UNIVERSIDADE D
COIMBRA

Josias Kuvingua Bernardo Niuka

A PROTEÇÃO DE DADOS PESSOAIS DE SAÚDE À LUZ DO RGPD

Volume 1

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Ciências Jurídico-Forenses (Conducente ao grau de Mestre)

Orientador: Professor Doutor André Gonçalo Dias Pereira

Coimbra, 28 de Maio de 2023

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

Josias Kuvingua Bernardo Niuka

A Proteção de Dados Pessoais de Saúde à luz do RGPD

The Protection of Personal Health Data in the Light of the General Data Protection Regulation (GDPR)

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Ciências Jurídico-Forenses (conducente ao grau de Mestre)

Orientada pelo Professor Doutor André Gonçalo Dias Pereira

(...) "ninguém tem o direito de com mão irrespeitosa e ávido olhar devassar a nossa intimidade, mesmo que, por nosso alvedrio e (infeliz) resolução, o queiramos patentear".

Prof. Doutor Walter Osswald

AGRADECIMENTOS

Agradeço de coração a Deus, aos meus pais, irmãos, familiares, namorada, amigos e às instituições que apoiam os estudantes. Que Deus os abençoe abundantemente. Quero expressar meu profundo reconhecimento aos meus mestres que estiveram ao meu lado durante minha jornada na Universidade de Coimbra, desde a licenciatura até o mestrado.

Gostaria de dedicar um agradecimento especial ao meu orientador, André Gonçalo Dias Pereira, que tem sido o principal responsável por impulsionar e guiar-me ao longo dessa longa jornada. Sua sabedoria e humildade ensinaram-me que tudo na vida é alcançado através da disciplina constante e da determinação incansável. Acreditem, cada um de vocês teve um papel fundamental no resultado final deste trabalho que apresento hoje.

O meu sincero agradecimento a todos vós.

RESUMO

A presente dissertação versa sobre A Proteção dos Dados Pessoais de Saúde à Luz do Regulamento Geral de Proteção de Dados Pessoais (RGPD) e das demais leis nacionais. Identifica e analisa os direitos dos titulares de dados pessoais de saúde face as violações da privacidade destes, pelas entidades que se dedicam a recolha e tratamento de dados pessoais no exercício das suas atividades, bem como analisa a relevância dos princípios, consentimento, privacidade, informações, divulgação, encarregado de proteção, esquecimento ou apagamento dos dados pessoais de saúde e os poderes da CNPD, num mundo cada vez mais global em que a nossa privacidade é constantemente posta em causa, com a prática de tratamento de dados pessoais pelas pessoas coletivas e demais entes, públicos ou privados. Considerando que nos dias que correm a luta pela proteção da nossa privacidade, não é apenas em muitas situações um caso individual, mas sim uma luta coletiva e que todos os afetados pela violação de seus direitos, juntem forças para uma maior defesa dessa nobre causa. Assim sendo, consubstancia tarefa do Estado, velar pela justiça e protegendo constantemente, esta esfera de intimidade que é natural a toda espécie humana. Neste sentido, protegendo os nossos dados, não apenas estaremos a proteger a nossa privacidade dos demais terceiros, mas como também estamos a proteger a dignidade dos seus titulares. Nesta era digital, tem sido cada vez mais visível a divulgação dos dados pessoais, quer seja sensível, bem como os não sensíveis em espaços públicos, pelos seus sujeitos e muitas vezes por desconhecimentos dos perigos que estas práticas podem causa-los quando desinformados.

Palavras-Chave: Dados Pessoais, Dados Pessoais de Saúde, Privacidade dos Dados Pessoais de Saúde, Violações dos Dados Pessoais, Poderes da CNPD.

ABSTRACT

This dissertation deals with The Protection of Personal Health Data in the Light of the General Data Protection Regulation (GDPR) and other national laws.It identifies and analyses the rights of the holders of personal health data in the face of violations of their privacy, by the entities that are dedicated to the collection of processing of personal data in the exercise of their activities, as well as analyses the relevance, of the principles, consent, privacy, information, disclosure, protection officer, forgetfulness or erasure of personal health data and the powers of the The Data Protection Commission "DPC", in an increasingly global world in which our privacy is constantly called into question, with the practice of processing personal data by legal persons and other entities, public or private. Considering that nowadays, the fight for the protection of our privacy is not in many situations an individual case, but rather the collective fight for all those affected by the violation of their rights to join forces for a greater defence of this noble cause. Therefore, it is the State's task to watch over justice and constantly protect this sphere of intimacy that is transversal to the human species. In this sense, by protecting our data, we are not only protecting our privacy, but also the dignity of others. In this new digital era, the disclosure of personal data, sensitive or not, in public spaces has become increasingly visible. This dissemination comes, many times, from the unawareness regarding the dangers of digital practices harmful to our well-being.

Keywords: Personal Data, Personal Health Data, Privacy of Personal Health Data, Personal Data Breaches, Powers of the DPC

Lista de Siglas e Abreviaturas

- AC - Acórdão
- AR - Assembleia da República
- CC - Código Civil
- CRP - Constituição da República Portuguesa
- CP - Código Penal
- CE - Comissão Europeia
- CNECV - Conselho Nacional de Ética para as Ciências da Vida
- CNPD - Comissão Nacional de Proteção de Dados
- CF - Confira
- DPO - Encarregado pela Proteção de Dados
- EU - União Europeia
- LPDP - Lei de Proteção de Dados Pessoais
- RGPD - Regulamento Geral de proteção de Dados Pessoais
- TFUE - Tratado de Funcionamento da União Europeia
- VIDE - Confira

ÍNDICE

1 INTRODUÇÃO

A presente dissertação desafia-nos a refletir sobre a proteção dos dados pessoais de saúde à luz do Regulamento Geral de Proteção de Dados Pessoais (RGPD), que entrou em vigor em maio de 2018 em todos os estados-membros da União Europeia (UE), sem a necessidade de transposição para os respetivos Estados membros, devido aos seus efeitos diretos decorrentes da supremacia dos regulamentos da União Europeia. Veremos que os dados pessoais são protegidos não apenas pelo RGPD, mas também por outras leis que visam proteger os direitos fundamentais dos cidadãos nos Estados membros, desde que não contradigam o direito da União.

Além disso, analisaremos o conceito de dados pessoais, que abrange todas as informações relacionadas às nossas vidas. Também examinaremos as categorias dos dados de saúde, a titularidade, os princípios relevantes no tratamento de dados, bem como o papel do encarregado de proteção de dados.

Abordaremos o tema do Consentimento no tratamento de dados de saúde, bem como a questão da privacidade, que não deve ser confundida com a autodeterminação informacional, embora estejam interligadas. Procederemos ainda à discussão sobre a importância da informação de saúde, que pertence exclusivamente ao proprietário e não a terceiros, e a oposição à divulgação dos dados pessoais de saúde. Além disso, exploraremos o direito ao esquecimento, assim como os poderes da Comissão Nacional de Proteção de Dados (CNPD).

O regime sancionatório da proteção de dados pessoais tem como objetivo afirmar e garantir a proteção dos dados pessoais, estabelecendo um equilíbrio na aplicação de medidas punitivas que se aplicam a entidades públicas e privadas que, no exercício de suas funções, lidam com a recolha e o tratamento de dados pessoais. Uma análise abrangente exigiria uma exploração mais aprofundada de toda a temática relacionada à proteção de dados e à complexidade do seu regime. No entanto, neste modesto trabalho de redação, focaremos a nossa atenção principalmente nos dados pessoais de saúde e nos conflitos que envolvem o acesso às informações de saúde, de forma a abordar o assunto com certo nível de detalhe.

Para explorar os dados pessoais de saúde e os conflitos relacionados ao seu acesso, bem como o regime sancionatório, faremos referência a pesquisas bibliográficas, acórdãos, doutrina e jurisprudência, bem como, iremos considerar pareceres e diversas obras relacionadas a dados e acesso a informações de saúde, que nos permitirão sustentar que o regime dos

dados pessoais de saúde visa proteger assuntos sensíveis e a autonomia dos titulares dos dados tratados.

Através da aplicação de sanções decorrentes de sua violação, busca-se garantir equilíbrio, certeza e segurança jurídica no cumprimento e respeito das leis democráticas, tanto por parte de entidades públicas quanto de entidades privadas. Nesse contexto, a aplicação de medidas contraordenacionais ou sanções é de competência de uma autoridade de controle independente, como a CNPD.

Fica evidente, portanto, que os dados pessoais, assim como os dados especiais de saúde, assumem um significado imenso na atualidade, tanto no âmbito académico como nas sociedades contemporâneas. As constantes violações dos dados pessoais por parte de entidades públicas e privadas, causam grandes perturbações no equilíbrio social e nas relações pessoais. Tudo indica que devemos continuar a trabalhar para fornecer o melhor quadro possível visando uma resolução de disputas cada vez mais justa.

Hoje, o RGPD é amplamente discutido e debatido, pois trouxe regulamentações que visam prevenir e fornecer esperança às pessoas no que diz respeito à proteção de dados pessoais, em particular, a proteção dos dados pessoais de saúde. Este é o tema essencial que trataremos com maior ênfase ao longo da dissertação.

2 DADOS PESSOAIS

Atualmente, observa-se que no contexto europeu, há um novo instrumento que regula a proteção dos dados pessoais, proporcionando maior segurança e confiança aos cidadãos europeus no que diz respeito aos seus direitos fundamentais, assim como ao acesso e proteção da privacidade dos dados pessoais.

O Regulamento (UE) 2016/679, conhecido como Regulamento Geral sobre a Proteção de Dados (RGPD)[1] é um ato legislativo constituído com o objetivo de reforçar os direitos fundamentais das pessoas na era digital, mediante esclarecimento das normas aplicáveis às empresas e aos organismos públicos no mercado único digital[2].

Com efeito, é amplamente conhecido que os regulamentos emitidos pela União Europeia impõem obrigações aos Estados-membros, exigindo que adotem determinados comportamentos e proibindo qualquer ação ou omissão que prejudique o funcionamento adequado do direito da União, nesses termos:

> Este regulamento comunitário que, de acordo com o artigo 288.º do Tratado sobre o Funcionamento da União Europeia, é diretamente aplicável nos Estados-Membros da UE e obrigatório em todos os seus elementos, prevalece sobre a legislação nacional nos termos do artigo 8.º da Constituição. (Portuguesa D. d., 2016).

No âmbito europeu, qualquer tratamento, recolha e transferência de dados pessoais, seja a nível nacional ou internacional, devem obedecer a regras estabelecidas pelo RGPD e outras legislações que valorizam a proteção da dignidade humana. Portanto, todas as entidades, sejam elas coletivas ou privadas, no que diz respeito à proteção de dados, devem seguir as regras fundamentais do novo regime regulatório (RGPD).

De facto, qualquer interferência na privacidade dos indivíduos que afete os seus dados deve ser comunicada aos seus titulares, uma vez que estes devem estar cientes do propósito e justificação da coleta ou interferência nos seus dados, Cf, nº1 do art. 34º do RGPD. Além disso, consideramos que a duração e o tempo necessários para alcançar a finalidade da recolha, bem como o direito de acesso e exclusão dos dados coletados, possuem uma importância significativa na vida dos próprios indivíduos.

---

[1] O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE)
Obtido em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434>. Acesso em 28 maio 2023.

[2]Comissão Europeia. Obtido em <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt>. Acesso em 28 maio 2023.

Para (Zuboff, 2020), p. 533 "*O novo quadro regulamentar também impõe multas substanciais ao incumprimento das suas normas --- Sanções económicas que podem ascender até quatro por cento das receitas da empresa*". A defesa dos dados pessoais constitui tarefa dos Estados, bem como de todos os cidadãos, recorrendo a queixas e reclamções para uma proteção mais ágil dos seus direitos fundamentais, Cf, nº 1 do art. 52º da CRP.

Nesse contexto, torna-se relevante a proteção dos dados pessoais, o que nos leva a compreender a importância de lutar e preservar a democracia e os direitos humanos quando se trata da vida e da privacidade das pessoas. Pois, compete aos Estados da União proteger esses direitos, independentemente do local onde os cidadãos se encontrem, Cf, art. 3º RGPD.

Com base no exposto, O RGPD visa prporcionar estabilidade e segurança, na proteção dos pessoais dos cidadãos da UE.

Os dados pessoais são amplamente compreendidos como qualquer informação relacionada a uma pessoa que pode ser identificada ou tornada identificável. Em essência, trata-se de uma pessoa singular, o titular dos dados, detentor da sua singularidade e autodeterminação informacional, que possui direitos conferidos pelo RGPD[3].

Nesse sentido, os dados pessoais abrangem informações que dizem respeito à vida privada, familiar e social, e, com base nessas informações, é possível identificar uma pessoa específica. Isso ocorre quando nos referimos ao nome, data de nascimento, número de identificação civil, endereço residencial, dados clínicos e outros elementos que possam identificar uma pessoa humana.

Trata-se de informações que podem ser classificadas como sensíveis ou não, e que, em certos casos, possibilitam a identificação do sujeito titular dos dados, justificando assim a aplicação do RGPD.

Conforme (Cordeiro, 2020), p. 107-113, é essencial referir que o RGPD não se aplica quando estamos a lidar com objetos ou coisas, excepto se os objectos estiverem diretamente associados ao nome do titular dos dados, levando à sua identificação.

Com base nestas considerações, é plausível afirmar que o RGPD não se aplica a pessoas jurídicas, pois estas são entidades abstratas, desprovidas de capacidade de autodeterminação, dependendo de uma pessoa física para governá-las e garantir o seu progresso num mundo cada vez mais tecnológico, cf. (Cordeiro, 2020), p. 107-113.

[3] RGPD, art. 4º.

Diferente dos dados pessoais de caráter não sensível como o nome, número fiscal, os dados sensíveis dizem respeito, em geral, aos aspetos mais íntimos de uma pessoa, como os detalhes relacionados, por exemplo, à sua condição de saúde[4]. Devido à sua natureza mais delicada, esses dados requerem uma proteção especial no que diz respeito ao seu tratamento e armazenamento.

O RGPD visa proteger os dados pessoais, bem como prevenir possíveis violações que possam comprometer a privacidade e os direitos dos cidadãos da UE. Ao promover um ambiente seguro e confiável para o tratamento dessas informações, o regulamento tem efeitos humanistas, garantindo a autonomia e a liberdade individual e contribuindo para a construção de uma sociedade mais justa e respeitosa dos direitos fundamentais de cada pessoa. Assim, o tratamento e a coleta de dados sensíveis ocorrem durante a relação terapêutica entre o profissional de saúde e o paciente, titular dos dados. Esse processo está intrinsecamente ligado à proteção do princípio da dignidade da pessoa humana, o qual desempenha um papel fundamental nessas relações terapêuticas. Portanto, é essencial assegurar que o tratamento desses dados seja realizado de maneira cuidadosa e respeitosa, com o objetivo de preservar a dignidade e garantir o bem-estar do paciente, cf. (Sales Sarlet & Caldeira, 2019), p. 2 e 4.

Os dados pessoais, sejam eles sensíveis ou não, desempenham um papel significativo no contexto da proteção de dados. Neste sentido, o RGPD define dados pessoais de saúde como "d*ados pessoais relacionados a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde*", cf. art. 4º/15 do RGPD. Esses dados estão diretamente ligados ao histórico do titular desde o momento em que este estabelece um contrato de prestação de serviços com um profissional de saúde. Portanto, é essencial garantir a asua proteção, com o máximo sigilo que vigora nos cuidados médicos.

É importante ressaltar que, por meio das informações coletadas de um determinado sujeito que recebe cuidados médicos, é possível chegar ao histórico familiar e ascendência desse indivíduo. Sendo fundamental que as informações recolhidas não sejam manifestantemente excessivas em relação à finalidade específica da coleta e tratamento de dados. Isso significa que apenas deve colher-se somente os dados essencias para o alcance da finalidade desejada,

[4] RGPD, caput do art. 9º.

garantindo assim, a proteção da privacidade e minimizando qualquer potencial intrusão indevida na vida pessoal do titular dos dados, cf. (Pereira A. L., 2018), p. 304.

2.1 DADOS PESSOAIS DE SAÚDE

Estes não devem ser tratados como meros dados administrativos nos quais qualquer funcionário dos serviços teria acesso indiscriminado. Tal abordagem seria desrespeitosa e minimizaria a importância da privacidade dos titulares desses dados.

Os dados de saúde referem-se aos dados pessoais relacionados à saúde de uma pessoa, os quais são normalmente coletados, registados e utilizados pelos profissionais de saúde. Isto leva-nos a considerar que a recolha e o tratamento desses dados têm finalidades específicas e determinadas, em benefício do bem-estar do paciente. Éste, possui a liberdade de autorizar ou não a coleta e o tratamento dos seus dados, respeitando-se, assim, a sua autonomia enquanto titular. Nesse contexto, o respeito à autonomia do paciente é essencial na tomada de decisões relacionadas à gestão dos seus dados de saúde[5].

O dado de saúde, em muitas situações, vai além da simples informação sobre a saúde do seu titular[6]. É frequente ocorrer a interseção dessas informações com dados familiares, os quais não devem estar acessíveis a terceiros. A proteção desses dados sensíveis é fundamental para preservar a privacidade e a intimidade não apenas do indivíduo em questão, mas também de seus familiares.

A Lei nº 12/2005[7], adota o conceito de "informação de saúde" definindo-o, no seu artigo 2º, como "*todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua* história clínica e familiar". Isto, reflete a importância de proteger todas as informações relevantes para a saúde de um indivíduo, não apenas aquelas relacionadas a condições médicas atuais, mas também informações que possam influir na sua saúde no futuro, bem como detalhes da sua história médica e informações sobre a saúde dos seus familiares. Essa ampla definição busca garantir

[5] RGPD, art. 4º/15

[6] Regulamento de Deontologia Médica nº 707/2017. Obtido em <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2649&tabela=leis&ficha=1&pagina=1&so_miolo=>. Acesso em 28 maio 2023.

[7] Lei nº 12/2005, de 26 de janeiro. Obtido em <https://dre.pt/dre/detalhe/lei/12-2005-624463>. Acesso em 28 maio 2023.

a privacidade e a confidencialidade de todos os aspetos relacionados à saúde de uma pessoa, assegurando a proteção adequada desses dados.

Compreendemos que os dados de saúde possuem um fundamento especial devido à sua natureza, pois, o conhecimento destes, pelo profissional, ocorre no âmbito da relação médico paciente, visando fornecer cuidados terapêuticos adequados. Essa relação médica é construída com base nos princípios fundamentais da confiança e sigilo médico, que impõem aos profissionais o dever de manter a confidencialidade e a privacidade das informações de saúde dos pacientes.[8]

Assim, com a proteção dos dados pessoais, promove-se o bem-estar coletivo, fortalalecendo a própria estrutura social que se baseia no respeito à dignidade humana e na preservação dos direitos e valores de cada indivíduo.

