidentes que aconteceram durante 2020 têm a ver com alguma negligência da segurança da informação e algum foco na segurança das infraestruturas".

O perímetro de segurança, tradicionalmente bem definido, começou a desaparecer com a mudança para o trabalho remoto, como evidencia Luís Ramos, *Cybersecurity Specialist* da Cisco: "O ano passado foi muito desafiante, o que obrigou muitas empresas não só a reinventarem-se, mas também a dar um grande salto tecnológico que, provavelmente, já não davam há alguns anos". Destaca que, inicialmente, o foco foi assegurar que os sistemas de suporte estivessem preparados para viabilizar o trabalho à distância., o que levou a um investimento mais ponderado em cibersegurança, visando garantir níveis mínimos de segurança no acesso remoto.

Manuel Dias, *National Technology Officer da Microsoft*, corrobora esta visão, afirmando que "numa primeira fase, tivemos de construir as fundações para o trabalho remoto e a componente da videoconferência e a produtividade fossem os primeiros pontos a resolver. A seguir veio a segurança." Existiu um aumento de ciberataques desde março de 2020, especialmente por *phishing* e roubo de dados pessoais, observou-se que os colaboradores à distância muitas vezes careciam de medidas de proteção, como a autenticação multifatorial.

Paulo Pinto, *Business Developer Manager da Fortinet*, salienta que "para além da rapidez com que foi abordada a fase inicial", a partir do começo de 2021, após as restrições impostas, observou-se uma tentativa de adotar uma estratégia mais focada em horizontes de desenvolvimento a curto e a longo período. Comunica que presentemente "as empresas já estão

a tentar incluir soluções contemplando de forma mais sistematizada a segurança dos postos de trabalho, dos acessos aos serviços na cloud e a impor alguns requisitos que, na fase inicial, foram relaxados".

Miguel Souto, *Partner Business Manager* da HP, observou que "houve um investimento – os números assim o dizem –, mas é preciso analisarmos o que é que esse investimento nos diz; diz-nos que foi feito numa ótica muito mais tática do que estratégica". Sublinhou que, embora tenha havido alguma evolução em termos de segurança ao longo do ano, a maior parte dos investimentos concentrou-se nas grandes corporações, que constituem apenas uma fração reduzida do panorama empresarial em Portugal. "A maior parte das nossas empresas debatem-se com problemas de sobrevivência grandes e a cibersegurança não fez – e atrevo-me a dizer que não fará – parte das suas prioridades."

A transição para a telemedicina e o trabalho remoto trouxe desafios significativos em termos de segurança e privacidade. Apesar dos avanços iniciais e da criação de uma base para desenvolvimento, é evidente que há uma necessidade urgente de estratégias mais abrangentes e sustentáveis. Investir na construção de uma plataforma de informações nacional de recursos tecnológicos e num plano de desenvolvimento tecnológico, bem como reforçar as práticas de cibersegurança, são passos essenciais para garantir a proteção dos dados e a eficácia da prestação de cuidados em Portugal. A pandemia sublinhou a importância da segurança da informação, e as lições aprendidas durante este período deverão servir de guia para futuras inovações e adaptações no setor.

3.2. Proteção de Dados na Telemedicina: Garantindo a Confidencialidade

O Programa Governamental de Saúde destaca a necessidade de aprimorar os instrumentos de governação, enfatizando a introdução de medidas que promovam a transparência e a valorização, além da disseminação, das práticas recomendadas em todas as áreas de intervenção do setor. A crescente adoção de tecnologias pelos serviços e entidades de saúde tem permitido um acesso sem precedentes a funcionalidades que possibilitam a exploração de dados e indicadores de saúde. Estas ferramentas são fundamentais para que o Estado possa utilizar de maneira mais lógica e eficaz os meios acessíveis, otimizando a prestação de serviços à população.

As informações produzidas pelos serviços e organismos que integram a administração pública do Estado, assim como pelas instituições do setor público empresarial coletivo, são reconhecidas como um recurso público de grande valor. A gestão e proteção destes dados são essenciais, devendo a sua disponibilidade estar restrita ao cumprimento de interesses públicos específicos. Além disso, a sua gestão deverá seguir rigorosamente os princípios da legalidade, transparência e proporcionalidade, garantindo que o uso dos dados seja sempre conduzido de acordo com as normas legais e éticas que regem o setor.

O foco do governo na melhoria dos instrumentos de governação e na valorização das boas práticas reflete um compromisso com a eficiência e a ética na gestão da saúde pública. Ao garantir que as informações sejam utilizadas de maneira clara e ética, o governo procura não apenas proteger o interesse público, mas também promover uma cultura de boas práticas que permeie todas as suas ações no setor da saúde. Desta forma, o programa visa não apenas melhorar a governança, mas também garantir que a saúde pública em Portugal seja gerida com os mais altos padrões de responsabilidade e transparência.

A disponibilização de informações de saúde, embora desempenhe um papel crucial em investigações científicas e em iniciativas de saúde pública, deve ser tratada com o devido cuidado, dado o seu valor económico elevado e o consequente risco de práticas fraudulentas. A gestão adequada destes dados é vital para proteger tanto o interesse público quanto os direitos individuais dos pacientes.

Os serviços e organismos que operam sob a administração do Estado, no âmbito da Saúde, bem como organizações do setor empresarial, são regidos por normas restritas que proíbem o acesso de informações de saúde a organizações terceirizadas, seja sem custos ou com custos, sem que o membro do Governo, com responsabilidade pela saúde, tenha autorizado previamente. Esta regra é essencial para assegurar a privacidade das informações, sendo permitida exceção apenas quando a informação é solicitada por entidades judiciais ou administrativas, conforme estabelecido pela lei.

Para avaliar as práticas de confidencialidade e segurança dos dados médicos, foi necessário compreender o contexto operacional diário dos profissionais de saúde, analisando os comportamentos e procedimentos adotados para assegurar a proteção e integridade das informações fornecidas pelos pacientes. Esta análise permitiu identificar as estratégias

empregadas para minimizar riscos e fortalecer a segurança dos dados em todas as etapas do atendimento.

A importância de garantir que as informações de saúde sejam tratadas com o mais alto grau de confidencialidade não pode ser subestimada. A existência de regulamentações rigorosas e a vigilância constante sobre a aplicação destas normas são fundamentais para prevenir o uso indevido ou a exploração comercial indevida de dados sensíveis. Este compromisso para com a proteção da privacidade dos pacientes reforça a confiança no sistema de saúde e assegura que os dados sejam utilizados exclusivamente para fins legítimos e autorizados, sempre em conformidade com os princípios legais estabelecidos.

Ao garantir que os dados de saúde sejam resguardados contra possíveis ameaças e manipulações, o governo não apenas protege os direitos dos cidadãos, mas também assegura a integridade e a credibilidade das instituições. É crucial para a preservação do sistema atender às necessidades da população com eficácia e ética.

A segurança dos dados clínicos no contexto hospitalar é uma questão de importância crítica, especialmente no que se refere à salvaguarda da confidencialidade dos pacientes. No Hospital Espírito Santo de Évora (HESE), os auxiliares de saúde desempenham um papel essencial na implementação de medidas de segurança, utilizando mecanismos como o "número mecanográfico" e a "impressão digital" para assegurar que apenas indivíduos autorizados tenham acesso às informações sensíveis.

O reconhecimento da importância da cibersegurança é evidente entre os profissionais de saúde, ficando explícito na perspetiva apresentada na entrevista realizada.
Bruna Guerreiro, auxiliar de saúde no HESE, ressalta a relevância desse aspeto ao afirmar: “Creio que sim, pois estamos a tratar de dados clínicos de pacientes, que de si, são dados delicados associados a uma necessidade de privacidade.” Esta declaração reflete uma compreensão clara de que a proteção dos dados clínicos não é apenas uma responsabilidade técnica, mas também ética, dada a natureza sensível das informações tratadas no ambiente hospitalar.

Apesar desta consciência sobre a importância da cibersegurança, há ainda lacunas significativas no que se refere ao conhecimento sobre a identificação e a resposta a ciberataques.

Mafalda Mendes, também auxiliar de saúde no HESE, admite: “Não tenho consciência de que problemas possam existir.” Esta afirmação evidencia uma área crítica a ser trabalhada, uma vez que o desconhecimento sobre potenciais problemas que possam pôr em risco a efetividade das ações implementadas e deixar os dados clínicos vulneráveis a ataques ou falhas.

Assim, embora o Hospital Espírito Santo de Évora tenha estabelecido mecanismos básicos para a proteção dos dados clínicos, como a identificação por impressão digital e número mecanográfico[7], a eficácia destas medidas pode ser limitada pela falta de conscientização e capacitação dos profissionais que prestam cuidados de saúde sobre cibersegurança. Para reforçar a integridade dos procedimentos hospitalares, é imperativo investir em programas de capacitação que ampliem o conhecimento dos auxiliares de saúde sobre as possíveis ameaças e as estratégias de mitigação de riscos.

A implementação de uma cultura de segurança informacional, baseada formação contínua e na atualização das práticas de proteção de dados, é essencial para que os especialistas em saúde estejam mais capacitados para reconhecer e responder a eventuais incidentes de cibersegurança. Este fortalecimento das capacidades internas, aliado ao uso de tecnologias avançadas, contribuirá significativamente para a salvaguarda das informações clínicas, assegurando que a confidencialidade dos pacientes seja respeitada em todas as circunstâncias.

O Hospital CUF Descobertas, localizado em Lisboa, tem enfrentado de maneira direta os crescentes ciberataques que assolam o setor da saúde. A consciência sobre a importância da segurança da informação tem aumentado, impulsionada pela necessidade de responder a situações adversas já vividas.

[7] número mecanográfico, número de identificação interno à instituição, e traduz-se na criação de um código, composto por seis dígitos, que identifica o colaborador, de forma única, em toda a instituição.

Na entrevista prestada, Álvaro Filipe, radiologista, confirmou a ocorrência de ciberataques no ambiente laboral: "Sim, existem", afirmou, referindo-se a uma realidade que não pode mais ser ignorada.

Um dos incidentes mais graves que Álvaro Filipe referiu ilustra a gravidade dos desafios enfrentados: “Recordo-me do maior e mais grave ataque que sofremos... Os doentes foram informados e este ataque tornou-se público, sendo esclarecido na comunicação social por parte do nosso gabinete de comunicação.” Este episódio evidencia a vulnerabilidade dos sistemas de saúde a ciberataques e a necessidade de uma comunicação transparente com os pacientes afetados e com o público em geral.

A valorização dos dados clínicos no contexto atual é uma preocupação crescente, como explica Álvaro Filipe: “No tempo que decorrem, os dados valem muito dinheiro. Caminhamos para a era do Big Data, em que os dados, se bem utilizados, poderão gerar algoritmos de reprodução automática. Isso permitirá criar novos meios de diagnóstico, novos tratamentos, novos tipos de abordagens ao doente, até mesmo relacionados com a qualidade dos cuidados prestados.” Essa afirmação ressalta o duplo risco que os dados de saúde representam: enquanto são fundamentais para avanços médicos e melhoria dos cuidados, também são alvos valiosos para cibercriminosos.

Apesar dessa crescente conscientização, Álvaro Filipe admite que no quotidiano do hospital, a perceção das ameaças ainda é limitada: “Na realidade, não temos a verdadeira consciência das ameaças que pairam sobre a rede informática.” Esta falta de consciência plena entre os profissionais de saúde representa um ponto crítico de vulnerabilidade, indicando que há um caminho a ser percorrido na formação e preparação para gerir os ciberataques.

A negligência na segurança e confidencialidade das informações é uma preocupação constante: “Penso que a segurança e a privacidade dos dados de saúde foram deixadas de lado. É nítido isso todos os dias, quando nos deparamos com situações específicas de doentes em que os resultados clínicos são dados a conhecer através das redes sociais e/ou comunicação social, algo que não deveria acontecer.” Esta observação revela as falhas sistemáticas na proteção das informações sensíveis e a consequente exposição dos pacientes a violações de privacidade.

O panorama dos ciberataques evoluiu significativamente ao longo dos anos. Como observa Álvaro Filipe, “As empresas e os utilizadores não contactam com vírus informáticos simples,

mas com uma amplitude de ciberataques cada vez mais sofisticados e complexos". Este cenário exige um fortalecimento contínuo das medidas de cibersegurança, um esforço conjunto para aumentar a consciência sobre ciberataques e a implementação de práticas rigorosas para a proteção dos dados de saúde.

Dessa forma, o Hospital CUF Descobertas ilustra os desafios e a urgência de desenvolver estratégias mais sólidas para proteger informações sensíveis, alinhadas com as exigências de segurança na era do Big Data. A experiência do hospital sublinha a necessidade de um compromisso institucional e individual para com a cibersegurança , visando a preservação da integridade e da privacidade dos dados de saúde a todos os níveis operacionais.

Perceções do meio envolvente:

Carlos Vieira, *Country Manager da WatchGuard*, considera que

"Os cibertaques vão continuar a evoluir. O *phishing* vai continuar a ser mais inteligente. Vamos ter de utilizar ferramentas que permitem inspecionar o tráfego de tudo, até porque mais de 80% do tráfego que geramos é HTTPS e temos de ter soluções que consigam fazer essa inspeção porque há imenso *malware* que nos chega em HTTPS. O roubo de códigos de acesso vai ser a tónica; assistimos a imensas cadeias de hotéis, empresas de videoconferência e continuamos a ver novas empresas que sofrem roubo de códigos de acesso que depois estão à venda na *dark web*. Assim, a implementação de *multi-factor authentication* tem visto um crescimento de 200%. Os ataques persistentes vão continuar a existir, principalmente nas grandes empresas. Também o *ransomware* vai continuar a aumentar; se calhar vamos deixar de ter *ransomware* a resgatar equipamentos para fazer reclamar dinheiro – embora seja uma tendência -, mas estamos a ver muito o crescimento de *cryptomining*".

