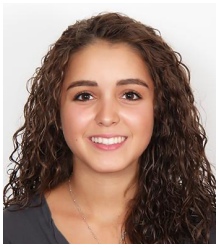
Universidade do Minho
Escola de Engenharia

Direito e Informação

Responsabilidade e proteção de dados em empresas de saúde

2023 / 2024



Bárbara Brito
PG52248

Sara Fontes
PG52740

Índice

Introdução

No âmbito da unidade curricular de Direito e Informação, foi-nos proposto, pelo docente Francisco Andrade, a elaboração de um trabalho de pesquisa sobre a responsabilidade e proteção de dados. Neste contexto, decidimos explorar este tema à volta das empresas na área da saúde.

O direito à informação é fundamental para garantir que todos tenham acesso a informações verídicas, completas e imparciais. É essencial para os direitos humanos, permitindo aos cidadãos lutarem pelos seus direitos. É também essencial para a democracia, uma vez que permite aos cidadãos participarem ativamente na vida pública e tomarem decisões informadas.

Na sociedade atual, o direito à informação torna-se ainda mais relevante, uma vez que vivemos num mundo cada vez mais conectado e dinâmico. Atualmente, as informações são produzidas e disseminadas rapidamente e de forma constante, sendo essencial que os cidadãos tenham acesso às mesmas de maneira a compreenderem o mundo que os rodeia.

A proteção da privacidade e dos dados pessoais é uma preocupação constante em sociedades democráticas, especialmente diante da rápida evolução tecnológica. No contexto das empresas de saúde, onde as informações dos pacientes são manipuladas, essa preocupação intensifica-se.

A adoção de medidas proativas por parte das empresas de saúde torna-se crucial devido à constante evolução tecnológica, que tem um avanço mais rápido do que a legislação pode acompanhar.

Diante deste cenário, a responsabilidade das empresas de saúde vai além do mero cumprimento das normas existentes. Estas empresas devem implementar políticas que passam pela segurança robusta dos dados, investimento em tecnologias de proteção de dados e ainda a promoção da consciencialização entre todos os colaboradores. A manutenção da privacidade dos pacientes não é apenas uma obrigação ética, mas uma medida indispensável para preservar a integridade do setor de saúde e garantir a confidencialidade das informações confiadas a essas organizações.

Palavras-Chave: direito, informação, RGPD, responsabilidade, proteção, privacidade, lei portuguesa

RGPD

A entrada em vigor do novo Regulamento Europeu de Proteção de Dados (RGPD), no dia 25 de maio de 2018, veio marcar um novo paradigma no que respeita à proteção de dados pessoais na Europa e substituir a Diretiva de Proteção de Dados Pessoais estabelecida em 1995. O regulamento estabelece diretrizes para a proteção dos dados pessoais de pessoas físicas na União Europeia e no Espaço Económico Europeu e tem como objetivo a proteção dos direitos fundamentais das pessoas, nomeadamente o direito à privacidade e à proteção dos seus dados pessoais.

O RGPD aplica-se a todas as entidades que lidam com dados pessoais de cidadãos da União Europeia, mesmo que essas entidades estejam sediadas fora da União Europeia. Neste regulamento estão estabelecidas uma série de obrigações que as entidades devem respeitar, tais como obter o consentimento do titular dos dados para tratamento dos seus dados pessoais, informar o titular sobre finalidade do tratamento dos seus dados pessoais, garantir a segurança dos dados pessoais e atender aos pedidos dos titulares dos dados [3].

No artigo 4º do RGPD está definido dados pessoais como sendo “qualquer informação relativa a uma pessoa singular identificada ou identificável”. Uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, por referência a um identificador, como um nome, um número, dados de localização, identificadores por via eletrónica, entre outros elementos que não estavam presentes na Diretiva 95/46/CE, mencionada anteriormente [1].

É também relevante destacar a importância da proteção de dados pessoais no contexto do mercado digital presente na atualidade. A UE reconhece que o desenvolvimento de um mercado digital forte e competitivo requer a proteção dos direitos fundamentais dos cidadãos, incluindo o direito à privacidade.

Aplicado todo este assunto no contexto das empresas de saúde, a proteção de dados revela-se ainda mais importante, uma vez que os dados de saúde são especialmente sensíveis. Por essa razão, as empresas de saúde devem adotar medida adequadas com o objetivo de proteger os dados de saúde dos pacientes, garantindo assim a sua confidencialidade, integridade e disponibilidade [2].

