DEPARTAMENTO DE DIREITO

MESTRADO EM DIREITO

ESPECIALIDADE EM CIÊNCIAS JURÍDICAS

UNIVERSIDADE AUTÓNOMA DE LISBOA

"LUÍS DE CAMÕES"

A RESPONSABILIDADE CIVIL PELA VIOLAÇÃO DE DADOS PESSOAIS DA SAÚDE À LUZ DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

Dissertação para a obtenção do grau de Mestre em Direito

Autora: Izabella Eliana Gonçalves Schroeder

Orientador: Professor Doutor Ricardo Lopes Dinis Pedro

Número da candidata: 30005436

Dezembro de 2022

Lisboa

DEDICATÓRIA

Ao meu pai que, embora não esteja presente em minha vida de forma física, deixou-me como eterno legado a necessidade de nunca deixar de me dedicar aos estudos e ao meu aprimoramento intelectual, pois o conhecimento e a educação sempre nos abrem portas e são capazes de mudar o mundo.

AGRADECIMENTOS

O desenvolvimento e a conclusão da presente dissertação não teriam sido possíveis sem o apoio dos meus familiares, amigos, colegas e de minha psicóloga, os quais me acolheram e estiveram ao meu lado, mesmo diante dos piores cenários, e me incentivaram a seguir em frente diante das adversidades.

Os meus agradecimentos ao Professor Doutor Ricardo Pedro, que contribuiu para o aprimoramento dos estudos realizados através de suas sugestões e orientações.

Agradeço à minha amada mãe, que sempre esteve ao meu lado em toda minha carreira acadêmica, que desde muito cedo me ensinou e instigou a sempre me dedicar aos estudos e ao meu aprimoramento pessoal.

Por fim, mas não menos importante, agradeço ao Maximilian, por toda a paciência, acolhimento e apoio despendidos comigo durante o período em que estive a frequentar as aulas e a escrever a presente dissertação.

RESUMO

A implantação e o aprimoramento tecnológico são grandes facilitadores para o desenvolvimento dos processos sociais em todas as suas vertentes, permitindo o acesso, compartilhamento e armazenamento de milhares de informações, documentos e dados em segundos. Este intenso progresso tecnológico, tem influência direta no desenvolvimento de grande parte do cotidiano e da vida social, como por exemplo, nos tribunais, na educação e principalmente no âmbito da saúde. Na medida em que, as transformações digitais têm se mostrado com um grande contributo para o armazenamento e compartilhamento de informações que permitem o desenvolvimento e aprimoramento da saúde em geral. Apesar dos benefícios acarretados pelo intenso desenvolvimento tecnológico, não podemos deixar de olvidar que a ameaça de invasão da privacidade dos seus utilizadores tem crescido exponencialmente, sobretudo no momento atual, em que a saúde tem tomado extrema relevância social. Assim, o principal objetivo da pesquisa realizada é estudar o alcance e os limites da responsabilidade civil prevista no Regulamento Geral de Proteção de Dados (RGPD), diante da divulgação indevida dos dados pessoais da saúde. A partir da utilização de meios que permitem a pesquisa bibliográfica, jurisprudencial e documental, através de artigos, notícias e estudos realizados sobre o tema. O primeiro capítulo do estudo trata da evolução histórica do direito à privacidade, permitindo uma ampla compreensão acerca do regime de proteção dos dados pessoais. Em seguida, passamos à análise do direito da saúde e a essencialidade do regime de proteção de dados para o desenvolvimento e aprimoramento deste direito na sociedade. Por fim, o terceiro e último capítulo trata responsabilidade civil diante da ocorrência da violação de dados à luz do disposto no RGPD, sobretudo do seu alcance e principais limites. A efetiva ocorrência da violação de dados relativos à saúde nos remete diretamente à pessoa do responsável pelo tratamento e ao subcontratante, em virtude da disposição legal que reconhece a responsabilização imediata destas duas figuras. Há a possibilidade de ocorrência de duas modalidades distintas de responsabilização civil diante da violação de dados da saúde, as quais correspondem à responsabilidade aquiliana, que se verifica diante do incumprimento do disposto no RGPD e a responsabilidade obrigacional que advém da obrigação contraída através de um contrato. Para que se possa definir o alcance da responsabilização, é imperioso que se realize uma análise da situação em concreto que envolve o tratamento de dados, uma vez que um único tratamento de dados pode acarretar em uma ou mais responsabilidades, existindo também a possibilidade de não haver a responsabilização do responsável pelo tratamento ou do subcontratante se estes provarem que não são responsáveis pelo fato que ocasionou o dano.

Palavras-chave: Dados pessoais. Dados relativos à saúde. Violação de dados. Responsabilidade Civil.

ABSTRACT

Technological deployment and improvement are significant facilitators for the development of all sorts of social processes, allowing instant access, sharing, and storage of large amounts of documents, information, and data. This powerful technological progress has a direct influence on the development of a large fraction of everyday and social life such as on courts, in education and, mainly, in healthcare. Specifically, the latter has benefitted from digital transformations in storage and sharing of data which allow the development and amelioration of health in general. Notwithstanding the advantages brought by the major technological development, we cannot overlook that the threats of privacy invasion for the users has increased exponentially, specially in present times, when health care has become extremely relevant. Thus, the main goal of this work is to study the reach and limits of civil liability as envisaged by the General Data Protection Regulation (GDPR) in the context of the violation of health personal data. This is done by means of bibliographic, jurisprudence, and documentary research on articles, news items and research pieces on the subject. The first chapter presents the historic evolution of privacy law, allowing a wide understanding of private data protection code. After this, we continue with the analysis of health law and the essentiality of the private data protection code to the development and amelioration of this law in society. Finally, the third and last chapter deals with civil liability (mostly, its reach and main limits) when faced with the violation of data, as defined by the GDPR. The effectual occurrence of a violation of personal health data refers us to the responsible for their treatment, and to the data processor, the immediate responsible as defined by the code. Two possibilities arise in terms of civil liability in the face of violation of health data. One is the aquilian responsibility, which arises from the non-compliance with the provisions of GDPR. Another possibility is the compulsory liability, which emerges from the contractual obligations. In order to define the reach of the accountability, it is imperative that a specific analysis of the case is performed. In particular, in what is related to the data processing, given the possibility of appearance of several responsibilities, as well as no liability from the responsible for their treatment and the data processor whatsoever proven that they are not liable for the fact originating the damage.

Keywords: Sensitive data. Health care. Data breach. Civil liability.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

ADPDSI - Associação para a Promoção e Desenvolvimento da Sociedade da Informação

CC - Código Civil

CNPD - Comissão Nacional de Proteção de Dados

CRP - Constituição da República Portuguesa

DGS - Direção-Geral da Saúde

RDIS - Rede Digital com Integração de Serviços

RGPD - Regulamento Geral de Proteção de Dados

STJ - Supremo Tribunal de Justiça

TJUE - Tribunal de Justiça da União Europeia

UE – União Europeia

INTRODUÇÃO

O conceito de privacidade foi desenvolvido a aprimorado em nossa sociedade durante anos e, é essencialmente marcado pela relação existente entre o indivíduo e o espaço por ele habitado, contribuindo com a sua existência e aprimoramento da sua consciência individual.

O desenvolvimento social aliado à crescente ideia de preservação da privacidade individual acarretou ao emulsionamento do resguardo da intimidade e da vida privada. Nesse mesmo contexto, passou-se a existir a necessidade de criação de meios jurisdicionais que se mostrassem capazes de proteger à vida intima dos indivíduos e da sociedade.

Este cenário sofreu significativa intensificação quando a sociedade passou a contar com grandes avanços ocasionados pelo progresso tecnológico, o qual tem se apresentado como verdadeiro facilitador social, especialmente em relação à facilidade de envio e recebimento instantâneo de todos os tipos de informações, documentos e dados.

Todavia, tais avanços também podem se apresentar como uma ameaça aos direitos e liberdades dos indivíduos, principalmente no que diz respeito ao direito à reserva da vida privada.

Tal situação tem causado certo desconforto jurídico, sobretudo, no que diz respeito aos riscos para a privacidade do homem comum, de modo a exigir a criação de um Direito da Proteção de Dados se adaptasse às atuais condições sociais para regular e proteger os titulares dos dados contra os possíveis danos que possam advir da sua utilização indevida.

O conceito atribuído aos dados pessoais é muito bem consolidado em todo o território Europeu e encontra-se regulado no artigo 4º, 1º do RGPD, corresponde à "[...] qualquer informação relativa a uma pessoa singular identificada ou identificável [...]". De modo que, toda informação, independentemente da forma em que está armazenada, apresenta relevância para a aplicação do Direito da Proteção de Dados e, tais dados devem, obrigatoriamente, estar relacionados à uma pessoa singular, independentemente da sua nacionalidade ou local de residência[1].

Este aparente campo de proteção absoluto não pode nos levar a acreditar que o sistema jurídico não reconhece a existência de diferentes modalidades de dados, os quais, em virtude do conteúdo expresso em si, exigem que a norma estabeleça cuidados especiais, uma vez que, o tratamento destes dados poderá acarretar em significativos riscos para os direitos e liberdades

[1] CORDEIRO, A. Barreto Menezes – **Direito da proteção de dados:** à luz do RGPD e da Lei nº 58/2019, p. 113.

dos seus titulares, tratam-se dos dados pessoais sensíveis ou também denominados dados pessoais especiais.

Os dados relativos à saúde encontram-se elencados neste rol de dados sensíveis, uma vez que, em virtude da sua própria natureza podem vir a acarretar em vultosos danos aos seus titulares, como, por exemplo, a discriminação.

O conceito de dados da saúde pode ser extraído do artigo 4º, 15) do RGPD que entende que estes dados estão [...] relacionados com 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".

A leitura deste diploma legal deve ser complementada pelo Considerando nº 35, o qual nos apresenta uma face mais extensa deste conceito, de modo a salientar que se consideram dados pessoais de saúde todos aqueles que se relacionam com o estado de saúde de seu titular, que revelem informações sobre a sua saúde mental ou física, independentemente se colhido no passado, no presente ou em tempo futuro.

Em virtude da natureza e dos riscos associados aos dados sensíveis, o RGPD consagra um regime especial de tratamento destes dados, apresentando requisitos mais rigorosos do que se verifica no tratamento dos demais tipos de dados, inclusive, em regra, o ordenamento proíbe a realização de tratamento destes dados, o qual apenas é permitido diante de questões excepcionais, justificadas e havendo o devido amparo legal.

Conforme salientamos anteriormente, a evolução tecnológica tem contribuído com o avanço social no desenvolvimento das mais variadas atividades, incluindo-se o desenvolvimento e aprimoramento do direito à saúde e do bem-estar.

A coleta e a realização das operações de tratamento destes tipos de dados permitem que os profissionais que prestam serviços de cuidados à saúde tenham acesso à vida pregressa de seus pacientes e, além disso, a coleta de informações acerca da vida pessoal e seu armazenamento permitem que o profissional avalie as condições de cada paciente e prescreva o tratamento adequado.

Todavia, não podemos deixar de mencionar que, apesar de a realização de tratamento destes dados ser realizada de forma muito intensa em locais e instituições que prestam serviços de cuidados da saúde e bem-estar, o avanço tecnológico também contribuiu e permitiu a criação de softwares, programas informáticos e novos aparelhos tecnológicos que tem como objetivo realizar a coleta e tratamento deste tipo de dados.

Atualmente, contamos o auxílio de diversos meios e programas que contam com avançadas funcionalidades da saúde, por exemplo, os relógios inteligentes que realizam a coleta

de dados relativos à contagem diária de consumo calórico, acompanhamento de ritmo cardíaco, medição do nível de oxigênio no sangue, detecção da temperatura corporal, acompanhamento do ciclo menstrual com estimativas de ovulação, dentre outros.

Portanto, a justificava da existência de um amparo legal especial para os denominados dados sensíveis, advém da natureza das informações que constam nos dados relativos à saúde e da significância que estas informações apresentam para os direitos e liberdades de seus titulares.

Em que pese a existência de um regime legal que tem o objetivo de conferir o máximo amparo aos dados sensíveis, não podemos deixar de levar em consideração a efetiva possibilidade de ocorrência da divulgação destes dados.

No que diz respeito à divulgação de dados devemos, inicialmente, realizar uma ponderação essencial para o desenvolvimento do presente estudo, na medida em que o artigo 4º, nº 2 do RGPD nos apresenta o conceito atribuído à violação de dados, a qual advém de uma violação na segurança de dados, que provoque a destruição, perda, alteração, divulgação ou acesso não autorizado de dados. Portanto, sempre que estivermos diante de situações em que se verifica a divulgação indevida de dados, estaremos diante da ocorrência de uma efetiva modalidade de violação de dados.

Assim, sempre que tratarmos da violação de dados, estaremos englobando a divulgação não autorizada ou indevida destes dados. Na medida em que, a própria norma de proteção aos dados pessoais, não realiza tal distinção, tratando apenas do tema de violação de modo a abranger todas as suas possíveis espécies.

De acordo com o disposto no Considerando nº 85 do RPGD, a violação de dados pessoais pode ocasionar danos aos titulares "como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação de identidade, perdas financeiras, a inversão não autorizada de pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares.".

Nesse contexto é que surgem os primeiros aspectos de uma possível responsabilização civil em decorrência da efetivação de danos materiais e/ou imateriais ocasionados pela violação de dados.

Sendo que, tal responsabilização poderá advir de duas esferas completamente diferentes, sejam elas de natureza obrigacional decorrente da violação de um contrato, ou seja, nos casos em que "[...] a legitimação para o tratamento de dados assente em base negocial"[2].

Também podemos falar em responsabilidade extracontratual, a qual tem surgimento diante da violação das normas constantes no RGPD, na medida em que o próprio dispositivo, em seu artigo 82º, preleciona que qualquer indivíduo que tenha sofrido danos, na esfera moral ou material, em virtude de uma violação ao próprio Regulamento, tem o direito de ser indenizado pelo responsável pelo tratamento ou pelo subcontratante.

Portanto, o principal objetivo do presente estudo consiste em analisar a proteção jurídica conferida aos dados relativos à saúde, de modo a verificar o alcance e os limites enfrentados pelo regime de responsabilidade civil em virtude da efetiva ocorrência da violação destes dados.

Para a consecução do estudo adotar-se-á, no tocante à metodologia, o método de abordagem hipotético-dedutivo, o qual permite uma análise global dos temas estudados acarretando na possibilidade de verificação do alcance que a responsabilidade civil pode alcançar nos casos em que há a efetiva violação de dados da saúde.

Por fim, é sabido que a transformação digital ocorrida na sociedade, sobretudo na área da saúde, tem mostrado extrema relevância social, principalmente nos últimos anos, em que toda a sociedade se encontrou diante de uma crise de saúde global que, ao ser somada com a facilidade da coleta, compartilhamento e armazenamento de informações e dados, acarretou na intensificação da relevância da proteção dos dados relativos à saúde para toda a comunidade global.

Evidentemente que tal situação, confere ensejo à necessidade de haver um constante zelo jurídico no que diz respeito à proteção destes dados, em virtude do impacto que a possível ocorrência de uma violação pode vir a causar aos seus utilizadores em relação aos seus direitos e interesses individuais e, principalmente em relação à sua esfera intima e à privacidade.

[2] BARBOSA, Mafalda Miranda - **Data controllers e data processors:** da responsabilidade pelo tratamento de dados à responsabilidade civil, p. 462.

1. O DIREITO À PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

Vivemos em uma era marcada pelo progresso tecnológico, o qual tem se mostrado como um facilitador social, a contribuir de forma significativa para o progresso humano, especialmente em relação à facilidade de envio e recebimento instantâneo de todos os tipos de informações, documentos e dados.

Consequentemente, tais avanços têm contribuído de forma significativa para com a intensificação na coleta e tratamento de dados pessoais, o que tem causado desconforto jurídico, sobretudo, no que diz respeito aos riscos para a privacidade do homem comum, de modo a exigir que o Direito da Proteção de Dados se adaptasse às atuais condições sociais para regular e proteger os titulares dos dados contra os possíveis danos que possam advir da sua utilização indevida.

Diante disso, podemos afirmar que o direito da proteção de dados é repleto de justificavas que o fazem existir, dentre elas a necessidade de proteção ao direito da privacidade, ou seja, da vida privada.

Para dar início ao estudo jurídico proposto, o qual corresponde à visualização da responsabilização civil em virtude da violação de dados pessoais da saúde, é indispensável o preliminar estudo histórico acerca do direito à privacidade em seu sentido amplo, o que irá permitir a compreensão acerca dos motivos e as evoluções sociais que levaram à criação e ao desenvolvimento do direito da proteção de dados pessoais.