Nuno Mendes, *CEO da WhiteHat*, perceciona que

"é conhecido da cibersegurança que o elemento humano é um dos pontos fracos e, atendendo ao nível de sofisticação dos ataques que têm ocorrido no último ano, ainda mais importância tem o conhecimento que as empresas deveriam dar aos seus colaboradores. É um facto que a movimentação que tem havido para a *cloud* para facilitar o trabalho remoto, a incidência de ataques por *phishing* e *spear phishing* aumentou. Há ataques muito mais direcionados a grandes empresas. Em Portugal, temos uma realidade um bocadinho diferente, uma vez que os números de grandes organizações contam-se pelos dedos das mãos, e a nossa realidade é bastante diferente, uma vez que estamos dominados por micro, pequenas e algumas médias empresas. A tecnologia existe, mas, no entanto, continua a ser necessário criar uma perceção para o ciber- risco e essa é a mensagem mais difícil de passar para as empresas e para os colaboradores".

Élio Oliveira, *Territory Channel Manager & SMB da Kaspersky*, afirma que

"há um incremento muito grande daquilo que foram os ataques em 2020. No entanto, aquilo que faz sentido reter é que não há perímetro, mas também que cada vez mais é preciso

ferramentas que protejam o *endpoint.* É preciso ter algo que me consiga proteger de forma muito concreta aquilo que é o nosso *endpoint* porque é aí que vamos estar a trabalhar, é aí que vai estar a minha informação, que vou fazer o intercâmbio da informação, seja com os sistemas da empresa ou que estão na *cloud.* O que necessitamos claramente é o apoio de todas as pessoas e de todos os fabricantes porque o *endpoint* é fundamental e tem de ser muito bom para responder automaticamente a incidentes".

"é fundamental que os colaboradores tenham *awareness* dos perigos daquilo que é a cibersegurança. É preciso falar com as empresas e explicar que os colaboradores devem ter noção e conhecimento dos perigos da cibersegurança, aquilo que, na realidade, pode ser uma porta de entrada; é o utilizador que vai receber o e-mail, carregar no *link* e encriptar o PC".

Manuel Dias explica que,

"até agora, o IT olhava para a cibersegurança mais como uma despesa e não como um investimento. Este último ano provou o quão importante é para a operação das organizações. Não é só uma questão de proteção, é uma questão operacional do dia a dia. Compromete não só a própria operação normal do negócio, como todos os acessos pelos colaboradores e por todo o ecossistema. Acho que olhar para a cibersegurança como um investimento é fundamental e, para mim, isso começa nas lideranças, nos CISO. Também é importante ter literacia; não somos só nós, mas de todos os colaboradores que se ligam de múltiplos *devices,* muitas das vezes não geridos pelas empresas e que podem comprometer a segurança. É fundamental passar esta informação às pessoas; se não a tiverem, podemos colocar muitas barreiras, muitos sistemas, mas a segurança começa nas pessoas".

Diogo Pereira, *Cybersecurity Business Development Manager da Ingecom*, indica que

"esta nova forma de trabalhar apenas veio agravar as deficiências existentes". Neste contexto, "é preciso assegurar que as pessoas que estão a entrar no sistema – e ainda mais porque não estão no seu local de trabalho normal, estão fora do escritório – são exatamente elas. Os ataques de *ransomware* de hoje não se limitam a encriptar informação, tentam roubar informação. Tentam que os dados saiam e sejam vendidos. Isto implica que é necessário proteger os dispositivos com soluções de *Endpoint Detection and Response* (EDR), fazer análise de

vulnerabilidades para as tentar mitigar e depois usar soluções de encriptação e proteção de informação que encriptam a informação e garante que só é acedida porque quem deve aceder; se alguém a tentar roubar, ela já está encriptada e só quem tem acesso à informação é que a vai conseguir visualizar".

Em síntese, a disponibilização de dados clínicos, observáveis sob múltiplas perspetivas e capazes de proporcionar uma clareza de diagnóstico sem precedentes, representa uma aplicação extremamente eficaz e inovadora da telemedicina. Esta abordagem permite uma convergência de informações e experiências, acessíveis de forma praticamente instantânea, que pode transformar radicalmente a prática médica.

Contudo, a potencial utilização indevida desses dados para fins alheios ao interesse público constitui uma das mais significativas vulnerabilidades na consolidação da confiança dos pacientes. A ameaça de práticas fraudulentas e o risco associado à exploração comercial dos dados clínicos não podem ser subestimados. Este cenário exige uma atenção redobrada e a implementação de medidas rigorosas de cibersegurança, essenciais para garantir a privacidade e a proteção da informação sensível dos pacientes.

Assim, enquanto a telemedicina avança como uma ferramenta poderosa no setor da saúde, a salvaguarda dos dados clínicos deve permanecer uma prioridade. A confiança dos pacientes no Sistema Nacional de Saúde depende, em grande parte, da capacidade das instituições de saúde em proteger e gerir adequadamente os seus dados, evitando a exposição a riscos que possam comprometer a integridade do serviço prestado.

A crescente complexidade dos ciberataques e a relevância da salvaguarda das informações de saúde realçam a necessidade de um investimento contínuo em cibersegurança. A salvaguarda da informação clínica, aliada à promoção da literacia digital entre os colaboradores das instituições de saúde, é fundamental para assegurar que a revolução digital na saúde seja conduzida com segurança e eficácia, preservando sempre a confiança e o bem-estar dos pacientes.

3.3. Capacitação Digital: Formação Tecnológica na Comunidade Médica

As entrevistas realizadas com integrantes da comunidade médica revelaram uma lacuna significativa na formação em cibersegurança, particularmente no contexto da telemedicina. No Hospital Espírito Santo (HESE), em Évora, os três auxiliares de saúde entrevistados admitiram não ter recebido qualquer tipo de formação específica sobre como responder a um ciberataque. Este fato evidencia uma área crítica que requer atenção urgente.

Para mitigar esta situação, é imperativo investir em informação, formação e palestras direcionadas, já que, conforme relatado, não existe uma estrutura de formação para o setor de saúde em relação á cibersegurança. Bruna Guerreiro, auxiliar de saúde no HESE, enfatiza a importância de "sensibilização através de ações de formação que eduquem para esta problemática," destacando práticas básicas como a alteração regular de senhas e a proteção de acessos às plataformas de trabalho.

Marco Santos, Auxiliar no HESE, reforça esta necessidade ao afirmar que "Informar e formar será sempre a melhor medida." No entanto, apesar dos reconhecidos ciberataques que o hospital enfrentou, não houve uma formação para os profissionais de saúde e equipas associadas sobre como criar mecanismos eficazes de defesa, como destacado por Bruna Guerreiro, que acredita que “Todo esse trabalho foi feito de forma mais central pela equipa de informática."

A falta de simulações e de uma formação local específica em cibersegurança reflete uma abordagem que, embora apoiada em estratégias centrais, poderia ser significativamente refinada com iniciativas mais direcionadas às necessidades locais. Marco Santos sugere que “poderiam ser efetuadas formações aos profissionais de saúde sobre cibersegurança: formações que deveriam ser ministradas no ato de admissão do colaborador e com um refresh anual obrigatório.” Demonstrando uma visão proativa sobre como estas lacunas podem ser preenchidas de forma contínua e estruturada.

A curto prazo, a comunicação e disseminação de informação sobre cibersegurança devem ser ampliadas. Embora estejam a ser planeados *webinars* sobre o tema, como mencionado por Marco Santos, e existam práticas obrigatórias como a mudança de palavra-passe a cada três meses, citada por Bruna Guerreiro, ainda há muito a ser feito para assegurar uma proteção abrangente e eficaz.

Os profissionais de saúde desempenham um papel central na cibersegurança das instituições médicas, sendo frequentemente o elo mais vulnerável na cadeia de defesa digital. A sua interação diária com sistemas de informação e dados clínicos sensíveis torna-os alvos potenciais para ciberataques, especialmente quando não estão adequadamente preparados para identificar e responder a ameaças digitais.

Estudos indicam que o erro humano é responsável por uma significativa proporção das violações de dados no setor da saúde. A falta de formação específica em cibersegurança contribui para comportamentos de risco, como o uso de palavras-passe fracas, a abertura de anexos suspeitos e o desconhecimento de práticas seguras de navegação.

Além disso, a ausência de programas de formação contínua em cibersegurança impede que os profissionais se mantenham atualizados face às ameaças emergentes. A implementação de formação prática e adaptada ao contexto clínico é essencial para capacitar os profissionais a reconhecer e mitigar riscos, promovendo uma cultura organizacional de segurança.

Investir na formação contínua dos profissionais de saúde não é apenas uma medida preventiva, mas uma necessidade crítica para garantir a integridade dos dados dos pacientes e a confiança no sistema de saúde.

A infraestrutura de rede que suporta a telemedicina é essencial para que o seu potencial seja plenamente explorado. Nos últimos anos, três fatores principais contribuíram para a expansão das tecnologias que facilitam a telemedicina: a mobilidade das comunicações, a sua disseminação, e a capacidade de transmissão de conteúdos. Estes avanços tornaram possível o estabelecimento de sistemas que possibilitam a prestação de serviços de saúde em praticamente qualquer local.

É essencial que os especialistas de saúde permaneçam devidamente capacitados para utilizar estas tecnologias de forma segura e eficiente. Na obra “Os Direitos Humanos por um fio?” a afirmação, “Estamos na esquina de uma via de não retorno da aceleração evolutiva do ser humano e, claro, perante uma alvorada de um novo humanismo,” (pág.210) destaca a inevitabilidade da integração cada vez maior digitalização e modernização no meio hospitalar.

No entanto, o uso generalizado das TIC na telemedicina exige que vários pressupostos sejam atendidos. Entre eles, destaca-se a necessidade de disponibilizar tecnologias e equipamentos adequados, bem como de assegurar que os profissionais estejam qualificados para utilizá-los

de forma produtiva. Garantir níveis de competência que correspondam às novas realidades tecnológicas é mais do que um objetivo; é uma necessidade urgente que deve ser abordada com rigor e objetividade.

O desenvolvimento das TIC exige também uma mudança de paradigma. Estas tecnologias devem ser vistas não apenas como ferramentas operacionais, mas como impulsionadores de novos conceitos de comunicação e integração, capazes de gerar uma telesaúde pública mais ampla, organizada e integrada com outros setores de atividade. A partilha de informação e novas maneiras de interagir com as comunidades, é a melhor maneira de maximizar o potencial tecnológico, uma ideia que na obra "Os Direitos Humanos por um fio?" resume ao afirmar que "Tal pressão emana dos novos poderes tecnológicos do homem, exercendo-se pelo simples facto da sua existência." (pág.214)

A pandemia COVID-19 acelerou o uso de plataformas digitais e linhas telefónicas para o atendimento dos pacientes num regime diferenciado, levantando atenção para questões de ordem informacional. Embora o telefone seja geralmente uma forma de comunicação segura, a utilização de plataformas como *Skype* e *FaceTime,* que não foram desenhadas com padrões de segurança específicos para a saúde, expôs vulnerabilidades significativas. Este cenário ressalta a necessidade urgente de capacitar os profissionais de saúde em cibersegurança, para que possam exercer suas funções com confiança.

Os três principais objetivos dos profissionais de saúde em relação à telemedicina são claros: assegurar a proteção e a confidencialidade dos pacientes, assegurar que os sistemas utilizados são adaptados ao utilizador, e manter um diálogo aberto que envolva tanto os profissionais quanto os pacientes na concepção e manutenção dessas abordagens. Para alcançar estes objetivos, é crucial focar na formação em cibersegurança, cibereducação e ciberhigiene.

Concluindo, a integração da cibersegurança como uma prioridade estratégica dentro do sistema de saúde é imperativa. Mostra-se necessário um investimento contínuo em formação e implementação de tecnologias avançadas, garantindo que o sistema de saúde esteja preparado para as dificuldades apresentadas por uma sociedade em crescente digitalização. Este foco não só protegerá os dados clínicos, mas também fortalecerá a credibilidade e a confiança dos pacientes no sistema de saúde.

3.4. Transformação Digital: A Adaptação do Serviço Nacional de Saúde

O Serviço Nacional de Saúde (SNS) enfrentou um período de pressão contínua, impulsionado por desafios complexos e inesperados que exigiram respostas rápidas e flexíveis dos gestores responsáveis pela governança dos diferentes setores que compõem o SNS. Neste contexto, o desenvolvimento tecnológico apresentou métodos cruciais, tanto no plano estratégico como no operacional, para as instituições prestadoras de atendimento médico, fornecendo o apoio necessário para atender às necessidades dos pacientes.

Como afirma a *Safeguarding Health in Conflict Coalition (SHCC)* (2002), "A utilização de tecnologias de informação e comunicação para a prestação de cuidados de saúde, nomeadamente consultas, diagnósticos, tratamentos e transferência de dados clínicos, resulta em atividade exclusiva da telemedicina. Podemos assim afirmar que a telemedicina corresponde sobretudo à forma de prestar cuidados de saúde à distância, utilizando a transmissão de imagens, dados, voz, vídeo (com base informática) e informações através de diversos tipos de meios de comunicações, nomeadamente sistemas satélite, fibra ótica e internet."