Proteção de Dados em Empresas de Saúde

A Comissão Europeia define os dados pessoais como “informação relativa a uma pessoa viva, identificada ou identificável”. Ou seja, qualquer informação que possa identificar uma pessoa, direta ou indiretamente, é considerada dado pessoal. O RGPD da União Europeia protege dados pessoais, incluindo aqueles descaracterizados, se ainda permitirem identificar alguém. A anonimização deve ser irreversível. A lei é neutra em termos de tecnologia e abrange tratamentos automatizados ou manuais, independentemente do meio de armazenamento. Exemplos de dados pessoais incluem nomes, endereços, e-mails e informações médicas [4].

Os dados sensíveis são um subtipo de dados pessoais que possuem um tratamento mais restrito, de acordo com o RGPD. São considerados dados sensíveis aqueles que incluem dados genéticos, biométricos, relativos à saúde e vida sexual. Empresas de saúde em Portugal devem ter precaução especial ao lidar com dados sensíveis, pois a sua divulgação indevida pode causar danos graves aos pacientes [5].

O Regulamento Geral sobre a Proteção dos Dados (RGPD), Regulamento (UE) 2016/679, estabelece as bases legais que permitem o tratamento de dados pessoais em Portugal. Estas bases legais são hipóteses que autorizam o responsável pelo tratamento a realizar o tratamento dos dados pessoais, desde que observados os princípios e as garantias previstos no RGPD. Estas bases legais incluem o consentimento do titular, cumprimento de obrigações legais, execução de contratos, proteção de interesses vitais, tarefas de interesse público e legítimo interesse do responsável pelo tratamento [9].

Empresas de saúde em Portugal recolhem dados pessoais em quatro categorias principais: identificação, saúde, financeiros e contato. Além disso, podem incluir informações sobre estilo de vida, participação em pesquisas médicas e uso de serviços de saúde online. A proteção destes dados é vital, seguindo as regras do RGPD. Medidas como senhas fortes, criptografia, firewalls, backup regular de dados e políticas de segurança são essenciais. Os pacientes têm direitos, incluindo acesso e retificação dos dados. Boas práticas incluem políticas de segurança, avaliação de riscos e informação transparente aos pacientes [6].

Empresas de saúde em Portugal utilizam dados pessoais para quatro finalidades principais: prestação de serviços de saúde, administração de sistemas internos, realização de pesquisas e promoção de produtos e serviços. Estes dados são essenciais para identificar pacientes, administrar tratamentos, conduzir estudos científicos e promover práticas de marketing, sempre de forma transparente e com o consentimento dos pacientes. O tratamento ético e legal dessas informações é crucial para garantir a eficiência e a confiança nos serviços de saúde [6].

Devem ser adotadas medidas de segurança em empresas de saúde, conforme exigido pelo RGPD, por forma a proteger os dados pessoais dos pacientes. Estas medidas incluem o uso de senhas fortes, criptografia de dados, firewalls, controlo de acesso, entre outros. A implementação adequada das mesmas é crucial para evitar fuga e perda de dados, preservando a privacidade e prevenindo potenciais discriminações. Empresas que negligenciam a segurança podem enfrentar sanções administrativas, civis e/ou penais [6].

A abrangência da proteção de dados vai além da preservação da privacidade, estabelecendo-se à defesa de outros interesses e direitos fundamentais dos indivíduos, como é o caso da liberdade de expressão e religiosa, entre outros.

A importância da proteção dos dados fica mais clara quando pensamos em como as informações pessoais são processadas. As normas relativas à proteção de dados não são formuladas como proibições, mas sim como limitações. Estes parâmetros visam regular minuciosamente como as informações pessoais são tratadas, garantindo que o processo seja transparente e impondo responsabilidades às pessoas envolvidas nesta transformação de informação. Este método não só preserva a privacidade das pessoas, mas também define padrões claros de comportamento, construindo confiança e integridade em diversas áreas que lidam com dados sensíveis.

Lei 58/2019, de 8 de agosto

No que concerne à legislação portuguesa, a lei 58/2019, de 8 de agosto, estabelece o regime jurídico da proteção de dados pessoais que se aplica a todas as entidades que tratam dados pessoais, incluindo as instituições de saúde. A lei define os dados pessoais como “qualquer informação relativa a uma pessoa singular identificada ou identificável”, e estabelece ainda que os dados de saúde são dados sensíveis, o que implica um nível de proteção superior.