1.1 O SURGIMENTO E EVOLUÇÃO DO DIREITO À PRIVACIDADE

O conceito de privacidade está diretamente correlacionado às transformações políticas e sociais ocorridas durante toda a história da sociedade, inicialmente marcada pela relação entre o ser humano e o espaço em que habita, de modo a construir a sua existência e sua própria consciência individual.

Assim, é fundamental tratarmos do desenvolvimento histórico do conceito de privacidade sob o aspecto público e privado, uma vez que se tratam de conceitos que sofreram diversas alterações no decorrer da história, de modo a analisar a relação entre tais esferas (pública e privada) desde a antiguidade Grega até a sua transformação na contemporaneidade.

A antiguidade grega pode ser definida como um marco significativo para a distinção e divisão entre o poder público e o privado. De modo que, naquela época a sociedade poderia ser segregada em dois grandes núcleos, em que, a *pólis* corresponderia a esfera em que os cidadãos

livres interagiam entre si, enquanto que na *oikos*, as interações se apresentavam de forma mais privada entre os indivíduos da sociedade[3].

Entendia-se que, ao exercer a função política na esfera da *pólis*, o indivíduo estava inserido em uma espécie de segunda vida, a qual se separava completamente de sua atuação na esfera familiar, que se encontrava muito mais relacionada à execução de tarefas básicas da natureza humana. Assim, podemos afirmar que havia a inserção da esfera privada, denominada *oikos*, na esfera pública, todavia, ambas funcionavam de maneira autônoma.

De acordo com os ensinamentos de Cancelier[4], a esfera familiar poderia ser transitória, terrena e rudimentar, e se materializava no cotidiano do lar. Ao passo que, a esfera pública era o momento em que o cidadão poderia se apresentar para a sociedade, demonstrando quem realmente era e marcando a sociedade com suas habilidades físicas e intelectuais.

Havia um enorme contraste entre as duas esferas, na medida em que a esfera pública era garantida por um poder não coercitivo, que se fundamentava na existência de diálogo entre seus membros, podendo ser visualizado como um espaço de igualdade. Por outro lado, a esfera familiar era considerada uma necessidade básica do cidadão, apresentando-se como uma figura materialista e desigual[5].

Sendo que, o que hoje entendemos como a manifestação do íntimo, era possível apenas em um local, onde todos os seus membros fossem iguais. Nesse contexto, é importante ressaltar que a igualdade a que nos referimos não pode ser confundida com a justiça, uma vez que o que tornava os cidadãos iguais era o fato de serem cidadãos livres, com participação na esfera pública e ser detentor do comando nas esferas familiares[6].

Em contraposição ao sistema grego, os romanos, reconheciam a importância da coexistência da esfera pública e privada na vida dos cidadãos. Assim, pode-se afirmar que a noção contemporânea da privacidade teria se originado em Roma[7].

Seguindo o traçado histórico, com a queda do Império Romano do Ocidente o continente europeu passou a ser marcado pela descentralização do poder, onde os nobres passaram a ter o seu domínio segmentado, o que acarretou no surgimento a figura do status da pessoa pública.

---

[3] HABERMAS, Jürgen - **Mudança estrutural da esfera pública:** investigações sobre uma categoria da sociedade burguesa, p. 97-98.
[4] CANCELIER, Mikhail Vieira de Lorenzi - **Infinito Particular:** Privacidade no Século XXI e a Manutenção do Direito de estar só, p. 43.
[5] ARENDT, Hannah - **Entre o passado e o futuro**, p. 45.
[6] CANCELIER, *Op. Cit.*, p.43.
[7] ARENDT, *Op. Cit.*, p. 48.

Assim, a figura do nobre feudal passa a ser inserida na esfera pública, fazendo com que tal esfera seja reservada aos indivíduos que possuíam privilégios especiais[8].

Avançando para a Idade Média, a linha que distingue a esfera pública da privada, apresenta-se cada vez mais tênue, na medida em que se verifica uma valorização do privado, que se deu em virtude das alianças formadas, casamentos entre os filhos de lordes e as rivalidades entre as autoridades da época. O ambiente familiar passou a deter grande significância para a sociedade, de modo que as casas se tornaram ligadas a grandes dinastias[9]. Fazendo com que a busca pelo isolamento se tronasse cada vez mais evidente, bem como, reservada às famílias abastadas e nobres, dando ensejo a uma esfera privada que muito se assemelha à atual.

Não podemos deixar de mencionar que tal mudança na privacidade se limitava apenas a determinadas pessoas, as quais, em função de sua posição social, poderiam almejar o isolamento. Uma vez que, grande parte da população era privada até mesmo de ter acesso a esfera pública, de modo que, a necessidade de proteger os atos íntimos da vida civil não apresentava utilidade para grande parte da população.

A gradual queda do feudalismo acarretou na extinção da autoridade do senhor feudal, o qual passou a ser substituído pela administração pública. Portanto, o poder público passou a se ligar diretamente ao cargo público, de modo que a figura da autoridade deixou de ser um requisito que tornava possível a participação pública[10].

Na modernidade, tem-se o ressurgimento das cidades e o consequente retorno da ideia do estado-nação, e ainda, verifica-se uma crescente queda na imposição do conhecimento religioso, o qual passa a ser substituído pelo conhecimento científico. De modo que, a figura do Estado se apresentava como um elemento indispensável para o início da separação da esfera social da individual e, a consequente a dicotomia e definição entre as esferas privada e pública.

Pode-se afirmar que o direito à privacidade passou a ser uma prerrogativa atribuída tão somente à classe burguesa, que dela se utilizou para marcar sua identidade no âmbito social, e ainda, para proporcionar que o indivíduo possa isolar-se dentro da sua própria classe[11].

Assim, na modernidade, a liberdade humana era baseada em uma espécie de individualismo possessivo[12], em que a separação entre as esferas privada e pública, pode ser

[8] CACHAPUZ, Maria Claúdia Mércio - **Privacidade, proteção de dados e autodeterminação informativa**, p. 60.
[9] AGOSTINI, Leonardo Cesar de - **A intimidade e a vida privada como expressões da liberdade humana**, p. 120.
[10] CANCELIER, *Op. Cit*., p. 49.
[11] DONEDA, Danilo - **Da privacidade à proteção de dados pessoais**, p. 128.
[12] DONEDA, *Op*. *Cit.*, p.129.

vislumbrada como um meio de expressão da personalidade, ou seja, de se individualizar diante da sociedade em um espaço próprio. Para tanto, na constante busca pelo isolamento, a classe burguesa passou a se apropriar de locais, de modo que, o lar passou a ser visualizado como o único meio de praticar a individualidade. Portanto, podemos verificar que a propriedade de bens imóveis se tornou um elemento essencial para o pleno alcance da privacidade[13].

Nesse sentido, vale ressaltar que, o lar passou a se reestruturar para satisfazer esta nova necessidade pela intimidade, tomamos o exemplo de Thibes[14], a qual nos ensina que na Europa do Século XVIII, o lar não detinha a função de servir como abrigo, mas sim como um local para o desenvolvimento de atividades diversas, com grande fluxo de pessoas, o qual, muitas vezes, atendida a função de local de trabalho. Também se nota a diferença no cotidiano social, de forma que se verifica um aumento significativo no uso de diários, com o objetivo de armazenar informações de cunho íntimo e a utilização de cartas privadas.

Todavia, infelizmente a privacidade permanecia sendo um privilégio para poucos, na medida em que as classes mais desprovidas de recursos apenas tiveram a possibilidade de alcançar a privacidade depois que os meios materiais, que até então eram de exclusividade da burguesia, passaram a ser acessíveis a todos os cidadãos.

Na medida em que a sociedade burguesa passou a estabelecer o contraponto entre o íntimo e o social, os cidadãos acabaram por criar uma espécie de censura coletiva, formada por uma sociedade que se mostrava obcecada por padrões sociais e morais.

Este aumento significativo da preocupação com a aparência na esfera social fez com que a opinião sobre a vida do outro se tornasse algo fundamental no desenvolvimento da sociedade e, consequentemente, aumentando cada vez mais o interesse pela intimidade alheia, tornando-se uma realidade cada vez mais presente na sociedade.

Nesse mesmo contexto, as tecnologias surgidas na Revolução Industrial contribuíram para que, no início do Século IXI, a imprensa ganhasse força. De acordo com os ensinamentos de Cancelier[15] o valor acessível de exemplares acarretava no maior número de consumidores e o interesse pelo mercado de informações se tornava cada vez mais atrativo e acessível à toda a população.

Com o aperfeiçoamento tecnológico da imprensa começa a surgir o comércio de periódicos e jornais que continham informações da vida privada dos cidadãos, transformando a

[13] DONEDA, *Op. Cit.*, p. 130-131.
[14] THIBES, Mariana Zanata - **As formas de manifestação da privacidade nos três espíritos do capitalismo: da intimidade burguesa ao exibicionismo de si nas redes sociais**, p. 324.
[15] CANCELIER, *Op. Cit.*, p. 54-55.

atração pela vida intima alheia em uma mercadoria. Portanto, a notícia era comercializada e servia como fonte de compartilhamento de informações e fatos que norteavam a vida pessoal dos indivíduos da sociedade.[16]

Tudo isso acarretou na crescente preocupação com o resguardo e cuidado da intimidade e da vida privada e, justamente neste contexto que passa a se verificar a latente necessidade de criação de meios jurisdicionais capazes de conferir proteção à vida intima dos indivíduos da sociedade.

1.1.2 O surgimento do Direito à Proteção de Dados como resultado do desenvolvimento do Direito à Privacidade

O avanço da sociedade e o desenvolvimento e progresso tecnológico intensificaram cada vez mais a necessidade de preservação da esfera intima íntima dos indivíduos, acarretando na necessidade de instituição de um sistema jurídico que oferecesse maior amparo ao direito da privacidade, de modo a exigir que esta ramificação do direito se adaptasse à crescente realidade que vinha se desenvolvendo e dando espaço à necessidade de conferir amparo à proteção de dados pessoais.

Inicialmente, cumpre-nos salientar que o desenvolvimento histórico do direito à proteção de dados pessoais pode ser dividido em quatro grandes gerações, as quais contribuem com a compreensão sobre a evolução social e tecnológica e a sua influência no desenvolvimento da proteção de dados em todo o mundo.

Por este motivo, optamos por realizar um breve apanhado acerca de cada uma destas gerações e, em seguida, avançar os estudos com maior profundidade, de modo a tratar dos marcos históricos deste desenvolvimento.

A primeira geração da proteção de dados é marcada pela coleta e tratamento de dados pelo setor público, na medida em que a maior parte das normas que existiam sobre o tema eram aplicadas unicamente à esfera pública.

Enquanto que, a segunda geração é marcada pelo avanço da tutela jurisdicional no setor privado. Todavia, grande parte das normas tratavam a privacidade e a proteção de dados como uma liberdade negativa, uma vez que o seu objetivo principal consistia em oferecer um sistema que permitisse que os cidadãos identificassem a utilização indevida de seus dados e informações e pleiteassem a sua tutela.

[16] *Idem*.

Apesar de apresentar um certo avanço no sentido de incluir a esfera privada, esta geração logo deixou de ser suficiente para amparar a evolução tecnológica que se iniciava, uma vez que, a coleta e o fornecimento de dados pessoas pelos cidadãos e o seu aproveitamento tanto pelo Estado, como pelos entes privados, se mostrou como um fator fundamental para a sociedade.

Assim, verificamos o avanço da terceira geração, na medida em que se passou a ver o tratamento de dados não apenas como uma permissão ou não do seu uso, mas como um processo no qual se estimulava a participação ativa e consciente do titular dos dados, promovendo ao indivíduo uma série de garantias específicas como, por exemplo, o direito à informação.

Apesar desta geração se apresentar como o passo inicial para a autodeterminação informativa, a aplicação prática da participação ativa do titular era limitada na vida prática, pois o processo de exercer a tutela jurisdicional sobre o direito à autodeterminação informativa tinha preço elevado e, além disso, grande parte dos cidadãos não tinham o conhecimento da efetiva importância da preservação e cuidado com os dados pessoais.

As normas de quarta geração, são aquelas que atualmente compõem o direito à proteção de dados, as quais são diariamente desafiadas pelo constante desenvolvimento tecnológico aliado à necessidade de preservação da esfera privada dos cidadãos.

Realizado este breve apanhado sobre a evolução histórica do Direito à proteção de dados, passamos ao estudo pormenorizado da sua evolução no mundo e especialmente, na União Europeia.

Podemos afirmar que os primeiros passos da primeira geração do direito à proteção de dados ocorreram na década de 60, onde em 1965 iniciava-se a discussão legislativa nos Estados Unidos da América do *Special Subcommittee on Invasion of Privacy*, por meio de uma série de audiências que objetivavam aliar a necessidade de amparo jurídico dos cidadãos com a realidade que estava sendo vivenciada na época.

Ao total, foram realizados três conjuntos de audiências, os quais se deram entre os anos de 1965 a 1968, onde foram debatidos os seguintes temas: a violação da privacidade dos cidadãos por parte das agências federais, a necessidade da criação de um banco de dados único que centralizasse todas as informações recolhidas pelo Estado e os dados pessoais que eram colhidos pelas agências de crédito.

Passados oito anos da última audiência realizada, finalmente, aos 31 de dezembro de 1974, foi aprovado o *Privacy Act*, o qual apesar de tratar sobre a recolha, conservação, utilização e disseminação de informações pelas agências federais, deixou de “regular de forma

transversal o direito à autodeterminação informacional, recorrendo à expressão continental [...]"[17].

Em que pese a existência de intensas discussões acerca da matéria nos Estados Unidos da América, não podemos deixar de mencionar que esta preocupação também fazia parte do cenário Europeu, o qual teve a primeira norma relativa a proteção de dados aprovada no ano de 1970 pelo Parlamento do Estado de Hesse, na Alemanha.

De acordo com os ensinamentos de Menezes Cordeiro[18], o campo de aplicação desta norma se restringia às entidades públicas não continha qualquer preceito que limitasse o processo de tratamento dos dados e apenas reconhecia direitos secundários dos titulares dos dados, como, por exemplo, o direito de restaurar dados alterados ilicitamente ou de corrigir os dados incorretos.

Apesar disso, o diploma legal reconhecia a figura do Supervisor de Dados Pessoais, que era a autoridade competente para supervisionar o cumprimento da norma e os tratamentos de dados realizados pelos entes estatais.

Os progressos vividos na época levantaram a necessidade de criação de um diploma sobre a matéria que tivesse aplicação em toda a Alemanha, pelo que, no final do ano de 1973 foi apresentado um projeto de lei com este objetivo, que foi aprovado em 1977 e entrou em vigor no dia 1 de janeiro do ano seguinte. Tal diploma, era aplicável a todos os tratamentos de dados, independentemente se o responsável pelo tratamento detinha natureza pública ou privada.

Em que pesem os avanços alcançados pelo Sistema Jurídico Alemão, em 1973 a Suécia criou uma norma com aplicação transversal e nacional, ou seja, aplicável às autoridades públicas e privadas de todo o território, a qual recebeu a denominação de *Datalog.*

Em continuidade na linha histórica, podemos observar que a consciência da necessidade de criação de normas que conferissem respaldo jurídico aos dados pessoais cresceu cada vez mais no mundo todo, sobretudo na Europa, impulsionando o surgimento de diversas normas regulatórias internas em todo o território europeu.

Diante de tal necessidade, em 1973 o Comitê de Ministros do Conselho da Europa publicou a Resolução nº 73 (22), de 26 de setembro, a qual regulamentava a proteção da privacidade das pessoas, sobretudo em relação aos bancos de dados eletrônicos do setor privado, com o objetivo de tutelar os interesses dos cidadãos contra o processamento automatizado de dados. No ano seguinte, entrou em vigor a Resolução nº 74 de 20 de setembro

[17] CORDEIRO, *Op. Cit*., p.58
[18] CORDEIRO, *Op. Cit.*, p. 64-65.

de 1974, a qual tutelava a utilização indevida dos dados pessoais nos bancos de dados públicos, apresentando grande similitude com a legislação criada no ano anterior.

Não podemos deixar de mencionar que, Portugal reconheceu e conferiu o respaldo constitucional à proteção de dados pessoais na Constituição da República Portuguesa, aprovada em 02 de abril do ano de 1976, especificamente no artigo 35º, o qual regulava a utilização dos meios informáticos, assegurando que "Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização. 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. 3. É proibida a atribuição de um número nacional único aos cidadãos.". Conferindo respaldo jurídico aos titulares de dados e garantindo a consecução de seus direitos.

Ainda, em 1978 a França, também movida pela crescente necessidade de regulamentar tal matéria, criou a Lei nº 78-77 de 06 de janeiro, a qual foi posteriormente modificada pela Lei 2018-493 de 20 de junho, tal alteração se deu em virtude da necessidade de adaptação das normas ao Regulamento Geral sobre a Proteção de Dados, sobre o qual trataremos mais adiante.