Embora os benefícios da telemedicina sejam claros, não se pode negar que a sua utilização também agrega desafios significativos, especialmente relacionados com aspetos legais, organizacionais e tecnológicos. A qualidade da informação transmitida, a aceitação dos profissionais e a satisfação dos pacientes surgem como fatores críticos para o desenvolvimento e disseminação eficazes da telemedicina.

Este capítulo aborda a adaptação do SNS à pandemia COVID-19, com foco nos mecanismos estratégicos coordenados que foram implementados. Embora os esforços tenham sido substanciais, persistem áreas de disfunção e resultados abaixo do esperado. A infraestrutura existente, conforme relatos de profissionais de saúde, não estava completamente preparada para o desafio. Como exemplificado por Mafalda Mendes, auxiliar no Hospital Espírito Santo em Évora (HESE), "Pacientes positivos passam por onde pessoas negativas passam, mesmo sendo desinfetados, existe um sentimento de insegurança."

O conceito de Cibersegurança, essencial para a proteção dos dados clínicos, é muitas vezes desconhecido no quotidiano laboral de alguns setores, como observado na afirmação de Mafalda Mendes: "Não connosco, mas suponho que exista em outros setores." Isto evidencia

uma lacuna significativa na formação e disseminação de dados críticos entre os especialistas do meio. A comunicação ineficaz é outra área problemática, com perceções como a de que "Deveríamos ter direito a certo tipo de informação que não temos, pois existe disfuncionalidade na comunicação de dados clínicos." (Mafalda Mendes, HESE).

Além da necessidade de uma comunicação mais direta entre setores, revela-se a urgência de investimento na modernização dos sistemas informáticos e na atualização dos sistemas de segurança. Mafalda Mendes ressalta a disfuncionalidade atual, observando que "Quando existe necessidade de modificar dados o sistema torna-se disfuncional dado a necessidade de auxílio para o processamento da informação."

Quanto à disponibilidade de informação para os pacientes, o HESE possui um regulamento de segurança informacional acessível, como mencionado por Marco Santos: "Sim. Temos uma política de proteção de dados que poderá ser consultada na morada virtual por qualquer paciente a qualquer hora." No que diz respeito à obtenção dos especialistas aos dados clínicos, existe uma categorização por privilégios, garantindo que "Cada profissional apenas tem acesso aos dados que lhe poderão ser de interesse para o desempenho das suas funções." (Marco Santos, HESE).

No entanto, a perceção de incentivos para formar hábitos de segurança na comunidade médica ainda é limitada, conforme Marco Santos afirma: "Não tenho a perceção que isso aconteça, ainda!". Em contraste, no Hospital CUF Infante Santo, uma instituição com maior exposição a informações e investimentos em segurança, a perspetiva é mais positiva. Álvaro Filipe destaca que "muito se tem investido no setor nos últimos anos", comparando a situação atual com a de uma década atrás, quando "não existia de todo um investimento, nem uma preocupação como a que existe atualmente para a problemática da proteção dos dados."

Apesar do progresso em algumas áreas, existe uma necessidade de uma mudança mais profunda nos comportamentos sociais e na conduta quotidiana, especialmente relativos à segurança e à preservação da informação pessoal. Álvaro Filipe observa, "Penso que em Portugal ainda não estamos preparados para esse pensamento. Ainda olhamos para os nossos dados como algo de pouca importância e com o qual não nos preocupamos ainda."

O investimento na modernização do SNS é, segundo Álvaro Filipe, "a melhor opção a longo prazo," como demonstrado pela resposta à pandemia COVID-19. A integração das TIC

melhorou os resultados obtidos pelas organizações de saúde, sendo crucial salientar o papel da telemedicina como facilitadora dos processos de integração, especialmente nas suas dimensões clínicas e informacionais.

Contudo, a fragmentação das responsabilidades e a falta de coordenação entre as tecnologias em uso, juntamente com a implementação descontrolada de novas ferramentas sem um plano abrangente bem definido, têm-se revelado inadequadas para a atualização eficaz do setor. É fundamental estabelecer um plano coeso que estruture a operacionalidade das políticas de saúde.

As deficiências no setor de informação e nos sistemas de base têm causado dificuldades na representação dos pacientes e na gestão das suas informações clínicas e administrativas, bem como na recolha e consolidação de dados críticos para o processo de escolha em toda a rede de prestação de cuidados. Estas deficiências representam um fardo oneroso para as organizações de saúde. Portanto, as reformas em curso no setor da saúde em Portugal devem ser complementadas para promover a modernização, especialmente nas áreas de acompanhamento de pacientes e na documentação correta das intervenções em saúde.

Apesar de o papel fundamental das TIC na evolução tecnológica do setor em Portugal ser amplamente reconhecido, é igualmente necessário adotar uma estratégia de informação para a saúde que seja capaz de apontar para as principais áreas de intervenção. Esta estratégia deve centrar-se no contato com o paciente e na responsabilidade pelo sistema de saúde, garantindo transparência dos atos praticados.

A introdução de uma estrutura de dados de saúde unificada e de uma entidade capaz de criar e executar é a estratégia mais eficiente para enfrentar as necessidades emergentes desta nova realidade comunicacional. A implementação de novas abordagens para a administração das intervenções em saúde possibilita estruturas de financiamento inovadoras para o setor e estratégias de saúde mais justas e eficazes, devendo ser considerada uma prioridade para garantir menores custos de funcionamento e uma estrutura social mais justa e orientada para o paciente.

A abordagem para as plataformas de informação de saúde será o impulso para a reorganização do SNS. Sem esta abordagem, será inviável torná-lo mais contemporâneo, atualizado, equitativo, eficiente e, sobretudo, centrado no paciente. Como afirma Maia (2020), "Uma

noção mais clara dos problemas que o SNS terá de gerir no futuro imediato. Refiro-me à suspensão da atividade programada não urgente (consultas, cirurgias, terapia e meios complementares de diagnóstico)", cujas consequências, segundo Nogueira (2020), "ainda não são bem conhecidas além do aumento da mortalidade 'não-Covid-19'".

Durante o período pandémico, constatou-se uma desregulação no acompanhamento de condições crónicas, na elaboração de avaliações e na deterioração da saúde psicológica. Torna-se, portanto, necessário atingir um ponto de equilíbrio. A resistência a mudanças necessárias é atribuída à ausência de acordo sobre a função do SNS no contexto da saúde, influenciado por políticas oscilantes e pela ausência de debates essenciais para garantir a conformidade com os valores fundamentais de acesso universal, abrangência e gratuitidade dos cuidados.

Estas questões destacam a urgência de reconsiderar a estrutura de recursos financeiros do SNS, dadas as sucessivas dificuldades em transformar a disposição do trabalho entre os diversos grupos de especialistas e em definir o papel da prestação privada no contexto do SNS. Como sublinha a Presidência do Conselho de Ministros (2015), "A segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, militares ou civis, coletivos ou individuais."

Com base na urgência identificada e na responsabilidade partilhada entre os diversos atores do sistema de saúde, é essencial delinear políticas públicas específicas e projetos operacionais que fortaleçam a cibersegurança no Serviço Nacional de Saúde (SNS). Entre as estratégias possíveis, destacam-se:

1. **Plano Nacional de Cibersegurança em Saúde** – um programa coordenado que defina normas, protocolos e medidas técnicas obrigatórias para instituições públicas e privadas ligadas ao SNS, promovendo interoperabilidade segura e auditável.

2. **Programa de Formação Contínua Obrigatória** – políticas públicas que obriguem à formação certificada e regular em cibersegurança para todos os profissionais de saúde, com módulos adaptados a diferentes funções (médicos, enfermeiros, técnicos, administrativos).
3. **Financiamento Estruturado para Infraestruturas Digitais Seguras** – inclusão de linhas de financiamento específicas no Orçamento do Estado para modernização tecnológica e aquisição de sistemas de defesa avançada contra ciberataques.

4. **Criação de uma Entidade Nacional para a Segurança Digital em Saúde** – organismo autónomo responsável por monitorizar, auditar, responder a incidentes e emitir alertas e orientações.
5. **Protocolos Público-Privados em Segurança Digital** – incentivar parcerias com empresas tecnológicas certificadas para desenvolver soluções robustas, promovendo inovação responsável no setor.
6. **Campanhas Nacionais de Sensibilização Digital** – ações públicas dirigidas à população e aos profissionais de saúde sobre boas práticas digitais e riscos cibernéticos, reforçando a literacia digital e a confiança no sistema.

Estas políticas e projetos devem ser acompanhados de avaliação contínua, com indicadores de desempenho e impacto, garantindo um modelo sustentável, adaptável e centrado na segurança do utente.

Capítulo IV. A Telemedicina e a Pandemia Covid-19

4.1. A Pandemia como Impulsionador: A Oportunidade da Covid-19 para a Telemedicina

A pandemia COVID-19 provocou profundas mudanças nas interações sociais a nível global. Durante o período de isolamento, os indivíduos compreenderam a utilidade da digitalização, pois puderam auxiliar na manutenção do contato sem a necessidade de exposição ao vírus, tanto em contextos de trabalho e educação, quanto em interações familiares e sociais. Este uso intensificado das tecnologias digitais visava incentivar o cumprimento das orientações da Organização Mundial da Saúde (OMS) sobre o distanciamento social.

No que diz respeito aos serviços de saúde, a situação foi semelhante. Apesar da crise ter exercido uma pressão imensa sobre os sistemas de saúde na Europa, foram feitos esforços significativos para acelerar a digitalização, com a adoção de soluções tecnológicas que pudessem superar os desafios impostos.

Merrill Singer, nos anos 90, propôs uma reformulação dos termos relacionados ao desenvolvimento de epidemias, introduzindo o conceito de "sindemia". Este conceito implica uma abordagem diferenciada que reconhece que o vírus não atua de forma isolada, mas sim em interação com outras condições de saúde. Além disso, Singer destaca a importância da

disparidade social neste contexto. Com base nesse entendimento, surgiram observações que fortaleceram essa ideia. "A COVID-19 não é uma pandemia. É uma sindemia. A natureza sindémica da ameaça que enfrentamos exige uma abordagem mais diversificada se quisermos proteger a saúde de nossas comunidades" (Horton, 2020).

Esta visão interligada evidencia como fatores sociais e ambientais amplificam os impactos adversos que surgem da interação de determinadas patologias. Ao explorar as repercussões significativas de intervenções como o isolamento e o distanciamento social, torna-se claro que é essencial adotar uma abordagem mais abrangente nas respostas de saúde pública. Tal compreensão aprofunda o entendimento das doenças e destaca a importância de integrar múltiplas dimensões contextuais para abordar de forma eficaz as complexidades da saúde coletiva. Promover uma perspetiva integrada possibilita a formulação de estratégias mais adequadas e sensíveis às realidades enfrentadas pelas comunidades.

Segundo *Richard Horton*, que preserva um papel fundamental nas publicações médicas científicas britânicas, observa que as intervenções até agora concentraram-se em interromper a transmissão viral, baseando-se em abordagens convencionais para enfrentar surtos de doenças.

Horton afirma: "Duas categorias de doenças estão interagindo dentro de populações específicas – a síndrome respiratória aguda severa (SARS-CoV-2) e uma série de doenças não transmissíveis (DNTs). Estas condições agrupam-se dentro de grupos sociais de acordo com padrões de desigualdade profundamente enraizados na nossa sociedade. A agregação dessas doenças num contexto de disparidade social e económica exacerba os efeitos adversos de cada doença separadamente" (*Horton*, 2020).

As sindemias, conforme destacado por *Horton*, são marcadas por conexões físicas e sociais que intensificam a vulnerabilidade dos indivíduos, agravando seu estado de saúde ao contraírem uma doença. Observando que "o número total de pessoas que vivem com doenças crónicas está crescendo. Abordar o COVID-19 significa abordar a hipertensão, obesidade, diabetes, doenças cardiovasculares e respiratórias crónicas, e cancro" (*Horton*, 2020). *Horton* também enfatiza que "a menos que os governos elaborem políticas e programas para reverter as profundas disparidades, a sociedade nunca estará verdadeiramente segura da COVID-19" (*Horton*, 2020).

No início da propagação do vírus, a Organização Mundial da Saúde (OMS) e o Ministério da Saúde designaram o distanciamento social como uma das estratégias mais eficientes para mitigar o aumento de contágios. Desta forma, as consultas presenciais e agendadas foram suspensas ou canceladas. Nesse cenário, tornou-se imperativo desenvolver novas abordagens que garantissem a continuidade dos cuidados de saúde, mesmo que de forma remota.

Foi neste cenário que a e-saúde, especificamente, a consulta médica à distância e o acompanhamento remoto de pacientes surgiram como soluções eficazes para o setor da saúde. Embora estas opções não sejam novas, a sua utilização era limitada até então. A pandemia acelerou a adoção dessas tecnologias, que agora são consideradas essenciais para garantir o acesso contínuo aos cuidados de saúde durante períodos de restrições físicas.

"Portugal enfrenta, atualmente, ainda alguns desafios em relação a um maior desenvolvimento neste campo. Apesar de 87% dos hospitais públicos recorrerem à telemedicina" (*Organização Europeia EIT Health*).

Para assegurar a viabilidade financeira dos sistemas de saúde, é essencial que a saúde, tanto atualmente como no futuro, seja sustentada por tecnologias da informação que agilizem o dia a dia de cada paciente e profissional, tanto nas unidades de saúde como fora delas. Tecnologias que incluem sistemas de gestão de informações clínicas, plataformas de telemedicina e aplicações que permitem a monitorização remota. A integração destas soluções tecnológicas é fundamental para otimizar processos, melhorar a comunicação e garantir um atendimento de qualidade e acessível.