Neste sentido, a proteção dos direitos fundamentais por parte dos Estados, visam garantir a dignidade e a autonomia dos indivíduos, limitando o poder tanto das entidades públicas quanto das entidades privadas, cf., nº1 art.18º CRP.

Assim, ao proteger-se a privacidade dos dados, assegura-se aos indivíduos o controlo sobre as suas informações pessoais e a capacidade de decidir sobre a sua divulgação e uso. Protege-se os dados pessoais, a inviolabilidade do lar, a correspondência privada, etc, cf, (Deodato, 2017), p. 26 e ss.

Ainda para Deodato (2017, p. 26), a intervenção em saúde não se resume apenas ao conhecimento da pessoa num aspeto isolado, mas busca compreender a pessoa como um todo, considerando a sua dimensão física, psicológica, social, etc.

Ao considerarmos todos estes aspetos, é possível entender não apenas as doenças presentes, mas também o historial clínico, possíveis origens e fatores de risco, bem como a influência de aspetos hereditários. Isso proporciona uma visão mais holística do paciente, permitindo uma intervenção mais personalizada e eficaz. Desta forma, a intervenção em saúde busca compreender a pessoa como um todo, considerando todos os aspetos relevantes, com vista a um cuidado terapêutico adequado[9].

[8] Cf. Deodato Sérgio. A proteção dos dados pessoais de saúde, p. 10-13.
[9] Vide (Deodato), 2017, p. 17.

Para Deodato (2017, p. 17) "*Os dados pessoais de saúde emergem desta relação de natureza profissional, em que uma pessoa (profissional de saúde) passa conhecer informações sobre a vida de outrem*". Podemos considerar que as entidades hospitalares e outras instituições de saúde têm a responsabilidade de coletar, armazenar e processar esses dados pessoais de saúde em conformidade com as leis e regulamentos aplicáveis de proteção de dados. Essas instituições devem adotar medidas adequadas para garantir a segurança, a confidencialidade e a integridade dessas informações. Cf, alínea f), nº 1 do art. 5º do RGPD

O fato de os dados de saúde pertencerem aos próprios titulares reforça a importância do respeito pela privacidade e autodeterminação desses indivíduos. Os pacientes têm o direito de controlar as suas informações de saúde, de decidir quem tem acesso a estas e de consentir ou não com o seu uso e partilha, o que denota a importância das instituições adotarem regulamentações que promovam a transparência, o consentimento informado e o respeito pelos direitos dos titulares dos dados pessoais de saúde. Isso implica que os pacientes exerçam os seus direitos de acesso, retificação, exclusão e portabilidade dos seus dados. Assim, proíbe-se o acesso a dados pessoias sem consentimento do titular, Cf. nº 4 do art. 35º CRP.

Deste modo, a relação médico-paciente é baseada na confiança e no sigilo profissional, permitindo que os pacientes partilhem informações sensíveis sobre a sua saúde com o médico sem receio de que essas sejam divulgadas ou utilizadas de forma inadequada.

Portanto, concordamos com a importância de restringir o acesso a dados pessoais de saúde de proteger a confidencialidade dessas informações. Essas medidas são essenciais para preservar a privacidade dos pacientes, garantir a qualidade do atendimento médico e manter a integridade da relação médico-paciente.

As informações relacionadas à saúde dos titulares dos dados podem abranger tanto aspetos positivos como negativos, levando em consideração os diagnósticos e avaliações realizadas pelos profissionais de saúde. O acesso indevido a dados pessoais de saúde podem ter graves consequências, como violação da privacidade, discriminação ou uso inadequado das informações. É, assim, necessário que sejam estabelecidos mecanismos e medidas de segurança para proteger esses dados e garantir que sejam acessíveis apenas a pessoas autorizadas e em conformidade com a legislação em vigor.

A proteção deste dado especial é fundamental para preservar a confiança na relação médico-paciente, assegurar a qualidade do atendimento médico e respeitar os direitos fundamentais dos indivíduos, sendo essencial que haja uma abordagem responsável e ética no tratamento dessas informações, visando sempre o bem-estar e a privacidade dos titulares dos dados. Cf, (Deodato) 2017, p.17ss.

Os dados pessoais de saúde são considerados dados especiais, conforme estabelecido no nº1 do art. 9º do RGPD. Na relação médico-paciente é necessário agir de acordo com as orientações de proteção e conservação eficaz dos dados pessoais de saúde, visando fins específicos e determinados.

Para Pereira (2015, p. 32) a doutrina maioritária portuguesa entende que os tratamentos médicos realizados em hospitais públicos são regidos pelas regras de direito administrativo, em razão da proteção dos direitos fundamentais dos pacientes e a preservação do interesse público. Essa abordagem busca assegurar que a recolha e o tratamento dos dados pessoais de saúde sejam realizados de maneira adequada, em observância aos princípios éticos e legais. A proteção da privacidade dos pacientes, a segurança dos dados e a qualidade do atendimento são aspetos fundamentais nesse contexto.

As instituições de sáude pública ou privada, para garantir a privacidade dos dados, de acordo com o RGPD, adotam medidas que envolvem a implementação de políticas de privacidade robustas, a adoção de medidas de segurança adequadas e a consciencialização dos profissionais de saúde sobre a importância da proteção dos dados pessoais de saúde dos pacientes.

No âmbito da proteção dos dados pessoais de saúde, é fundamental garantir a confidencialidade das informações dos pacientes. Essas informações devem permanecer estritamente sob a alçada da relação entre médico e paciente, em conformidade com o princípio do segredo profissional.

Segundo Pereira (2015, p. 636): "*só é segredo médico aquilo que o médico sabe de outra pessoa, apenas porque é médico*;" "*não é segredo penalmente relevante aquilo que o agente conhece em veste puramente privada*".

Desse entendimento decorre que existem também outros princípios relevantes, como a dignidade da pessoa humana, a boa-fé e a justiça, princípios fundamentais no tratamento,

conservação e cuidado dos dados dos titulares, estabelecedores de diretrizes éticas e morais orientadores do trabalho dos profissionais de saúde.

Dessa forma, os princípios da confiança, dignidade da pessoa humana, boa-fé e justiça desempenham um papel crucial na garantia de um tratamento responsável e ético dos dados de saúde, contribuindo para a construção de uma relação médico-paciente baseada em valores humanísticos e respeito mútuo, bem como representam uma conquista civilizacional e refletem as características fundamentais dos estados democráticos. Cf. Pereira (2015, p. 640).

Atualmente, a proteção da privacidade tornou-se uma responsabilidade de todos os estados, pois vivemos numa era digital em que é fundamental preocuparmo-nos com a divulgação dos nossos dados por parte das entidades, bem como de terceiros. Cf. Pereira (2015, p. 642-643).

Em suma, partilhamos da visão de que cada indivíduo possui uma esfera de privacidade, um espaço íntimo e pessoal que deve ser protegido contra qualquer invasão. Esse espaço interior proporciona uma sensação de segurança, onde a pessoa tem a convicção de que seus dados sensíveis serão preservados, permitindo-lhe libertar-se das turbulências do mundo e evitar qualquer julgamento por parte dos outros, independentemente do tipo de doença que essa pessoa possa ter. É essencial respeitar e salvaguardar essa esfera de privacidade como parte fundamental do direito à intimidade e à dignidade da pessoa humana.

É indiscutível a importância dos dados clínicos no contexto dos dados pessoais. No âmbito europeu, têm sido implementadas políticas que incentivam os médicos a registar todas as informações relevantes durante as consultas médicas. Isso inclui análises, exames, formulários de consentimento e outras informações pertinentes sobre o paciente, todas com finalidades específicas e determinadas.

É crucial garantir a proteção adequada desses registos e informações, abrangendo tanto dados sensíveis quanto não sensíveis. Ao manter um histórico detalhado dessas informações, é possível obter uma visão ampla dos principais problemas de saúde enfrentados pelo paciente. Esses registos são mantidos e protegidos pelo profissional de saúde para futuras referências e, eventualmente, podem servir como evidências da condição de saúde do paciente no momento do diagnóstico inicial. Essa abordagem busca auxiliar na resolução

dos problemas de saúde do paciente e contribui para um tratamento mais efetivo e personalizado.

As informações colhidas e os exames sobre a situação do paciente, irão constar do processo clínico do seu titular que está sobre os cuidados de saúde. Consequentemente, os processos clínicos que se encontram nas instituições de saúde, gozam de uma garantia de confidencialidade, próprias da praxis médica. Não obstante, falar dos dados clínicos pressupõe também referir o que podemos entender por "ficha clínica", que consta do nº 2 do art. 40º do Regulamento de Deontologia Médica, nº 707/2016[10], como sendo o registo dos dados clínicos do doente, das anotações pessoais do médico e tem como finalidade a memória futura e a comunicação entre profissionais que tratem do doente[11].

Nos processos clínicos dos pacientes, é prática registar todas as informações relevantes relacionadas à sua situação médica, abrangendo o seu histórico completo. Essa abordagem visa permitir uma intervenção mais precisa e eficaz no estado de saúde do paciente. Através do consentimento informado, o paciente coopera ativamente fornecendo informações adicionais que podem contribuir para um diagnóstico mais preciso por parte do profissional de saúde.

Essa troca de informações entre paciente e profissional de saúde é crucial para estabelecer uma relação de confiança e permitir um cuidado médico mais personalizado. Ao registar todos os detalhes relevantes sobre a saúde do paciente, os profissionais de saúde podem ter uma visão completa do quadro clínico, permitindo uma avaliação abrangente e uma intervenção direcionada. Esse processo colaborativo entre médico e paciente fortalece a tomada de decisões compartilhadas e o bem-estar geral do paciente.

Ainda conforme Pereira (2013, p. 191-192), processo clínico deve incluir detalhadamente os seguintes dados acompanhados da identificação das pessoas envolvidas no respetivo procedimento (médicos, enfermeiros, etc):

> a) identificação do paciente;
> b) memória de anamnese (entrevista prévia ao paciente);

[10] Regulamento de Deontologia Médica, n.º 707/2016, de 21 de Julho, nº 2, art. 40º. Obtido em <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2649&tabela=leis&ficha=1&pagina=1&so_miolo=#:~:text=1%20%2D%20O%20m%C3%A9dico%2C%20no%20exerc%C3%ADcio,no%20exerc%C3%ADcio%20das%20fun%C3%A7%C3%B5es%20cl%C3%ADnicas.>. Acesso em 28 maio 2023.

[11] Cfra. Pereira (2013, p. 191-192).

> c) diagnóstico (incluindo resultados das análises, exames, etc.);
> d) estado de saúde do paciente à altura da admissão;
> e) evolução do seu estado de saúde;
> f) informação prestada a paciente, bem como o meio através do qual essa informação foi prestada;
> g) registo do consentimento informado por parte do paciente;
> h) correspondência com outros profissionais de saúde relativa ao paciente) métodos terapêuticos utilizados;
> j) monitorização do paciente;
> l) fármacos, produtos e materiais empregues (e respetiva dosagem, lote, marca e outros elementos relevantes) e
> m) prognóstico.

Uma questão relevante no âmbito dos dados de saúde prende-se com a realização de ensaios clínicos que, em certas ocasiões, envolvem o tratamento de dados sensíveis de saúde dos participantes. No entanto, é fundamental que a coleta e o tratamento desses dados sejam limitados ao estritamente necessário, com o objetivo específico do ensaio clínico em questão. Isso deve-se ao fato de que os dados de saúde de natureza sensível estarem sujeitos a uma proteção adicional, conforme estabelecido no RGPD.

Por regra, o tratamento de dados pessoias de saúde é proibido, a menos que seja permitido pelo titular dos dados através do consentimento ou autorizado por disposições expressas deste regulamento, cf, nº1 e 2, a) do artigo 9º do RGPD.

Os dados de saúde estão intrinsecamente ligados à vida privada das pessoas e são considerados direitos fundamentais, protegidos tanto pela legislação constitucional como por normas específicas, cf, nº 1 do art. 80º CC. O tratamento desses dados requer não apenas o consentimento do titular, mas também a observância das disposições legais aplicáveis.

Dada a sensibilidade dos dados de saúde, em muitas situações, é necessária uma supervisão adicional por parte da Comissão Nacional de Proteção de Dados (CNPD)[12], que é a autoridade de proteção de dados em Portugal.

A CNPD tem a responsabilidade de garantir que o tratamento de dados de saúde ocorra de acordo com as leis de proteção de dados e as diretrizes estabelecidas. A supervisão desta entidade desempenha um papel crucial na promoção da conformidade e no equilíbrio entre

[12] A Comissão Nacional de Proteção de Dados (CNPD) é uma entidade administrativa responsável pelo controle e fiscalização do cumprimento do RGPD. Obtido em <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>. Acesso em 28 maio 2023.

a disponibilidade de informações médicas necessárias e a proteção da privacidade e dos direitos dos indivíduos.

As questões relacionadas ao estado de saúde de uma pessoa, por se tratarem de assuntos relacionados à vida privada e serem considerados direitos fundamentais, geralmente são de competência legislativa reservada à Assembleia da República (AR)[13]. Isso significa que a legislação sobre essas matérias deve ser estabelecida por meio de leis ou decretos-leis autorizados. O Governo, ao legislar sobre aspetos que envolvem a vida familiar, histórico clínico ou outras questões relacionadas à saúde, deve fazê-lo dentro dos limites da sua competência e em conformidade com as normas constitucionais. Se esse ato for estabelecido por meio de um decreto-lei simples, sem a devida autorização legislativa, poderá ser considerada inconstitucional, conforme refere o Acórdão nº 355 /97.[14]

Portanto, é importante que o governo atue com base em normas constitucionais ao legislar sobre assuntos que afetam a privacidade e os direitos fundamentais das pessoas no contexto da saúde. A reserva de competência legislativa da AR nesse campo visa garantir um debate democrático e uma proteção adequada dos direitos e liberdades individuais. Neste caso, proteção da vida privada, pois os dados de saúde "integram a categoria de dados relativos à vida privada, tais como as informações referentes à origem étnica, à vida familiar, a vida sexual, condenações em processo criminal, situação patrimonial e financeira". Cf. Pinheiro (2015, p. 723).

Contudo, estamos a viver num mundo cada vez mais globalizado e digitalizado, onde a facilidade de acesso e compartilhamento de dados é uma realidade que também traz consigo desafios e preocupações. Especialmente, no que diz respeito à privacidade e proteção dos dados pessoais sensíveis, como os relacionados à saúde. É por demais lamentável constatar que algumas entidades empresariais têm coletado e utilizado dados pessoais sem o nosso consentimento. Esse comportamento é socialmente inadequado, pois coloca em risco a segurança e a privacidade de nossas informações, particularmente as de natureza sensível, pois, merecem maior proteção. Nesse sentido, é fundamental promover pedagogias sobre a

[13] Assembleia da República é um dos órgãos de soberania eletivos previstos na CRP, constituído por uma câmara de Deputados única. Obtido em <https://www.parlamento.pai.pt/>. Acesso em 30 maio 2023.
[14] Acórdão nº 355/97, processo nº 182/97, proferido pelo Tribunal Constitucional. Plenário. Obtido em <https://www.tribunalconstitucional.pt/tc/acordaos/19970355.html>. Acesso em 28 maio 2023.

importância da proteção dos dados pessoais, especialmente os de saúde, e garantir que as medidas adequadas sejam implementadas por forma a prevenir o acesso indevido, o uso não autorizado e a divulgação inadequada dessas informações.

Quando ocorre a violação de dados pessoais, relacionados à saúde, por entidades públicas ou privadas no exercício da sua atividade, os indivíduos têm o direito de procurar a sua reparação para proteger os seus direitos, tanto individualmente quanto coletivamente, através de uma ação coletiva, na qual um grupo de cidadãos lesados se une para buscar justiça e garantir uma maior privacidade e respeito pela proteção de seus dados.[15]

O tratamento de dados deve assumir uma finalidade específica, assim, é imprescindível agir de acordo com os princípios fundamentais, essencialmente, boa fé, licitude, transparência, com garantia de respepeito aos dados pessoias. Cf, art. 5º, RGPD.

Além disso, é essencial proporcionar aos titulares dos dados o direito de acesso, retificação e eliminação de suas informações pessoais, Cf. Art. 16º do RGPD. O objetivo é criar uma cultura em que a privacidade e a proteção de dados sejam valorizadas e respeitadas por todas as partes envolvidas. Isso contribui para a confiança dos indivíduos no uso de seus dados pessoais e promove uma relação de transparência e responsabilidade entre as empresas e seus clientes.

Assim, compreende-se que ao disponibilizarmos dados pessoais de saúde, devemos ter cautela e considerar a finalidade e a legitimidade dessa partilha. É importante verificar se estamos a consentir informada e conscientemente para que os nossos dados sejam utilizados de maneira adequada e em conformidade com os princípios da proteção de dados.

2.2 TITULARIDADE DOS DADOS DE SAÚDE

A titularidade dos dados pessoais de saúde diz respeito aos seus titulares e as informações relacionadas com a sua privacidade devem ser tratadas com o máximo cuidado e respeito. Nesse contexto, as entidades de saúde têm a responsabilidade de proteger esses dados, garantindo a sua confidencialidade e segurança, além de utilizá-los apenas para os fins específicos autorizados pelo titular ou exigidos por lei. É fundamental compreender que os seus

[15] Por exemplo, por meio da ação popular, art. 52 da CRP.

titulares têm o direito de controlar o acesso e o uso das suas informações de saúde. Estes deverão ser informados sobre como os seus dados serão coletados, armazenados, utilizados e compartilhados, tendo a possibilidade de dar ou negar consentimento de forma livre e esclarecida.[16]

As entidades de saúde devem agir como guardiãs desses dados, adotando medidas técnicas, organizacionais e jurídicas adequadas para protegê-los contra acessos não autorizados, uso indevido ou divulgação inadequada. Além disso, devem ser transparentes em relação às suas práticas de tratamento de dados e estar em conformidade com as leis e regulamentos.

É importante ressaltar que a titularidade dos dados pessoais de saúde pertence aos próprios indivíduos, pois estes são sujeitos dotados de direitos de personalidade e capacidade jurídica, conforme estabelecido pela lei civil, no seu artigo 67º.

Como titulares desses dados, os seus titulares têm o direito de consentir, sempre que possível, com o tratamento e a recolha das suas informações de saúde, registos médicos e tudo quanto diga respeito a estes, com o objetivo de alcançar finalidades terapêuticas e defender sua saúde e bem-estar.

Embora em muitos casos, algumas pessoas possam entender que a titularidade dos dados de saúde deva pertencer principalmente às entidades depositárias dessas informações, como instituições de saúde, hospitais e outros prestadores de serviços de saúde.