Assim, resta evidente que a década de 80 é marcada pela consolidação da proteção de dados e de seus conceitos primordiais em todo o território europeu, dentre os documentos que contribuírem pera esta evolução, citamos a Convenção nº 108 do Conselho da Europa de 28 de janeiro de 1981 para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais.

Tal norma apresentou extrema importância para a consolidação dos princípios gerais e termos base que até hoje são utilizados, ou seja, "os princípios formadores do Direito da proteção de dados encontram aí, se não a sua origem, certamente as suas bases mais sólidas. "[19].

Trata-se da primeira ferramenta internacional com força vinculativa adotada no âmbito da proteção de dados e, sua criação deu-se com o objetivo de garantir o respeito pelos direitos fundamentais dos cidadãos, sobretudo, no que diz respeito à vida privada em detrimento do tratamento automatizado de dados pessoais.

Aos 29 de julho do ano de 1990 a Comissão apresentou novo grande avanço para o direito da proteção de dados, na medida em que apresentou duas Propostas de Diretrizes, uma relativa à proteção das pessoas, nomeadamente sobre o tratamento de seus dados e outra,

[19] CORDEIRO, *Op. Cit.*, p. 67.

relativa a proteção dos dados pessoais e da vida privada sob o viés da rede digital de serviços integrados e as redes públicas móveis digitais.

Passados cinco anos da apresentação da proposta, o diploma final restou aprovado, o qual corresponde a Diretiva nº 95/46/CE de 24 de outubro de 1995. Seu surgimento se deu em virtude da constatação da necessidade de criação de uma norma supranacional. Ou seja, uma norma que apresente aplicação em todo o território europeu, que pudesse diminuir a disparidade legislativa existente entre os Estados-membros, e ainda, estabelecesse respaldo jurídico à vida privada no âmbito da realização de procedimentos de tratamento de dados pessoais, sempre visando a constante evolução tecnológica.

Dentre as novidades apresentadas por tal norma, destacamos a inserção de alguns pontos que se encontram presentes na legislação mais atual sobre o tema, como, por exemplo, a recolha de dados com uma finalidade específica, o direito ao acesso dos dados pelo seu titular e a responsabilização acerca da segurança das informações armazenadas. Ainda, a norma determinava que os estados membros da União Europeia tivessem um órgão ou profissional responsável pela implementação e supervisão do cumprimento das normas.

Passados dois anos, com o avanço tecnológico, sobretudo diante da introdução da Rede Digital com Integração de Serviços (RDIS) e das redes móveis digitais, verificou-se a necessidade de conferir maior segurança jurídica ao tratamento de dados pessoais, o qual vinha se intensificando diariamente.

Diante disso, o Parlamento Europeu e o Conselho da União Europeia adotaram a Diretiva nº 97/66/CE, a qual passou a obrigar os Estados membros a estabelecerem normas que objetivassem garantir a confidencialidade das telecomunicações.

No ano de 2001 foi aprovado o Regulamento CE/45/2001 do Parlamento Europeu e Conselho de 18 de dezembro de 2000, o qual faz alusão à proteção das pessoas físicas quanto ao tratamento de dados pessoais pelas instituições e organismos comunitários e a livre circulação de dados.

A criação desta norma se justifica pela necessidade de criação de um sistema de proteção de dados que protegesse os diretos dos titulares de dados e, ao mesmo tempo, atribuísse determinados deveres aos indivíduos responsáveis pelo tratamento dos dados pessoais.

E ainda, diante da constatação da necessidade de criação de sanções adequadas aos infratores e da sua fiscalização por um órgão independente. Dando-se surgimento à figura do Supervisor Europeu de Proteção de Dados, com o objetivo de conferir maior proteção aos dados dos cidadãos que tiveram seus dados violados por organismos ou empresas em todo o território da União Europeia.

Logo em seguida, em virtude dos avanços advindos da evolução tecnológica, sobretudo do aprimoramento e acesso aos meios eletrônicos e a internet, verificou-se a necessidade da criação de novas normas que se adaptassem à realidade vivenciada por toda a sociedade.

De forma a tutelar os novos riscos à privacidade e aos dados pessoais. Diante desta necessidade, no ano de 2002 a Diretiva 97/66/CE restou substituída pela Diretiva nº 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho, a qual tinha como objetivo regular o procedimento de tratamento de dados e assegurar a proteção da privacidade no âmbito das comunicações eletrônicas.

Diante dos grandes casos de violação de dados ocorridos em todo o mundo nos anos seguintes, a União Europeia optou por rever as regras de proteção de dados para tanto e, deu vida ao Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, o qual passou a produzir efeitos em 25 de maio de 2018 com aplicação em todo o território da União Europeia e revogou a antiga Diretiva nº 95/46/CE.

Também denominado RGPD, este diploma é a maior mudança verificada na proteção de dados nos últimos vinte anos, o qual apresenta um conjunto de regras que devem ser implementadas por todos os Países-Membros da Comunidade Europeia com vista a dar controle aos cidadãos sobre os seus dados, sobretudo aos que se encontram em posse e cuidados de terceiros.

Diante de todo o contexto histórico traçado, é possível verificar a adaptabilidade e o constante desenvolvimento do direito à privacidade que, ao ser aliado à evolução social e tecnológica, gerou a necessidade de respaldo do ente Estatal, culminando na consequente necessidade de criação de normas acerca da proteção de dados com o objetivo de resguardar os direitos dos cidadãos em manterem suas vidas privadas em sigilo e evitando a violação de demais direitos fundamentais individuais, tendo em vista o constante e recorrente avanço das tecnologias e a facilidade na recolha e tratamento de dados.

Diante do exposto, podemos auferir que, atualmente, o regime de proteção de dados pessoais encontra amparo no Regulamento 2016/679 do Parlamento e do Conselho de 27 de abril de 2016, também denominado RGPD o qual tem aplicabilidade transversal em todo o território da União Europeia. O qual deve ser considerado de forma conjunta com a Lei nº 58/2019, a qual traz para o direito interno de Portugal, as prerrogativas dispostas no RGPD.

Assim, ambas as normas serão utilizadas como meio de amparo legal para a construção desenvolvimento do presente estudo, uma vez que, regulam toda a matéria de proteção de dados no âmbito interno e internacional.

1.2 O CONCEITO DE DADOS PESSOAIS À LUZ DO RGPD

Feitas as considerações pertinentes acerca do desenvolvimento e aprimoramento do direito da privacidade e a sua influência direta sobre o direito da proteção de dados, o qual teve surgimento diante da necessidade de criação de normas que conferissem maior segurança jurídica aos titulares de dados, em virtude do incessante desenvolvimento social.

Passamos agora ao estudo do conceito que o atual RGPD atribuí aos dados pessoais, o que permitirá uma melhor compreensão do tema sob estudo, e facilitará a compreensão do significado de dados relativos à saúde, que é um ponto essencial para a construção do presente estudo.

O RGPD atribuí um conceito muito claro sobre os dados pessoais, tornando-os muito bem consolidados em todo o território europeu. Portanto, para a construção do presente estudo tomaremos como base o conceito estabelecido no artigo 4º, 1) do aludido diploma legal, o qual os conceitua como: "qualquer informação relativa a uma pessoa singular identificada ou identificável".

Para que possamos compreender a extensão da lei e o objetivo do legislador quando da sua criação, é indispensável realizar uma análise acerca da extensão da norma de forma minuciosa, exigindo-se a análise de cada uma das expressões que compõe a norma.

Da expressão "[...] qualquer informação [...]" contida no preceito legal, podemos auferir que toda e qualquer informação é relevante para aplicação do Direito da proteção de dados. Ao realizar uma análise acerca desta expressão o autor Menezes Cordeiro[20] faz uma importante colocação ao sustentar que, o campo alcance desta expressão é muito amplo, uma vez que não há informação pessoal que não mereça proteção jurídica, por mais insignificante que aparente ser.

Incluem-se neste interim, todos os aspectos que possam envolver a vida profissional, privada, social, pública, mental, física, *etc*. A informação pode dizer a respeito de elementos que se prestam a identificar o indivíduo, como, por exemplo, nome, número do cartão cidadão, data de nascimento, filiação. E ainda, pode se referir a considerações intimas (opiniões, crenças), características físicas, patrimoniais, acadêmicas, ou seja, são inúmeros e incontáveis os tipos de informações que se encontram amparados pelo RGPD.

Levando-nos à conclusão de que, toda e qualquer informação merece proteção jurídica, independentemente do suporte em que está armazenada e da forma em que foi recolhida.

[20] CORDEIRO, *Op. Cit.*, p. 108.

Nesse sentido, a fim exemplificativo, tomamos alguns exemplos colhidos da jurisprudência do Tribunal de Justiça da União Europeia (TJUE), que reconhece a necessidade de proteção de jurídica sobre a vídeo vigilância com gravação de imagens (TJUE, de 11 de dezembro de 2014, processo nº C-212/13 de Ryneš), bem como de atas de reunião de pessoas jurídicas em que constem os nomes dos participantes (TJUE, de 29 de junho de 2010, processo nº C-28/08), e ainda reconhece a necessidade de proteção dos registros sobre os trabalhadores que são armazenados pelo empregador (TJUE, de 30 de maio de 2013, processo nº C-342/12).

Em continuidade à análise do dispositivo legal supramencionado, a segunda expressão contida no artigo 4º, 1) do RGPD - "[...] Relativa a pessoa [...]" – evidencia que, para que possa ter amparo desta norma e ser considerada um dado pessoal, a informação deverá ser diretamente relacionada a uma pessoa. Portanto, estão excluídas do âmbito de proteção do RGPD as informações que dizem respeito a "realidades jurídicas não subjetiváveis"[21] como, por exemplo, informações sobre objetos ou animais.

É necessário ter muito cuidado com este tipo de informação, uma vez que há uma linha tênue que divide os dados que dizem respeito à fatos e os dados relacionados às pessoas. Uma vez que, podem haver casos em que a informação colhida apresenta algum elemento que permita a identificação de seu titular, por mais insignificante que pareça ser, estaremos diante de um dado pessoal que, consequentemente, encontra-se respaldado pelas regras do RGPD.

Para melhor elucidar a questão, apresentamos o exemplo utilizado pelo Grupo de Trabalho do Artigo 29º[22], o qual nos ensina que, quando nos deparamos com a divulgação do valor de um determinado imóvel, não há que se falar na aplicação das normas de proteção dados, uma vez que a informação disponibilizada serve apenas para "ilustrar o nível dos preços do imobiliário".

Todavia, a questão se mostra completamente diferente se a analisarmos por outro prisma, em que o imóvel é um ativo do proprietário, o qual servirá para determinar a obrigação do proprietário em pagar terminados impostos. De acordo com o parecer supracitado, é indiscutível que tal informação deve ser considerada como um dado pessoal uma vez que se relaciona diretamente com uma pessoa.

Assim, o enquadramento de uma informação como um dado pessoal é marcado por uma linha extremamente tênue, a qual depende exclusivamente da natureza e do conteúdo da informação.

---

[21] CORDEIRO, *Op. Cit*., p. 110.

[22] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA - **Parecer nº 4/2007 sobre o conceito de dados pessoais**, p.10.

Seguindo os ensinamentos propostos pelo Grupo de Trabalhos do Artigo 29º[23], ainda no Parecer nº 04/2007, para considerar que os dados se relacionam a uma pessoa é necessário que se verifique a presença de um elemento de conteúdo, de finalidade ou ainda, de resultado.

O citado elemento de conteúdo encontra-se presente nos casos em que se fornece a informação acerca de determinado indivíduo, ou seja, quando estamos diante de uma informação em que o próprio titular dos dados é objeto de análise. A existência prática deste elemento pode ser verificada, por exemplo, nos resultados de análises clínicas, em que dizem respeito à um paciente.

Enquanto que a finalidade se encontra presente quando os dados utilizados levam em consideração uma circunstância específica, com o objetivo de avaliar ou influenciar um indivíduo.

Tomamos o exemplo dado pelo Grupo de Trabalho sobre o artigo 29º[24], em que o escritório de uma empresa faz o registro das chamadas de um telefone, de modo a armazenar as informações sobre as chamadas realizadas daquele aparelho de telefone que está ligado a uma determinada linha.

A linha telefônica é disponibilizada pela empresa, que faz o pagamento pela realização de chamadas. Sendo que, durante o período de trabalho, o aparelho telefônico poderá ficar sob o controle de um determinado empregado que efetua as chamadas, mas também, pode ser utilizado por outros empregados, como, por exemplo, o responsável pela limpeza. De modo que, as informações que dizem respeito às ligações podem ser relacionadas com diversos sujeitos.

Assim, pode-se sustentar que existem diversas finalidades, vez que a informação sobre o uso do aparelho pode ser relativa à empresa, ao empregado ou ao responsável pela limpeza. O conceito de dados pessoais abrange tanto as chamadas efetuadas como as recebidas, na medida em que todas as chamadas se relacionam com informações que estão diretamente relacionadas com as relações pessoais de comunicação de pessoas.

Na medida em que, entende-se como resultado, toda e qualquer informação em que seu conteúdo não diga respeito à uma pessoa e que não tenha a finalidade de influencia-la ou avaliá-la, mas que, em abstrato, é possível fazer. Ou seja, verifica-se a ausência dos elementos apresentados anteriormente (conteúdo e finalidade), porém a informação pode ter um impacto

[23] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEI, *Op. Cit.*, p. 09.
[24] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA, *Op. Cit.*, p. 11.

nos interesses do indivíduo, levando em consideração as circunstancias que norteiam o caso em específico.

Mais uma vez, tomamos o exemplo elucidativo apresentado pelo Grupo de Trabalhos sobre o Artigo 29º[25] em que uma empresa de taxis instala um sistema de localização por satélite em todos os veículos da frota, o que permite que tal empresa acompanhe a posição dos veículos disponíveis.

Em princípio, os dados coletados pelo sistema se relacionam aos carros e não aos motoristas. Porém este mesmo sistema permite que a empresa controle o desempenho do empregado, na medida em que permite que se verifique se estão a respeitar os limites de velocidade das vias, se estão trabalhando ou não, *etc*. Portanto, pode existir um impacto significativo para com os motoristas, de forma que tais dados passam a pertencer a pessoas singulares, ensejando a necessidade de invocação as regras de proteção de dados.

Os três elementos acima citados (conteúdo, finalidade e resultado) não devem ser considerados como condições cumulativas, mas sim como alternativas, na medida em que quando verificamos a presença do elemento de finalidade, não é necessário que os demais elementos estejam presentes para considerarmos a informação como um dado pessoal, e vice-versa.

Podemos perceber que há uma linha tênue que divide uma informação de um dado pessoal e que este primeiro pode facilmente se transformar no segundo, bastando que a informação de alguma forma e, mesmo que indiretamente permita a identificação do sujeito. Assim, não é necessário que a informação se concentre diretamente ou faça menção expressa a um indivíduo para que seja considerado um dado relativo à pessoa.

Portanto, para que seja possível determinar se um dado é relativo à uma determinada pessoa é imprescindível que seja realizada uma análise minuciosa e individual do dado em causa, levando-se em consideração todas as circunstâncias que se relacionam com o caso posto.

Avançando o estudo da literalidade legal contida no artigo 4º, nº 1 do RGPD, nos deparamos com a expressão "[...] pessoa singular [...]", a qual imediatamente nos remete ao campo de aplicação material das normas de proteção de dados. Levando-nos a acreditar que se encontram amparadas todas as pessoas singulares, independentemente de questões externas, como, por exemplo, do local em que fixam residência ou de sua nacionalidade, logicamente, excluindo-se as pessoas coletivas.

[25] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA, *Op. Cit.*, p. 12.

Podemos extrair do Considerando 14[26]: "O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva.".

Para melhor compreensão do termo, podemos extrair o conceito de pessoa singular apresentado no artigo 6º da Declaração Universal dos Direitos do Homem, a qual preleciona que "Todas as Pessoas têm o direito a serem reconhecidas como sujeitos perante a lei". A legislação civil portuguesa sublinha de forma mais precisa a capacidade jurídica das pessoas singulares, nomeadamente nos artigos 66º ao 68º do CC, determinando que seu início se dá diante do nascimento completo e com vida e perdura até a sua morte.

Em princípio, os dados pessoais dizem respeito às pessoas vivas, identificadas ou identificais, o que acaba por acarretar em uma série de questões que merecem atenção, sobretudo à possibilidade de existirem exceções no que diz respeito às pessoas mortas, pessoas coletivas e aos nascituros.

Por via de regra, as informações que dizem respeito às pessoas mortas não devem ser consideradas como dados pessoais, uma vez que, para o Direito Civil a personalidade jurídica se extingue com a morte. Contudo, há casos em que os dados que dizem respeito às pessoas falecidas podem e devem receber a proteção jurídica do RGPD.