Durante a pandemia, a telemedicina destacou-se como uma ferramenta valiosa, tanto para profissionais de saúde quanto para doentes, aliviando as falhas de comunicação que surgiram em praticamente todos os setores sociais. O contexto pandémico, portanto, proporcionou um terreno fértil para a dinamização da telemedicina na prática quotidiana.

Em Portugal, a pandemia motivou um aumento na utilização da telemedicina, embora sua aplicação já tenha várias décadas de história. Em 1995, o Dr. Eduardo Castela, Diretor do Serviço de Cardiologia Pediátrica do CHUC e Presidente da Associação Portuguesa de Telemedicina, vislumbrou a telemedicina como uma solução para a escassez de especialistas em cardiologia pediátrica e fetal em hospitais distritais, implementando com sucesso o apoio à região centro.

A evolução consistente do impacto positivo da telemedicina pode ser observada no "Plano Estratégico Nacional para a Telessaúde 2019-2022", desenvolvido pelos Serviços Partilhados do Ministério da Saúde (SPMS)[8] através do Centro Nacional de Telessaúde. Esta estratégia sublinha a importância da telemedicina como um instrumento que facilita a integração de processos, principalmente nas dimensões clínicas e informacionais, como salienta Hélio

Hamada e Renato Moreira (2019),” tendo em vista a importância do conhecimento atrelado á ação” (pág. 28).

Contudo, para garantir que as tecnologias de informações exerçam a sua influência de apoio á saúde, é necessário que existam estratégias de informação que apontem para as principais áreas de intervenção. Estas estratégias devem tornar prioritário o contato com o paciente e o fundamento da responsabilização nos serviços de saúde, incentivando a clareza nas ações realizadas.

Em suma, a adoção de uma estrutura integrada de dados no setor, juntamente com uma entidade capaz de desenvolver e executar essa estrutura., é a estratégia mais eficiente para atender às necessidades emergentes da nova realidade comunicacional. A introdução de novos mecanismos de gestão e supervisão dos serviços de saúde, permitindo o desenvolvimento de novos modelos de apoio financeiro, diretrizes de saúde mais justas e uma maior qualidade e eficiência operacional deve ser o objetivo central na reestruturação do sistema de saúde, sempre com foco na modernização e eficiência, orientada para o paciente.

A emergência sanitária provocada pela COVID-19 tornou evidente a importância de adotar a telemedicina como um recurso essencial para a promoção do bem-estar e o acesso a cuidados de excelência A telemedicina, contudo, enfrenta várias dificuldades para as entidades de assistência médica, não apenas ao nível da estrutura organizacional., mas também no que respeita ao necessário reforço de investimentos. É imperativo reconhecer a “rápida evolução

[8] O Centro Nacional de TeleSaúde da SPMS, EPE, preparou um plano estratégico (PENTS) para os anos de 2019 a 2022, aprovado pelas autoridades competentes, que visa estabelecer diretrizes para impulsionar o uso da Telessaúde em Portugal.

intrínseca ao ciberespaço e, consequentemente, a crescente evolução das ameaças, das vulnerabilidades, dos processos e das infraestruturas, bem como dos modelos económicos, sociais e culturais que assentam na sua utilização" (Presidência do Conselho de Ministros, 2015).

A necessidade de uma maior normalização e regulamentação no campo da telemedicina é evidente, dada a aceitação generalizada das suas vantagens para os indivíduos. A colaboração ativa dos pacientes ao longo de todo o processo de integração e avanço destas tecnologias é essencial, garantindo a inclusão de todos os intervenientes. O período de isolamento e suas implicações tornaram mais evidentes as vantagens que a telemedicina pode oferecer aos cuidados de saúde. Esta prática evoluiu de um mero recurso tecnológico utilizado para superar dificuldades de acesso a especialidades médicas, especialmente em regiões do território nacional onde essas especialidades estavam ausentes, para um meio comunicacional eficaz. Esta evolução permitiu a criação de relações de trabalho entre profissionais que, embora geograficamente distantes, puderam colaborar de forma eficiente, sem a necessidade de compartilharem o mesmo espaço físico.

Esta transição revelou uma nova dimensão na prática médica, onde a telemedicina demonstrou ser um pilar essencial para a modernização dos cuidados de saúde. Como expresso na obra "Os Direitos Humanos por um Fio?", "A ciência conduz à experimentação, e esta apresenta-se com o esplendor da esperança (otimismo) em uma mão e, na outra, os receios do inesperado" (pág.223). Esta citação captura a dualidade inerente ao avanço tecnológico na medicina: enquanto há esperança no potencial transformador da telemedicina, persiste o receio das incertezas e desafios que acompanham esta inovação.

A telemedicina, portanto, deixou de ser apenas uma solução temporária ou uma alternativa para contextos específicos, como a falta de especialistas em determinadas regiões. Ela consolidou-se como uma prática integrada e indispensável na disponibilidade de serviços, exigindo uma reação das instituições em termos de regulamentação, organização, e investimento contínuo. O sucesso na implementação da telemedicina não depende apenas da tecnologia, mas também da adaptabilidade das instituições a diferentes circunstâncias e de garantirem que todos os cidadãos, independentemente da sua localização ou condição social, tenham acesso igualitário a estes avanços.

Neste contexto, a telemedicina simboliza mais do que uma simples ferramenta tecnológica; ela representa uma evolução significativa na forma como os cuidados de saúde são concebidos e prestados. O desafio, agora, reside em garantir que esta evolução seja acompanhada por uma regulamentação adequada e pela inclusão ativa dos pacientes, assegurando que todos possam beneficiar das oportunidades que a medicina à distância oferece, com segurança, eficácia e equidade.

4.2. Redefinindo o Cuidado: O Impacto da Telemedicina no SNS

A emergência sanitária causada pelo COVID-19 impactou significativamente a funcionalidade do Serviço Nacional de Saúde (SNS) e setores associados, evidenciando restrições na acessibilidade aos serviços. Estas restrições manifestaram-se pela suspensão ou diminuição das atividades programadas nos estabelecimentos do SNS e pela paralisação das atividades em estabelecimentos das áreas privada, cooperativa e comunitária. Em resposta, no sentido de garantir a prestação contínua e segura de cuidados médicos, foram criadas diversas estruturas de atendimento remoto. Estes esforços abrangeram um número significativo de centros de consulta digital, tanto em ambiente hospitalar como nos cuidados de proximidade.

O principal objetivo de qualquer intervenção médica é promover o equilíbrio e a qualidade de vida do paciente. Dada essa importância, a forma como as aplicações clínicas da telemedicina influenciam a qualidade do cuidado e os seus resultados é uma questão central para qualquer sistema de saúde. Avaliações rigorosas desempenham um papel essencial no progresso de qualquer área médica, sendo a telemedicina uma área em que tais processos são especialmente necessários devido à escassez de evidências empíricas sobre a sua utilização. A realização de avaliações e a disseminação de resultados confiáveis são cruciais para o desenvolvimento de políticas e estratégias nacionais que otimizem a implementação da telemedicina e informem sobre seu potencial de desenvolvimento, como expressa Adriano Moreira (2009) “Perfilam-se desafiantes em relação á viabilidade, pelo menos a curto prazo” (pág.6).

No entanto, uma das barreiras mais prevalentes na implementação de programas de telemedicina a nível global foi a cultura organizacional desarticulada, que se refletiu na partilha e troca de conhecimentos entre profissionais e pacientes em locais remotos. A constituição de sistemas de telemedicina exige a aceitação dos envolvidos no processo; a resistência aos requisitos programáticos pode indicar uma falta de conscientização ou um desconforto quanto

ao uso dos próprios sistemas. Como apontado na obra "Politicas Públicas, Economia e Sociedade" (2015), "para além do impacto direto na capacidade de antecipação e resposta a situações de doença, as políticas públicas na área da saúde apresentam também fortes externalidades, positivas e negativas, noutros setores da nossa sociedade, como a educação, a economia, a proteção social ou a capacidade de manifestação desportiva e cultural dos povos". (Paulo Neto e Maria Manuel Serrano)

Os médicos desempenham um papel fundamental na adoção e difusão da telemedicina, e a validação por parte dos médicos locais é uma condição indispensável para a obtenção de resultados satisfatórios destes programas, especialmente no serviço de urgência e nas unidades de cuidados continuados. Os métodos que promovem a interação médico-paciente, aumenta a confiança entre os prestadores de cuidados e incrementa a conscientização sobre o facto de tratamentos bem-sucedidos serem vitais para alterar atitudes e aumentar a adesão à telemedicina.

A telemedicina tem emergido como uma ferramenta cada vez mais requisitada para enfrentar os desafios no cuidado de emergências e nas unidades de cuidados continuados, incluindo o acesso facilitado de médicos a áreas remotas e a alta requisição por especialistas, tanto em áreas rurais como urbanas. Para avaliar o impacto gerado pela telemedicina, é necessário validar todas as suas dimensões, que incluem a capacidade técnica, a precisão de diagnósticos confiáveis, o impacto desses diagnósticos na terapia e o estado final do paciente o que na perspetiva de Hélio Hamada e Renato Moreira (2019) "a torna prática e consciente da responsabilidade de produzir resultados" (pág.28).

Com a inclusão da telemedicina nos algoritmos de apoio à decisão, verificaram-se mudanças culturais na organização dos cuidados de saúde, que impactaram positivamente a qualidade e a segurança na assistência aos pacientes. A troca de conhecimentos entre profissionais de saúde, facilitada pelo uso mais frequente de consultas por telemedicina, pode levar a um aumento na compilação comum de conhecimento e uma maior quantidade de tratamentos administrados por profissionais interconectados. Neste contexto, como sublinham Paulo Neto e Maria Manuel Serrano (2015), "a inovação e a internacionalização constituem processos em que a aprendizagem e a decorrente acumulação de conhecimento são a via mais segura de evitar os riscos sempre presentes da réplica e da imitação".

A comunicação e o envolvimento dos intervenientes são cruciais antes da implementação de programas de telemedicina, pois é necessário mitigar conflitos, tais como, preocupações relacionadas à responsabilidade, à carga de trabalho adicional e à identificação de quando

esta ferramenta é necessária. Programas de telemedicina que não foram bem-sucedidos geralmente falharam por percecionarem-se como entidades separadas da organização em geral, com objetivos independentes. O potencial total da telemedicina só será alcançado com mudanças na cultura médica e nas atitudes dos intervenientes, promovendo um novo paradigma na disponibilidade de cuidados, onde a partilha de conhecimento permite que organizações de saúde prestem serviços de alta qualidade, independentemente das barreiras geográficas.

Gustavo Scapini, cirurgião geral e gerente médico da Johnson & Johnson Medical Devices, alerta para as consequências da demora do reconhecimento e intervenção na assistência dos indivíduos, enfatizando que "quanto mais tarde diagnosticarmos uma doença, maior a probabilidade de o paciente ter uma doença grave e maior o risco de ele desenvolver complicações mais sérias. Em termos de investimento em saúde, um paciente com maior gravidade consome mais recursos humanos, tem um pior prognóstico e menor expectativa de vida. Usando um velho bordão, 'é melhor prevenir do que remediar'. Infelizmente, os anos de 2021 e 2022 serão de remediações e não sabemos ao certo quando conseguiremos reorganizar o sistema".

A telemedicina, impulsionada pelo desenvolvimento da digitalização e modernização tecnológica, tem progressivamente, permitindo a transferência de quantidades crescentes de dados transmitidos à distância, utilizando diferentes soluções de comunicação A inclusão de elementos visuais e a expansão das redes atualmente disponibiliza alternativas criativas para problemas preexistentes. A crise pandémica impulsionou ainda mais a sua integração como parte da rotina diária, projetando que "a pressão sobre a capacidade de resposta dos sistemas de saúde é hoje, e será no futuro, muito significativa" (Paulo Neto e Maria Manuel Serrano, (2015)).

Embora represente uma solução excecional que permite o acesso a atendimentos especializados e reuniões com especialistas sem a necessidade de deslocamentos físicos, a integração da medicina à distância nos serviços de saúde tem avançado de forma inconsistente e mais demorada do que se previa. Como observado na obra "Gestão Moderna de Projetos" (2019),

“é necessário ajustar a abordagem ao projeto, não o contrário. Para tal, é necessário um bom conhecimento de uma variedade de metodologias e uma compreensão do modo como as misturar e combinar, conforme o necessário” (António Miguel, PMP).

As epidemias tendem a intensificar a situação dos cuidados prestados a pacientes com condições crónicas, e o uso da telemedicina contribuiu para mitigar este impacto negativo.

Uma vantagem adicional foi a compreensão da possibilidade de substituir de forma adequada as consultas presenciais, que muitas vezes eram mantidas apenas por tradição e pelo domínio de processos conservadores. A telemedicina promove uma melhor coordenação e favorece decisões mais informadas em relação aos pacientes, que têm a oportunidade de se envolver ativamente no seu próprio tratamento.

4.3. Ferramentas do Futuro: Plataformas Digitais na Telemedicina

A necessidade de isolamento decorrente da pandemia COVID-19 destacou a conectividade como elemento essencial na redefinição do atendimento e na formulação de estratégias de saúde digital. Esta transformação, já prevista e em processo de planeamento por diversas instituições, foi acelerada e prontamente implementada.