É fundamental compreender que os indivíduos são os principais interessados e beneficiários dos seus próprios dados de saúde. Eles têm o direito de saber como é que as suas informações estão a ser tratadas, quem tem acesso a elas e quais as finalidades para que estão a ser utilizadas. A decisão sobre a partilha e o uso desses dados deve ser, sempre que possível, de responsabilidade do próprio titular, desde que não haja restrições legais ou riscos à saúde pública.

A titularidade dos dados de saúde pertence aos indivíduos, garantindo-lhes o direito de consentir e controlar o tratamento dessas informações, de acordo com os princípios de proteção de dados e os direitos fundamentais relacionados com a privacidade e a autodeterminação informacional.

As entidades de saúde desempenham um papel importante na gestão adequada dos dados de saúde, mas a titularidade e o controlo permanecem com os indivíduos, como sujeitos dotados

[16] (Deodato), 2017, p. 22-24.

de direitos de personalidade e capacidade jurídica. Ainda para (Deodato), 2017, p. 24 "*Os dados de saúde, sendo dados pessoais, não poderão ter outro titular que não a própria pessoa. O seu conhecimento ou a sua posse, não significa titularidade, mas apenas um acesso justificado pelo fim terapêutico dos cuidados de saúde*".

De acordo com o art. 3º, nº1 da Lei nº 12/2005, a informação de saúde é considerada parte da vida privada do seu titular, conferindo-lhe a competência para aceder às suas próprias informações de saúde. O titular dos dados tem o direito de, sempre que possível, aceder, alterar ou corrigir as suas informações de saúde, com a premissa de que essas informações devem ser protegidas contra a curiosidade de terceiros, salvo quando houver consentimento explícito do titular para permitir o acesso por outra pessoa.

É essencial que o titular dos dados de saúde tenha acesso às suas informações para que possa tomar decisões claras e consentir livremente em intervenções médicas ou cirúrgicas, contribuindo para uma melhor prestação de serviços relacionados ao seu estado de saúde. Nesse sentido, é compreensível que o titular dos dados deseje, em muitos casos, ter acesso aos seus registos médicos. No entanto, existem exceções em que o acesso a essas informações pode ser negado se houver motivos prejudiciais à saúde do titular, visando sempre o interesse do paciente.

No processo clínico de um paciente, é importante entender que nem todas as informações nele contidas estão prontamente disponíveis para o seu acesso. Isso ocorre, principalmente, porque muitas dessas informações são anotações de natureza pessoal feitas pelo profissional de saúde, as chamadas de "*natureza não clínica"*[17]. Portanto, entende-se que essas anotações, embora façam parte do processo clínico, não devem ser acessíveis ao paciente, uma vez que são informações de propriedade do médico e resultam de sua expertise profissional, baseada nas *leges artis*.

Essa separação entre informações de caráter pessoal do profissional de saúde e os dados clínicos relevantes para o paciente é feita para preservar a privacidade do profissional de saúde e garantir que o processo de tratamento seja conduzido de maneira adequada. Assim, algumas anotações e informações podem não ser disponibilizadas integralmente ao paciente, respeitando a natureza profissional e privada dessas informações.

[17] Vide Pereira, 2013, p. 195

Para (Fernandes), 2020, p. 34: "*Assim, as anotações clínicas cuja função é melhorar a qualidade dos cuidados de saúde do utente podem ser úteis para conhecer e acompanhar o estado de saúde do utente e sua evolução. Os utentes não têm acesso, mas os profissionais de saúde sim*". De seguida, a autora faz referência ao pensamento de André Gonçalo Dias Pereira, dizendo que:

> a separação entre o processo clínico, enquanto suporte material e a própria informação de saúde nele contida, tem a vantagem adicional de abrir caminho para a criação de soluções que se destinem a tutelar direitos de terceiros, como por exemplo, os direitos de personalidade de familiares do utente, no caso da informação genética e do próprio médico, considerando, sobretudo as suas anotações pessoais (que podem constar do suporte utilizado). (Fernandes), 2020, p. 35.

Podemos considerar que o direito de acesso aos dados de saúde pertence, em primeira instância, ao seu titular. No entanto, existem situações em que o titular pode delegar o acesso a esses dados a terceiros, desde que haja consentimento prévio.

Essa delegação deve obedecer a princípios da proporcionalidade e boa-fé, garantindo que o terceiro tenha acesso apenas às informações necessárias, visando o benefício do titular que concedeu o acesso. Neste sentido, partimos do pressuposto de que, quando o interesse em questão for especialmente pessoal, legítimo e de terceiros, o acesso deve ser limitado ao estritamente necessário para salvaguardar os direitos constitucionalmente protegidos do titular dos dados.

Assim, o acesso a dados de saúde por terceiros deve ser cuidadosamente avaliado, levando em consideração a necessidade e a finalidade específica desse acesso, bem como os direitos e interesses do titular dos dados. A restrição do acesso é uma medida de proteção dos direitos e da privacidade do titular, assegurando que apenas as informações relevantes sejam compartilhadas com terceiros, de acordo com os princípios legais e éticos estabelecidos.

O titular dos dados deve aceder às suas informações pessoais por intermédio de um profissional de saúde qualificado. Ao envolver um profissional de saúde nesse processo, garantimos que a divulgação das informações seja feita de maneira responsável e segura. O profissional será capaz de fornecer orientações adequadas, interpretar os dados e esclarecer eventuais dúvidas do paciente, assegurando que ele compreende plenamente a sua situação de saúde. Além disso, fortalecemos a relação de confiança entre o paciente e a equipa médica, fomentando uma abordagem colaborativa e empática no cuidado à saúde.

A presença do profissional de saúde no acesso às informações de saúde é fundamental para evitar erros de interpretação por parte do paciente. O profissional pode contextualizar as informações, explicar terminologias técnicas e fornecer orientações personalizadas com base nas necessidades e condições do paciente.

É importante reconhecer que os utentes muitas vezes estão numa posição vulnerável, em busca de cuidados de saúde e confiando no conhecimento e na experiência dos respetivos profissionais. Essa dependência resulta da sua condição de vulnerabilidade e leva-os a depositar confiança no profissional de saúde, que detém um estatuto profissional e uma posição de autoridade. Nesse sentido, é fundamental que as relações estabelecidas entre ambas as partes sejam norteadas por princípios bioéticos, como justiça, boa-fé e dignidade da pessoa humana, que são consagrados constitucionalmente.

Esses princípios bioéticos são essenciais para garantir uma relação equilibrada, ética e respeitosa entre os profissionais de saúde e os pacientes. Eles estabelecem um padrão de conduta que promove a proteção dos direitos e a preservação da autonomia do paciente, ao mesmo tempo em que reconhecem a responsabilidade e o dever dos profissionais de saúde no que toca a fornecer cuidados de qualidade e respeitar a privacidade dos dados de saúde dos utentes.

É imperioso lembrar que, em algum momento, qualquer pessoa pode precisar recorrer às instituições de saúde em busca de cuidados e tratamentos. Nesse sentido, é fundamental que sejamos tratados com dignidade e respeito, evitando as negligências e descuidos por parte das instituições ou profissionais de saúde que lidam diariamente com vidas humanas. Isso implica exigir que as instituições de saúde e os profissionais estejam devidamente preparados, atualizados e comprometidos com a prestação de cuidados de qualidade, respeitando os direitos dos pacientes e garantindo a proteção de seus dados de saúde.

A defesa desses princípios éticos é fundamental para garantir a justiça, a equidade e a qualidade no atendimento em saúde, além de fortalecer a confiança dos utentes no sistema de saúde. Devemos continuar a promover a conscientização sobre essas questões, a fim de assegurar que os direitos dos pacientes sejam respeitados e que todos sejam tratados com

dignidade, independentemente de sua condição de saúde ou de qualquer outra circunstância[18]. Cf, Data Vénia, (Fernandes), p. 31-38.

É importante ressaltar que o direito de acesso às informações de saúde, embora seja um direito fundamental do titular, não é absoluto. Em certas circunstâncias, quando o acesso a essas informações possam causar danos à vida do titular ou causar instabilidade psicológica, este pode ser negado ou limitado. Isso ocorre para proteger o bem-estar e a saúde mental do próprio indivíduo. Além disso, há situações em que o titular das informações de saúde está inconsciente ou não possui capacidade para tomar decisões sobre o acesso aos seus dados. Nessas situações, terceiros não terão permissão para aceder a essas informações em nome do titular, a menos que haja um consentimento prévio estabelecido ou uma autorização legal específica.

As informações de saúde pessoais de um indivíduo que está incapacitado de exercer o seu domínio mental são consideradas extremamente sensíveis e devem ser tratadas com o máximo sigilo e confidencialidade pelas entidades responsáveis pela sua guarda. O acesso a essas informações é restrito apenas a pessoas autorizadas, e será realizado sob estritas medidas de segurança e proteção da privacidade.

O equilíbrio entre o direito de acesso às informações de saúde e a proteção da privacidade e do bem-estar dos titulares é um desafio constante, e cabe aos órgãos reguladores, legisladores e profissionais de saúde estabelecerem diretrizes claras e éticas para garantir o tratamento adequado e justo dessas questões.

Analisando o Acórdão AC 0394/18[19], referente à titularidade do acesso à informação de saúde, suscitam algumas questões. Pense-se, por exemplo, no caso específico em que um filho deseja aceder às informações de saúde do seu pai, como terceiro. Existem aqui questões legais e éticas a serem consideradas. A titularidade dos dados de saúde pertence ao próprio indivíduo, ou seja, ao pai, e está relacionada com o seu direito à privacidade e proteção de dados pessoais.

---

[18] Cf, Data Vénia, (Fernandes), p. 31-38.

[19] Acórdão AC 0394/18, proferido pelo Supremo Tribunal Administrativo - STA). Obtido em: <http://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/0c71c84fe9dbf65d802582f90046182f?OpenDocument&ExpandSection=1>. Acesso em: 05 de jan. de 2023.

Conforme se depreende do Acordão acima referido, é importante ressaltar que as leis podem variar dependendo do país e do contexto jurídico específico. Em certas situações, pode haver mecanismos legais que permitam que um filho, enquanto terceiro, aceda às informações de saúde de seu pai, como em casos de tutela ou quando houver uma procuração ou autorização específica concedida pelo titular. Porém, a proteção da privacidade e dos direitos do titular dos dados de saúde deve ser levada em consideração, bem como a busca de soluções que equilibrem os interesses e necessidades de todas as partes envolvidas.

Entretanto, existem casos em que os acessos a estas informações de saúde, em princípio, estão proibidos e vedados a terceiros. Estes, apenas com o consentimento do titular, terão o respetivo acesso, desde que se limitem ao estritamente necessário para defesa dos direitos do titular, bem como o interesse do terceiro. Neste sentido, autorizado o acesso a informação sobre os dados de saúde do utente ou titular, tem de ser por intermédio de um profissional e deve ter acesso a informação de saúde apenas na medida do necessário, preservando sempre outras informações médicas que em princípio lhe estão vedadas, conforme a Lei nº 12/2005[20].

No acesso a dados de saúde, a curiosidade de um terceiro, em momento algum, deve prevalecer sobre os direitos fundamentais do titular de dados, tudo porque o direito à proteção de dados, atualmente tem sido entendido como um direito humano e por esta razão digno de proteção por todos nós.

Assim, verifica-se que não há informação que podemos considerar desnecessária, sempre que diga respeito ao seu titular devemos de protegê-la, tomar em consideração, por mais insignificante que seja.

O titular dos dados tem o direito de corrigir, retificar as informações que lhe dizem respeito, resulta da manifestação do seu direito à autodeterminação informacional. Neste contexto, sobre o acesso aos dados pelo titular, pode ler-se: "*A sua relevância manifesta-se na proteção constitucional que o artigo 8º da Carta lhes confere: 'todas as pessoas têm o direito a aceder aos dados coligidos que que lhe digam respeito*". Cf. (Cordeiro, 2020), p. 232 e 262.

[20] Lei nº 12/2005 de 26 de janeiro, nº3 do art. 3º. Informação genética pessoal e informação de saúde. Obtido em <https://dre.pt/dre/detalhe/lei/12-2005-624463>. Acesso em 28 maio 2023.

Contudo, no caso concreto, há outro entendimento no sentido de que o filho, sendo detentor de um grau parentesco direto, tem um interesse direto, legitimo e pessoal, no acesso a tais informações de saúde do seu progenitor. Estando ele inconsciente, em princípio, é legitimo que o filho aceda as informações de saúde, desde que se limite ao estritamente necessário e por intermédio de um profissional de saúde.

Em suma, seguimos o entendimento de que os dados pessoais sensíveis, sendo de caráter *pessoal*, são propriedade do seu titular, estando o seu acesso, por via de regra, vedados a todos os terceiros.

3. DIREITO À PRIVACIDADE DOS DADOS DE SAÚDE

Os dados de saúde podem ser compreendidos à luz do princípio estabelecido no artigo 26º, nº 1 da CRP e no artigo 80º do CC, que reconhecem a proteção dos direitos fundamentais de personalidade e a "reserva da intimidade da vida privada e familiar*"*.[21] A informação relacionada à saúde é considerada parte integrante desses direitos.

Na privacidade dos dados de saúde, segundo LOUIS PORTE *apud* PEREIRA (2015, p. 628-629) é fundamental estabelecer uma relação de confiança entre médico e paciente, pois "*não existe medicina sem confiança, tal como não existe confiança sem confidências nem confidencias sem segredo", Nesse sentido, o autor faz referência a*o Código Internacional de Ética Médica, que afirma o seguinte: "*o médico deve respeitar o direito do paciente à confidencialidade"*.

Ainda no entendimento do autor, existem situações éticas em que a revelação de informações confidenciais pode ser justificada. Isso ocorre quando o paciente dá o seu consentimento ou quando existe uma ameaça real e iminente para a segurança do paciente ou de terceiros, e a quebra da confidencialidade é necessária para afastar essa ameaça.

Em suma, a proteção da confidencialidade dos dados de saúde é essencial para preservar a privacidade e a dignidade dos indivíduos. A relação de confiança entre médico e paciente deve ser cultivada, garantindo que a divulgação de informações confidenciais ocorra de maneira ética e justificada, em conformidade com os princípios éticos e legais aplicáveis.

A proteção do segredo e da confidencialidade desempenha um papel fundamental na convivência comunitária, especialmente nos relacionamentos interpessoais. A preservação da

[21] Cf. (Deodato), 2017, p. 27.

privacidade é um princípio essencial que reconhece a importância de mantermos certos aspetos de nossa vida em sigilo, sem expô-los ao público em geral.

Ao confiarmos os nossos dados pessoais a um profissional de saúde, esperamos que ele os trate com o devido *cuidado*, respeitando as normas éticas e legais que regem o sigilo médico. Essas informações são intrinsecamente ligadas à nossa intimidade, envolvendo dimensões sensíveis das nossas vidas.

Quando um profissional de saúde negligencia ou desconsidera o sigilo, expondo indevidamente os nossos dados pessoais, o profissional compromete não apenas a confidencialidade das informações, mas também nossa dignidade enquanto indivíduos. A revelação não autorizada de informações privadas pode ter impacto sobre a nossa reputação, bem-estar emocional e até mesmo relações pessoais e profissionais.

É mister reconhecer que a informação de saúde do paciente está intrinsecamente vinculada à proteção da reserva da intimidade da vida privada e familiar. Portanto, essa informação está sob a responsabilidade dos profissionais de saúde, que, no exercício da sua profissão, estão sujeitos a deveres de sigilo e às normas deontológicas que regem a prática médica.

A informação de saúde do paciente, em princípio, não pode ser divulgada pelos profissionais, a menos que haja o consentimento do titular ou que a divulgação seja necessária para proteger outros interesses igualmente importantes ou de maior relevância. Isso ressalta a importância da confidencialidade como um pilar fundamental da relação médico-paciente.

Assim sendo, o sigilo médico é um princípio ético essencial que visa garantir a integridade e a confiança no sistema de saúde. Ao protegerem a informação de saúde do titular, respeitando a sua privacidade e mantendo o sigilo adequado, os profissionais de saúde demonstram o compromisso de agir em benefício do paciente, promovendo um ambiente seguro e confiável para o cuidado da sua saúde.

É importante destacar que o consentimento do titular é fundamental quando se trata da divulgação de informações de saúde. Esse consentimento deve ser expresso, livre e informado, permitindo que o paciente exerça o seu direito de decidir sobre a partilha dos seus dados médicos.

A proteção da informação de saúde do paciente está intimamente ligada à salvaguarda da reserva da intimidade da vida privada e familiar. Os profissionais de saúde têm a responsabilidade ética e legal de preservar o sigilo e o segredo médico, garantindo a confidencialidade das informações do paciente, salvo nos casos em que o consentimento do titular é obtido ou

em situações excecionais em que a divulgação é necessária para proteger interesses igualmente relevantes. Cf. Pereira (2015, p. 628 a 629), a proteção da reserva da intimidade da vida privada é fundamental na relação entre médico e paciente[22].

Os profissionais de saúde têm a responsabilidade de proteger todas as informações pessoais e familiares relacionadas ao paciente. Isso inclui dados como filiação, residência, número de telefone, estado de saúde, vida conjugal, amorosa e afetiva, eventos que ocorrem no ambiente familiar, informações transmitidas por meio de correspondência ou outros meios de comunicação, tal como acontecimentos passados que caíram no esquecimento.

No contexto da saúde, todas as informações privadas dos pacientes que o médico obtém no exercício da sua função e em decorrência dela são abrangidas pelo segredo médico. Portanto, essas informações não devem ser reveladas a terceiros sem a autorização do titular.

No entanto, é importante destacar que, no campo da saúde, a coleta de dados tem, em primeira instância, finalidades terapêuticas. Isso significa que as informações são obtidas tendo em vista o tratamento do paciente. No entanto, se o titular dos dados consentir explicitamente, essas informações podem ser utilizadas para outras finalidades que sejam benéficas para ele.

O consentimento do paciente desempenha um papel importante na definição dos limites da divulgação ou compartilhamento de informações de saúde, permitindo que ele tenha controlo sobre o uso e divulgação de seus dados pessoais.

A revelação ou divulgação arbitrárias e não justificadas de informações confidenciais, sem o consentimento do paciente, configura um ato socialmente intolerável que viola bens jurídicos protegidos criminalmente. Essas condutas podem ser punidas tanto como devassa da vida privada, nos termos do art. 192º do Código Penal, quanto como violação de segredo, de acordo com o art. 195º do mesmo código. Cf. Pereira (2015, p. 635 a 636).