Primeiramente, devemos levar em consideração que nem sempre o responsável pelo tratamento dos dados pode estar em posição de determinar se o titular dos dados se encontra vivo ou se já faleceu. De acordo com o Parecer nº 4/2007 emitido pelo Grupo de Trabalho de Proteção de Dados do Artigo 29º, as informações que dizem respeito às pessoas falecidas podem ser tratadas "ao abrigo do mesmo regime aplicado aos vivos, sem distinção"[27] e continua, ao sugerir que, na prática, seria muito mais fácil realizar o tratamento dos dados de pessoas falecidas da mesma forma imposta pela regra de proteção de dados, ao invés de separar as informações em dois grupos, uma vez que o responsável pelo tratamento dos dados está atrelado ao cumprimento das obrigações dispostas no RGPD.

Analisando o tratamento de dados de pessoas falecidas sob outro panorama, não podemos deixar de mencionar que os dados ou informações de uma pessoa morta podem também fazer referência à uma pessoa que esteja viva, ainda que, de forma indireta. Como, por

[26] REGULAMENTO (UE) 2016/679 - **Jornal Oficial da União Europeia**, p. 02.
[27] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA, *Op. Cit.*, p. 23.

exemplo, a informação de que uma pessoa faleceu em virtude de uma doença genética, o que indica que seus filhos também sofrem ou podem vir a sofrer da mesma doença.

Portanto, quando o dado contém informações sobre pessoas falecidas e que puderem de alguma forma, ser relacionadas com pessoas vivas, estamos diante de um dado pessoal que é sujeito às normas do RGPD. De forma que, os dados da pessoa morta usufruem, ainda que indiretamente do amparo jurídico consagrado pelas regras de proteção de dados.

Não podemos deixar de mencionar que as informações que dizem respeito sobre pessoas já falecidas podem ser sujeitas a uma proteção específica, atribuída por regras que vão além do RGPD, como, por exemplo, a obrigação de confidencialidade médica que não finda com a morte do paciente (Regulamento da Ordem dos Médicos n.º 707/2016).

Nesse mesmo sentido, não podemos deixar de lembrar que, o avanço da ciência e da medicina tem facilitado a recolha de diversas informações que dizem respeito aos nascituros, desde análises do líquido amniótico à ecografias e exames em geral que se prestam a verificar e acompanhar o desenvolvimento da vida e da saúde do nascituro.

O debate acerca da proteção de dados dos nascituros não pode ser analisado única e exclusivamente sobre a perspectiva do RGPD, uma vez que a aplicação de tais normas depende diretamente do posicionamento dos sistemas jurídicos de cada um dos Estados-Membros sobre a proteção dos direitos dos nascituros.

Portanto, para que possamos determinar se as disposições de um determinado Estado-Membro conferem proteção jurídica aos dados dos nascituros é indispensável analisar e considerar a abordagem geral do ordenamento jurídico, juntamente com a ideia de que o objetivo das regras de proteção de dados é justamente proteger a pessoa.

Conforme dito anteriormente, o artigo 66º do CC trata do início da personalidade, a qual é adquirida no momento do nascimento completo e com vida, salientando em seu parágrafo 2º que "Os direitos que a lei reconhece aos nascituros dependem do seu nascimento. ".

Não restam dúvidas de que os dados pessoas dos nascituros merecem proteção jurídica, porém levando em consideração o disposto na lei supracitada, questiona-se a que título a proteção dever ser realizada, ou seja, se estamos diante de dados pessoais da genitora ou dos dados pessoais do nascituro.

Para o autor Menezes Cordeiro[28] os direitos que a lei confere aos nascituros depende tão somente do seu nascimento. Assim, pode-se considerar que, independente da pessoa a quem a

[28] CORDEIRO, *Op. Cit.*, p. 114.

titularidade é atribuída, durante o período que se estende entre o momento da concepção e o nascimento completo, os dados pessoas serão pertencentes ao nascituro.

O último elemento a ser analisado e que compõem o conceito legal atribuído aos dados pessoais enfrenta uma situação peculiar, vez que se encontra parcialmente conceituado no RGPD. Isto porque o legislador apenas quedou-se a identificar o que se entende pela expressão "identificável", sem tratar do conceito que deve ser atribuído à expressão identificada.

Por este motivo é que inicialmente, iremos estudar o conceito atribuído à palavra identificável, conforme preleciona o artigo 4º do RGPD: "[...] é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.".

Complementando o disposto no artigo supracitado, o Considerando nº 26[29] também trata do tem sob análise, ao afirmar que "Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados [...] para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.".

O cuidado dispensado pelo legislador em conceituar e elucidar o elemento evidenciam a sua maior complexidade e a relevância para o conceito a ser atribuído aos dados pessoais.

Conforme elucidamos no início do presente capítulo, o legislador não atribui um conceito definido à expressão "identificada", bem como, não realizou nenhuma distinção em relação à, já estudada, expressão identificável.

Todavia, tal distinção não nos parece ser determinante, uma vez que, independente do titular dos dados ser uma pessoa identificável ou identificada, a proteção jurídica conferida pelo ordenamento será sempre a mesma. Em contrapartida, o esclarecimento legal de cada um dos termos impossibilita o entendimento completo acerca do conceito de dados pessoais.

Acreditamos que, estaremos diante de uma pessoa identificada, sempre que uma determinada informação por si só é suficiente para identificar o indivíduo, sem a necessidade

[29] REGULAMENTO (UE) 2016/679 - *Op. Cit*., p. 19.

de recorrer à dados adicionais. Por exemplo, o nome completo de uma pessoa, o número de contribuinte, número da Segurança Social ou impressões digitais, dentre outros[30].

Nesse sentido, não podemos deixar de mencionar que a possibilidade de identificação do titular dependerá da circunstância em concreto sob o qual a informação diz respeito. Portanto, para que seja possível determinarmos se estamos diante de uma informação de pessoa identificada é necessário avaliar a informação como um todo, bem como os aspectos exteriores que se relacionam diretamente com o dado.

Em contrapartida, estaremos diante de uma informação que diz respeito à um sujeito determinável sempre que for possível identificar o titular de dados ao conjugar a informação principal já detida à outra informação secundária, que também pode ser denominada como informação adicional.

Nesse sentido, aos 22 de abril do ano de 2020, a Comissão Nacional de Proteção de Dados (CNPD)[31] emitiu um quadro de orientações "Sobre a divulgação de informação relativa a infetados por Covid-19" em virtude de alguns questionamentos que estavam a ser levantados pela população acerca da constante disponibilização e divulgação de informações que diziam respeito à quantidade de infectados por região.

Uma das orientações emitidas pela CNPD emitidas no aludido documento, pode-nos servir de exemplo para o tema sob debate, vez que a Comissão se posicionou no sentido de ser proibida a publicação de dados que informam a quantidade de infectados pela Covid-19, mesmo sem a identificação dos pacientes, quando em virtude do reduzido número habitacional em uma determinada circunscrição territorial permita a identificação dos contaminados.

Vejamos: " [...] não podem ser publicados dados de saúde, mesmo sem identificação dos doentes, quando o seu reduzido número numa determinada circunscrição territorial, em função da respetiva dimensão populacional, permita a identificação das pessoas contaminadas [...]. Assim, a divulgação de dados que permita a identificação do seu titular, ainda que de forma indireta e subsidiária (porque precisa de algum outro dado ou informação para que se possa concluir a quem pertence o dado) é completamente proibida.

Tal questão é mais profunda do que pode parecer, a doutrina e jurisprudência têm se dividido acerca da relevância ou irrelevância dos conhecimentos e meios dos terceiros. Dando surgimento a duas grandes teorias: a teoria relativa, que compreende a análise da razoabilidade aos conhecimentos e meios detidos pelo responsável pelo tratamento e a teoria objetiva que

[30] CORDEIRO, *Op. Cit*., p. 121.
[31] COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS - **Orientações: Sobre divulgação de informação relativa a infetados por Covid-19**, p. 03.

compreende a análise da razoabilidade aos conhecimentos e meios detidos pelo responsável e por terceiros.

Para a construção do presente estudo iremos levar em consideração a teoria objetiva, porém não em sua forma pura, mas de forma a flexibiliza-la, levando em consideração a interpretação da norma que rege o tema.

O artigo 4º, nº 1º do RGPD não faz qualquer menção acerca da relevância dos conhecimentos detidos por terceiros ao tratar do conceito atribuído aos dados pessoais, vejamos: "«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;"

Tal indicação também pode ser observada no Considerando nº 26[32] da mesma norma, vejamos: "Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular.".

Evidente que o legislador europeu não acolheu a intitulada teoria objetiva pura na medida em que a própria lei determina que apenas podem ser considerados os meios razoáveis, excluindo-se todos os meios. De modo que devem ser considerados apenas os meios suscetíveis de serem razoavelmente utilizados.

Portanto, adotamos o posicionamento de que devemos dar atenção aos meios detidos por todos os sujeitos, porém a análise casuística deverá se limitar aos conhecimentos que os terceiros tenham à sua disposição.

Após identificarmos as nuances que permeiam o conceito de dado pessoal sob o prisma do RGPD, permitindo a delimitação e identificação das informações que se encontram abarcadas pelo regime jurídico de proteção de dados. Passamos a aprofundar os estudos desenvolvidos até então de modo a tratar dos dados sensíveis, sobretudo os dados relativos à saúde, de modo a identificá-los e situar o leitor acerca do tema em debate para que futuramente, possamos tratar com propriedade acerca da responsabilidade civil no âmbito da violação de tais dados.

[32] REGULAMENTO (UE) 2016/679 - *Op. Cit.*, p. 17.

1.2.1 Dados Sensíveis

Conforme restou salientado anteriormente, o direito da proteção de dados confere proteção jurídica a todos os dados pessoais, por mais triviais que possam aparentar ser. Todavia, a generalidade e a abrangência da proteção que é conferida a tais dados não significa que o sistema jurídico atual não reconheça diferentes modalidades de dados em virtude do seu conteúdo.

O RGPD criou uma distinção de alguns dados que apresentam a necessidade de maiores cuidados, intitulando-os de dados sensíveis ou dados especiais. Tal distinção se justifica pela natureza destes dados, os quais se mostram especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais. Eis que, o tratamento de tais dados pode vir a implicar em riscos significativos para os direitos e liberdades fundamentais do seu titular.

O artigo 4º do RGPD, apresenta três categorias concretas dos considerados dados especiais, sendo elas: dados genéticos, dados biométricos e dados relativos à saúde. Ainda, o legislador europeu no artigo 9º da mesma norma, elencou de forma taxativa os dados que, em virtude de sua natureza, merecem tal definição, podendo ser divididos em dois grandes blocos.

O primeiro bloco diz respeito aos resultados decorrentes do tratamento e consistem em: os tratamentos que revelem a origem étnica ou racial, filiação sindical ou convicções religiosas. Enquanto que o segundo bloco, por sua vez, trata das categorias de dados genéticos, biométricos, dados relativos à orientação sexual ou vida sexual e dados relativos à saúde.

Nesse sentido, o autor Menezes Cordeiro[33] trata das razões que levaram o legislador a fundamentar a eleição de tais categorias, as quais levam em consideração a proibição da discriminação consagrada no artigo 21º da Carta dos Direitos Fundamentais da União Europeia e no artigo 26, nº 1º da Constituição da República Portuguesa, acrescida a natureza de direito fundamental de tais dados, bem como, a situação vulnerável em que o titular se encontra ou os possíveis efeitos prejudiciais que possam resultar do seu tratamento.

Ressaltamos que o artigo 9º, nº 1º do RGPD, em regra, proíbe o tratamento dos dados pessoais sensíveis, salvo algumas exceções previstas no nº 2º do mesmo artigo, a qual iremos abordar com maior profundidade no capítulo dedicado ao estudo e análise do tratamento dos dados sensíveis.

Feitas breves considerações acerca dos dados especiais, os quais são merecedores do maior respaldo jurídico em virtude de sua natureza e do risco que o seu tratamento pode oferecer

[33] CORDEIRO, *Op. Cit.*, p. 133.

para os seus titulares, passamos a estudar e conceituar os dados relativos à saúde e a sua relevância para o atual sistema jurídico e social.

1.2.1.1 Dados relativos à saúde

Inicialmente, passaremos à análise dos dados relativos à saúde, considerando-os integrados na categoria dos dados pessoais sensíveis, o que nos leva a tomar como referência generalizada o RGPD e, como norma regular especial o Regime Jurídico da Informação de Saúde.

O artigo 4º, nº 15 do RGPD nos apresenta a definição legal de dados relativos à saúde na medida em que preleciona que se tratam de "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde que revelem informações sobre seu estado de saúde".

O texto legal é complementado e, melhor esclarecido, pelo Considerando nº 35, o qual preleciona que "Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde [...]".

Em sentido amplo, os dados pessoais relativos à saúde dizem respeito ao estado de saúde e bem-estar se seu titular e são, em sua grande maioria, recolhidos, utilizados e registrados pelos profissionais da saúde, no exercício de sua profissão.

Ainda, a Lei nº 12/2005 de 26 de janeiro que regula a informação genética pessoal e de saúde, conceitua as informações relativas à saúde como "todo 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"[34].

De acordo com Deodato[35] os dados da saúde são resultados de um contexto específico e detém uma finalidade particular. O contexto em que se encontram inseridos advém de uma relação terapêutica entre a pessoa (titular de dados) e o profissional da saúde, sendo que, a sua finalidade consiste na assistência, ou seja, na intervenção terapêutica, paliativa ou diagnóstica.

Todavia, as informações relativas à saúde não se restringem ao conhecimento do profissional e de sua equipe multidisciplinar, existem diversos meios e métodos de

[34] Artigo 2º da Lei 12/2005, de 26 de janeiro.
[35] DEODATO, Sérgio – **A proteção dos dados pessoais de Saúde**, p. 16.

disponibilização, recolha e manutenção destas informações, como, por exemplo, *softwares*, programas e aplicativos eletrônicos que realizam a monitorização da saúde e do bem-estar.

Portanto, a assistência em saúde tem apresentado um contexto cada vez mais amplo e complexo, onde a proteção jurídica de tais dados exigem uma resposta rápida e eficaz. De forma a expandir o seu campo de aplicação, ampliando-se para além do âmbito das organizações de saúde, como centros de saúde e hospitais e atingindo o crescimento e expansão tecnológica.

Conforme salientamos anteriormente, a proteção normativa dos dados essenciais encontra a justificativa de sua denominação como categoria especial em virtude da relevância das informações com que se relacionam. Nessa perspectiva, devemos nos dedicar a compreender a especificidade das informações relativas à saúde, em relação ao seu conteúdo.

Os dados relativos à saúde contêm diferentes informações, as quais podem ser certas, incertas, boas ou ruins. Assim, nos registros de saúde de uma determinada pessoa podemos encontrar dados de sua vida e saúde que podem se apresentar como certezas objetivas, como por exemplo, uma cirurgia realizada ou um tratamento médico que alcançou a cura do paciente. Como também podemos nos deparar com informações que conduzem à algumas incertezas, por exemplo, diagnósticos inconclusos.

Visualizando a questão sobre outra perspectiva, os registros de saúde podem conter notícias que possam ser boas ao paciente, como, por exemplo, a cura de uma doença grave. Como também pode conter informações ruins, como o desenvolvimento de uma doença incurável ou ainda uma doença que possa ser vista de forma ruim e até mesmo preconceituosa por grande parte da sociedade. Estas especificidades que as informações da saúde apresentam, acarretam na necessidade de um cuidado específico de tais dados, os quais podem gerar graves danos aos seus titulares caos venham a ser de conhecimento de terceiros.

Estamos diante da transmissão de informações que resultam da interpretação de diversos dados e fatores que restaram revelados e colhidos. Não podemos deixar de esquecer dos princípios jurídicos e éticos que regulam e protegem os dados pessoais da saúde, sobretudo a sua transmissão ao paciente (titular dos dados) e à terceiros.

No âmbito das informações colhidas no exercício de atividades relacionadas ao cuidado de saúde, sobretudo nos centros de saúde, hospitais, clinicas e consultórios médicos. Há o dever de sigilo profissional que se apresenta como um dos deveres deontológicos mais antigos dos profissionais da saúde.

Antes mesmo que se pensasse na existência dos atuais regimes jurídicos que conferem segurança jurídica as informações recolhidas no âmbito da saúde, o dever de sigilo já era

considerado uma peça fundamental para o exercício de grande parte das profissões relacionados com o cuidado da saúde, como os médicos e enfermeiros.

Assim, podemos afirmar que o dever deontológico de sigilo quanto às informações colhidas no âmbito da prestação de cuidados da saúde antecede a proteção de tratamento de dados.