A telemedicina, que outrora era apenas uma opção, tornou-se uma aliada indispensável para médicos e pacientes no contexto da assistência à saúde. Com o surgimento da pandemia, a autorização para a prática da telessaúde e telemedicina revelou-se crucial, uma vez que o isolamento social imposto exigiu alternativas para que os pacientes tivessem acesso a atendimento e cuidado em dinâmicas de menor gravidade, bem como para aconselhamento e monitorização de pacientes crónicos.

A emergência da necessidade de conectividade e transferência de informações, com o objetivo de estabelecer uma estratégia de atendimento digital, incentivou a criação de alternativas por setores inovadores, tanto de caráter individual quanto coletivo. As plataformas digitais emergiram como uma solução que evidenciou o impacto positivo da conectividade digital no meio da crise comunicacional provocada pela pandemia, como evidencia Adriano Moreira (2014) “Temos desafios que são identificadamente novos” (pág.6).

Uma dessas alternativas foi a plataforma Doctorino, que, com mais de 1000 médicos associados, passou a oferecer a opção de videoconsulta através da tecnologia desenvolvida pela *Knok*. O objetivo era tornar esta modalidade de atendimento mais acessível tanto para profissionais de saúde quanto para pacientes. Embora alguns médicos já realizassem videoconsultas de forma independente, não existia até então uma plataforma profissional em Portugal que pudesse reunir estes profissionais e simplificar o processo de videoconsulta. A funcionalidade da videoconsulta estava inicialmente planeada a médio prazo, mas foi antecipada devido à chegada do COVID-19 a Portugal. Como Nuno Gonçalves, cofundador da Doctorino, afirma: “O lançamento do serviço já estava no nosso roadmap, mas com a chegada do COVID-19 a Portugal, achámos que o mais importante era fazer um sprint e disponibilizar a opção de videoconsulta o mais cedo possível. O futuro da saúde passará cada vez mais pela telemedicina e queremos estar preparados.”

Neste sentido, José Bastos, CEO da Knok Healthcare, reforça a importância da parceria: “A

Knok Healthcare desenvolveu uma plataforma para videoconsulta que tem sido enormemente usada, sobretudo no momento que atravessamos e que exige o afastamento dos típicos locais de prestação de serviços de saúde, aliando o efeito imediato de obtenção de diagnóstico médico à poupança de tempo e ausência de deslocações. Para nós, a parceria com a Doctorino constitui mais um passo importante no sentido de garantir o acesso a cuidados de saúde primários a toda a população."

Apesar do seu impacto significativo na digitalização da saúde em Portugal, a Doctorino cessou as suas operações. Embora não existam informações públicas detalhadas sobre as razões específicas do encerramento, é possível que fatores como a intensificação da concorrência no setor da saúde digital, desafios na sustentabilidade financeira e a rápida evolução tecnológica tenham contribuído para essa decisão.

O legado da Doctorino permanece como um marco na transformação digital dos serviços de saúde em Portugal, evidenciando a importância da inovação e da adaptabilidade no setor.

No âmbito da atenção primária à saúde, o projeto "PrimaryCare@COVID-19" desenvolveu uma plataforma digital para apoiar e monitorizar pacientes crónicos durante a pandemia incluindo componentes "inteligentes", com algoritmos que geram alertas para médicos e enfermeiros, aprimorando a monitorização e a gestão dos pacientes. O projeto é financiado pela Fundação para a Ciência e a Tecnologia (FCT), no âmbito do Research4COVID-19, e contou com o apoio da Universidade Nova de Lisboa (UNL) e da Administração Regional de Saúde de Lisboa e Vale do Tejo (ARS LVT), além de parceiros como o INOV INESC Inovação[9], na área da inovação, e uma colaboração com a unidade de doenças crónicas do Hospital Universitário de Genebra, na Suíça.

Esta plataforma digital oferece aos portadores de doenças crónicas a opção de realizar teleconsultas como alternativa às consultas presenciais, permitindo que médicos e enfermeiros dos cuidados primários possam acompanhar os pacientes à distância. O projeto insere-se no

[9] O **INOV - INESC Inovação** é pioneiro em investigação e inovação, impulsionando o avanço tecnológico e soluções para desafios sociais.

contexto de saúde digital, apresentando uma oportunidade valiosa para gerir o cuidado de pacientes crónicos durante epidemias, evitando descompensações das suas condições e reduzindo idas desnecessárias aos serviços de saúde e às urgências.

Este conjunto de iniciativas demonstram a importância crescente da telemedicina e das plataformas digitais na redefinição dos cuidados de saúde em tempos de pandemia, ressaltando a necessidade de adaptação e inovação contínuas para garantir a acessibilidade e padrão nos serviços.

A plataforma digital *Virtual Healthcare*, dedicada à partilha de informações no campo da telesaúde, desenvolveu uma formação específica em medicina à distância e no uso de alternativas digitais voltada para especialistas. Esta formação consistiu numa academia virtual em formato *e-learning*, objetivando habilitar os especialistas no uso eficaz e seguro destas tecnologias na prática clínica.

Cada módulo da formação incluiu uma avaliação no final, garantindo que os participantes adquirissem o conhecimento necessário. Os profissionais de saúde que completaram todos os módulos com sucesso receberam um certificado reconhecido pelas sociedades médicas que apoiaram a iniciativa. Ricardo Ladeiras Lopes, coordenador da Academia *Virtual Healthcare*, destacou a importância da formação ao afirmar: "A telemedicina já era vista há algum tempo como uma ferramenta muito importante no futuro dos cuidados de saúde, mas a pandemia veio acelerar a sua implementação. É muito importante conhecer a tecnologia, os seus benefícios e também as regras a cumprir aquando da sua utilização e esta Academia propõe-se a disponibilizar informação para que os participantes adquiram estes conhecimentos de uma forma prática e rápida."

Tiago Amieiro, diretor-geral da Amgen Biofarmacêutica em Portugal, reforçou a relevância desta capacitação no contexto atual: "Nos últimos anos temos assistido a uma evolução sem precedentes no que diz respeito às tecnologias da saúde e a pandemia Covid-19 obrigou governos e profissionais de saúde a reequacionar o tipo de acompanhamento que é dado aos doentes, bem como as formas mais sustentáveis de dar respostas na área da saúde. Os profissionais de saúde tiveram de se adaptar e aumentar a sua atividade no mundo digital, mas para que esta mudança seja feita de forma sustentada e consciente, é importante capacitar todos os intervenientes, de modo a aproveitarem o potencial destas ferramentas no exercício da sua

prática clínica. É isso que pretendemos fazer com esta Academia *Virtual Healthcare* e com a plataforma *Virtual Healthcare*, que conta já com seis meses de existência."

Ainda no âmbito de resposta à pandemia, o Serviço Partilhados do Ministério da Saúde (SPMS) destacou a eficácia do uso do 2424 para o envio de mensagens SMS, foram transmitidas mais de 70 milhões de comunicações aos cidadãos portugueses através deste contato. O SPMS comentou a relevância deste serviço ao afirmar que "A adoção do número 2424 permitiu aos pacientes identificar com facilidade a origem da SMS, promovendo a confiança no processo de vacinação e contribuindo para a elevada taxa de vacinação atingida."

Estas iniciativas ilustram a crescente integração das tecnologias digitais no setor, enfatizando a relevância da formação, inovação e confiança pública na efetiva implementação destas ferramentas para enfrentar os desafios contemporâneos e aprimorar o padrão de oferta no atendimento.

4.4. Cibersegurança na proteção e confidencialidade dos dados médicos

A introdução de novas tecnologias, especialmente no contexto da saúde, costuma gerar preocupações e reticências, principalmente entre indivíduos ou grupos mais conservadores, que ainda compõem uma parte significativa das Autoridades Administrativas. A medicina à distância, caracterizada por um leque de ferramentas tecnológicas e soluções digitais, possibilita a execução de intervenções médicas remotamente, já está amplamente aplicada em praticamente todos os ramos da medicina. Incluindo áreas complexas e minuciosas, como a cirurgia e a cardiologia, até especialidades mais rotineiras ou destinadas a rastreios.

Reconhecendo as suas valências, o poder legislativo tem regulamentado a telemedicina através de normativas legais, na dimensão europeia quanto na legislação interna, e também através de diretrizes estruturadas pelas Autoridades Administrativas Portuguesas. No entanto, apesar das inegáveis vantagens proporcionadas pela digitalização e modernização da tecnologia associadas à medicina e á sua regulamentação legal, persiste uma resistência significativa à sua adoção. Como em qualquer área que envolve o uso de tecnologia, o uso da medicina digital apresenta desafios e algumas restrições.

Os principais obstáculos que podem surgir na comunicação entre profissionais de saúde e pacientes incluem interrupções que podem comprometer o processo de diagnóstico, assim como a dificuldade em assegurar que a autorização para tratamento seja obtida de forma clara e plenamente informada. É fundamental reconhecer que as informações de saúde são consideradas dados sensíveis e estão sujeitas a um regime específico, conforme disposto no artigo 9.º do Regulamento Geral de Proteção de Dados (RGPD). Esta classificação especial enfatiza a necessidade de garantir que tanto a comunicação quanto a obtenção de consentimento sejam conduzidas de maneira transparente e ética, a fim de proteger os direitos dos pacientes.

Conforme estipulado no artigo 9.º do Regulamento Geral de Proteção de Dados (RGPD), o tratamento de informações de saúde é autorizado apenas em situações específicas. Isso inclui casos em que o indivíduo titular dos dados oferece seu consentimento explícito para o processamento de suas informações pessoais para fins determinados, ou quando essa ação é imprescindível para realizar diagnósticos médicos, proporcionar cuidados ou tratamentos de saúde, ou ainda em decorrência de um acordo estabelecido com um profissional da área da saúde.

Esta regulamentação visa garantir que o tratamento de dados sensíveis ocorra de maneira ética e respeitosa em relação à privacidade dos indivíduos, o tratamento de dados deve ser realizado exclusivamente por um profissional que esteja vinculado ao dever de confidencialidade ou por outra pessoa que compartilhe esta obrigação, assegurando assim que a privacidade e o segredo profissional sejam respeitados em todas as situações.

Este regime deve ser compatível com o artigo 29.º da Lei de Execução Nacional do RGPD, o qual amplia o dever de confidencialidade para todos os membros dos órgãos, colaboradores e prestadores de serviços do responsável pelo tratamento. Além disso, abrange também estudantes e investigadores na área da saúde que tenham acesso a esses dados sensíveis, garantindo assim a proteção integral das informações pessoais. O artigo enfatiza a importância da implementação de medidas de segurança proporcionais aos riscos associados ao tratamento dessas informações. Adicionalmente, conforme o estipulado, é fundamental que o titular dos dados seja informado sobre qualquer acesso que ocorra aos seus dados pessoais. A responsabilidade de garantir que um mecanismo eficaz de rastreabilidade e notificação esteja em vigor recai sobre o responsável pelo tratamento, assegurando assim a transparência e a proteção dos direitos dos indivíduos.

Apesar das vantagens e potencialidades que a telemedicina e, de forma mais ampla, a utilização de tecnologias de comunicação à distância proporcionam ao setor da saúde, o quadro regulatório levanta várias questões jurídicas. Estas questões são fundamentais para acompanhar a transformação digital que envolve inovações como robótica, blockchain e inteligência artificial, sendo igualmente essenciais para reforçar a confiança dos intervenientes, sejam eles pacientes ou especialistas. É fundamental encontrar um equilíbrio entre o avanço tecnológico e a proteção da segurança e da privacidade de todos os envolvidos.
As dificuldades iniciais geradas pela transição tecnológica manifestaram-se devido à oposição à inovação por parte de certos especialistas, que, por causa da falta de instrução específica, demonstraram dificuldades em utilizar computadores e softwares adequados. A nível institucional, a transição é marcada por uma baixa fluidez no processo, devido ao desconhecimento dos projetos em curso nas diversas unidades de saúde, com as quais poderiam ser celebrados protocolos de colaboração. Além disso, restrições orçamentais e dificuldades em ajustar horários dentro das normas vigentes também contribuíram para uma descoordenação dos canais já existentes, desproporcional à necessidade de garantir um acompanhamento médico de qualidade e uma comunicação eficiente.

A adaptação às competências necessárias para a interação tecnológica apresenta-se, portanto, como uma prioridade, nas palavras de Adriano Moreira (2009) revela-se necessário um "..ponto de referência convergente ás instâncias desafiadas a elaborar uma estratégia de resposta" (pág.3). É imperativo que as plataformas tecnológicas implementadas por diferentes organizações sejam interoperáveis em termos de equipamento e programas, algo que, infelizmente, nem sempre ocorre. No âmbito da regulamentação institucional, é também crucial que a teleconsulta receba um reconhecimento formal como uma função equivalente às demais realizadas nas instituições de saúde, com períodos de atendimento estabelecidos e especialistas atribuídos para a sua realização. Além disso, deve existir uma definição clara acerca da responsabilidade clínica dos intervenientes numa consulta á distância.

A inovação tem-se revelado um elemento crucial para aprimorar as ferramentas digitais, com o intuito de fortalecer a articulação entre os serviços de saúde, minimizar a falta de consultas e garantir a conformidade com as listas e os tempos de espera. Este planeamento transformase numa vantagem significativa para o paciente, fomentando um serviço mais acessível e equitativo.

4.5 Desafios à Implementação: Obstáculos na Adoção da Telemedicina

O cibercrime pode ser definido como a utilização de recursos informáticos para a realização de atividades ilegais online, com o intuito de causar danos a organizações ou indivíduos que utilizam a Internet. Este conceito abrange não apenas os crimes especificados na Lei do Cibercrime (Lei nº 109/2009), mas também uma variedade de outras infrações contempladas no Código Penal. Nos últimos anos, verificou-se um aumento exponencial do cibercrime, intensificado pelas medidas adotadas no combate à pandemia Covid-19. Com a obrigatoriedade do teletrabalho e o ensino à distância, muitas pessoas passaram a depender mais da tecnologia, proporcionando novas oportunidades para cibercriminosos explorarem as fragilidades do sistema.