Considerando que os dados de saúde estão envoltos por um manto de sigilo e pertencem à esfera privada dos seus titulares, a proteção da sua privacidade assume um caráter essencial. Estamos diante de uma violação da privacidade dos titulares dos dados, uma vez que tais informações envolvem aspetos intrínsecos de sua personalidade, que estes desejam preservar do escrutínio ou conhecimento de terceiros.

[22] Os parágrafos refletem o pensamento de Pereira (2015, p. 628 a 629).

A obtenção de acesso a dados pessoais será considerada ilícita quando o conhecimento dessas informações envolver aspetos vitais ou essenciais da personalidade dos indivíduos, a ponto de qualificar tal conhecimento por parte de terceiros como uma violação ou intrusão. Estamos diante de uma violação ou intromissão na privacidade dos titulares dos dados, uma vez que esses dados dizem respeito a dimensões mais íntimas da personalidade, relativamente às quais os titulares desejam preservar o resguardo contra a indiscrição ou conhecimento de terceiros. Cf. (Matos F. m.), 2018, p. 60.

O interesse do indivíduo em preservar sua privacidade compreende o desejo de evitar a atenção indesejada de terceiros, impedir o acesso a si mesmo e evitar a divulgação de informações pessoais. Essa dimensão da privacidade visa resguardar a esfera íntima do indivíduo, permitindo-lhe exercer controlo sobre quem tem conhecimento e acesso aos detalhes da sua vida pessoal. Trata-se, portanto, de um direito fundamental que visa proteger a autonomia e a dignidade do indivíduo, proporcionando-lhe o poder de decidir sobre a divulgação ou não de informações pessoais e resguardando sua esfera de intimidade dos olhos e dos ouvidos alheios. Cf. Pinheiro (2015, p. 771).

A proteção da privacidade vai além do conceito restrito de intimidade da vida privada ou do ambiente familiar, cf, artigo 26º, nº 1 da CRP. Compreendemos que o direito à privacidade não se limita ao espaço íntimo do lar ou da família. Uma pessoa não é apenas privada, íntima ou reservada quando está dentro da sua casa. Em qualquer espaço público a pessoa continua a ter uma esfera privada ao seu redor, sem que os outros possam invadir essa esfera pessoal, cf. Pinheiro (2015, p. 773).

Assim compreendemos que, os profissionais de saúde, ao preservarem a privacidade dos titulares, estes estarão a observar os princípios éticos, e constitucionais que protegem os direitos fundamentais dos pacientes. É típioco de um Estado de Direito democrático, valorizar entre outros, o direito à reserva da intimidade da vida privada, art. 26º, nº 1 da CRP, o direito à dignidade humana, art.1º da CRP, proporcionalidade, nº 2 do art. 18º da CRP, bem como outras disposições referentes à utilização da informática nos nºs 1, 2, 3, 4 do art. 35º da CRP e na legislação civil, como a tutela geral da personalidade e a reserva da intimidade da vida privada, presentes nos artigos 70º e 80º do Código Civil.

A LPDP e RGPD protegem os dados pessoais de saúde, bem como as diversas normas jurídicas de âmbito nacional. Nesse sentido, o respeito à privacidade dos dados pessoais enquadra-se dentro da proteção do princípio da dignidade da pessoa humana. Assim, compreende-

se que a dignidade da pessoa humana não é apenas um princípio limitador no âmbito jurídico-constitucional, mas possui um valor intrínseco e uma dimensão normativa específica.
A proteção da dignidade da pessoa humana está intrinsecamente ligada à concretização do princípio "*antrópico*" ou "*personicêntrico*" que fundamenta diversos direitos fundamentais, tais como o direito à vida, o direito ao desenvolvimento da personalidade, o direito à integridade física e psíquica, o direito à identidade pessoal e o direito à identidade genética. Além disso, a dignidade humana é um princípio essencial que sustenta a igualdade, proibindo qualquer forma de discriminação ou hierarquização de dignidades: tanto as pessoas consideradas "deficientes", "criminosas" ou "desviantes" possuem a mesma dignidade que aquelas consideradas "normais" ou "padrão", cf. (Canotilho & Moreira, 2014), p. 198-199.
Pelo exposto, entendemos que a dignidade humana é de caráter nuclear para a afirmação da nossa personalidade, esta permite-nos aceitar e reconhecer o outro como nosso semelhante, traduzindo uma representação única de uma essência humana comum. É à luz desse prisma que a dignidade humana se revela como um limite essencial à atuação dos poderes do Estado, resguardando a integridade e os direitos fundamentais de cada ser humano.

4 PRINCÍPIOS FUNDAMENTAIS NO TRATAMENTO DOS DADOS DE SAÚDE

A proteção dos dados pessoais de saúde é regida por várias leis, com o objetivo de garantir a privacidade e os direitos dos titulares desses dados. Tratando-se de dados pessoais, dispõe a Lei de Proteção de Dados Pessoais (LPDP), nº 58/2019[23], que assegura a execução da RGPD. No contexto do RGPD e da LPDP, existem disposições específicas relacionadas ao tratamento de dados de saúde:

(i) De acordo com o RGPD, os dados de saúde são considerados dados pessoais sensíveis e estão sujeitos a uma proteção especial. O Art. 4º, nº 15 do RGPD define os "dados relativos à saúde" como dados relacionados com a saúde física ou mental de uma pessoa, incluindo a prestação de serviços de saúde que revelem informações sobre o estado de saúde dessa pessoa.
(ii) A LPDP também aborda o tratamento de dados de saúde, incluindo os dados genéticos. O Artigo 29º, nº 1 da LPDP menciona explicitamente o tratamento de dados de saúde e dados genéticos como categorias especiais de dados pessoais que requerem proteção adicional.
(iii) Além disso, o Artigo 9º, nº 2, alínea h, do RGPD, especifica que o tratamento de dados de saúde é permitido quando é necessário para fins de prestação de cuidados de saúde ou tratamentos médicos, bem como a gestão de sistemas e serviços de saúde.

[23] Lei de Proteção de Dados Pessoais (LPDP) nº 58/2019, de 8 de agosto. Diário da República. Obtido em <https://dre.pt/dre/detalhe/lei/58-2019-123815982>. Acesso em 28 maio 2023.

(iv) A Lei nº 12/2005[24] também trata da informação de saúde, estabelecendo diretrizes específicas para a proteção e o tratamento adequado desses dados.

Essas leis e regulamento,visam proteger a privacidade, a confidencialidade e os direitos dos titulares de dados de saúde, garantindo que seu tratamento seja realizado de forma legal, transparente e segura.

Assim sendo, no tratamento dos dados pessoais de saúde, é fundamental observar diversos princípios que visam a proteção adequada dessas informações sensíveis, dentre eles citamos alguns:

i. Princípio da Privacidade: Os dados pessoais de saúde devem ser tratados com o mais alto grau de confidencialidade e proteção. Isso implica que apenas pessoas autorizadas tenham acesso a esses dados e que sejam tomadas medidas de segurança apropriadas para evitar o acesso não autorizado[25]. Cf. nº1 do art. 26º da CRP e art. 5º nº 1, f) do RGPD.
ii. Princípio da Autodeterminação Informacional: Os titulares dos dados têm o direito de exercer controlo sobre suas informações de saúde. Isso significa que devem ser informados sobre como seus dados serão usados, quem terá acesso a eles e quais são seus direitos em relação ao tratamento dos dados em questão[26]. Cf. art. 35º da CRP e art. 15º do RGPD.
iii. Princípio do Consentimento: Em muitos casos, o consentimento do titular dos dados é necessário para o tratamento de seus dados de saúde. O consentimento deve ser obtido de forma clara, específica e informada, permitindo que a pessoa tome uma decisão consciente sobre o uso de seus dados[27]. Cf. nº 11 do art. 5º do RGPD, e art. 20º do Regulamentado Deotologia Médica, Lei nº 707/2016[28].
iv. Princípio da Minimização de Dados: A coleta e o tratamento de dados de saúde devem ser limitados ao mínimo necessário para alcançar a finalidade específica para a qual os dados estão sendo processados. Isso implica que apenas as informações

[24] [24]Lei nº 12/2005, de 26 de janeiro. Obtido em <https://dre.pt/dre/detalhe/lei/12-2005-624463>. Acesso em 28 maio 2023.
[25] Vide PASSINI, Rosana Principe. Implicações éticas do princípio da privacidade na interação médico-paciente. 2019. 210 f., il. Tese (Doutorado em Ciências da Saúde) - Universidade de Brasília, Brasília, 2019.
[26] Vide SABEC, Daniel Augusto; SIMÃO FILHO, Viana Adalberto. Democracia, Propaganda Eleitoral e Proteção de Dados. Anais do Congresso Brasileiro de Processo Coletivo e Cidadania, n. 8, p.156-173, out/2020, p. 158. Obtido em <https://revistas.unaerp.br/cbpcc/article/view/2190/1598>. Acesso em 13 fev. 2023.
[27] Vide LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de; Da Evolução das Legislações sobre Proteção de Dados: A Necessidade de Reavaliação do Papel do Consentimento como Garantidor da Autodeterminação Informativa. Revista De Direito | Viçosa, 2020, p. 15 - 20. Obtido em <https://www.repositorio.ufop.br/bitstream/123456789/14359/1/ARTIGO_Evolu%c3%a7%c3%a3oLegisla%c3%a7%c3%b5es-Prote%c3%a7%c3%a3o.pdf>. Obtido em 12 fev 2023.
[28] Regulamento de Deontologia Médica, n.º 707/2016, de 21 de Julho, nº 2, art. 40º. Obtido em <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2649&tabela=leis&ficha=1&pagina=1&so_miolo=#:~:text=1%20%2D%20O%20m%C3%A9dico%2C%20no%20exerc%C3%ADcio,no%20exerc%C3%ADcio%20das%20fun%C3%A7%C3%B5es%20cl%C3%ADnicas.>. Acesso em 28 maio 2023.

relevantes e essenciais devem ser coletadas e mantidas[29]. Cf. c) do nº 1 do art. 5º, do RGPD.

v. Princípio da Finalidade: Os dados de saúde devem ser coletados e utilizados apenas para fins legítimos e específicos. É importante que os fins do tratamento sejam claramente definidos e comunicados aos titulares dos dados[30].Cf. b) do nº1 do art. 5º RGPD.
vi. Princípio da Transparência: Os titulares dos dados devem ser informados de forma clara e transparente sobre o tratamento de seus dados de saúde, incluindo a finalidade do processamento, os destinatários dos dados e seus direitos em relação ao tratamento[31]. Cf. nº 1 do art. 5º RGPD.
vii. Princípio da Retenção Limitada: Os dados de saúde devem ser mantidos apenas pelo tempo necessário para cumprir a finalidade do tratamento, respeitando os prazos legais e regulamentares aplicáveis[32]. Cf. e) do nº1 do art. 5º do RGPD.
viii. Princípio da Responsabilidade: As instituições de saúde e os profissionais médicos devem assumir a responsabilidade pela proteção dos dados pessoais de saúde, implementando medidas adequadas de segurança, controlo e gestão dos dados[33]. Cf. nº 2 do art. 5º do RGPD.
ix. Princípio da Não Discriminação: Os dados de saúde não devem ser usados para discriminar ou prejudicar os titulares dos dados, garantindo que o tratamento seja realizado de forma justa e equitativa[34]. Cf. 13º CRP e 9º 1 do RGPD.

Estes são apenas alguns exemplos dos princípios que devem ser considerados no tratamento ético e legal dos dados pessoais de saúde. Entretanto, a sua aplicação pode variar dependendo da legislação e regulamentação específica de cada país. Porém, é essencial que as instituições de saúde, os profissionais médicos e as partes envolvidas respeitem esses princípios para garantir a privacidade, a segurança e os direitos dos titulares dos dados de saúde.

[29] Vide NETO BARROS, Inocêncio. Proteção de Dados na Computação em Nuvem. 2021, Dissertação para obtenção do Grau de Mestre em Informática, p. 43. Obtido em <https://co-mum.rcaap.pt/bitstream/10400.26/39868/1/99991908_Inoc%c3%aancio_Barros.pdf> Acesso em 12 fev. 2023.

[30] Ibdem, p. 14.

[31] Idbem, p. 14.

[32] Idbem, p. 43.

[33] BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. 2020, p. 19-21. Obtido em <https://civilistica.emnuvens.com.br/redc/article/view/662/506>. Acesso em 12 fev 2023.

[34] BONDO, Pitra António dos Santos. Princípio da Não Discriminação. Dissertação de Mestrado. Universidade Católica Portuguesa, Porto; Junho 2015, p. 12-28. Obtido em <https://repositorio.ucp.pt/bitstream/10400.14/18259/1/FINAL_Tese%20Pitra%20Bondo.pdf>. Acesso em 28 fev. 2023.

5 PAPEL DO ENCARREGADO DE PROTEÇÃO DOS DADOS DE SAÚDE

O encarregado de proteção de dados, também conhecido como *Data Protection Officer* - DPO[35], desempenha um papel fundamental na proteção dos dados pessoais, incluindo os dados de saúde. Assegura que a organização esteja em conformidade com as leis e regulamentos de proteção de dados, incluindo a legislação específica relacionada aos dados de saúde.

O encarregado de proteção de dados atua como um especialista na área de proteção de dados e é designado pelo responsável pelo tratamento dos dados ou pelo subcontratante. A sua função principal é supervisionar as atividades internas da organização em relação à proteção de dados e garantir que todas as operações estejam em conformidade com as leis e regulamentos aplicáveis.

Além disso, o encarregado de proteção de dados é responsável por acompanhar as mudanças e atualizações na legislação de proteção de dados, garantindo que a organização esteja atualizada e adaptada às novas exigências legais. Ele também desempenha um papel importante na identificação e prevenção de possíveis violações de proteção de dados, bem como na gestão de incidentes de segurança e no estabelecimento de medidas de segurança adequadas.

Em resumo, o EPD desempenha um papel crucial na garantia da conformidade legal e na proteção dos direitos fundamentais dos titulares dos dados, incluindo os seus direitos em relação aos dados de saúde. A sua atuação contribui para a promoção da confiança e transparência no tratamento de dados pessoais no âmbito da organização.

O EPD, deve ser designados com base nos seus conhecimentos em matérias de dados pessoais. Cf. art. 37º, 5 do RGPD. A designação de juristas como encarregados de proteção de dados é frequentemente preferida, pois estes possuem um conhecimento aprofundado das leis e regulamentos relacionados à proteção de dados. Outros profissionais com especialização em proteção de dados e experiência prática também podem desempenhar essa

[35] DPO (*Data Protection Officer)* figura o Delegado de proteção de dados, implantado com a entrada em vigência da RGPD*,* Obtido em <https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en>. Acesso em 28 fev 2023.

função, desde que possuam as qualidades e habilidades necessárias para cumprir as funções estabelecidas no artigo 39º do RGPD.

O encarregado de proteção de dados atua como conselheiro e intermediário entre a organização, os titulares dos dados e a autoridade de controlo, que no caso de Portugal é a CNPD. A colaboração com a autoridade de controlo é uma parte essencial do trabalho do encarregado de proteção de dados. Este coopera, fornecendo informações necessárias, respondendo a consultas e participando de processos de avaliação de conformidade. Essa colaboração visa garantir que a organização esteja em conformidade com as obrigações legais e promover a transparência e a confiança no tratamento de dados pessoais. O EPD, além de promover o aconcelhamento interno sobre o funcionamento do RGPD, garante a segurança no tratamento de dados pessoais.

Além da obrigação do responsável pelo tratamento de dados ou subcontratante de designar um encarregado de proteção de dados qualificado, o próprio encarregado de proteção de dados também está sujeito a obrigações de confidencialidade e sigilo. O encarregado de proteção de dados deve manter a confidencialidade das informações às quais tem acesso no exercício de suas funções. Isso inclui não apenas as informações relacionadas aos dados pessoais tratados e aos processamentos realizados, mas também as informações relacionadas à própria atividade da entidade que o nomeou, tanto no presente como no futuro. Essa obrigação de confidencialidade visa garantir a proteção dos dados pessoais e a preservação da integridade e segurança das informações relacionadas ao tratamento de dados.

O EPD, Protege a privacidade das informações envolvidas. O incumprimento das obrigações de confidencialidade por parte do DPO pode resultar em consequências legais, incluindo a possibilidade de imposição de sanções ou penas. Portanto, é essencial que o encarregado de proteção de dados trate as informações confidenciais com o devido cuidado e diligência, garantindo sua segurança e sigilo adequados, Cf. (Andrade, 2020), p. 31.

Subscrevemos da perspetiva exposta anteriormente e percebemos que não implica necessariamente que outros profissionais não possam ser contratados para desempenhar as funções de EPD, pode sim, desde que estes, profissionais possuam um entendimento aprofundado das atividades realizadas pelo responsável ou subcontratante. Demonstrarem

responsabilidade mínima e competência técnica para desempenhar as tarefas relacionadas ao domínio da proteção de dados pessoais.

No cumprimento das suas responsabilidades, esses profissionais têm autonomia para emitir recomendações, aconselhando as empresas a agirem em conformidade com a legislação de proteção de dados. Além disto, estes, não tomam decisões vinculativas sobre questões relacionadas à proteção de dados, porque a decisão final sobre o cumprimento ou não da lei cabe à empresa, representada pelo responsável pela proteção de dados.

Dessa forma, reconhecemos a importância de garantir que o encarregado de proteção de dados seja adequadamente qualificado e especializado e atue com máxima diligência na proteção da privacidade dos dados de saúde. Esses profissionais desempenham um papel consultivo e auxiliam as empresas a conformarem as suas práticas às exigências da proteção de dados pessoais, por meio de recomendações devidamente sustentadas no seu conhecimento técnico. No entanto, a responsabilidade final pela conformidade com a lei recai sobre a empresa, na figura do responsável pela proteção de dados[36]. Em contrapartida:

> (…) quanto ao controlo que passa a ser efetivado pela autoridade nacional de proteção de dados, esta entidade vê reduzidos os poderes de controlo prévio, passando a sua intervenção a assentar essencialmente numa atuação a posteriori traduzida em funções de fiscalização, regulação, de sancionamento, instituindo-se designadamente que, em caso de violação de dados pessoais suscetível de gerar risco para os direitos dos titulares, deve o responsável pelo tratamento notificar esse fato à autoridade de controlo competente, num período de 72h, bem como ao titular dos dados, sem demora injustificada, quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os seus direitos e liberdades." Cf, (Calvão & Maçãs, 2020), p. 47.

Para (Cordeiro, 2020), p. 363, este entendimento parece estar alinhado com a proteção pretendida pela lei, pois, em primeiro lugar, o responsável pelo tratamento e o encarregado de proteção de dados procuram internamente analisar se o tratamento dos dados dos titulares está integralmente em conformidade, garantindo que os dados sensíveis estejam devidamente protegidos e invioláveis, dada a sua natureza especial. O objetivo é garantir a conformidade com o RGPD e evitar eventuais sanções por parte da autoridade reguladora.