A evolução dos dispositivos legais e deontológicos nesse aspecto, exigiu que todas as profissões relacionadas ao cuidado da saúde tenham o dever de sigilo inscrito em suas deontologias profissionais. Tal dever abrange todas as informações que sejam de conhecimento do profissional e, encontra-se sujeito às sanções de um regime disciplinar específico no caso de violações. Assim, os códigos de ética atuais dos profissionais da saúde, não só prescrevem o dever, mas também preveem sanções disciplinares pela violação do sigilo imposto.

O dever de manter sigilo e guarda das informações colhidas no âmbito da prestação de serviços à saúde também se estende às organizações e saúde públicas e privadas, as quais são depositárias de registros de saúde dos pacientes assistidos, competindo à estas instituições a prerrogativa de instituir e implementar planos de ação que garantam que tal privacidade seja mantida.

Todavia, conforme salientamos anteriormente, os dados relativos à saúde vão muito além daqueles que surgem diante da relação entre o paciente e o profissional da saúde.

Atualmente, contamos com um leque enorme de sistemas informáticos que se destinam ao acompanhamento da saúde, como por exemplo, aplicações *fitness*, *smart whatches*, aplicações e sistemas que acompanham o desenvolvimento da gravidez e a saúde da gestante, dentre outros sistemas tecnológicos que fazem a captação de dados que se relacionam com a saúde do seu utilizador e que não precisam necessariamente estar diretamente ligado à um profissional da saúde.

Assim, consideram-se dados pessoais relativos à saúde toda e qualquer informação que se relacione com o estado de saúde do seu titular, incluindo-se as informações recolhidas para atendimento e prestação de serviços da saúde, qualquer símbolo ou sinal que permita a identificação, analises clinicas ou exames em geral e ainda, os meios digitais que realizam a recolha e tratamento de dados.

1.3 A OPERAÇÃO DE TRATAMENTO DE DADOS PESSOAIS

Realizadas as ponderações necessárias para se estabelecer uma clara definição dos dados sensíveis e suas nuances, permitindo identificar e compreender o que são considerados os dados

relativos à saúde. O estudo e a compreensão sobre a forma como deve ser realizado o tratamento dos dados recolhidos se faz essencial, principalmente para a futura compreensão da extensão da responsabilização civil pela violação de dados.

Compreender o tratamento de dados é essencial para que se possa ter uma visualização mais completa acerca do direito da proteção de dados, uma vez que este pode ser visto como o elemento legal que se encontra diretamente ligado à aplicação prática do RGPD.

O conceito de tratamento pode ser extraído do artigo 4º, nº2 do RGPD que o reconhece como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados [...]"[36].

Nesse sentido, colhemos os ensinamentos de Menezes Cordeiro[37] o qual sustenta que o termo operação se assemelha às expressões já consolidados do Direito bancário e no Direito dos valores imobiliários e o conceitua como um ato humano realizado sobre dados pessoais, enquanto que as operações correspondem à vários atos jurídicos e materiais também realizados sobre dados pessoais.

Importante salientar também que, apesar do legislador europeu não ter atribuído um conceito aos meios autonomizados, podemos entender que se tratam de operações que envolvem equipamentos de processamento de dados em aspecto amplo. Enquanto que, podemos entender como meios não automatizados todos os tratamentos que são realizados de forma manual[38].

Ainda, é importante destacar que as regras instituídas pelo RGPD não são aplicáveis a todos os tratamentos de dados não automatizados, a norma apenas tem aplicabilidade aos dados que são armazenados em ficheiro ou que são destinados a ele.

O conceito de ficheiros também pode ser extraído do RGPD que o classifica como "qualquer conjunto estruturado de dados pessoais, acessível [...]". Portanto, podemos considerar como ficheiro uma compilação de diversos dados pessoais pertencente a diversos titulares.

Os ficheiros devem estar organizados ou, como a própria lei diz, devem se encontrar predispostos de forma estruturada. Assim, os dados devem ser arrumados de acordo com algum processo metodológico, mesmo que tal método organizativo seja pouco estruturado. Sendo que, o não preenchimento deste requisito acarreta na inaplicabilidade do RGPD, nos termos do

[36] REGULAMENTO (UE) 2016/679 - *Op. Cit*., art. 4º, nº 2.
[37] CORDEIRO, *Op. Cit*., p. 143.
[38] CORDEIRO, *Op. Cit*., p. 85.

Considerando nº 15[39]: "[...] os ficheiros ou os conjuntos de ficheiros bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser abrangidos pelo âmbito de aplicação do presente regulamento. ".

Ainda, o conjunto de dados pessoais deve ser acessível à terceiros, ou seja, qualquer pessoa pode ter acesso ao ficheiro de forma lícita e conseguir consulta-lo por meio de critérios pré-determinados. Como, por exemplo, as fichas médicas de pacientes que são organizadas por ordem alfabética.

Feitos estes breves apontamentos, interessa-nos mencionar que o legislador europeu, apresenta uma lista exemplificativa, que reúne os atos que são considerados como tratamentos de dados pessoais. Os quais consistem na "[...] recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição."[40]

Todavia, não devemos nos apegar totalmente ao rol apresentado acima para determinar as modalidades e espécies de tratamento, uma vez que o rol apresentado não é taxativo, tendo apenas cunho exemplificativo. Fato este, que amplia ainda mais o alcance do conceito atribuído ao tratamento de dados.

Com o objetivo exemplificar as ações humanas que a norma supracitada reconhece como tratamento, tomamos como exemplo a recolha e registro de dados, sendo que ambas operações dizem respeito ao momento em que ocorre a entrada dos dados pessoais na esfera jurídica do responsável pelo tratamento.

A organização e estruturação também fazem parte do tratamento de dados, e consistem em manter os dados organizados de acordo com uma metodologia pré-definida. Enquanto que, a conservação, como o próprio nome diz, pode ser vista como o ato de armazenamento e manutenção dos dados.

Ainda, no âmbito das modalidades de tratamento de dados temos a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação ou transmissão dos dados para um terceiro, a comparação ou a interconexão de dados, a limitação de dados que pode ser visualizada como uma restrição ao tratamento e, por fim, o apagamento ou destruição.

Portanto, o tratamento de dados apresenta-se como parte fundamental para o regime de proteção de dados, o qual tem ampla abrangência, abarcando toda e qualquer operação ou um

[39] REGULAMENTO (UE) 2016/679 - *Op. Cit.*, p. 03.
[40] REGULAMENTO (UE) 2016/679 - *Op. Cit.*, art. 4º, nº 2.

conjunto de várias operações realizadas sobre um ou mais dados pessoais, independentemente da forma em que estes dados se encontram armazenados, em meios físicos ou eletrônicos.

1.3.1 Princípios que norteiam a atividade de tratamento de dados pessoais

Para uma melhor compreensão do tema abordado, é indispensável o estudo acerca dos princípios que regem a atividade do tratamento, verificando a forma com que tais princípios influenciam o desenvolvimento da atividade de tratamento de dados, tal análise permite a compreensão da efetiva intenção do legislador.

Antes de adentrarmos no estudo pormenorizado de cada um dos princípios que norteiam a atividade de tratamento de dados, é importante salientar que nem todos doutrinadores e estudiosos do tema apresentam um rol idêntico acerca dos princípios relativos ao tratamento de dados.

Portanto, para elaboração do presente capítulo, iremos nos utilizar dos princípios que se encontram elencados no RGPD, os quais consistem em: princípio da licitude, lealdade, transparência, limitação da finalidade, minimização de dados, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade.

O primeiro princípio listado (princípio da licitude), encontra-se consubstanciado no artigo 6º do RGPD, pode-se afirmar em sentido amplo que, tal princípio pressupõem que o tratamento deve ser feito em observância e cumprimento das normas de proteção de dados pessoais. Vejamos: “O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: [...]”.

Assim, de acordo com este princípio o tratamento de dados somente pode ser considerado lícito se realizado em pelo menos uma das situações listadas na norma. Dentre elas, se o titular dos dados tiver consentido com o tratamento dos seus dados, o tratamento deve se mostrar necessário para execução de um contrato no qual o titular é parte ou para diligências pré-contratuais, e ainda, para o cumprimento de uma obrigação jurídica em que o responsável pelo tratamento esteja sujeito

O diploma legal também determina a necessidade de ser demonstrar que o tratamento deve ser necessário para a defesa dos interesses vitais do titular dos dados ou de um terceiro, igualmente se for necessário para o exercício de funções que contenham interesse público ou para o exercício da autoridade pública.

Haverá licitude nos tratamentos que se mostrarem necessários para efeito dos interesses legítimos do responsável pelo tratamento ou por terceiros, com exceção no caso de haver

interesses ou direitos e liberdades fundamentais do titular, especialmente se o titular se tratar de uma criança ou, por exemplo, se o titular se encontrar acometido por uma doença, colocando-o em uma situação de vulnerabilidade.

De todos os requisitos de licitude do tratamento, damos especial enfoque à necessidade do consentimento do titular, uma vez que se trata de um ponto de suma importância para a legalidade do tratamento, pois pode ser visualizado como uma das principais garantias da proteção dos interesses individuais.

Nos termos do artigo 4º, nº 11 do RGPD o consentimento pode ser entendido como uma manifestação de vontade por meio da qual o titular aceita que os seus dados sejam objeto de tratamento, mediante uma declaração ou ato positivo inequívoco.

O artigo 7º do RGPD determina as condições sobre as quais o consentimento deve ser externado, sendo que, se o consentimento do titular deixar de observar as normas ali elencadas não terá validade alguma.

Sempre que o tratamento de dados for realizado com base no consentimento exprimido pelo seu titular, o responsável pelo tratamento deverá demonstrar que o titular efetivamente deu seu consentimento para que o tratamento fosse realizado.

Inclusive, o artigo citado determina que, se o consentimento do titular for realizado por meio de uma declaração escrita que envolva outros assuntos, o pedido de consentimento deve ser apresentado de forma em que possa ser distinguido dos ouros assuntos, de forma fácil e por meio de uma linguagem simples e clara.

A qualquer tempo o titular dos dados pode retirar o seu consentimento de forma facilitada. Inclusive, tal retirada não compromete a licitude do tratamento realizado com base no consentimento exarado em momento anterior.

A autodeterminação informativa garante ao titular o direito ao controle de seus dados, na medida em que impõe limitações no tratamento, acesso e divulgação, os quais apenas são possíveis se houver a autorização do titular ou alguma regulamentação legal que a autorize. Pode-se afirmar ainda que a autodeterminação ampara a tutela dos direitos fundamentais da privacidade e da liberdade dos titulares de dados.

Portanto, podemos considerar o princípio da licitude como o pilar fundamental para o tratamento de dados, uma vez que, o não preenchimento dos requisitos legais para o tratamento acarretará na sua ilicitude.

O princípio da lealdade "está longe de se encontrar [...] harmonizado nas várias versões do RGPD"[41], isto porque nas versões redigidas nas línguas espanhola, francesa e portuguesa utilizou-se a expressão lealdade, enquanto na língua alemã utilizou-se: boa-fé, na medida em que na inglesa e italiana utilizou-se da expressão correção.[42]

Tais diferenças linguísticas acarretaram em um impacto significativo na interpretação local adotada pelas ciências jurídicas dos diversos países que compõe a União Europeia, causando grande debate na doutrina, a qual tem sedimentado o seu entendimento no sentido de que o intérprete-aplicador da norma não deverá recorrer única e exclusivamente ao ordenamento jurídico interno, devendo levar em consideração os desenvolvimentos e ponderações realizados pelo direito europeu, sob pena de desvirtuar as reais pretensões do regulamento.

Diante disso, fica evidente que a análise e o estudo do princípio da lealdade deve ser feito com base no disposto nos artigos e Considerandos do RGPD, os quais utilizam-se da expressão "tratamento equitativo" para densificar o princípio da lealdade, vejamos:

> Artigo 13º: "[...]2. Para além das informações referidas no n.o 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um **tratamento equitativo e transparente**: [...]" – Grifou-se
> Artigo 40º [...] 2.As associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes podem elaborar códigos de conduta, alterar ou aditar a esses códigos, a fim de especificar a aplicação do presente regulamento, como por exemplo: a) **O tratamento equitativo e transparente**; - Grifou-se
> Considerando 60: "Os princípios do tratamento equitativo e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. [...]"

O princípio da lealdade impõe aos responsáveis pelo tratamento de dados a obrigação de sempre atenderem aos interesses dos titulares, "trata-se de um conceito aberto, passível de ser invocado em situações que contradigam o RGPD"[43].

Por seu turno, o princípio da transparência deve ser encontrado em todo o processo de tratamento de dados, desde os primeiros contatos com o possível titular de dados futuros, mantendo-se durante todo o processo de tratamento e perdurando mesmo após o término da relação.

---

[41] CORDEIRO, *Op. Cit.*, p. 153.
[42] *Idem*.
[43] *Ibidem*.

A transparência deve englobar tanto o conteúdo das informações como todo o procedimento de transmissão e não se esgota no exercício do direito à informação que os titulares de dados detêm.

Este princípio pode ser observado em diversos artigos do RGPD, como por exemplo:

> Artigo 12º - 1.O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.o e 14.o e qualquer comunicação prevista nos artigos 15.o a 22.o e 34.o a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças.
>
> Artigo 34º - 1.Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.

Portanto, o princípio da transparência atravessa absolutamente todo o processo de tratamento em todas as suas vertentes e tem como objetivo primordial manter o titular dos dados ciente de todo procedimento e do estado em que os seus dados se encontram, mantendo uma relação de efetiva transparência.

O princípio da limitação da finalidade determina que a recolha e o tratamento de dados devem ser limitados às finalidades que se apresentam como determinadas, explícitas e legítimas, as quais devem prevalecer durante todo o processo de tratamento de dados. De modo que, os tratamentos que se mostrarem incompatíveis com as finalidades inicialmente indicadas pelo responsável pelo tratamento, são vedados pelo ordenamento jurídico.

Todo e qualquer tratamento de dados deve ser encontrar diretamente vinculado à uma finalidade específica e pré-determinada, as quais devem ser observadas em todos os passos e procedimentos percorridos pelos dados.

O objetivo da finalidade é limitar e definir os contornos em que se dará o tratamento e pode ser considerada um dos pontos centrais do direito à proteção de dados, principalmente se levarmos em consideração as incontáveis possibilidades de recombinação de dados, que podem ainda ser aliados a uma enorme captação e associação de dados.

As finalidades que dizem respeito ao tratamento devem ser determinadas antes mesmo do início do processo de recolha de dados, em hipótese alguma, o estabelecimento e determinação destas finalidades podem se dar em um evento futuro ou serem adiadas.

Portanto, o primeiro passo a ser tomado antes de haver o efetivo tratamento de dados é estabelecer qual será sua finalidade, cabendo ao responsável pelo tratamento realizar um exame prévio que permita a identificação dos propósitos que se pretende alcançar.

Nesse aspecto, salientamos que as finalidades devem ser reveladas a todo o universo que envolve a proteção de dados, ou seja, devem ser reveladas ao titular dos dados, às

autoridades de controle, ao responsável pelo tratamento, aos subcontratantes e a terceiros envolvidos com a operação de tratamento de dados.

Acreditamos que o legislador deu vida à tais exigências com o objetivo de garantir que os titulares de dados tenham controle sobre o direito à autodeterminação informacional.

Não se pode deixar de mencionar que as exigências legais acerca da determinabilidade, explicitude e das finalidades é colocada em questionamento quando parte-se para a análise do artigo 5º, nº1, b) do RGPD, que preleciona: "1.Os dados pessoais são: [...] Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»);".

Este dispositivo legal permite que o responsável pelo tratamento utilize os dados para finalidades diversas das estipuladas em um primeiro momento, desde que não sejam incompatíveis entre si. Para Menezes Cordeiro[44], cabe ao interprete e aplicador da norma o dever de analisar a questão em concreto e determinar se efetivamente há ou não incompatibilidade entre as finalidades pré-estabelecidas.

O princípio da minimização de dados possui uma estreita conexão com o princípio analisado acima, uma vez que determina que a captação e o tratamento de dados devem ser limitados em termos qualitativos e quantitativos. De modo que, os dados somente podem ser considerados como adequados à finalidade quando se mostrarem necessários para o alcance de tal finalidade, ou seja, este princípio obriga que os agentes de tratamento de dados apenas captem e tratem dados quando não houver outra possibilidade de consegui-los.

Este princípio é composto por três pilares fundamentais de sustentação, os quais consistem em: pertinência, adequação e necessidade. Na medida em que o primeiro (pertinência), "circunscreve as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades"[45].

Enquanto que a adequação determina que apenas podem ser tratados os dados pessoais que se enquadrem nas finalidades objetivadas e, consequentemente, os dados que se mostrarem inapropriados devem ser excluídos.

[44] CORDEIRO, *Op. Cit*., p. 157.
[45] CORDEIRO, *Op. Cit.*, p. 159.