Neste contexto pandémico, os cibercriminosos aproveitaram-se da crescente dependência da tecnologia para o trabalho remoto e para a realização de atividades quotidianas, bem como do caos e preocupação generalizada provocados pelo novo vírus. A cibersegurança, particularmente para a proteção e confidencialidade de dados médicos, emergiu como a ferramenta mais viável para responder às necessidades contemporâneas. A delicada importância dos dados médicos exige uma abordagem que vá além da simples previsão de ciberataques, impondo a necessidade de ações concretas e imediatas. A implementação de barreiras eficazes contra cibercriminosos tornou-se uma prioridade na estruturação da transição tecnológica em curso.

Com a emergência da crise provocada pelo Covid-19, todo o processo de modernização tecnológica e a respetiva adaptação tiveram de ser acelerados para atender às novas e emergentes necessidades. A cibersegurança passou a ser considerada uma prioridade absoluta. Durante este período, os cibercriminosos identificaram lacunas significativas na infraestrutura digital das entidades de saúde, que se encontravam especialmente vulneráveis devido às circunstâncias. Unidades hospitalares, além de organizações e instituições associadas ao setor da saúde tornaram-se alvos frequentes, incluindo a Organização Mundial da Saúde (OMS).

Uma das tentativas mais expressivas foi o ciberataque contra a OMS, dirigido por um grupo de *hackers* identificado como *DarkHotel47*. Este grupo criou uma página fraudulenta que simulava a plataforma de correio eletrónico interno da OMS, numa tentativa de enganar os

utilizadores e roubar informações confidenciais. Este incidente levou a OMS a emitir um alerta público, avisando que os *hackers* estavam a personificar a agência para roubar dinheiro e dados sensíveis.

Desde o início da crise de saúde pública provocada pelo Covid-19, a Organização Mundial de Saúde (OMS) registou uma subida acentuada no volume de ciberataques dirigidos aos seus colaboradores. Os métodos utilizados pelos criminosos incluíram a aquisição de vários *e-mails* e senhas ativas da OMS, com o objetivo de divulgar as informações *online*. Além disso, milhares de *e-mails* que pertenciam a pessoas envolvidas na resposta ao coronavírus foram comprometidos, e ataques de *phishing* foram lançados contra o público em geral, com criminosos a personificarem a OMS para solicitar doações a um fundo fictício.

Para reforçar a segurança, a OMS tem aprimorado os seus sistemas de autenticação. Paralelamente, no setor da saúde, têm sido adotadas várias inovações, como equipamentos de inteligência artificial, dispositivos com sensores, tratamentos digitais e consultas remotas. Contudo, estas novas tecnologias também introduzem riscos, uma vez que podem colocar em risco a integridade e confidencialidade dos pacientes. As informações clínicas, em particular, são particularmente expostas a ciberataques, existindo o risco de os indivíduos serem identificados mesmo com dados anónimos.

Jürgen Stock, Secretário-Geral da *INTERPOL*, salientou a gravidade da situação, afirmando: "O bloqueio de sistemas críticos dos hospitais não apenas atrasa a rápida resposta médica necessária durante estes tempos sem precedentes, como também pode levar diretamente a mortes". Este comentário sublinha a importância vital dos sistemas de saúde, que são considerados parte da infraestrutura crítica de um país. Quando os sistemas estão comprometidos, todos os outros setores também sofrem as consequências.

Além dos ciberataques, surgiram preocupações adicionais relacionadas com a utilização de dados dos cidadãos para exploração comercial. Foi noticiado pelo jornal Expresso que "os principais endereços do Sistema Nacional de Saúde (SNS) têm disponibilizado dados dos cidadãos para exploração comercial da *Google* e de outras marcas ligadas à publicidade". Segundo a notícia, além de registos de fluxo de utilizadores recolhidos através da ferramenta de monitorização da Google, nas páginas SNS24.pt e SNS.gov.pt "recolhem dados para campanhas publicitárias através do serviço *Doubleclick*[12]".

Através de métodos para análise de fluxo de dados, verificou-se que a captação de informações, "também contempla áreas que o SNS.gov.pt disponibiliza para pacientes, como o agendamento de vacinas contra o Covid-19 e a solicitação de medicamentos para o HIV". Em resposta, os Serviços Partilhados do Ministério da Saúde (SPMS) asseguraram que as informações são utilizadas exclusivamente para análises estatísticas e permanecem desidentificadas, assegurando que "não há partilha de dados pessoais com o *Google* ou com qualquer outra entidade externa". Contudo, após a divulgação da notícia, os SPMS decidiram suspender a utilização da ferramenta *Google Analytics*.

O jornal Expresso apontou ainda que "o anonimato dos dados impede que o nome do internauta seja revelado, mas não que as empresas de publicidade criem perfis do utilizador com base em localizações, temáticas preferidas, sites visitados, compras efetuadas ou endereços IP armazenados pelo histórico de navegação na internet". Além dos sites do SNS, outros portais governamentais, como o Parlamento Nacional, Guarda Nacional Republicana, Polícia de Segurança Pública, bem como portais de apoio ao cidadão e autenticação online, observa-se igualmente a utilização comercial dos vestígios digitais dos cidadãos.

Este cenário sublinha a necessidade urgente de reforçar as medidas de cibersegurança e a salvaguarda de informações pessoais, especialmente no setor da saúde, que é crucial para a segurança e o desenvolvimento sustentável dos setores intervenientes.

---

[12] DoubleClick é uma empresa de marketing digital focada em média eletrónica e atualmente integra o Google Inc. Fundada em 1998 e sediada em Nova Iorque, a DoubleClick foi comprada em julho de 2005 pelo grupo de private equity Hellman & Friedman. Em abril de 2007, a Google adquiriu a DoubleClick, incorporando-a às suas soluções publicitárias.

O ex-Secretário Regional da Saúde dos Açores, Clélio Meneses, admitiu, a 28 de junho de 2021, que houve um atraso significativo na comunicação dos resultados dos testes negativos de
Covid-19 na região. Este revés ocorreu devido a um ciberataque que afetou os sistemas do Hospital Divino Espírito Santo (HDES) em Ponta Delgada, comprometendo a capacidade de processamento e divulgação da informação crucial para a saúde pública. Meneses sublinhou a

gravidade da situação, afirmando: "A nossa preocupação foi notificar os casos positivos. Está a haver um trabalho de recuperação de todos aqueles negativos que não foram notificados, por impossibilidade. Não foi por incompetência, não foi por má vontade, foi por impossibilidade de proceder a esta notificação". Este reconhecimento ilustra as complexidades e desafios impostos pelos ciberataques ao sistema de saúde, especialmente em momentos de pandemia.

Clélio Meneses caracterizou o ataque como um "problema grave", que demandou uma "resposta imediata", a todas as horas, para "evitar que tivesse ainda mais danos" para outras estruturas do Serviço Regional de Saúde ou para o "próprio Governo Regional". O ataque revelou-se uma crise que exigiu esforços consideráveis dos técnicos da região, particularmente do HDES, para garantir a segurança e continuidade das comunicações dos testes ao Covid-19, um elemento essencial durante a pandemia.

A tentativa de inserção no sistema digital do Hospital de Ponta Delgada foi detetada a 24 de junho de 2021, informado pelo Governo dos Açores, que prontamente acionou um plano de contingência. O Presidente do Governo dos Açores, José Manuel Bolieiro, demonstrou elevada apreensão perante o ataque informático, classificado como "grave," e reforçou a importância de a área "preparar-se devidamente para estes ataques informáticos que são obviamente mal-intencionados. A sua preocupação reflete a crescente ameaça que o cibercrime representa para a infraestrutura crítica, especialmente no setor da saúde.

Os resultados apresentados pelo Relatório Riscos e Conflitos de 2021, elaborado pelo Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNC), estão alinhados com tendências observadas anteriormente. Segundo o relatório, “A principal diferença em relação ao passado diz respeito ao aumento verificado do número de atividades ilícitas online e alguns modos de atuação, os quais tornaram-se particularmente oportunistas”. Este aumento de atividades ilícitas evidencia a correlação entre o crescimento do cibercrime e os períodos de isolamento social decorrentes da crise sanitária, como destacado no relatório:
"O volume de incidentes de cibersegurança e os indicadores de cibercrime cresceram de forma significativa, mostrando com frequência uma coincidência temporal entre esse crescimento e os períodos de confinamento social fruto da pandemia Covid-19".

O risco de uma organização enfrentar uma violação de segurança intensificou consideravelmente, com uma elevação de 94% em 2020, percentual que se reduziu para 86% em 2021, como relatado pelo CNC. Os ciberataques mais notáveis nesta conjuntura incluíram *phishing/smishing*, sistemas infetados por *malware* e *ransomware,* sendo a primeira a mais prevalente. As estratégias de manipulação desempenharam um papel tão determinante quanto as ferramentas digitais nas mãos dos cibercriminosos.

As previsões do Observatório de Cibersegurança do CNC sugere que "A persistência da pandemia e dos seus efeitos permitem antever a continuidade no futuro próximo de muitas dos ciberataques identificados em 2020". Esta análise alerta para a continuidade dos ciberataques oportunistas, com o aumento da dependência do trabalho á distância e o protagonismo crescente do ambiente online, as fragilidades que surgiram tornam-se cada vez mais evidentes. Setores vitais, como a área financeira e a saúde, estão agora mais expostos a riscos, devido a esta transformação digital acelerada.

As instituições que pretendem manter-se em operação em futuros momentos de crise deverão investir significativamente em programas de cibersegurança, revela-se ser a estratégia mais viável para assegurar aos cidadãos, que recorrem diariamente a serviços sociais e privados, a segurança e a credibilidade necessárias para fomentar uma interação dinâmica protegida de danos desnecessários e destrutivos. A crescente pressão sobre os sistemas de saúde é particularmente alarmante, ao ponto de ponderar-se, "Políticas Públicas, Economia e Sociedade" (2015) "a hipótese da sua rutura enquanto garantes sociais com capacidade universal, geral e tendencial gratuitidade (nos casos tipo SNS)". (Paulo Neto, Maria Manuel Serrano)

Durante a primeira vaga da emergência sanitária Covid 19, a área clínica tornou-se um alvo privilegiado para os cibercriminosos, uma vez que os hospitais, altamente dependentes da tecnologia digital, foram frequentemente alvo de chantagem através de ataques de ransomware. Estes ataques forçavam as instituições a pagar resgates após terem os seus sistemas informáticos comprometidos.

Em Portugal, em resposta a estes ciberataques existe o Gabinete de Coordenação das atividades do Ministério Público na área da Cibercriminalidade (Gabinete Cibercrime), instituído a 7 de dezembro de 2011. Este órgão tem como missão garantir a articulação interna do Ministério Público na investigação de crimes digitais, promover a formação especializada na área e criar

canais de comunicação eficazes com os fornecedores de serviços de acesso às redes de telecomunicações. Dessa forma, facilita a colaboração necessária para a apuração de infrações no ambiente digital.

Apesar da crescente prevalência do cibercrime, há um claro desconhecimento da população em geral, e até mesmo entre alguns profissionais da área jurídica, relativamente às suas implicações. Portanto, é crucial que tanto o Governo como os estabelecimentos de educação e os veículos de comunicação intensifiquem esforços para formar e consciencializar os cidadãos sobre esta temática. A maioria dos golpes e fraudes perpetrados por cibercriminosos explora o fator humano, manipulando sentimentos, vulnerabilidades e crenças, especialmente no contexto pandémico, que exacerbou a ansiedade e a preocupação generalizada.

Este cenário destaca a necessidade urgente de promover e melhorar a sensibilização para a cibersegurança dentro das organizações, desenvolvendo uma estratégia eficaz que incorpore a segurança na cultura organizacional. Mostra-se vital para garantir que cada colaborador compreenda a importância da cibersegurança e o impacto desestruturador que uma violação de dados pode ter. A implementação e a atualização contínua de instrumentos de defesa devem ser solidificadas, dada a necessidade contínua de manter o cumprimento das medidas de segurança.

As constantes mudanças e evoluções no panorama da segurança cibernética demonstram a necessidade de manter os colaboradores preparados para responder adequadamente às ameaças mais recentes. Para garantir um controlo consistente, são necessárias avaliações regulares para identificar possíveis vulnerabilidades no sistema e coordenar as respostas apropriadas.

Em suma, é essencial desenvolver programas de sensibilização para a segurança, capacitando os colaboradores para identificar e responder adequadamente à crescente diversidade de ameaças à cibersegurança. Em todos os setores organizacionais, os colaboradores devem receber formação contínua, que seja cativante e informativa, fornecendo-lhes a compreensão necessária sobre o que é esperado deles e a importância da sua intervenção na proteção dos dados organizacionais. Ao promover uma cultura de segurança, as organizações podem garantir uma maior conformidade e proteção contra ciberataques.

Conclusão

A evolução da tecnologia tem sido um fator determinante na transformação das sociedades ao longo da história, moldando técnicas, lógicas e, consequentemente, a realidade em que

vivemos. Esta evolução tem proporcionado maior conforto e conveniência, principalmente ao responder às necessidades e estímulos externos que o ser humano enfrenta. Neste contexto, a telemedicina emergiu como uma alternativa tecnológica inovadora, oferecendo um fluxo de informações mais dinâmico, com a capacidade de impactar diretamente a resposta às necessidades imediatas. A importância da mobilidade física foi reduzida, assim como os problemas relacionados à sua exigência.