Nesse sentido, a obrigação de designar encarregados de proteção de dados não se limita apenas aos responsáveis e encarregados cuja atividade principal seja o tratamento de dados pessoais, abrangendo também todos aqueles cuja atividade principal envolva o tratamento

[36] Vide (Andrade, 2020), p. 27-30.

de dados pessoais. Os exemplos fornecidos pelo GT 29 (atual Comité Europeu para a Proteção de Dados)[37] são esclarecedores nesse sentido:

> No caso de um hospital, a sua atividade principal é a prestação de cuidados de saúde. No entanto, um hospital não poderia fornecer cuidados de saúde de maneira segura e eficaz sem o tratamento de dados de saúde, como os registos de saúde dos pacientes. Portanto, o tratamento desses dados deve ser considerado uma das atividades principais de qualquer hospital, tornando-se necessário a nomeação de encarregados de proteção de dados.
> Noutro exemplo, uma empresa de segurança privada realiza a vigilância de centros comerciais privados e espaços públicos. A vigilância é a atividade principal da empresa, que está intrinsecamente ligada ao tratamento de dados pessoais. Portanto, essa empresa também deve designar um encarregado de proteção de dados.

Esses exemplos ilustram como a nomeação de encarregados de proteção de dados é abrangente e se aplica a todas as entidades cujas atividades principais envolvam o tratamento de dados pessoais, independentemente do setor em que atuam conforme entendimento de (Cordeiro, 2020), p. 363.

Nos cuidados de saúde, a proteção dos registos clínicos dos pacientes é de extrema importância, uma vez que se valoriza a preservação da sua privacidade e confidencialidade. Nesse contexto, o encarregado de proteção de dados (EPD), desempenha um papel fundamental na supervisão das atividades das entidades coletivas, garantindo a segurança e conformidade dos dados, bem como o cumprimento das disposições estabelecidas pelo RGPD.

A presença do encarregado de proteção de dados é indispensável, especialmente quando se trata de tratamento de dados pessoais sensíveis em grande escala. Cf, alínea c), nº1 do art.37º e art. 9º do RGPD. Essa designação torna-se obrigatória, garantindo assim o cumprimento das diretrizes e normas de proteção de dados estabelecidas pelo regulamento.

Para a tarefa de EPD, pode-se designar não apenas pessoas físicas, mas como também pessoas jurídicas, como veremos abaixo em Cordeiro, a propósito do (GT29). Assim sendo, os resresponsáveis pelo tratamento de dados pessoais têm a possibilidade de buscar serviços de consultoria de outras entidades especializadas em proteção de dados, a fim de proteger os seus interesses e os interesses dos titulares de dados. O Grupo de Trabalho do Art. 29

[37] Grupo de Trabalho do Artigo 29.º. Obtido em <https://edpb.europa.eu/par-edak/vairak-par-edak/article-29-working-party_pt>. Acesso em 29 maio 2023.

(GT29)[38] considera que a função de encarregado de proteção de dados também pode ser desempenhada por uma pessoa jurídica, desde que cada membro da organização que exerça essa função atenda a todos os requisitos aplicáveis. Dessa forma, a contratação de consultorias externas ou a nomeação de pessoas coletivas para agirem como EPD pode ser uma estratégia adotada pelos responsáveis pelo tratamento de dados para garantir uma gestão eficiente e em conformidade com as obrigações legais de proteção de dados. (Cordeiro, 2020), p. 368.

Cremos que ao proporcionar-se um modelo alargado da figura do DPO, quer designando pessoa física ou jurídica para o desempenho das funções de EPD, quer-se garantir maior alternativa aos responsáveis na escolha da contratação de mais pessoas especializadas na proteção de dados pessoais. Essa abordagem visa proteger e prevenir violações recorrentes das leis de proteção de dados e dos direitos dos titulares dos dados. Ao incluir pessoas jurídicas na função de EPD, busca-se fortalecer a conformidade com as regulamentações de proteção de dados e garantir uma gestão eficaz e responsável das informações pessoais.

Com base no exposto, podemos observar que as organizações que atuam no setor de cuidados de saúde têm a obrigação de designar um EPD que garanta o cumprimento das normas estabelecidas pelo RGPD. O EPD desempenha um papel fundamental ao emitir opiniões e orientações que visam garantir a conformidade com as boas práticas no tratamento de dados pessoais por parte dos responsáveis e subcontratantes.

Neste sentido, aproteção da privacidade dos dados, está inteiramente ligada ao dever de sigilo reservado aos funcionários. Pois, a violações das informações de saúde por parte dos profissionais estão sujeitas a sanções disciplinares, e o não cumprimentos do EPD, com as suas obrigações poderá originar sanções de natureza contraordenacional.

A obrigação de sigilo das informações está consagrada no regime jurídico do artigo 4º da Lei nº 12/2005 de 26 de janeiro, alterada pela Lei nº 26/2016 de 22 de agosto, estabelecendo que os profissionais responsáveis pelo tratamento das informações de saúde, devem tomar

[38] Grupo de Trabalho do Artigo 29.º (GT do artigo 29.º), criado pela Diretiva 95/46/CE. Adotadas em 13 de dezembro de 2016.

todas as precauções necessárias, para garantir a segurança das instalações, equipamentos, e o acesso destas, bem como protegendo o sigilo. Cf. (Deodato), p. 31 a 32.

Em síntese, violando-se as regras de segurança e do sigilo relacionadas à proteção de dados pessoais, poderá resultar a aplicação de sanções, esta, será determinada com base na avaliação da culpa e do tipo de infração cometida, classificadas como muito graves, graves ou leves.

Concordamos com o entendimento dos autores acima referidos, pois, a implementação de uma sólida política de segurança de dados pessoais de saúde por parte das entidades responsáveis, juntamente com a adesão a princípios deontológicos nos cuidados de saúde, contribuirá para preservar a privacidade dos titulares de dados. Isso, por sua vez, ajudará a evitar a imposição de sanções disciplinares e contraordenacionais sobre os profissionais envolvidos[39].

A CNPD quer evitar constantes violações dos dados pessoais pelas empresas, que se dedicam a colheita e tratamento de dados, recomenda boas práticas aos responsáveis para que designem um EPD, para melhor proteção dos dados dos titualares.Cf, 37º ss do RGPD e 9º ss LPDP.

6 RELEVÂNCIA DO CONSENTIMENTO NO TRATAMENTO DE DADOS DE SAÚDE

O consentimento é fruto de uma vontade autónoma da pessoa. Cf, art. 4º/11 do RGPD. É nesse sentido que o seu titular deve manifestá-lo de modo livre, específico, informado e explícito. Por outras palavras, o silêncio, as opções pré-selecionadas ou a falta de manifestação não podem ser considerados como constituindo consentimento válido.

Quando o titular dos dados não tem uma escolha verdadeiramente livre nem pode recusar ou retirar o consentimento sem sofrer prejuízos, diz-se que o consentimento não foi dado de forma livre. Portanto, as organizações devem investigar como e em que circunstâncias é obtido o consentimento, a fim de garantir sua validade.

Cabe ao responsável pelo tratamento dos dados comprovar que o titular deu seu consentimento para o processamento dos dados (Artigo 7º, nº 1 do RGPD). Se o consentimento tiver

[39] Curso ministrado por (Pereira A. , I Curso de Pós-Graduação Avançada em Direito da Proteção de Dados, 2020).

sido dado por escrito num documento relacionado a outros assuntos, deve estar claramente redigido numa linguagem compreensível, de fácil acesso e destacado dos demais assuntos do documento (Artigo 7º, nº 2).

Além disso, o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento (Artigo 7º, nº 3). No caso do consentimento de menores ou de seus representantes legais, devem ser observados os requisitos específicos estabelecidos no regulamento (Artigo 8º do RGPD).[40]

Dada a natureza intrinsecamente pessoal do direito em questão, que pertence exclusivamente ao paciente, é ao próprio que cabe o direito de dar o seu consentimento para uma intervenção médica, desde que se encontre capaz de discernir e julgar de maneira adequada. Privar alguém dessa decisão, pessoalíssima, seria uma forma de interferir na própria essência humana, o que é totalmente inaceitável.

O exercício do direito à autodeterminação no contexto dos cuidados de saúde e da livre disposição da integridade física deve ser guiado pelo princípio da autonomia. Sempre que a pessoa esteja capacitada para consentir, cabe exclusivamente a ela, com plena soberania, tomar decisões sobre os cuidados de saúde a serem prestados. Cf. Pereira (2004, p. 205).

No contexto dos cuidados de saúde, destaca-se um caso relevante (AC do TCAN Proc nº 00884/12.BEBRG)[41], envolvendo a violação do consentimento informado por parte de um médico de um hospital público. Neste caso específico, o médico realizou uma intervenção médico-cirúrgica num paciente sem informá-lo sobre possíveis riscos conhecidos e associados ao procedimento.

É fundamental que as intervenções médicas e cirúrgicas sejam conduzidas com a devida prestação de informações precisas, claras e exatas aos pacientes, antes da execução do procedimento, a fim de permitir que o paciente possa consentir de maneira segura, livre e consciente, exercendo sua autonomia e direito à autodeterminação informada.

---

[40] Cf. Nunes Ferreira Alexandre Gonçalo, O tratamento de dados pessoais de saúde à luz do regulamento Geral Europeu de Proteção de dados pessoais, p. 15, 2019, Coimbra.

[41] AC do Tribunal Central Administrativo Norte - TCAN, 30/10/2020 (Proc. nº 00884/12.BEBRG). Obtido em <http://www.gde.mj.pt/jtcn.nsf/89d1c0288c2dd49c802575c8003279c7/3839bd8185d5c6e38025861d00443c68>. Acesso em 22 fev 2023.

Como resultado dessa conduta, o hospital foi condenado pelo tribunal *a quo*, que determinou o pagamento de uma indemnização de mil euros por danos não patrimoniais causados ao paciente, decisão ratificada pelo tribunal *ad quem*.

Com efeito, é compreensível que a falta dessas informações possa resultar em responsabilidade civil por parte do profissional de saúde, que tem o dever de garantir os direitos dos titulares de dados. A decisão foi amparada, dentre outras normativas, pelos art.s 494º, 496º, nº1, 4 e 566º nº3 do Código Civil.

Por fim, o processo foi submetido ao Supremo Tribunal Administrativo que, em 16/12/2021, emitiu nova decisão (AC 0884/12.0BEBRG)[42], reconhecendo a violação do dever de infomaçao, aplicando uma indemnização ao hospital, proporcional à gravidade do dano sofrido pela paciente, no valor de 16 mil euros, a título de danos não patrimoniais.

Nesse sentido, à luz da reflexão de Pereira (2021, p. 15 - 41)[43] a decisão do Acórdão em referência foi aclamada, pelo aumento do valor inicialmente arbitrado, e conclui que "*não há diminuição de cidadania no âmbito do SNS"*. Para Pereira (2021, p. 41):

> Estamos convictos de que a notícia desta condenação (ainda que os montantes não sejam elevados) sinalizarão junto dos profissionais de saúde, em especial os médicos, e as administrações hospitalares (também dos hospitais públicos) a necessidade de cumprirem e fazerem cumprir a lei, a deontologia e a ética e intensificar o respeito pelos direitos dos doentes, designadamente o direito a tomar decisões livres, informadas e esclarecidas.

Assim, à luz do acórdão em questão, fica evidente que o direito dos pacientes a receber informações precisas, esclarecidas e conscientes sobre os riscos associados a uma intervenção médico-cirúrgica nos seus corpos é crucial para que possam tomar uma decisão informada sobre a realização do procedimento.

A figura do consentimento, é essencial, porque reflete a autonomia do individuo, em consentir ou não na prática de atos médicos.

---

[42] Acórdão do Supremo Tribunal Administrativo, 16/12/2021, (Proc. 0884/12.0BEBRG). Obtido em <http://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/1d48c6e74692b044802587b8005f1610?OpenDocument&ExpandSection=1#_Section1>. Acesso em 31 maio 2023.

[43] PEREIRA, André Gonçalo Dias. Relatório Justiça Administrativa e Fiscal - Qualidade e Celeridade - Impasses e Soluções. O Acórdão do Supremo Tribunal Administrativo de 16 de dezembro de 2021 (1 Secção; Relator: Cons. Carlos Carvalho (proc. 0884/12.0BEBRG) - um passo decisivo para proteção do direito ao consentimento informado nos hospitais públicos. ASJP. Obtido em <https://www.asjp.pt/wp-content/uploads/2023/01/EBOOK-2-Justic%CC%A7a-Administrativa-e-Fiscal_Intervenc%CC%A7o%CC%83es-Confere%CC%82ncia_23.12.2022.pdf>. 2022, p. 15-41. Acesso em 31 de maio 2023.

Verificando-se os requisitos da autonomia, presume-se que o paciente está em condições de consentir na prática de determinado ato, salvo haver motivos atendiveis, que impeçam o titluar de dar o seu consetimento, como estado de incapcidade.

Havendo falta de capacidade para consentir é relevante destacar que o tratamento de dados especiais requer uma condição adicional: o tratamento só é permitido quando se comprove que o titular dos dados está física ou legalmente incapacitado de dar seu consentimento.

Essa exigência de incapacidade física ou legal abrange uma ampla gama de situações em que não é possível obter o consentimento do titular, seja de forma temporária ou permanente, devido a condições como doença, acidente ou até mesmo desaparecimento. No entanto, mesmo nessas circunstâncias, é necessário analisar, com base em critérios objetivos, a vontade presumida do titular dos dados, a fim de garantir uma proteção adequada de seus direitos. Cf. (Cordeiro, 2020), p. 243.

Ao refletir sobre a dualidade das incapacidades e a necessidade de considerar a vontade hipotética do titular dos dados, reconhecemos a importância de um equilíbrio entre a proteção dos direitos individuais e a necessidade legítima de tratamento de dados para fins específicos. Essa abordagem cautelosa e baseada em critérios objetivos ajuda a assegurar a integridade do sistema de proteção de dados pessoais, promovendo a transparência, a responsabilidade e o respeito à privacidade dos indivíduos em todas as circunstâncias.

7 INFORMAÇÕES DE SAÚDE

As informações de saúde são consideradas dados sensíveis e possuem uma natureza especial devido à sua relação direta com a intimidade e a vida privada das pessoas. Esses dados abrangem informações sobre o estado de saúde, tratamentos médicos, histórico médico, condições genéticas, entre outros aspectos relacionados à saúde física e mental dos indivíduos.

Em virtude da sua sensibilidade e potencial impacto na vida das pessoas, a proteção e o tratamento adequado das informações de saúde são temas de grande relevância jurídica e ética. As informações de saúde podem levar à identificação do titular dos dados pessoais, conforme estabelecido no artigo 3º da Lei nº 12/2005, que dispõe o seguinte:

> 1 - A informação de saúde, incluindo os dados clínicos registados, resultados de análises e outros exames subsidiários, intervenções e diagnósticos, é propriedade da pessoa, sendo as unidades do sistema de saúde os depositários da informação, a qual não pode ser utilizada para outros fins que não os da prestação de cuidados e a investigação em saúde e outros estabelecidos pela lei.

> 2 - O titular da informação de saúde tem o direito de, querendo, tomar conhecimento de todo o processo clínico que lhe diga respeito, salvo circunstâncias excepcionais devidamente justificadas e em que seja inequivocamente demonstrado que isso lhe possa ser prejudicial, ou de o fazer comunicar a quem seja por si indicado.
> 3 - O acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento ou nos termos da lei, é exercido por intermédio de médico, com habilitação própria, se o titular da informação o solicitar.
> 4 - Na impossibilidade de apuramento da vontade do titular quanto ao acesso, o mesmo é sempre realizado com intermediação de médico.[44]

As informações de saúde desempenham um papel de extrema importância no contexto dos direitos, liberdades e garantias. Por se tratar de dados sensíveis, tanto as entidades públicas quanto as privadas e outros envolvidos buscam preservar a integridade e confidencialidade dessas informações pessoais de natureza delicada. Além disso, procura-se salvaguardar a esfera de segredo do indivíduo, reconhecendo-o como o proprietário dos registos clínicos e dos dados de saúde que lhe dizem respeito. Assim, somente o titular desses dados de saúde tem o poder de consentir o acesso à suas informações por terceiros. Essa proteção visa garantir a privacidade e a autonomia do indivíduo no que diz respeito às suas informações de saúde.

Dessa forma, busca-se evitar a interferência indevida de terceiros na vida privada do titular dos dados. Portanto, é de extrema importância considerar a responsabilidade de cada uma das partes envolvidas na relação jurídica, a fim de não ultrapassar os princípios de proporcionalidade, ética e valores que regem as relações médicas. Isso visa proporcionar uma melhor assistência nos cuidados de saúde do paciente, sempre protegendo a dignidade da pessoa humana. Esse é um princípio civilizacional dos Estados democráticos e de Direito, que busca assegurar a integridade e o respeito aos direitos fundamentais de cada indivíduo. Cf, (Ferreira, et al., 2012).

Além disso, no âmbito do acesso às informações de saúde do titular dos dados, tem sido estabelecido que o próprio titular só pode ter acesso através de um profissional médico devidamente habilitado para essa finalidade. Cf, nº 1 do art. 15º do RGPD e nº 3 do art. 3º da Lei nº 12/2005. Esse tipo de acesso às informações do paciente ou titular de dados por meio do médico é denominado de "sistema de acesso indireto". Cf. Pereira (2015, p. 607-608).

[44] Lei 12/2005, de 26 de janeiro. Obtido em <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1660A0010&nid=1660&tabela=leis&pagina=1&ficha=1&nversao=>. Acesso em 22 maio 2023.

Nessa perspetiva, parece-nos que o titular dos dados não poderá ter acesso ou conhecimento direto sobre sua própria situação de saúde sem a existência de um profissional. Embora referira o nº 2 do art. 268º Da CRP, que o titular tenha acesso relacionada as informações, arquivos e registos administrativos que lhe digam respeito.

O acesso direto às informações de saúde é o regime predominante na Europa, incluindo nos países de tradição latina. Esse acesso direto concede ao titular dos dados o direito de ter acesso direto aos registos clínicos que se referem à sua vida, sendo que esse direito também é protegido pelo RGPD. Isso facilita o acesso às informações pessoais do titular, dentro dos limites das informações que não estão sob a sua titularidade, Cf. P. (609), 1ª edição fevereiro de 2015 e o consentimento informado na relação médico-paciente, p. 531.

Porém, a alínea a) do número 1 do artigo 15º do RGPD refere que o titular dos dados possui o direito de aceder aos dados pessoais que lhe dizem respeito, bem como obter informações sobre as finalidades do seu tratamento.