A lei 58/2019 estipula certas obrigações que as instituições devem respeitar no que diz respeito ao tratamento de dados pessoais dos pacientes. São elas as seguintes:

- Obter consentimento do paciente para o tratamento dos seus dados pessoais. Este consentimento deve ser livre e inequívoco.
- Informar o paciente sobre as finalidades do tratamento dos seus dados pessoais.
- Garantir a segurança dos dados pessoais, tomando medidas técnicas e organizáveis adequadas com vista à proteção dos dados.
- Atender aos pedidos dos pacientes. Os pacientes têm direito a aceder aos seus dados pessoais e de corrigi-los ou eliminá-los.

A entidade responsável pela fiscalização do cumprimento das leis de proteção de dados pessoais, em Portugal, é a Comissão Nacional de Proteção de Dados (CNPD).

Tecnologias de proteção de dados

Para que seja conseguida a proteção dos dados em entidades de saúde são necessários também mecanismos tecnológicos, como por exemplo, *firewalls*, criptografia, autenticação multifatorial, entre outros. Vamos de seguida destacar apenas a importância dos *firewalls* e criptografia em empresas de saúde.

Importância dos firewalls

No que concerne ao mundo virtual e das tecnologias, uma *firewall* representa uma entidade que impede o acesso de ataques e invasões cibernéticas. É um software de segurança que atua como escudo contra ações suspeitas, salvaguardando os sistemas internos da empresa. Funciona de maneira análoga a uma muralha, resguardando os dispositivos vinculados a uma rede ao isolar o computador da internet. Além disso, realiza análises dos utilizadores da rede conforme estes se aproximam, determinando através dessa inspeção se têm permissão para transpor essa barreira.

A implementação deste programa traz vantagens como a proteção das bases de dados, o auxílio no controle de acesso, proteção de redes locais, permite a verificação de conexões remotas, entre outros [11].

No âmbito da sua implementação em empresas de saúde é importante ter em conta aspectos como a arquitetura da rede, os requisitos de segurança e os recursos de gestão e é também relevante escolher o tipo de *firewall* que se adequa melhor às características da organização, uma vez que existem inúmeros tipos de *firewalls* [12].

Criptografia

A criptografia é um processo que formata os dados para uma forma em que não podem ser lidos sem uma chave de descriptografia. É uma metodologia utilizada para a proteção de dados e por essa razão é um método que pode ser utilizado também em empresas de saúde.

Nesse âmbito, as empresas de saúde em Portugal e na União Europeia devem adotar medidas de criptografia para garantir a segurança dos dados pessoais dos seus pacientes. A

criptografia pode ser empregada tanto para proteger informações em movimento, como aquelas enviadas pela Internet, quanto para dados em repouso, como os armazenados em servidores [13].

Responsabilidade nas empresas de saúde

Por responsabilidade civil entende-se como a obrigação de compensar os prejuízos causados a outra pessoa. Este princípio está presente em todos os sistemas legais, mas a sua definição e extensão podem diferir de acordo com as políticas, a cultura e a história de cada país. Em Portugal, a responsabilidade civil é regulada pelo Código Civil, nos artigos 483.º a 799.º.

A responsabilidade civil pode ser classificada em três tipos: extracontratual, contratual e por factos ilícitos. A primeira decorre da violação de deveres impostos por lei, como danos causados por animais perigosos. A segunda surge do descumprimento de um contrato, como a responsabilidade do vendedor por produtos defeituosos. A terceira resulta da violação de direitos legalmente protegidos, como danos causados por conduta negligente.

Para que haja responsabilidade civil, é necessário que sejam atendidos quatro requisitos: a existência de dano (lesão a um interesse legalmente protegido), ilicitude (violação de um dever jurídico), culpa (conduta do agente que contribuiu para o dano) e nexo de causalidade (relação entre a conduta do agente e o dano). Se esses requisitos forem cumpridos, o agente responsável deve reparar o dano, geralmente por meio de uma indemnização [14].

Empresas de saúde podem ser responsabilizadas por diversos tipos de danos causados a pacientes, incluindo danos materiais, morais e estéticos. No caso de danos materiais, decorrentes de falhas na prestação de cuidados de saúde, a empresa pode ser responsável pelos custos de tratamento. Danos morais, resultantes de violações dos direitos do paciente, como intervenções desnecessárias, podem levar à responsabilidade da empresa pelos danos emocionais sofridos. Danos estéticos, provenientes de intervenções médicas que alteram a aparência do paciente, também podem levar à responsabilização da empresa.