Ao longo da emergência de saúde pública global, a telemedicina e as plataformas digitais associadas desempenharam um papel crucial na gestão informacional e de diagnóstico, contribuindo para descongestionar os serviços de saúde e, assim, contribuindo a conter a propagação do vírus. Este período revelou a telemedicina como uma solução viável e necessária no quotidiano, destacando resultados favoráveis, como a economia de recursos financeiros, maior disponibilidade e qualidade no atendimento, e a melhoria na disponibilidade de assistência médica. Contudo, a crescente adoção da telemedicina trouxe à tona a necessidade de atenção redobrada à cibersegurança.

A cibersegurança visa proteger as informações processadas, armazenadas e transmitidas nos sistemas interligados das organizações sociais. A segurança no espaço digital é fundamental para garantir que a comunicação ocorra de forma segura e eficiente. No entanto, os ciberataques têm-se expandido exponencialmente, comprometendo a credibilidade e a estabilidade das plataformas digitais. Diversas instituições, em específico no setor de saúde, já foram alvo de ciberataques, resultando na exposição de dados sensíveis a interesses externos.

Em resposta a estes ataques, houve um aumento no investimento em formação e desenvolvimento de sistemas de proteção, com a finalidade de garantir a confidencialidade da informação. A telemedicina, sendo um serviço que gere informações extremamente pessoais e sensíveis, depende de um sistema sólido de cibersegurança para operar de forma legítima e confiável. Um sistema desprotegido para além de gerar desconfiança, também compromete a eficácia do serviço, especialmente num cenário pós-pandémico, onde a telemedicina tornou-se ainda mais relevante.

As entrevistas realizadas no setor hospitalar revelaram um desconhecimento generalizado sobre os mecanismos necessários para combater os ciberataques. As respostas indicaram que as medidas de segurança implementadas pelas instituições de saúde são insuficientes diante da diversidade de ciberataques existentes. O foco tem sido na proteção básica, como a utilização

de senhas, enquanto os processos de defesa mais avançados são frequentemente negligenciados.

Foi identificada uma necessidade urgente de investir em formação digital voltada para a defesa contra ciberataques. A maioria dos profissionais entrevistados possuía apenas um conhecimento básico sobre cibersegurança, limitado ao uso de senhas e programas diários. Além disso, não existe, até ao momento, uma formação interna específica nas instituições de saúde voltada para a prevenção de ciberataques, o que aumenta o seu risco. É, portanto, essencial que a comunidade médica seja capacitada para interagir com segurança no palco digital.

A emergência de saúde pública global acelerou a demanda por desenvolver ferramentas e projetos que promovam a telemedicina e a monitorização remota. Contudo, é necessário desconsiderar as despesas iniciais da inovação tecnológica, valorizando os benefícios proporcionados nos processos de diagnóstico e tratamento. É fundamental assegurar que todos os indivíduos possam usufruir de assistência médica essencial adequada, independentemente de suas condições socioeconómicas, e que os especialistas em saúde consigam comunicar e consultar dados clínicos com segurança, respeitando a privacidade e a autoridade individual sobre os dados pessoais.

Desde o início da pandemia, empresas do setor de saúde, especialmente aquelas envolvidas em pesquisa e desenvolvimento de medicamentos, hospitais e laboratórios, tornaram-se alvos frequentes de cibercriminosos. A exploração de vulnerabilidades humanas e tecnológicas tem sido a principal causa destes ataques. Muitos profissionais de saúde desconhecem medidas básicas de cibersegurança, o que os torna, junto com as infraestruturas em que trabalham, vulneráveis a ciberataques. Além disso, a proliferação da Internet das Coisas (IoT) conectando equipamentos médicos e outros componentes críticos expõe ainda mais o setor de saúde a riscos.

As organizações de saúde enfrentam potenciais perdas quando expostas a ciberataques, desde a saúde dos pacientes até á reputação e o valor de mercado das instituições. O Regulamento Geral de Proteção de Dados (RGPD), em aplicação desde agosto de 2021, impõe penalizações significativas para o descumprimento dos parâmetros de proteção informacional, o que reforça a necessidade de capacitar os profissionais do setor em cibersegurança.

Em resposta a essas necessidades, torna-se imperativo desenvolver uma infraestrutura de comunicação segura e confiável, especialmente no âmbito do Sistema Público de Saúde. A cibersegurança na telemedicina, embora emergente e com grande potencial, ainda enfrenta desafios críticos devido à insuficiência das medidas de proteção atuais. Políticas governamentais específicas são essenciais para fortalecer a segurança dos dados sensíveis dos pacientes e garantir a integridade das plataformas de telemedicina. Estas políticas devem incluir a padronização de protocolos de criptografia, auditorias regulares de segurança e diretrizes para o armazenamento seguro de dados em *cloud*.

A crise de saúde global por COVID-19 evidenciou a importância da assistência médica online, ao mesmo tempo que expôs vulnerabilidades significativas nos sistemas de cibersegurança. O aumento súbito e massivo do uso destas tecnologias destacou falhas de segurança que, se não forem abordadas, podem representar um risco real em futuras crises globais. Investir na formação contínua de profissionais de saúde e técnicos em cibersegurança, bem como incentivar o desenvolvimento de tecnologias avançadas de proteção, como a inteligência artificial para deteção de inserções externas ao sistema, é crucial para preparar um ambiente seguro para o avanço da telemedicina. Somente através de um esforço coordenado e estratégico será possível garantir a segurança e a confiabilidade da telemedicina em cenários futuros.

A ascensão da telemedicina, embora promissora, está intrinsecamente ligada à necessidade imperativa de proteger dados sensíveis. A insuficiência das medidas atuais de cibersegurança não só compromete a confiança do público, como também coloca em risco a própria sustentabilidade deste novo modelo de atendimento. Ignorar a importância da cibersegurança num mundo cada vez mais digitalizado é preparar o terreno para futuras crises, com consequências potencialmente catastróficas.

O futuro da telemedicina não depende apenas da inovação tecnológica, mas da capacidade de implementar políticas eficazes de proteção de dados, de investir na formação contínua dos especialistas e de desenvolver instrumentos tecnológicos de ciberdefesa. Somente através de uma ação coordenada e consciente podemos garantir que a telemedicina alcance o seu verdadeiro potencial, proporcionando um futuro em que saúde, segurança e confiança estejam plenamente assegurados. A pandemia COVID-19 foi um alerta; teremos de agir com determinação para evitar que vulnerabilidades semelhantes comprometam a transformação e desenvolvimento das infraestruturas de informação digital

O preenchimento da margem de tempo com preparação e precaução revela-se necessário, estará o Sistema Nacional de Saúde funcional para o conceber?

Bibliografia/Referências

Amgen Foundation. (2020). Amgen em Portugal e Fundação Amgen apoiam ativamente o combate à COVID-19. Entrevista com Tiago Amieiro. *Health News,* 7 de maio de 2020. Obtido de Health News.

Centro Nacional de Cibersegurança. (2021). Relatório Riscos & Conflitos 2021: Indicadores e Análise de Cibersegurança. Observatório de Cibersegurança. Recolha e análise de dados de cibersegurança com base em contributos de parceiros e dados de inquéritos à comunidade. Obtido de: https://www.cncs.gov.pt

Centro Nacional de Cibersegurança (Portugal). (2020). Alerta COVID-19 e as ciberameaças. Obtido de: https://www.cncs.gov.pt/recursos/noticias/alerta-covid-19-e-as-ciberameacas/. Acesso a 9 maio 2023.

CNCS. (2023). Boletim 03/2020. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.

COVID-19: Cibercrime em Tempo de Pandemia. (2020). Gabinete Cibercrime Ministério Público, 17 de abril. Obtido de: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/cibercrime_em_tempo_de_pandemia-20-04-2020.pdf. Acesso a 11 maio 2023.

Craig, J., & Petterson, V. (2021). *Introduction to the practice of telemedicine. Journal of Telemedicine and Telecare,* 3–9, maio.

Damião, R. (2021, 11 de fevereiro). A crescente importância da cibersegurança para as organizações. IT Channel. Obtido de: https://www.itchannel.pt

EC - European Commission. (2023). *Special Eurobarometer 499: Europeans' Attitudes Towards Cyber Security.* Brussels: European Commission.

ENISA - European Union Agency for Cybersecurity. (2023). *Good practices for the security of Healthcare services.*

EUROPOL. (2020). *Catching the virus – cybercrime, disinformation and the COVID-19 pandemic.* 3 abril. Obtido de: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrimedisinformation-and-covid-19-pandemic. Acesso a 11 maio 2023.

Eurostat. (2023). *Security incidents and consequences.*

Expresso. (2020, 13 de julho). Incidentes de cibersegurança aumentam 101%: setor bancário entre os mais expostos. Expresso. Obtido de: https://expresso.pt/economia/2020-07-13-Incidentes-de-ciberseguranca-aumentam-101.-Sector-bancario-entre-os-mais-expostos.

Gouveia, J. B. (2018). Direito da segurança: cidadania, soberania e cosmopolitismo. Lisboa: Almedina. ISBN 9789724074924.

Hamada, H. H., & Moreira, R. P. (2019). Teoria e práticas de Inteligência de Segurança Pública - Série inteligência, estratégia e defesa social. Editora D'Plácido, 6-24. ISBN: 9786580444007.

Horton, R. (2020). *COVID-19 is not a pandemic. The Lancet,* 396(10255), 874. https://doi.org/10.1016/S0140-6736(20)32000-6

Johnson & Johnson. (2020). Minha Saúde Não Pode Esperar. Lançada a 9 de dezembro de 2020, esta campanha ressalta a urgência de manter a continuidade nos cuidados de saúde durante a pandemia de COVID-19. O Dr. Gustavo Scapini alerta sobre os riscos associados a atrasos no tratamento e a importância da telemedicina como alternativa.

Lopes, R. L. (2020). A importância da formação na telemedicina. Academia Virtual Healthcare, Universidade de Coimbra.

Miguel, A. (2019). Gestão moderna de projetos. Lisboa: FCA - Editora de Informática. ISBN 9789727228881.

Ministério da Saúde. (2006). Portaria n.º 567/2006, que aprova as tabelas de preços a praticar pelo Serviço Nacional de Saúde, e aprova o respetivo regulamento. Diário da República, 2.ª série, n.º 112.

Ministério da Saúde. (2013). Despacho n.º 3571/2013: Colaboração entre os serviços de saúde e o Instituto Português do Sangue e da Transplantação. Diário da República, 2.ª série, n.º 46, 6 de março de 2013. Obtido de: https://diariodarepublica.pt/dr/detalhe/despacho/3571-2013-1759945

Moreira, A. A língua e o Conceito Estratégico Português. Editora Academia das ciências de Lisboa, 6-24. ISBN 9789726231868.

Moreira, A. (2009). Terrorismo e Liberdade (A sociedade insegura). Comunicação apresentada no XXIII Encontro de Filosofia. Edição APF - Associação de professores de filosofia, 3 - 9.

Neto, P., & Serrano, M. M. (2015). Políticas públicas, economia e sociedade. Alcochete: Nexo Literário. ISBN 9789898529527.

Observador. (2021, junho 28). Ciberataque a hospital de Ponta Delgada atrasa divulgação dos resultados de testes Covid-19. Agência Lusa. Obtido de: https://observador.pt/2021/06/28/ciberataque-a-hospital-de-ponta-delgada-atrasa-divulgacao-dos-resultados-de-testes/

Portugal. (2009). Lei n.º 109/2009 de 15 de setembro - Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Diário da República, 1.ª série, n.º 179, 6319.

Presidência do Conselho de Ministros. (2015). Resolução do Conselho de Ministros n.º 36/2015, de 12 de Junho. Diário da República, n.º 113/2015, Série I. Obtido de: Diário da República.

RASI - Relatório Anual de Segurança Interna. (2019). *Relatório Anual de Segurança Interna 2019.* Sistema de Segurança Interna, 2023.

Rocha-Cunha, S., Vasques, R. F., & Martins, M. A. B. (2020). Os direitos humanos por um fio: perspetivas transdisciplinares em torno dos direitos humanos em tempos difíceis. Barcelos: Edições Humus. ISBN 9789897554186.

União Europeia. (2016). 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 - RGPD). Jornal Oficial da União Europeia, L 119, 1–88.

Walker, J., & Whetton, S. (2021). *The diffusion of innovation: factors influencing the uptake of telehealth. Journal of Telemedicine and Telecare,* v. 6.

WHO Group Consultation on Health Telematics (1997: Geneva, Switzerland). (1998). *A health telematics policy in support of WHO's Health-for-all strategy for global health development: report of the WHO Group Consultation on Health Telematics, 11-16 December, Geneva, 1997.* Geneva: World Health Organization.

World Health Organization. *Telemedicine in Member States - Opportunities and developments: report on the second global survey on eHealth.* Global Observatory for eHealth series, Volume 2. Geneva: World Health Organization.