Em suma, considerando que as informações de saúde sejam exclusiva do seu titular, parece-nos que o acesso a esses dados deve ser concedido ao próprio titular. Dessa forma, defendemos a ideia de um acesso direto, em vez de um acesso indireto por meio do médico.

Porém, em muitas situações prevalecerá a prática de acesso aos dados de saúde pelo paciente de forma indireta, por meio de um profissional de saúde: há casos em que tal abordagem se justifica. Isto dá-se quando o paciente apresenta limitações extraordinárias a nível cognitivo ou na capacidade de compreensão das informações contidas nos registos clínicos. Essas limitações podem ser decorrentes de uma baixa alfabetização, falta de familiaridade com terminologia médica ou dificuldades cognitivas.

O assunto em questão é abordado à luz das reflexões apresentadas por Rosalvo Almeida no Parecer 60/CNEV/2011[45], que trata da informação de saúde e dos registos informáticos de saúde. No parecer, é ressaltado que, atualmente, são os próprios titulares dos dados que compartilham informações de saúde em conversas com amigos, muitas vezes sem saberem que essa revelação constitui uma violação da esfera íntima, que diz respeito apenas ao titular. Assim, destaca-se que a titularidade do direito de acesso às informações pessoais pelo titular deriva do direito à autodeterminação, permitindo que este possa consentir livremente na prática do ato médico.

[45] Parecer n.º 60/CNECV/2011.

Observa-se que, em casos de conflito entre o acesso aos dados pessoais de saúde pelo profissional e a proteção da privacidade do titular, é necessário encontrar um equilíbrio e realizar concessões.

Assim, em primeira instância, o direito de acesso aos dados de saúde pertence exclusivamente ao próprio titular. Somente o profissional responsável pelo atendimento médico, que presta assistência ao paciente, tem o direito de aceder a esses dados. No entanto, terceiros que desejam aceder a tais informações devem obter autorização do titular e preencher um formulário, desde que haja uma justificação estritamente fundamentada para o tal acesso.

De acordo com o mesmo parecer, o Conselho Nacional de Ética para as Ciências da Vida recomendou que, além da existência de um espaço para anotações de caráter pessoal, restrito apenas ao profissional de saúde, fosse possível bloquear certos dados pessoais de natureza mais íntima, a pedido do titular, de forma a não estarem acessíveis a outros profissionais além daqueles aos quais foram confiados.

Nesse contexto, também foi recomendado que, em situações justificadas, houvesse a possibilidade de "*partir o vidro*", ou seja, de permitir o acesso a esses dados bloqueados quando houvesse uma necessidade legítima e fundamentada. Essa medida visa conciliar a proteção da privacidade do titular com situações em que o acesso a essas informações possa ser essencial para o adequado cuidado médico[46].

Sob análise do parecer verificou-se que a informações de saúde são relevantes não apenas para pessoas doentes, mas também para indivíduos saudáveis.

Atualmente, os registos de dados de saúde não são mais realizados apenas em formato físico, como papel, mas também por meios digitais. Isso é vantajoso em termos de acessibilidade, compreensão e rapidez no uso desses dispositivos, o que facilita o acesso dos usuários às suas informações pessoais de forma mais natural.

No entanto, é sabido que o uso desses meios também acarreta consigo desvantagens. Por exemplo, existe o risco de *hackers* (piratas informáticos) acederem facilmente às nossas informações pessoais e dados, com o objetivo de utilizá-los para propagandas de serviços e outras finalidades indesejadas ou até simplesmente perigosas[47]. A isto estamos cada vez mais vulneráveis, sendo os nossos dados registados por meio de plataformas digitais.

[46] Parecer n.º 60/CNECV/2011.
[47] (Ferreira, et al., 2012), p. 26.

Portanto, é necessário adotar medidas de segurança adequadas para proteger as informações de saúde e garantir a privacidade dos titulares dos dados. Isso inclui o uso de sistemas de proteção, criptografia e medidas de segurança cibernética para evitar acessos não autorizados e salvaguardar a confidencialidade dos registos de saúde. cf, (Ferreira, et al., 2012), p. 26.

O acesso a informção de saúde, é restrito ao profissional de saúde diretamente envolvido nos cuidados do paciente, com a obrigação de manter o sigilo decorrente da prática médica.

Em não raras situações, é negado ao titular o acesso às informações de saúde. Mesmo que ele deseje conhecer essas informações, prevalece o respeito ao privilégio terapêutico. Isso significa que a compreensão é de que a divulgação das informações de saúde ao titular pode causar danos graves à sua vida ou saúde, e, portanto, deve ser pura e simplesmente evitada.

Essa abordagem visa proteger o bem-estar do paciente, pois há situações em que o conhecimento das informações de saúde pode gerar ansiedade, agravar condições médicas ou interferir no processo terapêutico. Nesses casos, a decisão é tomada levando em consideração o princípio da não maleficência, garantindo que a informação é dinamizada responsavelmente, preservando a saúde e o bem-estar do titular dos dados.

É importante ressaltar que, embora exista essa restrição ao acesso direto das informações de saúde pelo titular, o profissional de saúde deve fornecer ao paciente as explicações necessárias, em linguagem acessível, para que ele compreenda o mais ampla e profundamente possível qual é a sua condição de saúde, quais são os tratamentos recomendados e possa tomar decisões informadas em relação à sua saúde.

Neste sesntido, compreende-se que a relação entre médico e paciente seja fundamentada no princípio da confiança no sigilo médico. Isso significa que não apenas se busca proteger a privacidade dos dados de saúde do paciente, mas também se visa preservar a reputação social do profissional, que é confiada a proteção zelosa das informações obtidas no exercício da sua profissão.

Embora o dever de confidencialidade das informações de saúde do paciente não seja absoluto, ele pode ser quebrado em situações em que a proteção de terceiros ou outros interesses superiores são considerados, sempre respeitando os princípios da proporcionalidade e da dignidade humana. Essas exceções à confidencialidade podem ocorrer, por exemplo, quando há risco iminente para a vida ou integridade física de terceiros, quando há a necessidade de notificação de doenças contagiosas ou quando é exigido por lei em determinadas circunstâncias.

Observa-se porém, que as normas e princípios que regulam os dados pessoais destacam a importância de uma proteção especial para os dados de saúde, devido à sua natureza sensível, e ressaltam a necessidade de respeitar a privacidade e a autodeterminação informacional. Cf, 26º e 35º da CRP.

Assim sendo, faz parte da autodeterminação informacional do titular dos dados o direito de saber ou não saber sobre sua situação de saúde. Isto está relacionado ao controlo sobre sua própria condição de saúde e à justa oposição a que terceiros a invadam e divulguem. Assim, a proteção da privacidade e a autodeterminação informacional não se confundem, embora estejam interligadas. São abordadas em artigos distintos da CRP.

Atualmente, devido à globalização e à prevalência de sistemas eletrónicos, tornou-se tanto mais fácil proteger nossos dados de saúde de forma absoluta quanto mais expostos e vulneráveis eles estão perante os impactos do atual rumo para a ubiquidade do digital. Os sistemas eletrónicos são considerados vantajosos e desvantajosos ao mesmo tempo, para o tratamento dos nossos dados.

Tais sistemas possibilitam um acesso conveniente em muitas situações, mas também tornam os dados vulneráveis a ataques informáticos por parte de *hackers*, indivíduos que muitas vezes possuem maior conhecimento tecnológico sozinhos do que gabinetes de informática inteiros de importantes instituições. Portanto, é essencial tomar medidas adequadas para garantir a segurança e a proteção dos dados de saúde, equilibrando o uso das tecnologias com a necessidade de preservar a privacidade e a confidencialidade dessas informações.

Consequentemente, as autoras (Barbosa & Moniz), p. 249 e 262 referem no comentário sobre artigo 10º, que "os elementos respeitantes à saúde, tais como, por exemplo, a história clínica da pessoa, integram também, sem dúvida, a vida privada protegida", recordando que "*no Acórdão nº355/97 o Tribunal constitucional afirmou que o tratamento automatizado de dados relativo a doença oncológicas integram-se na esfera da privacidade dos doentes, interferindo, nessa medida, na definição do conteúdo da vida privada, matéria respeitante a direitos, liberdades e garantias*".

Os dados de saúde estão incluídos na categoria de dados relacionados à vida privada, assim como informações sobre origem étnica, vida familiar, vida sexual, condenações criminais, situação patrimonial e financeira. Esses dados fazem parte da vida privada de cada indivíduo

e estão sujeitos à proteção e respeito pela privacidade. Cf. (Pinto, 2000, p. 167) *apud* (Barbosa & Moniz), p. 249 e 262.

Em relação ao direito à autodeterminação informacional, este confere a cada pessoa o direito de controlar as informações disponíveis sobre si mesma, impedindo que a pessoa seja reduzida a um mero objeto de informação. Isso significa que cada indivíduo tem o poder de decidir quais informações pessoais deseja compartilhar e como elas serão utilizadas, assegurando assim sua dignidade e autonomia no que diz respeito ao tratamento dos seus dados. Cf. (Barbosa & Moniz), p. 249 e 262.

7.1 DIVULGAÇÃO DOS DADOS DE SAÚDE

Esta consiste na partilha de informações pessoais pelo próprio ou pelos terceiros. Sendo cada vez mais comum encontrar situações em que informações sobre a vida ou o estado de saúde de indivíduos são divulgados em diversos setores, principalmente em redes sociais. Além disso, aqueles que partilham essas informações em muitas situações não têm consciência dos potenciais danos que essa divulgação pode causar à saúde psicológica dos titulares desses dados.

Um exemplo relevante do que ocorreu durante a pandemia foi a grande curiosidade da comunidade em saber e divulgar quem estava infetado com a Covid-19, mesmo que muitas das informações compartilhadas fossem falsas. Essa situação evidenciou a necessidade de conscientização sobre a proteção dos dados de saúde e a importância de evitar a divulgação irresponsável e não autorizada.

Não apenas os cidadãos, mas também entidades públicas e privadas - que não possuem competência para lidar com informações de saúde - acabaram por divulgar, de forma sistemática, dados pessoais de saúde dos indivíduos das respetivas comunidades, o que constitui uma violação dos direitos dos indivíduos e, portanto, a CNPD advertiu que a divulgação de informações de saúde não é uma competência dessas entidades.

Pois, é essencial respeitar o princípio do sigilo profissional, que implicaria não divulgar dados pessoais que possam identificar os indivíduos afetados, no caso vertente, pela Covid-19. A divulgação irresponsável dessas informações pode levar a formas diversificadas de discriminação desses indivíduos em relação aos demais. Portanto, é essencial observar a ética e o profissionalismo ao lidar com dados de saúde e garantir a proteção da privacidade dos titulares.

No entanto, é importante ressaltar que a divulgação de informações pessoais de saúde só pode ocorrer para fins legítimos, com o consentimento dos titulares dos dados ou com autorização da CNPD, sempre observando o princípio da proporcionalidade e o cumprimento das leis de proteção de dados pessoais.

A CNPD emitiu orientações específicas sobre a divulgação de informações relacionadas aos infetados por Covid-19. De acordo com as orientações, tanto entidades públicas quanto privadas não autorizadas não podem publicar dados de saúde, mesmo sem identificação dos pacientes, quando o número reduzido de casos em uma determinada geografia, em relação à sua população, viabilize a identificação das pessoas infetadas.

Essa restrição tem o objetivo de garantir a privacidade e proteger a identidade dos indivíduos afetados, evitando qualquer forma de discriminação ou estigmatização. Portanto, é fundamental respeitar essas diretrizes e agir de acordo com as leis de proteção de dados ao lidar com informações de saúde, mesmo que elas sejam compartilhadas de forma não identificável[48].

A informação clínica não deve ser compartilhada com terceiros, a menos que seja necessário garantir a continuidade dos cuidados de saúde. Nesse caso, é responsabilidade do profissional garantir que o compartilhamento seja feito de forma segura e confidencial, apenas com outro profissional que também esteja sujeito a obrigações de confidencialidade e sigilo. É importante tomar todos os cuidados necessários ao compartilhar informações para proteger a privacidade do paciente e garantir que as informações sejam transmitidas de maneira apropriada e segura, cf. (Saúde).[49]

A questão do desequilíbrio na geração de dados é um problema que merece atenção. O fenómeno da colonização de dados destaca a disparidade entre aqueles que recolhem, acumulam e controlam os dados e aqueles que os fornecem, mas têm pouco controlo sobre como estes dados são utilizados. Isso cria um cenário em que a privacidade e a autonomia dos indivíduos podem ser comprometidas, já que a tomada de decisões e o controlo sobre os dados estão nas mãos de poucos.

---

[48] Cf. disponível em: (Dados). Sobre divulgação de informação relativa a infetados por Covid-19 Obtido em <https://www.cnpd.pt/media/juelxzcj/orientacoes_divulgacao_informacao_infetados_covid-19.pdf>. Acesso em 12 fev. 2023.

[49] Cf. (Saúde) Privacidade da Informacoes no setor da Saúde. Obtido em <http://www.arsalentejo.min-saude.pt/arsalentejo/Noticias/Documents/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2%20(1).pdf#:~:text=Nesse%20sentido%2C%20a%20SPMS%20elaborou%20o%20presente%20Guia,rela%C3%A7%C3%A3o%20ao%20tratamento%20de%20dados%> Acesso em 12 fev. 2023.

Essa assimetria de poder pode resultar em situações em que os dados são explorados de maneiras que não são benéficas para aqueles que os fornecem. É essencial abordar essa questão para garantir que os indivíduos tenham maior controle sobre seus próprios dados e possam tomar decisões informadas sobre os seus usos. Isso envolve a implementação de regulamentações e políticas que promovam a transparência, a proteção da privacidade e a participação ativa dos indivíduos no processo de geração e utilização de dados. Cf. (Neves, 2021), p. 39.

Ao disponibilizarmos nossos dados pessoais para as empresas, elas adquirem um poder e controle sobre nós. É por isso que as autoridades reguladoras e os defensores da privacidade devem lutar para garantir que tais práticas não comprometam os valores e princípios defendidos pelas grandes democracias, que prezam pela proteção dos direitos fundamentais dos cidadãos.

É importante que sejam estabelecidas medidas e regulamentações que protejam a privacidade e garantam o controle dos indivíduos sobre seus próprios dados. A conscientização e a defesa ativa da privacidade são fundamentais para preservar nossos direitos e liberdades no mundo digital em constante evolução.[50]

No contexto da saúde, a proteção do interesse direto do paciente é primordial, poi é ele o titular da sua intimidade e liberdade. Em seguida, surge a proteção dos familiares, que muitas vezes desejam saber o que está a acontecer com o seu ente querido, posto sob cuidados de saúde.

Estes dados estão relacionados aos direitos fundamentais do titular, especificamente às informações sobre a sua saúde, e somente o próprio indivíduo tem o direito de aceder-lhes e decidir quando deseja compartilhar com os seus familiares ou pessoas próximas. A privacidade e a autonomia do paciente devem ser preservadas, garantindo que ele tenha controle sobre suas informações de saúde e possa consentir ou recusar a divulgação, conforme sua vontade.

Existem situações em que a comunicação ou divulgação das informações de saúde do paciente se torna necessária. Um exemplo relevante é quando o paciente é cônjuge de alguém e é portador de uma doença contagiosa, como uma doença sexualmente transmissível. Nesse caso, é essencial que o paciente ou o médico, com o consentimento do paciente, revele sua

[50] O "colonialismo de dados" e o novo capital (2019). Obtido em: <https://outraspalavras.net/outrasmidias/o-colonialismo-de-dados-e-novo-capital/.> Acesso em: 23 de fev. 2023.

condição de saúde à outra parte, ou seja, ao cônjuge. Contextos assim atestam o caráter não absoluto do direito ao sigilo.

Também existem situações em que a comunicação de dados de saúde é necessária para proteger terceiros ou para garantir um interesse público digno de proteção legal. Nesses casos, é necessário equilibrar os interesses em conflito, ou seja, a proteção da situação de saúde do titular e um interesse superior que a lei procura proteger, como seja a proteção da saúde pública. Contextos há em que o direito ao sigilo do estado de saúde do titular é restrito, em função de um interesse superior.

De um modo geral, os dados de saúde são considerados confidenciais, sendo protegidos pelas entidades de saúde, sejam elas públicas ou privadas, a fim de garantir os princípios de confidencialidade que regem as profissões de natureza médica. No campo da saúde, não se busca promover boatos ou especulações sobre o estado de saúde dos pacientes, razão pela qual a lei proíbe a intromissão de terceiros na vida privada do titular dos dados. O sigilo é essencial para preservar a privacidade e a dignidade dos indivíduos em relação às suas informações de saúde. Cfra, (Deodato), p. 33-38.

A propósito da divulgação ou partilha de informações de saúde, afirma Daniel Serrão:

> A tradição hipocrática estabelecia que tudo o que o médico conhecia da pessoa doente que estava a assistir, era matéria sigilosa, pelo que o doente sabia que nada da sua doença seria comunicado em nenhuma circunstância. A fidelidade do médico a esta obrigação de guardar segredo dava á relação médico/ doente um clima de confiança absoluta.
> A evolução cultural e sociológica trouxe algumas alterações a este dever absoluto e, hoje, em certas situações de relevante interesse público, o médico pode ter de revelar dados de saúde da pessoa que trata ou tratou. Como é o caso do exercício do poder judicial em situações concretas. [51]

A proteção dos dados pessoais de saúde é de suma importância no mundo em que vivemos, pois, observa-se uma crescente exposição dos nossos dados devido à sua partilha por diversas entidades, sejam elas públicas ou privadas, muitas vezes com fins económicos.

Assim, é proibida a partilha de dados pessoais de saúde com terceiros sem o consentimento do titular, salvo nos casos previstos na lei que sejam do interesse do próprio titular ou de maior relevância jurídica.

No complexo mundo dos dados pessoais, é importante proteger a nossa privacidade, evitando a exposição dos dados de saúde nas vias digitais, onde cada informação partilhada pode revelar a nossa identidade. Pois, entre a necessidade de socialização e a salvaguarda da

[51] Cf. (Ferreira, et al., 2012).

individualidade, encontramos o desafio de sermos guardiões de nossa própria identidade, buscando encontrar harmonia no jardim digital que floresce a nosso redor.

8 DIREITO AO ESQUECIMENTO OU APAGAMENTO DOS DADOS

O direito ao apagamento dos dados, ou o "*direito a ser esquecido*", é um poderoso instrumento que o titular dos dados possui para preservar sua privacidade e controlar suas informações pessoais. Consagrado no artigo 17º do RGPD, esse direito estabelece que o titular tem o direito de exigir do responsável pelo tratamento o apagamento dos seus dados pessoais, de forma rápida e justificada.