Assim, sempre que possível, deve-se evitar a realização do tratamento de dados pessoais, sendo que sempre que houver outra possibilidade de substitui-lo deverá ser feito, de modo a minimizar os riscos que o tratamento pode acarretar ao titular do dado.

Em contrapartida, o princípio da exatidão encontra-se elencado no artigo 5º, 1º do RGPD e abrange três dimensões distintas. A primeira dimensão trata-se do impedimento de recolha e armazenagem de dados incorretos, a segunda dimensão determina que os dados coletados sejam atualizados e, por fim, os dados incorretos devem ser retificados ou apagados.

Portanto, como a própria denominação do princípio preleciona, os dados pessoais devem corresponder à exata realidade, uma vez que sua inexatidão pode acarretar em um enorme impacto na vida de seus titulares.

Nesse sentido, assinalamos que pode haver flexibilização deste princípio, sobretudo em relação a atualização dos dados. Há dados que nem sempre devem estar atualizados, uma vez que apenas apresentam interesse se se mantiverem desatualizados, como, por exemplo, dados médicos que descrevem um acompanhamento médico antigo. Portanto, este princípio pode ser flexibilizado de acordo com a finalidade pela qual foi tratado.

O princípio da limitação da conservação encontra-se previsto no artigo 5º, 1º, alínea e) do RGPD e trata da limitação temporal de manutenção dos dados colhidos, determinando que os dados podem ser conservados apenas durante o período de tempo necessário para alcançar as finalidades para as quais foram tratados inicialmente.

Cabendo ao responsável pelo tratamento fixar os prazos para apagamento dos dados ou para sua revisão periódica, com o objetivo de assegurar que os dados pessoais sejam conservados apenas durante o tempo em que se fizerem necessários, de acordo com a finalidade pré-estabelecida.

A norma supracitada apresenta uma exceção, permitindo a conservação de dados por períodos alargados desde que haja uma real justificativa para tanto, seja para fins de interesse público, arquivo, investigação cientifica ou histórica e para fins estatísticos. Sendo que, é dever do responsável pelo tratamento buscar medidas técnicas e organizativas para o cumprimento das normas e disposições do RGPD, sempre observando a proteção dos direitos e liberdades dos titulares de dados.

De acordo com o artigo 5º, nº 1, alínea f) do RGPD, o tratamento de dados deve ser realizado de forma que garanta a segurança e confidencialidade dos dados. Podemos afirmar que este dispositivo legal reflete o princípio da integridade e confidencialidade, o qual inclui a proteção contra o tratamento ilícito ou não autorizado e, contra a perda, danificação ou destruição acidental.

De modo que, o próprio disposto legal atribui aos responsáveis pelo tratamento o dever de adotar medidas organizativas e técnicas adequadas para garantir o cumprimento destes princípios e das demais normas do RGPD.

Por fim, o princípio da responsabilidade pode ser visualizado como um dos princípios mais importantes para a estruturação do presente estudo, elencado no artigo 5º, nº 2 do RGPD, determina que é dever do responsável pelo tratamento observar aos princípios estabelecidos no RGPD, bem como, deve conseguir demonstrar às autoridades públicas o efetivo cumprimento destes princípios.

No que diz respeito ao dever de comprovar o cumprimento do RGPD, tal dever não pode ser confundido com possibilidade de inversão do ônus de provar. Sendo que, se o responsável pelo tratamento não for capaz de provar que seguiu as normas que lhe são impostas, apenas será responsabilizado pelo incumprimento do dever de provar que lhe é incumbido[46].

O legislador não clarifica de que forma que o cumprimento dos princípios que norteiam o tratamento de dados pode ser comprovado, mas partindo-se de uma breve interpretação do disposto nos artigos 40º e 42º do RGPD, é possível verificar que tal comprovação poderá ser feita através da demonstração da efetiva aplicação dos códigos de conduta durante todo o procedimento de tratamento, bem como, demonstrando os procedimentos de certificação adotados.

Diante de todo o exposto, pode-se perceber que o objetivo primordial do legislador, ao instituir uma série de princípios que norteiam a atividade de tratamento de dados, é conferir segurança jurídica ao titular de dados, de modo a criar mecanismos que objetivam, sobretudo, resguardar os direitos e liberdades destes titulares.

1.3.2 As especificidades presentes no tratamento de dados sensíveis

Conforme salientado anteriormente, o RGPD reconhece uma categoria de dados especiais em virtude de sua natureza e de sua significância para com os direitos e liberdades fundamentais de seus titulares.

Tais dados receberam a denominação de dados sensíveis, em virtude desta significância, o RGPD criou um regime diferenciado para o tratamento destes dados, com o objetivo de conferir maior segurança jurídica aos seus titulares.

[46] CORDEIRO, *Op. Cit.*, p. 162

Ao confrontarmos o regime comum de proteção de dados com o regime especial, que é aplicado aos denominados dados sensíveis, podemos verificar a existência de um agravamento dos requisitos legais para o tratamento neste último. Como, por exemplo, quando estamos diante de dados sensíveis, o consentimento deve ser prestado de forma explícita.

A principal diferença registrada entre o regime comum e o especial, no que diz respeito à necessidade de haver o consentimento do titular, reside na necessidade deste último, em ter preenchido o requisito da explicitude, na medida em que acreditamos que tal termo é empregue como sinônimo de "expresso".

Todavia, tal exceção poderá ser afastada se "União ou de um Estado-Membro previr que a proibição [...] não pode ser anulada pelo titular dos dados". Por exemplo, um Estado-Membro que decreta uma norma que limite o direito à autodeterminação informacional, proibindo o titular de autorizar a utilização de seus próprios dados.

A título de exemplo prático do tema sob estudo, tomamos as orientações emitidas pela CNPD em 22 de agosto de 2022 ao se manifestar "Sobre divulgação de informação relativa a infetados por Covid-19".

Ao se manifestar acerca da publicação reiterada de dados de saúde, a Comissão sustentou que as autarquias locais estão impedidas de publicar quaisquer dados relativos à saúde que contenham identificação dos seus titulares.

Sustentando que, tal tipo de informação encontra-se sujeita à um regime especialmente protegido, justamente por se tratarem de informações que pessoais que são suscetíveis de promover a discriminação.

Em continuidade, salienta que ainda que o argumento da necessidade de divulgar dados de saúde, de forma individualizada ou que permita a identificação dos utentes, com o objetivo de garantir a saúde e proteção civil da população, não pode ser acatado. Pois, tal tratamento dependeria exclusivamente que uma disposição normativa que previsse tal situação e acautelasse os direitos e interesses dos titulares.

Todavia, tal legislação não existe atualmente, o que torna tal tratamento completamente ilegal. Inclusive, " [...] é duvidoso que a prossecução do interesse público de saúde pública seja diretamente atribuição das autarquias locais"[47].

Poder-se-ia ainda, sustentar tal tratamento com base no artigo 9°, n° 2, alínea g) do RGPD, o qual preleciona: "Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro", porém tal invocação

[47] COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS – *Op. Cit.*, p. 04.

depende da existência de um diploma legal expresso, que apresente medidas específicas e completamente adequadas à proteção dos interesses e direitos dos titulares.

Assim, pode-se afirmar que, em regra, o tratamento dos dados sensíveis é proibido. Todavia, o tratamento poderá ser realizado desde que observados os fundamentos legais previstos no artigo 9º, nº 2 do RGPD os quais abordaremos a seguir.

O artigo 9º do RGPD permite o tratamento de dados sensíveis que demonstrem ser necessários para o cumprimento de obrigações e para o exercício de determinados direitos do titular ou do responsável pelo tratamento.

Contudo, tal exceção apenas é aplicável em sede de normas laborais, de proteção e segurança social e desde que, haja permissão para tanto no Direito da União ou no direito dos Estados-Membros ou em convenções coletivas de trabalho.

Também é permitido o tratamento de dados pessoais sensíveis com fundamento nos interesses vitais do titular ou de terceiros. Para alcançarmos um conceito de interesses vitais, devemos levar nossa atenção ao Considerando nº 46 do RGPD, o qual preceitua: "[...] se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana. [...]", portanto podemos considerar que se tratam de situações em que a integridade física ou a própria vida do titular ou de terceiro esteja em perigo.

Nesse aspecto, o tratamento de dados pressupõe uma condição extra, o qual somente poderá ocorrer se o titular dos dados se encontrar em situação física ou legal que impossibilite o seu consentimento. De forma que devem ser levadas em consideração a vontade hipotética do titular e ainda, deve ser considerada a possibilidade de existirem representantes legais do titular que possam vir a suprir a falta de consentimento.

Igualmente, é permitido o tratamento de dados essenciais a ser realizado por fundações, associações ou qualquer outra entidade sem fins lucrativos, porém somente se forem destinadas a prosseguir interesses políticos. A forma que tais entidades assumem é completamente irrelevante para o direito, porém deve haver um nível de organização e de estrutura interna mínima que sejam capazes de permitir o exercício de atividades[48].

O tratamento de dados que foram tornados públicos pelo seu titular também consiste em uma das exceções para o tratamento de dados sensíveis. Acreditamos que, ao editar tal norma, o legislador partiu do pressuposto de que se um indivíduo por si só torna seus dados públicos,

[48] CORDEIRO, *Op. Cit.*, p. 244.

é porque reconhece, ainda que indiretamente, que tais dados não lhe trazem desconforto ou podem lhe prejudicar, pois se assim fosse não teria o próprio tornado públicos.

Também é permitido o tratamento de dados sensíveis sempre que o mesmo seja necessário para o exercício, declarar ou para a defesa de um direito em um processo judicial ou para a atuação dos Tribunais dentro de sua função jurisdicional, conforme o artigo 9º, nº 2, alínea 'f' do RGPD. Portanto, tal exceção se justifica na necessidade de administração da justiça.

Outra exceção à proibição de tratamento de dados sensíveis encontra-se elencada na alínea f) do artigo 9º, 2º, e diz respeito aos interesses públicos importantes. Para que se verifique tal exceção é necessário exista previsão no direito da União Europeia ou dos Estados-Membros, além disso, o tratamento deve ser proporcional ao interesse público e deve observar o direito à autodeterminação informacional do titular, devendo ser realizado por meio de medidas específicas e adequadas que contribuam com a salvaguarda dos interesses e direitos fundamentais do titular.

Por fim, passamos a estudar a exceção que mais nos interessa para a persecução do presente estudo que são os dados relativos aos cuidados de saúde, os quais englobam a medicina do trabalho e preventiva, avaliação da capacidade de trabalho, diagnóstico médico, prestação de cuidados ou tratamentos de saúde, gestão de sistemas e serviços de saúde ou de ação social, dentre outros.

O tratamento destes dados deverá ser fundamentado no Direito da União ou no dos Estados-Membros nos termos supracitados ou em virtude de uma relação jurídica estabelecida com um profissional da saúde sujeito a obrigação de sigilo e de confidencialidade.

O interesse público no âmbito da saúde pública também se apresenta como uma exceção à regra geral, sendo permitido o tratamento sempre que seja necessário e exista previsão legal para tanto. Em termos genéricos, o que difere os cuidados relativos à saúde da saúde pública é que neste primeiro estamos diante de individuais, enquanto no segundo estamos diante de um interesse público, sendo que a importância do dado se mostra irrelevante.

Para a persecução do presente estudo, tomaremos como base o conceito de saúde pública apresentada pelo artigo 3º, 1, alínea c) do Regulamento (CE) nº 1338/2008, de 16 de dezembro, o qual dispõe que "[...] todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a mobilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade;".

Portanto, quaisquer um destes elementos são capazes de justificar o tratamento de dados considerados sensíveis, desde que verificado o interesse público e a existência de norma.

Nesse sentido, o artigo 9º, 4º do RGPD confere aos Estados-Membros a possibilidade de manterem ou criarem novas condições ou limitações para o tratamento dos dados biométricos, genéticos e dados relativos à saúde.

Tal dispositivo legal atribui competências aos Estados para legislarem de modo a regular o tratamento destas categorias de dados sensíveis, com o objetivo de proteger os direitos e prerrogativas inerentes aos titulares de dados. O legislador português optou por realizar tal regulamentação no artigo 29º da Lei nº 58/2019, de 08 de agosto, o qual trata exclusivamente de regular o tratamento de dados de saúde e de dados genéticos.

Para Menezes Cordeiro[49], o artigo citado acima consagra o denominado princípio *need to know* e a sua inclusão foi motivada pelas orientações apresentadas pela CNPD, nomeadamente no Parecer nº 20/2018. De forma, que todo o qualquer tratamento deverá observar a necessidade do titular de conhecer a informação que será objeto do tratamento.

Tal princípio traduz a ideia de que os funcionários e prestadores de serviço e terceiros que auxiliam o tratamento de dados somente podem ter acesso à tais dados se estes se mostrarem necessários para o exercício da função.

Situação semelhante se verifica nos números 4º e 5º do artigo citado, os quais impõem um dever de confidencialidade a três grandes grupos que possam ter acesso aos dados relativos à saúde, sendo eles: titulares de órgãos, prestadores de serviços e trabalhadores e os encarregados à proteção de dados dos responsáveis pelo tratamento de dados relativos à saúde e dados genéticos, bem como, os estudantes e os investigadores e demais profissionais da área da saúde, por fim, os titulares de órgãos e trabalhadores que possam ter acesso a dados de saúde por meio do exercício das atividade de fiscalização ou financiamento de cuidados da saúde.

Importante ressaltar que os números 4º e 5º do artigo 29 da Lei nº 58/2019, de 08 de agosto não podem ser interpretados como "uma porta aberta ao tratamento de dados sensíveis"[50], pois o seu objetivo é impor o rígido dever de sigilo a todas as classes de indivíduos.

O número 7º do artigo 29º trata das medidas de segurança e os requisitos de segurança que devem ser implementadas no âmbito do tratamento de dados da saúde e genéticos, sustentando que os mesmos devem ser "[..] aprovados por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça, que deve regulamentar, nomeadamente, as

[49] CORDEIRO, *Op. Cit.*, p. 253
[50] CORDEIRO, *Op. Cit.*, p. 254.

seguintes matérias: a) Estabelecimento de permissões de acesso aos dados pessoais diferenciados, em razão da necessidade de conhecer e da segregação de funções; b) Requisitos de autenticação prévia de quem acede; c) Registo eletrónico dos acessos e dos dados acedidos.”.

Em que pese haver tal disposição legal, até o presente momento, não há qualquer portaria publicada para regular tal matéria, o que faz com que tal matéria não tenha regulamentação legal específica no território de Portugal, devendo ser aplicadas as normas do RGPD quanto ao tema.

O procedimento de tratamento destes dados deve ser conjugado ao artigo 32º e seguintes do RGPD, de modo que, caberá ao responsável pelo tratamento e aos subcontratantes a adoção e implementação das medidas necessárias para assegurar um bom nível de segurança, levando-se em consideração o risco em concreto que tal situação apresenta.

2. O DIREITO FUNDAMENTAL À SAÚDE E A SUA INTERLIGAÇÃO COM O REGIME DE PROTEÇÃO DE DADOS

Realizadas as ponderações necessárias para que seja possível compreender o conceito atribuído aos dados, nomeadamente aos dados relativos à saúde. Para a construção do presente estudo, é de suma importância afunilar os estudos de modo a tratar acerca da saúde como um direito fundamental e inerente a todos os indivíduos da sociedade e interliga-la às operações de tratamento de dados, as quais podem ser visualizadas como um fator essencial para o desenvolvimento e aprimoramento deste direito.

Tal análise permitirá a realização de uma avaliação acerca do sistema de proteção e segurança dos dados da saúde, o qual é composto por dois domínios completamente diversos, que correspondem ao já estudado sistema de proteção de dados pessoais estabelecido pelo RGPD e, por outro lado, não se pode esquecer da existência de normas deontológicas que conferem proteção a estes dados no âmbito da prática clínica, nomeadamente na prestação de cuidados à saúde.

2.1 A SAÚDE COMO UM DIREITO FUNDAMENTAL E A COLETA DE DADOS COMO FATOR ESSENCIAL PARA SUA PERSECUÇÃO

Notório que, atualmente, a maior parte dos países reconhece a necessidade de se conferir amparo jurídico ao direito à proteção da saúde, inserindo-o em um quadro de direitos positivos. Isto se dá em virtude da significância que tal direito apresenta para o desenvolvimento e aprimoramento social como um todo.

De acordo com os ensinamentos de Rui Nunes[51], o direito à proteção da saúde pode ser visualizado como uma das mais importantes conquistas alcançadas pela sociedade ao longo dos séculos, ou seja, trata-se de um direito que possui natureza civilizacional, que pode ser considerado como uma forma pura de expressão da dignidade da pessoa humana.