ABREVIATURAS/ACRÓNIMOS

AEMI – Advanced Environment for Medical Image Interpretation

ADAM – Advanced Architecture in Medicine

AIM – Autorização de Introdução no Mercado

ACES – Agrupamentos de Centros de Saúde

ARS – Administrações Regionais de Saúde

ATA – Advanced Technology Attachment

CDOM – Código Deontológico da Ordem dos Médicos

CHUC – Centro Hospitalar e Universitário de Coimbra

CIEDT – Comissão de Acompanhamento da Iniciativa Estratégica para o Desenvolvimento da Telemedicina

CISO – Chief Information Security Officer

CNCS – Centro Nacional de Cibersegurança

CNPD – Comissão Nacional de Proteção de Dados

CNTS – Centro Nacional de TeleSaúde

DPOC – Doença Pulmonar Obstrutiva Crónica

DNS – Domain Name System

EDR – Endpoint Detection and Response

EHR – Electronic Health Records

EMR – Electronic Medical Records

ENISA – European Union Agency for Cybersecurity

EPIC – European Prototype for Integrated Care

ERS – Entidade Reguladora da Saúde

FEST – Framework of European Services in Telemedicine

GTT – Grupo de Teatro Terapêutico

HDES – Hospital Divino Espírito Santo

HTTPS – Hypertext Transfer Protocol Secure

IA – Inteligência Artificial

IMF – International Monetary Fund

IoT – Internet of Things

IPO – Instituto Português de Oncologia

IPOC – Instituto Português de Osteopatia Clássica

ISDN – Integrated Services Digital Network

KISS – Knowledge-Based Interactive Signal Monitoring System

NASA – Administração Nacional da Aeronáutica e Espaço (National Aeronautics and Space Administration)

NHS – National Health Service (Sistema Público de Saúde Britânico)

OCS – Observatório de Cibersegurança

OMS – Organização Mundial de Saúde

PDS – Plataforma de Dados de Saúde

PEG – Percutaneous Endoscopic Gastrostomy

RGPD – Regulamento Geral de Proteção de Dados Pessoais

SHCC – Safeguarding Health in Conflict Coalition

SIRP – Sistema de Informações da República Portuguesa

SMISHING – Semelhante ao phishing, exceto na forma de uma mensagem de texto. Contendo normalmente um link fraudulento.

SNS – Serviço Nacional de Saúde

SPMS – Serviços Partilhados do Ministério da Saúde

TIC – Tecnologias da Informação e Comunicação

TI – Tecnologias de Informação

ANEXOS

Entrevista

Para a condução da entrevista, foi adotado o método de entrevistas aprofundadas, considerado uma abordagem qualitativa que permite examinar um ou mais tópicos com maior detalhe do que as entrevistas comuns presenciais. Estas últimas focam-se predominantemente em obter dados quantificáveis, sendo que as perguntas são estruturadas para este propósito, utilizando um leque de perguntas fechadas, abertas ou semiabertas, facilitando uma posterior classificação e análise dos dados recolhidos. A técnica qualitativa empregada nas entrevistas em profundidade permite flexibilidade na utilização do guião, que não é fixo. Este método permite que o guião se ajuste ao contexto e ao desenvolvimento do diálogo, sendo adaptado em função das perceções e interpretações que emergem ao longo da conversa. Tal abordagem busca "compreender" e "explicar" em profundidade as realidades ou fenómenos analisados, promovendo uma exploração crítica e ajustada às especificidades da situação em estudo. A abordagem exploratória deste tipo de entrevistas revelou-se adequada para este estudo, especialmente útil em investigações sobre tópicos sensíveis ou em áreas com pouca informação

prévia. Para esta entrevista específica, aplicou-se um modelo semiaberto, com perguntas iniciais preparadas previamente, que se ajustam conforme o progresso da conversa.

Será apresentada uma entrevista a figuras de influência:

➢ Bruna Guerreiro: Auxiliar de Saúde, Hospital do Espírito Santo

➢ Emanuel Gouveia: Médico Oncologista, IPO Lisboa

➢ Mafalda Mendes: Auxiliar de Saúde, Hospital do Espírito Santo

➢ Marco Santos: Auxiliar de Saúde, Hospital Espírito Santo

➢ Álvaro Filipe: Radiologista, CUF

As questões apresentadas serão enquadradas às modificações geradas no setor da saúde pela introdução da telemedicina, as perspetivas futuras em relação à cibersegurança existente e os desafios atuais e para averiguar a sua situação relativamente à inserção da telemedicina na sua realidade quotidiana e integrar a importância da segurança e proteção de dados médicos necessária nessas unidades. Por último, tentar compreender como a adaptação está a acontecer nesses locais, na atual situação de pandemia Covid-19, onde se revela de extrema importância a sua inserção neste contexto.

Contexto da Entrevista

As entrevistas realizadas visam responder ao problema central deste estudo: De que forma as entidades de saúde estão a implementar medidas de cibersegurança no seu dia a dia? A relevância das entrevistas decorre da posição dos entrevistados, que têm uma influência direta e envolvente na área médica.

Estabelecimento dos Objetivos da Entrevista

Responder diretamente às questões formuladas.

1. Quais as práticas adotadas pela instituição para assegurar a privacidade e a proteção das informações dos pacientes?
2. Quais são os recursos que a instituição utiliza para garantir a proteção das informações fornecidas pelos pacientes?
3. Quais as atividades de prevenção aos ciberataques que têm vindo sendo desenvolvidas?
4. Que formações são disponibilizadas na instituição para a comunidade médica?

Entrevistados

Colaboradores (Auxiliares de Saúde (H. Espírito Santo)), (radiologista (CUF)) e oncologista)

Entrevistador

Maria Duarte - Mestrado de Políticas Públicas e Projetos

Prazos estabelecidos

O período de conclusão foi definido até o dia 3 de março.

Infraestruturas operacionais

Impressões do guião.

Possíveis entrevistas pelo Zoom.

Sessão de perguntas

Questão de pesquisa: "Que tipo de respostas é que as instituições medicas têm desenvolvido para a inserção da cibersegurança no quotidiano?"

Objetivo: Abordar as quatro questões de pesquisa:

1. Quais as estratégias implementadas pela instituição para assegurar a confidencialidade dos dados fornecidos?
2. Que meios é que dispõem para apoio à cibersegurança?
3. Quais as atividades de prevenção aos ciberataques que a instituição tem ao seu dispor?
4. O que é a instituição dispõe para formação na comunidade medica a nível de cibersegurança?

Dimensão:
abrangência local: (3 estabelecimentos de Saúde).

Entrevistados

- Diferentes áreas da Saúde

- Várias entidades

- Um grupo de 5 indivíduos entrevistados por um único responsável

- Modo de interação – verbal (registada, com autorização)

Ambiente

– Possíveis entrevistas pelo Zoom.

Duração da entrevista 30 a 45 minutos

• **Processo de decisão**

Fatores a serem analisados:

− Métodos de cibersegurança

− Formação à comunidade medica − Adaptações em tempo de pandemia COVID-19

Explicação dos componentes:

− Criação de perguntas organizadas em categorias e subdivisões

− Agendamento da conversa

− Determinação do local e duração da interação com o entrevistado
− Apresentar de forma breve o objetivo da entrevista em questão em questão

− Levar em conta as previsões do entrevistador

− Sintetizar a conversa no momento adequado

• **Processo de elaboração**

Apesar de realizar-se exclusivamente uma análise do conteúdo das palavras transcritas do entrevistado, é necessário considerar os seguintes aspetos:

− Condição emocional do entrevistado (autoconfiança, perplexidade, apreensão...).

− Incongruências nas falas do entrevistado.

− Instantes de manifestação emocional por parte do entrevistado.

− Gestos e posturas do corpo do entrevistado.

− Entonação e cadência na fala do entrevistado.

− Estilo de linguagem empregado.

Elementos formais a considerar na apresentação:

− Criar uma atmosfera acolhedora, demonstrando empatia e atenção em relação ao entrevistado;

− Manter uma postura profissional, incentivando o entrevistado a responder com clareza às questões e esclarecendo quaisquer dúvidas que possam surgir durante o processo **Apresentação do projeto:**

− Indicar a extensão e o propósito da entrevista.

Autorização:

− Pedir a permissão do entrevistado

Desenvolvimento da conversa:

− Auxiliar o entrevistado a comunicar-se de forma clara

− Dirigir a atenção do entrevistado para os tópicos essenciais.

− Incentivar o entrevistado a aprofundar os pontos mais relevantes.

Finalização da conversa:

− Respeitar o tempo estipulado para a conversa

− Resumir os principais pontos abordados.

− Expressar agradecimento de forma sincera no encerramento **Registar observações:**

− Registar as atitudes físicas e sentimentos do entrevistado.

− Caso a gravação não seja autorizada, proceder à transcrição imediata da conversa

• **Processo de realização**

Questão de pesquisa: "Que tipo de respostas é que as instituições medicas têm desenvolvido para a inserção da cibersegurança no quotidiano?"

Interrogações de estudo:

1. Que ações a organização adota para assegurar a proteção dos dados entregues?

2. Quais as atividades de prevenção a ciberataques que a instituição tem ao seu dispor?

3. O que é a instituição dispõe para formação na comunidade medica a nível de cibersegurança?

4. Dentro do contexto da pandemia Covid- 19, como foi monitorizada a segurança dos dados dos utentes?

Temas a considerar:

1. Quais estratégias a organização implementa para assegurar a proteção dos dados fornecidos?

1.1- Estratégias de proteção

1.2- Registo e divulgação de incidentes de cibersegurança

1. 3-Relação entre ciberataques e credibilidade do sistema de saúde

2. Quais as atividades de prevenção a ciberataques que a instituição tem ao seu dispor?

2.1- Identificação.

2.2- Apoios.

3. O que é a instituição dispõe para formação na comunidade medica a nível de cibersegurança?

3.1- Plataformas de aprendizagem

3.2- Projetos

4. Dentro do contexto da pandemia Covid- 19, como foi monitorizada a segurança dos dados dos pacientes?

4.1- Sistemas de proteção

4.2- Infraestruturas

Guião da entrevista

A) Estratégias de Proteção

1- Quais abordagens a organização adota para assegurar a confidencialidade e integridade dos dados que recebe?

1.1 – Quais desafios específicos você identifica atualmente no campo da segurança digital?

–

1.2 Quais ferramentas ou práticas de defesa contra ameaças externas a sua organização possui?

–

1.3 Na sua opinião, há uma lacuna de recursos ou conhecimento que justifique mais investimento nesta área?

B) Documentação e Divulgação de ciberataques

1.5 – Existe um registo sistemático de ocorrências relacionadas a ciberataques dentro da organização?

1.6 – São criados relatórios analíticos sobre a frequência e tipologia dos ciberataques?

1.7 – Esses relatórios são partilhados com os pacientes de forma transparente?

1.8 – Quando questionados sobre a proteção dos dados, a organização consegue comunicar claramente as medidas adotadas, utilizando uma linguagem acessível e compreensível para todos os pacientes?

C) Relação entre ciberataques e credibilidade do serviço nacional de saúde

1.8 – De acordo com a sua perspetiva, quais os fatores que contribuem para a origem dos ciberataques?

1.9 – Na sua opinião, acredita que os ciberataques podem comprometer a confiança pública e a legitimidade do Sistema Nacional de Saúde?

1.10 – Considera essencial promover uma sensibilização na comunidade médica sobre os riscos dos ciberataques e as suas repercussões, para que haja uma compreensão coletiva do problema?

2- Quais as atividades de prevenção a ciberataques que a instituição tem ao seu dispor?

A) Identificação

–

2.1 – Antivírus, anti-malwares e anti-ransomwares são programas de instalação obrigatória em qualquer instituição, neste momento estão em funcionamento na instituição?

2.2 Manter os sistemas, softwares e aplicações atualizadas serve para corrigir falhas e brechas de segurança. Neste momento, existe uma rotina de atualização da rede institucional em questão?

2.3 – Têm instalado um software de criptografia (A criptografia codifica os dados de modo que só podem ser traduzidos ou lidos por quem detém a chave, nesse caso, você)?

B) Serviços de apoio

2.4 – Dispõem de uma equipa especializada em tecnologia para oferecer assistência imediata em caso de ciberataque?

2.5 – Para além de técnicos especializados, os profissionais de saúde têm capacidade de criar mecanismos de defesa a ataques externos?

2.6 – Quais outros tipos de assistência poderiam ser implementados para oferecer suporte adicional aos profissionais de saúde

3- Que meios a instituição dispõe para formação na comunidade médica a nível de cibersegurança?

A) Plataformas de aprendizagem

3.1 – Os colaboradores recebem formação específica para reconhecer e lidar com os desafios relacionados à cibersegurança?

3.2 – Que hábitos de segurança para reconhecimento de ameaças em potencial existem nesta instituição?

–

B) Projetos

3.3 – Quais ações considera que poderiam ser implementadas para melhorar a eficácia na deteção de ciberataques?
3.4 Existe a realização de simulações, semelhante em processo, às de incêndio, para discernir as vulnerabilidades do sistema em questão?

3.5 – Que vulnerabilidades do sistema foram percecionadas pela comunidade médica?

4- Dentro do contexto da pandemia Covid- 19, como foi monitorizada a segurança dos dados dos utentes?

A) Sistema de proteção

4.1 – Dispõem de sistemas de proteção de dados? Se sim, quais?

4.2 – Se existir um ciberataque e o sistema for invadido existe um sistema de backup para dar continuidade às operações?

4.3 – Existe uma abordagem baseada em acesso privilegiado, impondo "zonas de acesso"? (Assim, um colaborador terá o acesso restrito a sistemas que não são necessários?

4.4 – Procuram incentivar a comunidade medica à prática de hábitos de segurança para reconhecimento de ameaças?

B) Infraestruturas

4.5 – Considera a infraestrutura vigente a mais indicada para o momento presente?

–

4.6 – Considera que o Estado Português deveria investir na modernização do serviço nacional de Saúde ou optar por investimentos privados?