Essa prerrogativa reflete a importância de respeitar a autonomia e a liberdade do indivíduo, permitindo que ele decida sobre o destino de suas informações, removendo-as do cenário digital quando assim desejar. Nesse contexto, o direito ao apagamento emerge como uma salvaguarda essencial, permitindo ao indivíduo moldar sua narrativa digital e reafirmar o seu poder de controlar a própria história, conforme RGPG, art. 17/1.

Na era digital em que vivemos, o impacto das tecnologias tem sido sentido de forma ampla e profunda nas vidas das pessoas. Essa realidade traz consigo desafios e oportunidades, especialmente no que diz respeito à proteção dos dados pessoais. O crescimento exponencial de bases de dados pessoais em diversos setores, sejam eles públicos ou privados, demanda a construção de um novo e abrangente quadro jurídico e organizacional.

A preservação da intimidade e privacidade torna-se ainda mais relevante, com a área da saúde sendo um exemplo expressivo. É necessário estabelecer mecanismos efetivos de proteção dos dados pessoais, garantindo que a utilização dessas informações seja pautada por princípios éticos e legais, preservando os direitos fundamentais dos indivíduos. Dessa forma, podemos buscar o equilíbrio entre o avanço tecnológico e a salvaguarda da privacidade, construindo um ambiente digital dignificado, mais seguro e respeitoso para todos.

O equilíbrio entre a proteção desses dados sensíveis e a sua utilização legítima torna-se essencial para garantir a segurança e a privacidade dos indivíduos, bem como um rumo mais satisfatório da sociedade como um todo.

É crucial resgatar e reafirmar o valor do artigo 12º da Declaração Universal dos Direitos Humanos, que afirma o direito de cada indivíduo à privacidade e à proteção contra intromissões arbitrárias na sua vida privada, família, domicílio e correspondência. Quando a

privacidade é violada, a pessoa passa a viver uma realidade de privação e medo, desdobrando-se em efeitos na sua qualidade de vida e bem-estar.

A proteção legal desses direitos fundamentais é essencial para garantir não apenas a privacidade, mas também a segurança humana. É por meio da tutela da lei que podemos assegurar a proteção básica e a tranquilidade necessária para uma vida digna e segura. Cf, (Fernando, 2016), p. 9 a 12.

No final de 2010, a Comissão Europeia (CE) iniciou uma consulta pública com o objetivo de estabelecer o direito ao esquecimento. Esse direito permitiria que as pessoas impedissem o tratamento contínuo de seus dados e que os mesmos fossem apagados quando não fossem mais necessários para fins legítimos.

O direito ao esquecimento é de fundamental importância, como exemplificado pela história de um respeitado professor que teve sua queixa acolhida pela Autoridade Europeia para a Proteção de Dados (AEPD). Essa queixa buscava restaurar sua dignidade, uma vez que uma notícia de 30 anos atrás, relatando uma multa que ele mesmo havia recebido por ter urinado em público quando jovem, havia surgido na internet. Cf. (Gomes, 2014), p. 79-80.

Com base nas reflexões apresentadas, concordamos com a importância de garantir a segurança e a proteção dos dados pessoais num mundo digital em constante evolução. É essencial que esses dados sejam tratados de maneira legítima e que tenhamos a possibilidade de retificar ou eliminar as informações que outora disponibililizamos, especialmente nos motores de busca, de forma ágil e eficiente. Essa abordagem visa preservar a nossa privacidade e assegurar que as nossas informações pessoais sejam tratadas com o devido cuidado e respeito. Contudo, o direito ao esquecimento, permite-nos deletar o histórico do passado, para que tais informações não influenciem negativamente na nossa vida presente.

Consequentemente, no plano do direto ao esquecimento (Pereira A. L., 2018) faz menção ao Acórdão Google Spain[52], em que um cidadão espanhol aparecia numa lista de resultado de pesquisa do Google, por dívidas ao fisco de um processo muito antigo, trecho *in verbis*:

> O cidadão espanhol solicitou a remoção desse resultado, que considerava ofensivo da sua honra e bom nome, mas a empresa Google alegou que não tinha o dever de proceder a esse bloqueio, desde logo por não estar estabelecida na União Europeia,

[52] Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. Processo C-131/12. Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Obtido em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>. Acesso em 01 jun. 2023.

> tendo aí apenas uma sucursal que geria o negócio da publicidade (…). No entender do Tribunal, a pessoa em causa tem o direito que a informação em questão sobre si "deixe de ser associada ao seu nome através de uma lista de resultados exibida na sequência de uma pesquisa efetuada a partir do seu nome, sem que, todavia, a constatação desse direito pressuponha que a inclusão dessa informação nessa lista causa prejuízo a essa pessoa. (...). No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão (…). O operador do motor de pesquisa é considerado o responsável pelo tratamento, isto é, a pessoa que determina os fins e os meios da atividade relevante dos dados mesmo que não seja a entidade fonte dessa informação. Na opinião do Tribunal, o responsável pelo tratamento tem um dever de controlo ativo, no sentido de lhe caber o apagamento dos dados ilegalmente tratados mesmo que as pessoas afetadas não tomem medidas nesse sentido. Ora, todos estes grupos de interesses são relevantes e afetados, mas na opinião do Tribunal a proteção de dados e da privacidade sobrepõe-se aos demais (…).

Conclui-se, na linha de reflexão do autor sobre o referido Acórdão, que, independentemente de os dados pessoais do titular serem tratados, nos mais distantes pontos geográficos do mundo, sempre que estejam envolvidos os dados de cidadãos da União Europeia, aplica-se a estes as regras do Regulamento da União Europeia que visa a proteção de dados pessoais, através das suas entidades de controlo independentes.

As actividades de tratamento de dados, ligadas aos motores de buscas devem ser protegidas pelo direito europeu, com vista a salvaguardar os Direitos fundamentais dos titulares, titulares de um direito à autodeterminação informativa, bem como o seu direito ao esquecimento e oposição ao tratamento ilícito de dados pelas empresas. Neste contexto, percebeu-se que, mesmo em caso de conflito entre o interesse do público, em aceder à informação do titular,- resultante dos motores de busca, consubstanciada assim, no direito destes de liberdade de expressão e informação-, e o interesse da proteção da privacidade do titular, prevalecerá sempre a última, perante a curiosidade dos terceiros em aceder as referidas informações pessoais.

Privilegiar-se-á assim, a proteção do público, no acesso a informação do titular, constante dos motores de busca, sendo o titular uma figura pública, a proteção da sua privacidade poderá ceder perante o interesse público.

9 PODERES DA CNPD

A Comisssão Nacional de Proteção de Dados é mencionada nos artigos 3ºss da LPDP[53], como autoridade de controle para efeito do presente Regulamento e da Lei de Proteção de Dados Pessoais.

No contexto da organização administrativa em Portugal, foi acrescentado o setor da "administração independente" à tipologia clássica. Administração independente é uma administração infraestadual realizada por órgãos administrativos que não estão integrados na administração direta do Estado e são livres da orientação e supervisão do Estado, mas que não correspondem à autogestão de interesses organizados. Trata-se de entidades administrativas que atuam de forma independente, mas sem serem totalmente autónomas em relação aos interesses organizados, cf. Pinheiro (2015, p. 733).

Ao abrigo do nº 3 do art. 267º da CRP, o legislador prevê a criação destas entidades e o nº 2 do art. 35º da CRP assegura a proteção dos dados pessoais dos cidadãos por meio desta.

Nesse sentido, a CNPD é considerada uma entidade administrativa independente, com personalidade jurídica de direito público, dotada de poderes de autoridade e com autonomia administrativa e financeira. A CNPD atua em colaboração com a Assembleia da República. Cf. (Cordeiro, 2020), p. 399.

A CNPD desempenha um papel fundamental na proteção dos dados pessoais, sendo responsável por supervisionar e controlar a conformidade das atividades das empresas, tanto do setor público quanto do setor privado, em relação ao tratamento de dados. Esta entidade assegura que essas empresas estejam em conformidade com as disposições estabelecidas no RGPD e outras leis de proteção de dados, que garantem os direitos fundamentais dos titulares dos dados.

É importante que tanto as entidades do setor público quanto as do setor privado colaborem com a CNPD para garantir que ela possa cumprir sua missão de forma eficaz, tendo em mente que os dados pessoais dizem respeito a todos nós, como seres humanos[54].

O art. 58º do RGPD aflora os poderes atribuídos a CNPD. Tendo esta legitimidade para emitir pareceres, deliberações, decisões, autorizações, consulta, advertências e aplicar

[53] Lei nº 58/2019, de 8 de agosto.
[54] Cf. CNPD. Obtido em: https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/.

coimas em casos mais graves que envolvem violação dos direitos fundamentais dos titulares de dados.

Além destes poderes, os Estados também podem conferir à CNPD poderes mais abrangentes em relação à proteção de dados pessoais.

Esta possui autonomia em relação aos demais poderes do Estado, conferindo-lhe, portanto, uma personalidade jurídica própria. A atividade desempenhada por essa entidade é isenta de qualquer forma de subordinação aos poderes de direção ou orientação do Governo, e não se sujeita ao controle ou fiscalização por parte da administração do Estado.

Somente em relação à esfera financeira é admitida uma exceção a esse controlo, mas vale ressaltar que tal fiscalização não pode comprometer a independência da autoridade, que possui orçamentos distintos e transparentes, os quais podem estar integrados no Orçamento de Estado. Cf. Artigo 52º, nº6 do RGP).

A atuação da CNPD está sujeita ao escrutínio judicial, garantindo-se, assim, a verificação do cumprimento das normas legais e a salvaguarda dos direitos das partes envolvidas. Vide artigo 78º, RGPD, (Moniz, 2018), p. 135.

Ao ser configurada como uma entidade administrativa independente, a CNPD desfruta de certa discricionariedade no exercício de suas atividades relacionadas à proteção de dados. Tal discricionariedade é inerente à própria função administrativa e encontra respaldo no disposto no número 3 do artigo 267º e no número 2 do artigo 35º da CRP.

Essa discricionariedade não é absoluta, estando sujeita aos princípios e normas que regem a proteção de dados e ao controlo judicial para verificar sua conformidade com a lei. Cf. Pinheiro (2015, p. 736).

A CNPD possui o poder de aplicar sanções de caráter contraordenacional como forma de cumprimento das suas funções. Essas sanções incluem a aplicação de coimas, sendo esta a medida mais severa.

É importante ressaltar que, antes de recorrer à aplicação de coimas, a CNPD opta por adotar medidas corretivas ou emitir advertências às entidades que tenham violado dados pessoais, independentemente de serem empresas públicas ou privadas e do interesse público ou lucrativo envolvido nas suas atividades.

Dessa forma, a CNPD procura promover a conformidade com as leis e demais instrumentos de proteção dos direitos, liberdades e garantias (DLG´s) dos titulares de dados. Somente em caso de reincidência ou violações graves é que a CNPD poderá aplicar coimas, levando em consideração a gravidade da infração e a culpabilidade do agente responsável, pressupostos previstos no artigo 18º, nº1, do Regime Geral de Contraordenações[55].

As coimas podem variar desde contra-ordenações graves até muito graves, dependendo das circunstâncias do caso em questão.

As violações graves a muito graves no âmbito da proteção de dados pessoais são definidas nas alíneas do artigo 37º e 38º da LPDP. Essas alíneas remetem para os artigos do RGPD que tratam dessas violações, sendo particularmente relevante a violação das regras estabelecidas no nº 1 e 2 do artigo 9º do RGPD, que dizem respeito ao tratamento de categorias especiais de dados pessoais.

A LPDP, por sua vez, estabelece o âmbito de aplicação das contraordenações no seu artigo 44º. Esse artigo determina as situações em que as contraordenações podem ser aplicadas, incluindo as violações graves e muito graves relacionadas com a proteção de dados pessoais.

A garantia efetiva para a aplicação de coimas no âmbito da proteção de dados está estabelecida no artigo 83º e seguintes do RGPD. Esses artigos estabelecem as "*Condições gerais para a aplicação de coimas*". No que diz respeito às sanções aplicadas pela CNPD e outras autoridades de controlo, é importante observar os dois pontos *infra.*

Em primeiro lugar: no âmbito do RGPD, a CE optou por não introduzir sanções penais no domínio da proteção de dados (Artigo 83º, nº 1 do Tratado sobre o Funcionamento da União Europeia ou TFUE). No entanto, os Estados-Membros têm a possibilidade de manter ou criar sanções desta natureza (Art. 84º, nº 1). Em segundo lugar: em vez de sanções penais, foram estabelecidas sanções pecuniárias administrativas, inspiradas nas regras de direito da concorrência, que podem ser aplicadas pelos Estados-Membros.

As referidas sanções podem atingir valores elevados, podendo chegar até 20 000 000 EUR ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial

[55] DL n.º 433/82, de 27 de Outubro. Da contra-ordenação e da coima em geral.

correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado" (art. 83º, nº 5 do RGPD) e têm como objetivo garantir a eficácia das medidas de proteção de dados.

Outro objetivo das sanções é desencorajar violações significativas das normas de proteção de dados. A aplicação das coimas deve ser feita de acordo com as disposições do RGPD e da legislação nacional pertinente, e é da responsabilidade das autoridades de controlo, como a CNPD, assegurar que as violações sejam sancionadas adequadamente. (Pereira A. , I Curso de Pós-Graduação Avançada em Direito da Proteção de Dados, 2020).

É evidente que todas as entidades envolvidas na recolha e tratamento de dados devem agir com o máximo zelo.

No que diz respeito às sanções contraordenacionais, estas podem incluir a aplicação de coimas, bem como penas acessórias. As penas acessórias podem implicar a proibição temporária ou definitiva do exercício das atividades relacionadas com o tratamento de dados pessoais por parte dos responsáveis das entidades em questão.

Tais medidas têm como objetivo garantir a conformidade com as normas de proteção de dados e proteger os direitos dos indivíduos em relação ao tratamento dos seus dados pessoais.

A CNPD não tem como objetivo primordial a imposição imediata de sanções severas, como as coimas. Pelo contrário, a CNPD prefere adotar uma abordagem de recomendação e aconselhamento às entidades públicas e privadas envolvidas no tratamento de dados pessoais. É crucial que essas entidades cumpram as regras estabelecidas para o tratamento de dados sensíveis, uma vez que esse tratamento é estritamente proibido e protegido pelos princípios da dignidade humana, proporcionalidade, boa-fé e outros que garantem os direitos fundamentais da pessoa.

A CNPD procura, em primeiro lugar, sensibilizar as entidades envolvidas sobre a importância de proteger os dados pessoais e incentivar a sua conformidade com as normas estabelecidas.

No entanto, caso ocorram violações graves no tratamento de dados pessoais, a CNPD poderá recorrer à aplicação de sanções, como as coimas, como último recurso. Essas sanções são aplicadas de acordo com os princípios da proporcionalidade e da legalidade, levando em consideração a gravidade da violação e o impacto nos direitos dos titulares dos dados.

Entretanto, os crimes em matéria de proteção de dados estão previstos no art. 46ºss da LPDP, e não no RGPD, porque a EU, não tem competência criminal.

O princípio da proporcionalidade desempenha um papel fundamental no contexto da aplicação de coimas no âmbito do RGPD.

O nº2 do art. 83º do RGPD estabelece que a autoridade de controlo não está obrigada a aplicar coimas em todos os casos de violação das normas. Em vez disso, a autoridade de controlo possui a discricionariedade de tomar outras medidas, como repreensão, advertência ou a ordem para adoção de medidas que levem ao cumprimento do RGPD.

Isso significa que a decisão de aplicar uma coima deve ser baseada numa avaliação casuística, levando em consideração a natureza e a gravidade da violação, bem como os efeitos sobre os direitos e liberdades dos titulares dos dados. Essa abordagem reflete a necessidade de equilibrar os interesses em jogo, garantindo a efetividade da proteção de dados, mas também evitando medidas punitivas desnecessárias ou excessivas. Assim, a aplicação de coimas deve ser uma medida adequada e proporcional ao caso concreto, levando em conta todas as circunstâncias relevantes.

O princípio da proporcionalidade assegura que a imposição de coimas seja reservada para casos de violações substanciais e graves das normas do RGPD, enquanto outras medidas menos gravosas podem ser adotadas quando a situação assim o permitir. Isso garante que a autoridade de controlo tenha flexibilidade para adequar sua resposta às diferentes circunstâncias, promovendo uma abordagem equilibrada e justa na aplicação das sanções. Cf. Pinheiro (2018, p. 641).

É fundamental exercer o máximo cuidado no respeito ao princípio da proporcionalidade no contexto da aplicação de coimas pela autoridade de controlo às empresas, sejam elas públicas ou privadas, que violem os dados pessoais. Essas sanções de natureza contraordenacional devem ser aplicadas apenas subsidiariamente, ou seja, após repetidas advertências aos responsáveis, no intuito de consciencializá-los sobre a importância de adotar medidas adequadas no tratamento de dados pessoais.

O objetivo principal da aplicação dessas coimas não se restringe apenas à proteção dos direitos individuais dos seus titulares e às empresas em si, mas também visa garantir a segurança e o cumprimento dos regulamentos emanados pela UE, que têm aplicação obrigatória em todos os Estados membros.

Essas medidas podem incluir orientações, advertências, recomendações e supervisão contínua, a fim de auxiliar as empresas no cumprimento das obrigações legais e promover a cultura de proteção de dados. Cf. Pinheiro (2018, p. 641).

Nesse sentido, a autoridade de controlo deve adotar uma abordagem gradual e educativa, dando prioridade a medidas corretivas e preventivas antes de recorrer à aplicação de coimas.

CONCLUSÃO

Ao longo desta dissertação, tivemos a oportunidade de abordar a problemática da proteção dos dados pessoais de saúde à luz do RGPD, bem como a sua salvaguarda por meio das demais leis em vigor a nível nacional.

Foram explorados os temas da definição de dados pessoais e dados pessoais de saúde no qual destacamos a importância desses dados no contexto da sociedade contemporânea, em que a sua utilização é cada vez mais frequente e abrangente.

Exploramos as particularidades desses dados, que revelam informações sobre o estado de saúde de uma pessoa, tratamentos médicos, histórico clínico e outras informações intimamente ligadas à esfera da saúde individual.

Foi aprofundada também a relação entre os dados pessoais de saúde e a intimidade da vida privada. Reconhecemos que estes estão intrinsecamente ligados ao âmbito privado do indivíduo, exigindo, portanto, uma proteção robusta para preservar a sua confidencialidade e evitar eventuais abusos ou violações.

Enfatizou-se a importância da autodeterminação informacional, que é o poder de cada pessoa decidir como as suas informações pessoais,- incluindo os dados de saúde-, serão utilizadas. Destacou-se a necessidade de haver consentimento informado e livre por parte do titular dos dados, assim como a relevância do princípio da transparência e da prestação de informações claras sobre o tratamento desses dados.