A legislação portuguesa, especificamente o Código Civil e leis específicas como a Lei n.º 29/98 e a Lei n.º 31/2012, regula a responsabilidade das empresas de saúde. Para que a responsabilidade exista, é necessário que sejam preenchidos requisitos como a presença de dano, ilicitude (violação de dever jurídico), culpa (contribuição para o dano por parte da empresa ou profissionais de saúde) e nexo de causalidade (relação entre a conduta e o dano, a ser provado pelo paciente).

Em caso de preenchimento desses requisitos, a empresa de saúde responsável deve reparar o dano, geralmente por meio de indemnização. Esta compensação pode abranger danos materiais (custos de tratamento), danos morais (sofrimento emocional) e danos estéticos (alterações na aparência). A indemnização deve ser concedida de forma a compensar integral e equitativamente o paciente pelos prejuízos sofridos [14].

Em Portugal, a responsabilização das empresas de saúde é regulamentada pelo Código Civil Português e também existe a possibilidade de sanções administrativas, com a Entidade Reguladora da Saúde impondo multas, apreensão de produtos ou serviços, suspensão ou cassação da licença de funcionamento.

Na União Europeia, os mecanismos de responsabilização são regulados pelo Regulamento Geral de Proteção de Dados (RGPD) relatado anteriormente. Empresas de saúde que operam na União Europeia devem cumprir o RGPD e podem ser responsabilizadas por danos causados aos pacientes em caso de fuga de dados.

Estes mecanismos visam proteger os direitos dos pacientes, e as empresas de saúde devem estar atentas às normas aplicáveis para evitar danos e responsabilidades consequentes [15].

Consciencialização dos profissionais de saúde

É essencial que os profissionais de saúde em Portugal e na União Europeia estejam conscientes da importância da proteção de dados pessoais, considerados sensíveis devido à natureza das informações dos pacientes. Com acesso a dados de saúde, financeiros e de identificação pessoal, é crucial que esses profissionais compreendam os riscos associados ao tratamento dessas informações e adotem medidas adequadas de proteção.

A conscientização dos profissionais de saúde sobre a proteção de dados é crucial pelos seguintes motivos:

- Proteger os direitos dos pacientes: os profissionais de saúde devem respeitar o direito à privacidade e à proteção de seus dados pessoais, implementando medidas para salvaguardar tais dados.
- Evitar riscos legais: a falta de proteção adequada dos dados dos pacientes pode sujeitar os profissionais de saúde a sanções legais.
- Prevenir danos aos pacientes: a divulgação inadequada de dados pessoais pode resultar em danos financeiros, psicológicos e físicos aos pacientes.

Promover a conscientização pode ser alcançado por meio de ações de formação, campanhas de sensibilização e outras iniciativas. Algumas medidas incluem a integração de conteúdos sobre proteção de dados em currículos de formação profissional, realização de formações contínuas para profissionais já formados e campanhas de sensibilização direcionadas a profissionais de saúde.

O papel das autoridades de proteção de dados

As autoridades de proteção de dados (APD) são entidades públicas independentes encarregadas de assegurar a conformidade com a legislação de proteção de dados. Em Portugal, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha esse papel, garantindo a aplicação das leis, promovendo a cultura da proteção de dados, investigando reclamações e tomando medidas de correção quando necessário.

A ANPD possui o poder de investigar e aplicar sanções, como multas, apreensão de produtos ou serviços, e até mesmo a suspensão ou revogação da licença de funcionamento, em casos de violações da legislação de proteção de dados.

No âmbito da União Europeia, as APD seguem o Regulamento Geral de Proteção de Dados (RGPD), que estipula que cada Estado-Membro deve designar uma APD. Essas autoridades colaboram para garantir a aplicação consistente do RGPD, sendo essa cooperação coordenada pela Autoridade Europeia para a Proteção de Dados (AEPD). A AEPD, como órgão independente da União Europeia, emite orientações e decisões vinculativas para as APD dos Estados-Membros, promovendo a uniformidade na aplicação do RGPD [16].

Tendências futuras da proteção de dados nas empresas de saúde

O futuro da proteção de dados nas empresas de saúde em Portugal e na União Europeia será moldado por várias tendências, como o aumento da digitalização da saúde, a evolução tecnológica e a crescente consciencialização sobre a proteção de dados. Para enfrentar esses desafios, as empresas de saúde devem adotar medidas para melhorar a segurança dos dados, cumprir a legislação aplicável, como o Regulamento Geral de Proteção de Dados (RGPD), e promover uma cultura de proteção de dados entre colaboradores, pacientes e parceiros.