Inclusive, o artigo 3º da Convenção sobre Direitos Humanos e Biomedicina (Conselho da Europa, 2001) reconhece a existência do direito da saúde, ainda que tal direito encontre limitação na esfera econômica verificada em determinados locais. O que evidencia que o direito à promoção e proteção à saúde é um fator determinante para o desenvolvimento e bem-estar social.

[51] NUNES, Rui - **Justiça Distributiva e Direito à Saúde**, p. 09.

No mesmo sentido, a Declaração Universal dos Direitos Humanos de 1984, nomeadamente em seu artigo 25º, reconhece que todos os indivíduos têm o direito de gozar de um nível de vida suficientes que garanta a saúde e o bem-estar. Trata-se aqui, não apenas do direito-dever de se ter acesso à assistência médica e aos sistemas de saúde propriamente ditos, mas algo muito mais amplo, que engloba o direito à alimentação, saneamento básico, vestuário, alojamento, dentre outros direitos que encontram-se diretamente ligados à qualidade de vida, bem-estar e saúde social.

No âmbito da legislação interna, a Constituição da República Portuguesa reconhece a saúde como um direito fundamental, vez que dedica um artigo denso à proteção da saúde, bem como, o dever de a defender e promover. Tal prerrogativa encontra-se prevista no capítulo que trata dos Direitos e Deveres Sociais, nomeadamente o artigo 64º, o qual reconhece que "Todos têm direito à proteção da saúde e o dever de a defender e promover".

Da leitura do dispositivo legal acima colacionado, pode-se auferir que ao mesmo tempo em que o Estado garante aos seus cidadãos o direito de proteção à saúde, é acrescentado um dever em sua esfera jurídica, o qual corresponde à sua defesa e proteção.

Para o autor Sérgio Deodato[52] estamos diante de um direito-dever, o qual pode ser assim compreendido porque encontra-se inserido na parte da Constituição que reconhece os direitos e deveres fundamentais.

Tal previsão legal não apenas consagra o direito à proteção da saúde, mas também, pode ser considerado como base fundamental para todo o regime jurídico interno que norteia e dá amparo à promoção e proteção da saúde, na medida em que todo o sistema se encontra estruturado de forma a assegurar a todos os cidadãos a prestação de cuidados da saúde, como forma de garantia de um direito fundamental.

Nesse sentido, tomamos a Lei nº 95/2019 de 04 de setembro, também conhecida como Lei de Bases da Saúde, a qual tem ampla abrangência, aplicando-se a todo o sistema, integrando as entidades, públicas, privadas e os profissionais liberais.

A intitulada Base I do aludido dispositivo legal acima citado, traz um importante conceito acerca do direito à saúde, evidenciando a necessidade de uma cooperação social para o seu desenvolvimento e progressão, na medida em que preleciona:

> Direito à proteção da saúde
> 1 - O direito à proteção da saúde é o direito de todas as pessoas gozarem do melhor estado de saúde físico, mental e social, pressupondo a criação e o desenvolvimento de condições económicas, sociais, culturais e ambientais que garantam níveis suficientes e saudáveis de vida, de trabalho e de lazer.

[52] DEODATO, *Op. Cit.*, p. 10.

> 2 - O direito à proteção da saúde constitui uma responsabilidade conjunta das pessoas, da sociedade e do Estado e compreende o acesso, ao longo da vida, à promoção, prevenção, tratamento e reabilitação da saúde, a cuidados continuados e a cuidados paliativos.
> 3 - A sociedade tem o dever de contribuir para a proteção da saúde em todas as políticas e setores de atividade.
> 4 - O Estado promove e garante o direito à proteção da saúde através do Serviço Nacional de Saúde (SNS), dos Serviços Regionais de Saúde e de outras instituições públicas, centrais, regionais e locais.

Da leitura do excerto colacionado acima, fica evidente que a norma sob estudo realiza neste dispositivo legal, uma densificação do que encontra-se disposto no artigo 64º da CRP, ou seja, tal regimento tem como objetivo, inserir os ditames constitucionais nos regimentos internos do país, fazendo cumprir o objetivo constitucional de promover e garantir o direito à saúde dos cidadãos.

Assim, tanto o direito Europeu como o direito interno de Portugal reconhecem a saúde como um direito humano fundamental e essencial para o desenvolvimento humano e social, garantindo á todos os cidadãos o resguardo e amparo deste direito, bem como, instituindo o dever de sua promoção.

No âmbito da prestação destes cuidados com a saúde, seja por parte do ente Estatal ou por meio de relações estabelecidas entre particulares, se pode verificar a coleta de inúmeros dados. Uma vez que, para que se tenha a prestação de cuidados da saúde é necessário que os prestadores deste tipo de serviço aprofundem seu conhecimento sobre o paciente para que seja possível emitir um diagnóstico e intervir de forma eficaz.

Nesse mesmo sentido, ressaltamos que "As ciências da saúde em geral, mas sobretudo a medicina e a enfermagem, lidam com um conjunto vasto de dados, necessários para este conhecimento aprofundado e amplo e que suporta as suas intervenções terapêuticas"[53].

Portanto, o próprio exercício das atividades relacionadas à saúde exige em sua grande maioria, que seja realizada a coleta de diversos dados relativos ao paciente, o que permite ao profissional da saúde uma avaliação ampla acerca da situação enfrentada pela pessoa assistida, e que leva á um diagnóstico. Assim, podemos afirmar que o tratamento de dados encontra-se totalmente ligado ao exercício das atividades de prestação de cuidados á saúde.

A crescente realização do tratamento de dados para o desenvolvimento da saúde em geral tem expandido de forma tão significativa que, no ano de 2019, verificou-se a necessidade de inclusão do tema na Lei de Bases da Saúde.

[53] DEODATO, *Op. Cit.*, p. 15.

Nesse sentido, damos ênfase à Base nº 2[54], que trata diretamente do direito à proteção da saúde: "1 - Todas as pessoas têm direito:
a) À proteção da saúde com respeito pelos princípios da igualdade, não discriminação, confidencialidade e privacidade;". Ocasião em que fica evidente que a aludida norma adotou os princípios que regulam as operações de tratamento de dados, inserindo-os no contexto da proteção da saúde.

Grande parte dos dados relativos à saúde são recolhidos, registrados e usados pelos profissionais da saúde no exercício de sua função. Ou seja, esta modalidade de dados é utilizada pelos profissionais da saúde no âmbito da prestação de serviços assistenciais, que geralmente são denominados como processos clínicos.

Usualmente, os dados relativos à saúde advêm de um contexto específico e, por isso, assumem uma particular finalidade. Tal contexto, corresponde à relação terapêutica que se estabelece entre o paciente e o profissional da saúde, enquanto que a finalidade corresponde à assistência à saúde deste primeiro, ou seja, a avaliação do paciente, o diagnóstico e o tratamento, seja ele terapêutico ou paliativo.

Esta relação terapêutica deve ter como base fundamental o critério da confiança que é estabelecido entre o profissional da saúde e o paciente. De acordo com Isabel Renaud[55], a confiança é algo inerente em todas as relações que se estabelecem entre os profissionais de saúde e as pessoas por eles assistidas, o que permite que o paciente se exponha de modo a revelar informações e dados que são essências para a boa continuidade do processo terapêutico.

Portanto, o contexto que envolve a recolha de dados pelo profissional da saúde envolve um relacionamento baseado na confiança, em que o paciente merece especial atenção no que diz respeito à proteção de sua privacidade, ou seja, que garanta a reserva dos dados disponibilizados.

Portanto, estes dados pessoais assumem a característica de dados relativos à saúde quando as informações relacionadas à sua saúde e bem-estar são reveladas pelo próprio paciente ou pelos seus familiares - nos casos em que este encontra-se impossibilitado de faze-lo -, também podem emergir da observação clínica e da realização de exames.

Tratam-se de informações que dizem respeito às situações mais íntimas da vida e ao funcionamento do corpo do paciente, que são transformadas em dados, na medida em que são transmitidas ou recolhidas pelo profissional da saúde, no âmbito do exercício de sua função.

---

[54] LEI n.º 95/2019 - **Diário da República, Série I**.
[55] RENAUD, Isabel Carmelo Rosa - Conferência Inicial: A confiança. **A Revista da Ordem dos Enfermeiros: Segurança da Informação**, p. 12-13.

De acordo com os ensinamentos de Deodato[56] tal garantia também deve se estender a todos aqueles que exercem funções dentro de organizações de saúde na qual as informações encontram-se armazenadas, o que obriga tais trabalhadores a terem especial cuidado na sua guarda e conservação.

Atualmente, a prestação de serviços no âmbito da saúde assume um contexto particularmente complexo, em que grande parte dos problemas relacionados à saúde das pessoas exige uma resposta que envolve mais de um profissional.

Tal cenário se verifica se forma muito constante no âmbito de organizações de saúde, como por exemplo, dentro de hospitais, onde as equipes contam com um sistema integrado de dados que possibilita o registro de diversos dados relativos à saúde de seus pacientes e, igualmente, confere à tais profissionais o acesso aos dados de outros pacientes.

Assim, o principal contexto de onde emergem os dados relativos à saúde, consistem em ambientes que contam com diversos profissionais, que realizam a recolha de dados que passam a ser registrados em bases eletrônicas e que podem ser facilmente acessados por todos aqueles que desempenham funções profissionais naquele âmbito.

Portanto, a vastidão de dados arquivados pelas instituições e organizações que tratam da saúde não os pertencem, mas dizem respeito ás informações pessoais de saúde de cada uma das pessoas que em algum momento contou com os serviços de assistência à saúde.

A criação e o fomento às bases de dados, neste contexto organizacional, e a recolha destes dados somente se faz possível porque os indivíduos buscam o sistema de saúde (público ou particular) com o objetivo de alcançar amparo e soluções para os seus problemas de saúde, doença e bem-estar.

É a busca terapêutica que leva as pessoas a permitirem o compartilhamento das suas mais intimas informações de saúde e vida. E justamente, com esta finalidade que os dados de saúde emergem em um contexto profissional, dentro do âmbito da prestação de cuidados da saúde. Assim, se não houvesse tal necessidade de cuidado, tais dados não chegariam ao conhecimento dos profissionais e das instituições de saúde.

Portanto, firma-se uma relação de confiança entre o paciente e a organização/instituição de cuidados e o profissional da saúde, da qual poderá emergir a concretização de um diagnóstico, a realização de tratamentos terapêuticos ou paliativos, constituindo um ambiente sob o qual emergem os dados de saúde. Tal especificidade é fundamental para a compreensão

[56] DEODATO, *Op. Cit.*, 15-17.

da criação e implantação dos regimes deontológicos e jurídicos que objetivam conferir maior segurança jurídica à tais dados.

2.1.1 O dever de sigilo imposto aos profissionais da saúde como um meio de proteção dos dados relativos à saúde

Conforme já restou dito em momento anterior, os dados relativos à saúde são compreendidos por um grande acervo de diferentes tipos de informações que se relacionam com a saúde física, mental, social e até mesmo espiritual do seu titular, dizendo respeito à sua vida privada atual e passada.

Os dados de saúde dizem respeito a situações e fatos extremamente íntimos de seu titular, podendo ocorrer casos, em que o próprio titular opta por manter estas informações pessoais em segredo total. Por exemplo, podem haver dados que dizem respeito à uma determinada doença que o seu titular opta por protege-los da sua vida pública e social, até mesmos no âmbito familiar.

Portanto, os dados relativos à saúde se encontram diretamente ligados à esfera da vida intima e privada de seu titular, e apenas podem ultrapassar a fronteira da privacidade quando há manifesta vontade do seu titular ou, independentemente da sua vontade, quando se está diante de uma situação de cuidados da saúde, que exige a revelação de tais dados para que possa surtir efeitos positivos.

Importa destacar que, o fato de ultrapassar a fronteira da privacidade não pode, em momento algum, ser visto como a exposição de informações e dados na esfera pública. A revelação de informações relativas à saúde de um paciente realizada diretamente aos profissionais da saúde e seu posterior registro em uma base de dados, não significa que houve uma alteração em sua natureza, os quais devem ser sempre tratados como dados privados e não como dados públicos, vez que dizem respeito à uma esfera extremamente intima de seu titular.

Pode-se auferir que a informação relativa à saúde, por se tratar de um aspecto da vida privada de seu titular, deve ser interpretada à luz do objeto do direito que diz respeito à "reserva da intimidade da vida privada e familiar" consagrada nos artigos 80º e 26º, nº 1, ambos do CC. Assim, a proteção dos dados e informações que dizem respeito à saúde encontra-se abarcada por duas relevantes categorias de direito.

Os quais consistem em direitos fundamentais, em virtude do amparo constitucional existente e os direitos relativos à personalidade, uma vez que também encontra amparo na norma civilista.

Portanto, a proteção de dados pessoais relativos à saúde pode ser visualizada como um direito que detém amplo amparo nas regras de proteção e reserva da vida privada. Também encontra respaldo legal em regimes específicos da saúde como, por exemplo, a Lei nº 26/2016 de 22 de agosto, que trata da informação genética e de saúde.

Na medida em que, a aludida norma, em seu artigo 3º, nº 1, preleciona que a informação relativa à saúde não pode "ser utilizada para outros fins que não os da prestação de cuidados e a investigação em saúde e outros estabelecidos pela lei".

Em continuidade, o artigo 4º, nº 3 da norma supracitada determina que as informações relativas à saúde do paciente apenas podem ser colhidas e utilizadas mediante a existência de uma autorização escrita do seu titular ou de seu representante. É sabido que, tanto a Lei de Proteção de Dados Pessoais (Lei nº 67/98 de 26 de outubro) como o RGPD, em regra, proíbem a realização do tratamento de dados que dizem respeito à saúde, havendo exceções nos casos em que há razões que o justifiquem.

A natureza privada dos dados pessoais de saúde e a sua relevância para com o seu titular acarretam em especiais implicações para aqueles que tratam diretamente com tais dados, nomeadamente para os profissionais e instituições e organizações de saúde.

Em virtude da existência do dever de sigilo profissional, os profissionais de saúde devem manter o sigilo e guardar as informações colhidas no âmbito da prestação de cuidados. O dever de manter o sigilo profissional consiste em um dos deveres mais antigos das profissões que tratam da saúde, "integrando o juramento de Hipócrates dos médicos e o juramento de Nightingale dos enfermeiros"[57], sendo visto como um dever essencial para o exercício destas atividades.

A imposição de tal dever advém do pressuposto de que os profissionais da saúde tomavam conhecimento de informações que não eram suas, mas sim das pessoas para a qual era prestado os serviços assistencial de saúde. Assim, pode-se afirmar que, o dever de sigilo profissional já integrava o quadro de deveres a serem observados pelos médicos e enfermeiros, mesmo antes de se falar na necessidade de proteção de dados pessoais.

Atualmente, todas as profissões relacionadas à saúde possuem normas deontológicas de sigilo que devem ser observadas, tal dever abrange todas as informações relacionadas à saúde que o profissional tem ao seu dispor no âmbito do exercício de suas atividades profissionais, sob o qual encontra-se sujeito à imposição de um regime disciplinar diante da sua violação.

[57] DEODATO, *Op. Cit.*, p. 30.

As normas deontológicas atuais não só impõem um dever ao profissional da saúde no âmbito do exercício de sua função - que consiste no dever de manter o sigilo sobre as informações do assistido -, mas também determina penas e medidas disciplinares diante da ocorrência da violação de tal dever.

As instituições e organizações que prestam serviços à saúde também se encontram adstritas à necessidade de manter o sigilo das informações acerca das pessoas que são assistidas em suas instalações. Na medida em que, compete aos seus responsáveis a implementação de meios e métodos que garantem a proteção da privacidade de seus pacientes.

A obrigação de manter em segredo as informações relativas aos assistidos encontra-se consagrada na Lei nº 12/2005 de 26 de janeiro, nomeadamente no artigo 4º, que determina: "Os responsáveis pelo tratamento da informação e saúde devem tomar as providências adequadas à proteção de sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais".

A informação relativa à saúde diz respeito à uma esfera intima da vida presente, passada e até mesmo futura do seu titular, assumindo o caráter de informação privada considerada como tal pela própria Constituição e demais leis esparsas, consagrando o direito de proteção destas informações.

Os profissionais de saúde, que no exercício de suas funções acabam por ter contato direto com informações relativas à saúde é imposto o dever de manter o sigilo, por meio de suas deontologias e pela própria lei, garantindo o respeito pelos direitos de seus assistidos. Igualmente, os responsáveis pelas organizações de saúde estão obrigados a manter estas informações em segredo.

Diante disso, pode-se auferir que em virtude da natureza privada que apresentam, todo o sistema jurídico promove a preservação da privacidade dos dados e informações pessoais relativos à saúde.

Nesse contexto, cabe ressaltar que os ambientes de prestação de cuidados à saúde deixaram de ser os únicos meios em que se verifica a coleta e tratamento de dados e informações relativas à saúde.