Foram também tidas em conta leis específicas que regulam a proteção de dados no contexto da saúde, bem como outras leis relacionadas à privacidade e aos direitos fundamentais dos indivíduos.

Ao abordar esses temas, foi procurado trazer à tona a importância da proteção dos dados pessoais de saúde e ressaltar a necessidade de um enquadramento jurídico sólido e abrangente para garantir a segurança e a privacidade desses dados. Reconhecemos que a preservação da intimidade da vida privada e o respeito à autodeterminação informacional são fundamentais para assegurar a dignidade e os direitos dos indivíduos no contexto do tratamento de dados pessoais de saúde.

No que se refere à titularidade dos dados de saúde, identificamos que estes pertencem à pessoa a quem os dados dizem respeito, conferindo-lhe o direito de controlar o seu tratamento e utilização. Reconhecemos a importância de assegurar que o titular dos dados exerça

o seu direito à autodeterminação informacional e possa decidir de forma livre e consciente sobre o tratamento dos seus dados pessoais de saúde.

Abordamos também "principiologias" do tratamento dos dados de saúde, ou seja, os princípios fundamentais que devem orientar o tratamento desses dados. Destacamos, entre outros, o princípio da minimização dos dados, que preconiza a coleta apenas dos dados estritamente necessários para a finalidade específica, bem como o princípio da finalidade, que determina que os dados de saúde sejam utilizados apenas para os fins legítimos e específicos para os quais foram recolhidos.

No contexto da proteção dos dados de saúde, discutimos o papel do encarregado de proteção de dados, um profissional designado pela entidade responsável pelo tratamento dos dados para assegurar o cumprimento das disposições legais e garantir a proteção dos direitos dos titulares. Ressaltamos a importância da independência desse encarregado no desempenho das suas funções, bem como o seu dever de sigilo.

Por fim, destacamos a relevância do consentimento no tratamento dos dados de saúde.

Reconhecemos que o consentimento do titular dos dados é uma base legal para o tratamento desses dados, devendo ser obtido de forma clara, informada e inequívoca. Salientamos que o consentimento é uma manifestação de vontade livre do titular, e a sua revogação deve ser igualmente respeitada.

Consideramos essas questões cruciais no contexto da proteção dos dados de saúde, uma vez que visam garantir a dignidade, a privacidade e os direitos dos indivíduos, bem como estabelecer os parâmetros éticos e legais para o tratamento desses dados tão sensíveis.

Sobre a proteção dos dados de saúde, abordamos a importância da privacidade desses dados. Reconhecemos que as informações relacionadas à saúde são extremamente sensíveis e devem ser tratadas com o máximo cuidado e respeito à privacidade dos indivíduos. Destacamos a necessidade de adotar medidas de segurança adequadas para evitar divulgações não autorizadas ou acessos indevidos a esses dados.

No contexto da divulgação de dados de saúde, ressaltamos a importância de respeitar o princípio da confidencialidade e de obter o consentimento explícito do titular antes de compartilhar suas informações de saúde com terceiros. Reconhecemos que a divulgação inadequada ou não autorizada desses dados pode comprometer a privacidade e a segurança dos indivíduos, bem como afetar a confiança no sistema de saúde.

Abordamos também o direito ao esquecimento ou apagamento de dados de saúde, reconhecendo que os titulares têm o direito de solicitar a eliminação de seus dados pessoais de saúde, especialmente quando não são mais necessários para os fins para os quais foram recolhidos ou quando o tratamento desses dados é ilícito. Destacamos a importância de garantir que os titulares possam exercer efetivamente esse direito, dentro dos limites estabelecidos pela legislação aplicável.

No que diz respeito aos poderes atribuídos à autoridade de controlo, notamos que a CNPD, como autoridade de controlo em Portugal, detém o poder máximo de aplicar sanções às pessoas coletivas que violem as normas de proteção de dados, incluindo aquelas relacionadas aos dados pessoais de saúde. Reconhecemos a importância desse poder como um mecanismo de dissuasão e garantia da conformidade com a legislação em vigor.

Por meio dessa reflexão sobre os dados pessoais de saúde à luz do RGPD, compreendemos a relevância dos conflitos que surgem no acesso às informações de saúde. Reconhecemos que essas informações são de propriedade exclusiva do titular e que o acesso a elas deve ser feito de forma segura, e evitando o acesso não autorizado ou indevido por terceiros.

Destacou-se a proteção da privacide dos dados de saúde que é fundamental para preservar a confidencialidade, a dignidade e os direitos dos indivíduos no contexto da sua saúde e bem-estar.

Constatámos que o direito do titular dos dados de saúde não é absoluto, e existem situações excepcionais em que esse direito pode ser limitado. Essas restrições podem ocorrer para proteger terceiros ou atender a um interesse público devidamente preponderante. Desde que não sejam desproporcionais.

Destacamos que as informações sensíveis, como os dados de saúde, são protegidas pelo princípio do sigilo profissional por parte dos profissionais de saúde. A partilha dessas informações entre os profissionais deve ocorrer de acordo com a tutela do interesse vital do paciente, seguindo o princípio do privilégio terapêutico. Isso significa que os profissionais de saúde devem avaliar cuidadosamente a divulgação de informações sensíveis ao titular dos dados, evitando prejudicar gravemente a saúde do paciente.

Vimos que é essencial garantir a confidencialidade e o sigilo das informações sensíveis, respeitando os princípios éticos e legais que regem a prática médica e a relação entre o paciente e o profissional de saúde.

É manifesto que há que estabelecer diretrizes claras e normas éticas para a utilização e partilha de dados de saúde, assegurando a confiança dos titulares dos dados e a integridade do sistema de saúde como um todo. A proteção dos dados de saúde não apenas preserva a privacidade individual, mas também garante a qualidade e a segurança dos cuidados de saúde oferecidos aos pacientes.

Considerando o direito à proteção de dados como um direito novo e protegido por uma entidade responsável, a CNPD, é fundamental ressaltar o papel dessa entidade na tutela dos direitos fundamentais em relação aos dados pessoais dos cidadãos. A CNPD é responsável por garantir o controle e o cumprimento do Regulamento Geral de Proteção de Dados (RGPD) e das leis nacionais de proteção de dados por parte das pessoas coletivas, sejam elas públicas ou privadas, que lidam com dados pessoais nas suas atividades, especialmente os dados pessoais de saúde, que são considerados dados especiais.

A CNPD, assumindo o papel de 'guardiã' da privacidade e dos dados pessoais, desempenha não apenas a função de aplicar coimas, mas também procura promover a adoção de boas práticas pelas empresas, visando um tratamento adequado e uma proteção efetiva dos dados. Assim, a CNPD não atua apenas como uma entidade sancionadora, mas também como uma aliada das empresas, incentivando-as a adotar comportamentos adequados no tratamento e proteção dos dados. Esperamos que, no futuro, os conflitos em torno da proteção da privacidade e do acesso aos dados pessoais de saúde sejam resolvidos de forma mais ágil, contribuindo para esclarecer com precisão a questão da propriedade e divulgação dessas informações sensíveis.

Do exposto, ressalta-se a notável relevância da proteção dos dados pessoais de saúde, dada a sua natureza delicada, que exige uma atenção especial e respeito em áreas sensíveis relacionadas à quebra da privacidade. Nesse contexto, o legislador adota uma abordagem mais rigorosa para salvaguardar devidamente tais dados.

No atual panorama, em que os seres humanos estão cada vez mais imersos na era digital e, particularmente, diante do surgimento da pandemia da COVID-19, em que a digitalização se tornou predominante em diversos setores, temos sido alvos fáceis da violação da nossa privacidade, tanto por entidades públicas e privadas quanto por terceiros, como os habilidosos piratas cibernéticos que exploram as nossas informações, sensíveis e não sensíveis, valendo-se de avançadas ferramentas tecnológicas.

Num mundo cada vez mais dominado pela tecnologia e conexão digital, proteger a nossa privacidade tornou-se um desafio complexo e incessante. Para salvaguardar nossos dados pessoais, é essencial unir forças e adotar ações diárias que visem a sua proteção. A defesa constante dos nossos dados é uma tarefa que requer comprometimento e vigilância, pois a privacidade é uma raridade que demanda cuidado e atenção.

Devemos ser diligentes ao navegar pelo mar digital, cientes de que a proteção dos nossos dados é um direito fundamental que deve ser preservado. Assim se encerra, após navegar pelas interrogações sucitadas pelo tema, esta dissertação sobre a proteção de dados pessoais. Num empenho incansável, tecemos as tramas de um futuro que exalta a dignidade de cada indivíduo e consagra a inviolabilidade de sua esfera pessoal. Que tais ações reverberem como ecos monumentais através dos tempos, inspirando gerações vindouras para que também elas protejam, com denodo, o sopro que preserva a integridade e a liberdade de cada ser humano: a sua privacidade.

REFERÊNCIAS

Acórdão do Tribunal Central Administrativo Norte, Proc. 00884/12.0BEBRG, de 30 de Outubro de 2020. Braga. Obtido http://www.gde.mj.pt/jtcn.nsf/89d1c0288c2dd49c802575c8003279c7/3839bd8185d5c6e38025861d00443c68

Acórdão do Supremo Tribunal Administrativo, 16-12-2021 - Relator: CARLOS CARVALHO (proc. 0884/12.0BEBRG). Obtido em <http://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/1d48c6e74692b044802587b8005f1610?OpenDocument&ExpandSection=1#_Section1>.

Andrade, R. R. (7 de Dezembro de 2020). Da Responsabilidade do Encarregado de Proteção de Dados. (F. d. Dados, Ed.) Obtido de https://www.cnpd.pt/media/5kajlbve/forum7_web.pdf

Barbosa, C., & Moniz, H. (s.d.). Comentário ao Artigo 10º. Obtido de http://www.centrodedireitobiomedico.org/sites/cdb-dru7-ph5.dd/files/Livro%20-%20Oviedo%20-%2010.pdf

BIONI, Bruno; DIAS, Daniel. Responsabilidade Civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. 2020, p. 19-21. Obtido em <https://civilistica.emnuvens.com.br/redc/article/view/662/506>.

BONDO, Pitra António dos Santos. Princípio da Não Discriminação. Dissertação de Mestrado. Universidade Católica Portuguesa, Porto; Junho 2015, p. 12-28. Obtido em <https://repositorio.ucp.pt/bitstream/10400.14/18259/1/FINAL_Tese%20Pitra%20Bondo.pdf >.

Calvão, F., & Maçãs, F. (Dezembro de 2020). O Encarregado de Proteção de Dados nas pessoas Coletivas públicas. Obtido de https://www.cnpd.pt/media/5kajlbve/forum7_web.pdf

Canotilho, J., & Moreira, V. (2014). *Constituição da República Portuguesa Anotada* (4ª ed., Vol. I).

Constituição da República Portuguesa (6ª ed.). (2019). Almedina.
Cordeiro. (2020). *Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019.* Almedia.

Costa, T. d. (7 de Maio de 1997). *Tribunal Constitucional de Portugal*. Obtido de Tribunal Constitucional de Portugal: https://www.tribunalconstitucional.pt/tc/acordaos/19970355.html

Dados, C. N. (s.d.). Obtido de https://www.cnpd.pt/media/juelxzcj/orientacoes_divulgacao_informacao_infetados_covid-19.pdf

Deodato, S. (s.d.). *A Proteção dos Dados Pessoais de Saúde.* Universidade Católica. 2017.

Fernandes, C. C. (s.d.). *Acesso à Informação de Saúde.*

Fernando, N. (2016). Novo Mundo, Privacidade e Política. *3*.

Ferreira, A., & Almeida Calhau, A. F. (s.d.). *Acesso à Informação de Saúde 1º Colóquio do Centro Hospitalar de São João e CADA.*

Ferreira, A., Almeida Calhau, A. F., Pimpão, A. J., Serrão, D., Duarte, D., Reis, F. C., . . . Oswald, W. (2012). *Acesso à informação de Saúde.* Porto.

Gomes, R. (2014). *Texto de Coolóquio na Procuradoria geral da República, Informação e Liberdade de Expressão na Internet e a Violação de Direitos Fundamentais, Comentários em Meios de Comunicação online. Imprenssa Nacional Casa da Moeda.*

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de; Da Evolução das Legislações sobre Proteção de Dados: A Necessidade de Reavaliação do Papel do Consentimento como Garantidor da Autodeterminação Informativa. Revista De Direito | Viçosa, 2020, p. 15. Obtido em <https://www.repositorio.ufop.br/bitstream/123456789/14359/1/ARTIGO_Evolu%c3%a7%c3%a3oLegisla%c3%a7%c3%b5esProte%c3%a7%c3%a3o.pdf >.

Matos, F. m. (s.d.). O Regulamento de Proteção de Dados Pessoais (2016/679) no Contexto dos desafios da Actividade Seguradora. (Nº3/2018). Revista BBS.

Miranda, I. d. (14 de Fevereiro de 2023). *Dados de utilizadores de aplicações de saúde mental disponíveis por centenas de euros*. Obtido de Visão: https://visao.sapo.pt/atualidade/sociedade/2023-02-14-dados-de-utilizadores-de-aplicacoes-de-saude-mental-disponiveis-por-centenas-de-euros/

Moniz, A. R. (2018). A Tutela Administrativa de Dados pessoais em Matérias de Seguro: Em Especial à Autoridade Reguladora. *3*. BBS.

NETO BARROS, Inocêncio. Proteção de Dados na Computação em Nuvem. 2021, Dissertação para obtenção do Grau de Mestre em Informática, p. 43. Obtido em <https://comum.rcaap.pt/bitstream/10400.26/39868/1/99991908_Inoc%c3%aancio_Barros.pdf>.

Neves, C. M. (2021). *Relatório sobre o Estado de Aplicação das novas tecnologias a vida humana, CNECV.*

PASSINI, Rosana Principe. Implicações éticas do princípio da privacidade na interação médico-paciente. 2019. 210 f., il. Tese (Doutorado em Ciências da Saúde) - Universidade de Brasília, Brasília, 2019.

Parecer nº 60 sobre Informação de Saúde e Registos Informáticos de Saúde. (Setembro de 2011). Obtido em <https://www.cnecv.pt/pt/pareceres/parecer-sobre-informacao-de-saude-e-registos-informaticos-de-sau?download_document=3117&token=8181b66dcd13f44d98c36f1192387cff>.

PEREIRA, André Gonçalo Dias. Relatório Justiça Administrativa e Fiscal - Qualidade e Celeridade - Impasses e Soluções. O Acórdão do Supremo Tribunal Administrativo de 16 de dezembro de 2021 (1 Secção; Relator: Cons. Carlos Carvalho (proc. 0884/12.0BEBRG) – um passo decisivo para proteção do direito ao consentimento informado nos hospitais públicos. ASJP, 2022, p. 15 - 41. Obtido em <https://www.asjp.pt/wp-content/uploads/2023/01/EBOOK-2-Justic%CC%A7a-Administrativa-e-Fiscal_Intervenc%CC%A7o%CC%83es-Confere%CC%82ncia_23.12.2022.pdf>.

Pereira, A. (2015). *Direito dos Pacientes e Responsabilidade Médica.* Coimbra Editora.

Pereira, A. (MArço de 2020). I Curso de Pós-Graduação Avançada em Direito da Proteção de Dados.

Pereira, A. G. (2004). *O Consentimento Inforfmado na Relação Médico - Paciente, Estudo de Direto Civil.* Coimbra Editora.

Pereira, A. G. (10 de Outubro de 2013). Processo Clínico e Mudança de Unidade de Saúde: Anotação ao Acórdão do Tribnal da Relação de Coimbra. (19). Coimbra: Lex Medicinae. Obtido de <https://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/revistas/lex-medicinae-ano-10-n%C2%BA-19-revista-portuguesa-de-direito-da-sa%C3%BAde>.

Pereira, A. G. (2015). *Direitos dos Pacientes e Responsabilidade Médica.* Coimbra.

Pereira, A. L. (2018). A proteção de Dados Pessoais e o Direito à Segurança Informática no Comércio Eletrónico. (3). BBS. Obtido de https://www.fd.uc.pt/bbs/wp-content/uploads/2019/01/bbs3_final_2p.pdf

Pereira, A. L. (2018). *Big Data, E-Halth e «Autodterminaçãi informativa» A lei 67/98, a Jurisprudência e o regulamento 20116/679 (GDPR)* (Vol. 29). Lex Medicina.

Pessoais, C. N. (s.d.). *Tratamentos de Dados de Saúde, Estudos e Ensaios Clínicos.* Comissão Nacional de Proteção de Dados Pessoais.

Pinheiro (Coord.), A., Pimenta, C., Duarte, T., Gonçalves, C. J., & Gonçalves, C. P. (2018). *Comentário ao Regulamento Geral de Proteção de Dados.* Coimbra.

Pinheiro, A. S. (2015). *Privacy e Proteção de Dados Pessoais: A Consrução Dogmática do Direito á Identidade Informacional.* AAFDL Editora.

Portuguesa, D. d. (27 de Abril de 2016). *Princípio da finalidade (tratamento de dados pessoais)*. Obtido de Diário da República Portuguesa: https://dre.pt/dre/lexionario/termo/principio-finalidade-tratamento-dados-pessoais

Portuguesa, D. d. (s.d.). *Dados relativos à saúde*. Obtido de Diário da Républica

Portuguesa: https://dre.pt/dre/lexionario/termo/dados-relativos-a-saude

Regulamento de Deontologia Médica, n.º 707/2016, de 21 de Julho, nº 2, art. 40º.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE).

República, A. d. (8 de Agosto de 2019). Lei nº 58/2019.

SABEC, Daniel Augusto; SIMÃO FILHO, Viana Adalberto. Democracia, Propaganda Eleitoral e Proteção de Dados. Anais do Congresso Brasileiro de Processo Coletivo e Cidadania, n. 8, p.156-173, out/2020, p. 158. Obtido em <https://revistas.unaerp.br/cbpcc/article/view/2190/1598>.

Sales Sarlet, G. B., & Caldeira, C. (2019). *O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brazil para a integral da pessoa humana.* Obtido de Revista Eletrónica de Direito Civil: https://civilistica.com/

Saúde, S. P. (s.d.). Privacidade da Informação no Setor de Saúde. Obtido de http://www.arsalentejo.min-saude.pt/arsalentejo/Noticias/Documents/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2%20(1).pdf#:~:text=Nesse%20sentido%2C%20a%20SPMS%20elaborou%20o%20presente%20Guia,rela%C3%A7%C3%A3o%20ao%20tratamento%20de%20dados%

Zuboff, S. (2020). *A era do capitalismo de Vigilância.* Relógo d' Água.