Tendências específicas incluem o aumento do uso de tecnologias de proteção de dados, como criptografia e autenticação multifatorial, o desenvolvimento de novos modelos de gestão de dados para garantir conformidade com as leis de proteção de dados e a proteção efetiva dos dados pessoais de saúde. Além disso, espera-se a adoção de uma abordagem holística, abrangendo segurança dos dados, conformidade legislativa e promoção da cultura

de proteção de dados. Este aspeto é essencial para que as empresas de saúde enfrentem com sucesso os desafios futuros da proteção de dados [18].

Conclusão

O presente trabalho de pesquisa dedicou-se à investigação da responsabilidade e proteção de dados em empresas do setor de saúde, examinando a legislação tanto em Portugal quanto na União Europeia.

Dentre todas as conclusões alcançadas, destaca-se a constatação de que a proteção de dados pessoais é um direito fundamental dos cidadãos, exigindo respeito por parte de todas as entidades que lidam com esses dados, especialmente as empresas de saúde.

A categoria de dados de saúde foi identificada como sensível, requerendo um nível de proteção mais elevado. Neste contexto, as empresas de saúde assumem uma responsabilidade acrescida na proteção desses dados, sendo passíveis de responsabilização por danos causados em caso de violação da legislação de proteção de dados.

A conscientização dos profissionais de saúde sobre a importância da proteção de dados foi reconhecida como um elemento essencial para garantir a conformidade com a legislação vigente e para proteger efetivamente os direitos dos pacientes. Além disso, as autoridades de proteção de dados desempenham um papel fundamental na promoção da proteção de dados e na aplicação das leis pertinentes.

Os avanços tecnológicos e a crescente conscientização sobre a proteção de dados apresentarão novos desafios para as empresas de saúde. Diante disto destaca-se a necessidade de preparar estas empresas para que as mesmas estejam dotadas de medidas que melhorem a segurança dos dados, estando em conformidade com a legislação aplicável, de forma a promoverem uma cultura de proteção de dados entre colaboradores, pacientes e parceiros.

Em suma, estamos satisfeitas com os resultados alcançados e compreendemos o valor intrínseco de aplicar os conhecimentos adquiridos na prática. O comprometimento demonstrado e a abordagem pro-ativa permitiram não apenas alcançar metas, mas também superar desafios, contribuindo para uma aprendizagem enriquecedora ao longo deste semestre.

Bibliografia

1. Togofor-Homes. (2023). *Política de Privacidade*. Recuperado de: https://www.togofor-homes.com/pt/Pol%C3%ADtica-de-Privacidade/
2. Simões, M.I.A.D.S. (2019). *O regime sancionatório da proteção de dados pessoais: paradigma ou paradoxo?* (Doctoral dissertation).
3. Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Regulation (eu)*, *679*, 2016.
4. Grupo de Trabalho do Artigo 29. "Opinion 4/2007 on the concept of personal data (WP 136)."
5. Krzysztofek, M. (2018). *GDPR: General Data Protection Regulation (EU) 2016/679: Post-reform Personal Data Protection in the European Union*. Kluwer Law International BV.
6. Oliveira, M. V. G. D. (2016). *Proteção de dados pessoais nas comunicações electrónicas: o papel da CNPD e da ANACOM* (Doctoral dissertation).
7. DGERT (2019). *Regulamento Geral sobre a Proteção de Dados.*
8. Gomes, R. M. N. U. (2018). Impacto do RGPD nos Sistemas de Informação de Organizações do Sector da Economia Social.
9. EUR-Lex (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)*.
10. 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*.
11. Ribeiro, M. (2021). *Por que um firewall é indispensável para sua empresa*. LinkedIn.
12. Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall best practices for securing smart healthcare environment: A review. *Applied Sciences*, *11*(19), 9183.
13. Delfs, H., Knebl, H., & Knebl, H. (2002). *Introduction to cryptography* (Vol. 2). Heidelberg: Springer.
14. Portugal (1996). *Decreto-Lei n.º 47344*. Diário da República Eletrónico.
15. Marques, E. N. A. D. C. (2023). *O Regulamento (EU) 2016/679: algumas notas sobre o encarregado de protecção de dados* (Doctoral dissertation).
16. Gomes, R. M. N. U. (2018). Impacto do RGPD nos Sistemas de Informação de Organizações do Sector da Economia Social.
17. de Sousa, P. (2007). PRESIDÊNCIA DO CONSELHO DE MINISTROS. *Cultura*, *29*(368), 000.

18. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, *113*, 73-80.