O avanço tecnológico tem apresentado cada vez mais, novos meios e métodos de controle e averiguação da saúde e do bem-estar, os quais transpassam o exercício das atividades relativas à saúde e podem fazer parte da vida cotidiana de uma sociedade.

Para melhor elucidar, tomamos como exemplo os aplicativos e softwares desenvolvidos para realização de monitoramento constante dos batimentos cardíacos, consumo de calorias

diárias, acompanhamento do desenvolvimento gestacional, dentre tantos outros sistemas que têm sido criados com o objetivo de assegurar uma maior qualidade de vida para os seus usuários e utilizadores.

Tanto as informações que são disponibilizadas pelos seus utilizadores, como as informações colhidas pelos aplicativos de forma automática, sem que haja uma interferência humana que alimente o sistema diretamente com as informações referenciais como, por exemplo, a utilização de relógios inteligentes que, automaticamente medem a frequência cardíaca e o gasto e consumo diário de calorias, consistem em dados e informações que dizem respeito à esfera privada de seus utilizadores, nomeadamente, dizem respeito à sua qualidade de vida e saúde.

Por isso, há um campo muito vasto em que se pode realizar a coleta e o tratamento de dados relativos à saúde, os quais vão muito além dos dados recolhidos no âmbito da prestação de cuidados para com a saúde.

Diante disso, é que se justifica a existência de diversas normas jurídicas e deontológicas no atual sistema jurídico que tem o objetivo de conferir proteção aos dados pessoais, as quais tratam de conferir segurança jurídica aos seus titulares, garantindo uma série de direitos que se encontram diretamente correlacionados à proteção de dados.

2.2 A SEGURANÇA DE DADOS COMO UM FATOR ESSENCIAL PARA A PROTEÇÃO DOS DIREITOS E INTERESSES DE SEUS TITULARES

A criação e existência de regras deontológicas que regulam o dever de sigilo imposto aos profissionais que atuam com o cuidado à saúde, pode ser entendida como uma busca pela manutenção da segurança jurídica em relação às informações e dados dos seus titulares.

O respaldo normativo oferecido pelas regras deontológicas apresenta significância para o âmbito de proteção de dados, principalmente no que diz respeito à realização da coleta destes dados pelos profissionais da saúde. Todavia estas normas não abarcam as situações específicas de tratamento dos dados, às quais são aplicadas as normas de proteção e segurança de dados contidas na legislação interna e no âmbito dos Estados-Membros.

Portanto, o estudo acerca do regime de segurança de dados que se impõem diante da realização do tratamento dos dados relativos à saúde permitirá uma compreensão global do tema, principalmente no que diz respeito às medidas técnicas e organizativas que devem ser tomadas pelo responsável pelo tratamento e pelo subcontratante para evitar a ocorrência da

violação de dados, bem como, as atitudes de que devem ser tomadas diante da efetiva ocorrência de uma violação.

Não restam dúvidas de que o tratamento de dados pessoais é uma parte muito importante no âmbito do tratamento de dados, uma vez que a sua aplicação prática deve sempre observar as normas que tratam da segurança dos dados, garantindo que o tratamento realizado apresente um nível adequado de segurança para os seus titulares.

A segurança dos dados pode ser visualizada como peça principal e essencial do Regulamento da Proteção de Dados e da realização da operação de tratamento, uma vez que impõe regras e diretrizes que devem ser seguidos com o intuito de conferir efetiva segurança para os dados pessoais, de modo a atravessar todo o regime jurídico de proteção de dados de forma transversal.

A importância desta matéria é ainda mais evidenciada quando verificamos que o legislador criou uma Secção específica no RGPD para tratar da segurança dos dados pessoais, a qual é constituída pelos artigos 32º a 34º, que serão objeto de estudo.

O artigo 32º do aludido diploma legal define uma espécie de modelo a seguir para que se obtenha um tratamento seguro, obrigando os responsáveis pelo tratamento dos dados e os subcontratantes a adotarem e aplicarem "medidas técnicas e organizativas" que se mostrem necessárias para assegurar um nível adequado de segurança e de riscos.

Igualmente, o mesmo diploma legal, determina que devem ser levadas em consideração as "técnicas mais avançadas", a "natureza" do dado, o contexto, âmbito, as razões que conduzem as operações de tratamento de dados, bem como, os riscos corridos pelos titulares que podem advir das aludidas operações.

Pode-se verificar a forte presença do princípio da proporcionalidade, ao passo em que as medidas técnicas e organizativas a serem implementadas devem sempre observar os riscos em concreto que estão envolvidos com a atividade de cada tratamento em particular.

Nesse sentido, entendemos que, quando se está diante de dados relativos à saúde, estes cuidados devem ser observados com muita cautela e sempre se levando em consideração os danos que uma possível violação poderá acarretar para os seus titulares.

Este dispositivo legal também evidencia a preocupação do legislador em apresentar algumas sugestões de medidas de segurança que podem ser implementadas consoante a situação concreta verificada.

Tais sugestões correspondem a: pseudominização e a cifragem dos dados, a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, a capacidade de estabelecer a disponibilidade e o acesso

aos dados pessoais de forma atempada no caso de ocorrer um incidente físico ou técnico e um processo para testar, apreciar e avaliar regularmente a eficácia das medidas organizativas adotadas.

Cumpre-nos esclarecer os conceitos atribuídos à pseudominização e à cifragem de dados, na medida em que, a primeira pode ser interpretada como uma forma de tratamento que tem o escopo de evitar que determinados dados possam ser atribuídos a um titular específico. Ou seja, é um procedimento que tona o dado anônimo, no qual os campos que contêm informações que permitam a identificação do titular são substituídos por um pseudônimo ou por um identificador artificial.

Enquanto que, a definição de cifragem pode ser analisada a partir da conceituação atribuída pelo Glossário da Sociedade da Informação da Associação para a Promoção e Desenvolvimento da Sociedade da Informação (ADPDSI)[58], qual seja, "Utilização de uma cifra na conversão de uma mensagem original numa mensagem não inteligível (criptograma), que não permita a sua leitura por pessoas não autorizadas".

Assim, a cifragem que também recebe a denominação de encriptação pode ser entendida como um processo que se transforma uma mensagem original em uma cifra tornando-a inteligível, de modo a não permitir a leitura e compreensão por pessoas que não se encontram autorizadas, garantindo a confidencialidade do dado.

Conforme verificaremos a seguir, um único tratamento de dados pode acarretar no envolvimento de diversas pessoas, vez que pode ser realizado pelo responsável pelo tratamento, pelo subcontratante ou por um terceiro contratado que atue sob sua responsabilidade.

Nesses casos, o responsável pelo tratamento e o subcontratante devem adotar as medidas necessárias para garantir que este terceiro que têm acesso aos dados pessoais, apenas possam proceder com o tratamento se detiverem claras instruções emanadas pelo responsável, salvo se determinado em contrário pelo Direito da União ou do Estado-Membro.

Nesse sentido, salientamos os ensinamentos de Menezes Cordeiro[59], que nos remete à necessidade de haver uma interpretação extensiva do aludido diploma legal, o qual deve ser abrangido por todas as pessoas singulares.

Ou seja, não apenas os funcionários contratados pelo responsável pelo tratamento, mas todos os indivíduos que se encontram nesta relação como, por exemplo, o contrato de prestação de serviços ou de trabalho. Ainda, o mesmo autor, nos atenta para o fato de que a norma deve

[58] Disponível em: https://apdsi.pt/glossario/
[59] CORDEIRO, *Op. Cit.*, p. 350.

ser interpretada no sentido de não incluir apenas o acesso aos dados, mas também o acesso ao próprio sistema de tratamento.

Nesse sentido, é importante lembrar que, o artigo 10º da Lei nº 58/20019 de 08 de agosto, impõem o dever de sigilo e confidencialidade à toda e qualquer pessoa que possa intervir em operações de dados, incluindo-se os terceiros e subcontratantes.

Ainda, o artigo 51º do mesmo diploma legal, determina as sanções aplicáveis para aqueles que, sem justa causa ou sem consentimento, divulgam ou relevam dado pessoais. Apesar de tal previsão legal não estar consagrada na Seção II do RGPD, acreditamos que ela foi introduzida às normas do direito português com o objetivo de assegurar maior segurança jurídica aos titulares de dados.

Todavia, acreditamos que há uma importante questão que deve ser levantada neste momento, principalmente se levarmos em consideração que o objetivo do presente estudo reside nos dados considerados sensíveis.

Em um momento anterior, verificamos a preocupação do legislador quando se está diante do tratamento de dados que possam, em virtude de sua natureza, causar grandes prejuízos ao seu titular. Diante disso, o legislador deu luz aos denominados dados sensíveis, os quais carecem especial atenção, porque se relacionam com direitos fundamentais dos titulares.

Todavia, apesar do próprio regulamento realizar esta segmentação de dados, é certo que não há diploma legal que regule de forma especial a segurança dos dados sensíveis, não fazendo distinção entre as medidas de segurança que devem ser implementadas quando se está diante de tais dados, o que, ao nosso ver, é uma matéria que merece a máxima atenção do sistema jurídico e legal.

Uma vez que, não nos parece fazer sentido a lei reconhecer a existência de dados que, em virtude de sua natureza, podem ferir diretamente e com maior intensidade os direitos e interesses individuais e deixa de estabelecer medidas especiais de cuidado e proteção dos dados sensíveis.

2.3 A VIOLAÇÃO DE DADOS PESSOAIS

Em que pese a existência de normas que objetivam alcançar a máxima segurança dos dados pessoais, não se pode deixar de levar em consideração a efetiva e real possibilidade de violação de dados.

O conceito de violação de dados pode ser extraído do artigo 4º, nº12 do RGPD: "«Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental

ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;".

Portanto, pode-se considerar como uma violação de segurança de dados toda ação ou fato que acarrete, de forma ilícita ou acidental, a perda, destruição, alteração, o acesso ou a divulgação de dados pessoais que se encontrem sujeitos a qualquer tipo de tratamento.

O Grupo de Trabalho do artigo 29º[60], ao emitir orientações acerca da notificação diante da ocorrência de uma violação de dados pessoais esclarece que o termo 'perda' utilizado pelo legislador, deve ser interpretado de forma a considerar que os dados continuam a existir, porém o responsável pelo tratamento perdeu a posse, o acesso ou o controle dos dados. Em contraposição, a destruição se refere aos dados pessoais que propriamente deixam de existir ou que deixam de existir em um formato que seja de alguma utilizado para o responsável.

O aludido grupo de estudos salienta também que o significado de dano se refere aos dados que foram corrompidos, alterados ou se encontram incompletos. Ou seja, encontram-se inseridos nesta modalidade de violação todos os dados que sofreram algum dano que acarretou já mudança do estado original.

O tratamento considerado ilícito ou não autorizado pode incluir a divulgação ou acesso de dados pessoais a terceiros que não tem autorização para aceder aos dados, bem como, qualquer outra forma que viole o disposto no RGPD.

Só podendo se verificar a situação de violação pela ilicitude quando se está diante de uma prévia violação da segurança, ou seja, um incidente ocorrido nas medidas organizativas que são implementadas pelo responsável ou pelo subcontratante.

Ainda de acordo com o Grupo de Trabalhos do artigo 29º[61], a consequência desta violação é que o responsável não pode assegurar o cumprimento dos princípios relativos ao tratamento dos dados pessoais, estudados anteriormente.

Facto este que realça a distinção entre um mero incidente de segurança e uma efetiva violação de dados, na medida em que todas as violações de dados pessoais podem ser consideradas como incidentes de segurança, todavia, nem todos os incidentes de segurança acarretam em violações dos dados pessoais.

Resta evidente que deverá sempre haver uma efetiva violação de dados, não bastando a abstrata potencial possibilidade de sua ocorrência. Questão completamente diversa da ora

[60] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. **Parecer nº 03/2014 relativo à notificação da violação de dados pessoais**, p. 12-15.
[61] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. *Op. Cit.*, p. 18.

colocada e que não deve ser confundida pois, diz respeito ao incumprimento dos deveres de segurança estabelecidos pela lei, os quais não se configuram uma violação de dados por si só, mas sim uma contraordenação ao que norma estabelece. Igualmente, os tratamentos realizados de forma ilícita também não podem ser confundidos com a violação de dados.

2.3.1 Espécies de violações de dados pessoais

De acordo com o Grupo de Trabalhos do artigo 29º[62], as violações aos dados pessoais podem ser categorizadas com base em três princípios da segurança da informação, os quais correspondem a: violação da confidencialidade, quando há acesso não autorizado ou acidental ou divulgação. Violação da integridade, quando há uma alteração no dado que não autorizada ou que ocorreu de forma acidental. Violação da disponibilidade, quando há perda ao acesso ou a destruição não autorizada ou acidental.

Ao passo em que, é perfeitamente possível que em uma única ocasião ou tratamento se verifique mais de um tipo de violação, como por exemplo, violação de disponibilidade e de integridade ocorrendo de forma conjunta e simultânea.

A realização da distinção entre a ocorrência de uma violação de integridade ou de confidencialidade parece ser uma tarefa relativamente clara. Enquanto que determinar a ocorrência de um a violação da disponibilidade do dado parece ser uma questão mais dificultosa.

Para elucidar melhor o referido, tomamos como exemplo um caso hipotético em que o responsável pelo tratamento não consiga efetuar manobras que restaurem o acesso à determinados dados que foram deletados, por exemplo, utilizando-se de uma cópia de segurança. Nesse caso, se estará diante de uma perda da disponibilidade permanente do dado.

Também se verifica a perda da disponibilidade quando há interrupção do serviço de uma organização, por exemplo, pela ausência de energia elétrica durante um determinado tempo, tornando indisponível o acesso aos dados pessoais.

Nesse sentido, é importante ressaltar que, no exemplo acima, mesmo se tratando de uma perda de disponibilidade temporária, porque assim que os serviços de abastecimento de energia elétrica se estabilizarem, a situação perda de disponibilidade deixará de existir, existe a necessidade de notificação do incidente.

[62] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. **Parecer nº 03/2014 relativo à notificação da violação de dados pessoais**, p. 21

O artigo 32º do RGPD, ao tratar da segurança no procedimento de tratamento de dados, preleciona que durante a aplicação das medidas técnicas e organizativas que visam assegurar um adequado nível de segurança ao risco, deve-se levar em consideração a " [...] capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e serviços de tratamento[...]" e ainda a " [...] capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente [...]".

Portanto, um incidente de segurança que acarrete na indisponibilidade de dados, ainda que temporária é um tipo de violação, uma vez que a impossibilidade de acesso aos dados ainda que temporariamente, pode acarretar em um significativo impacto sobre os direitos e as liberdades dos seus titulares.

Sempre que houver qualquer violação de dados, ainda que se trate de uma situação temporária, deve haver o registro e documentação do incidente, conforme preleciona o artigo 33º, nº 5 do RGPD: "[...]5.O responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.".

A elaboração de tal documento também poderá vir a servir como um fator de auxílio para o responsável pelo tratamento para demonstrar para a autoridade de controle de que este agiu em conformidade com as normas relativas ao tratamento. Esclarecendo sua responsabilidade, caso venha a ser questionado.

A notificação sobre a violação que deve ser direcionada para a autoridade de controle e para as pessoas afetadas, deve levar em consideração as circunstâncias em concreto e o risco que pode existir em virtude da violação. De modo que, é dever do responsável pelo tratamento avaliar a probabilidade e gravidade que a violação resultante da indisponibilidade dos dados pode acarretar sobre os direitos e liberdades das pessoas singulares.

Ainda, o artigo 33º do RGPD determina que o responsável pelo tratamento deve proceder com a notificação, salvo se a violação dos dados não possa acarretar em riscos para os direitos e liberdades de seus titulares. Vejamos: "1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo [...] a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.".

Portanto, sempre que houver qualquer tipo de violação de dados, caberá ao responsável pelo tratamento analisar minuciosamente a situação ocorrida, bem como verificar a efetiva ocorrência da violação e avaliar todas as possíveis consequências que podem surgir em

momento futuro. Para que, depois disso, possa tomar as medidas necessárias e pertinentes, como, por exemplo, notificar a autoridade de controle e o titular de dados, conforme verificaremos a seguir.

2.4 A OCORRÊNCIA DA VIOLAÇÃO DE DADOS E AS MEDIDAS DE SEGURANÇA QUE DEVEM SER TOMADAS PELO RESPONSÁVEL PELO TRATAMENTO

Sempre que houver uma violação de dados, o responsável pelo tratamento deve analisar a extensão dos danos causados e as possíveis consequências futuras. Ocorre que, uma única violação de dados pode acarretar em um extenso leque de efeitos adversos com extrema significância sobre a vida pessoal de seus titulares ou terceiros, que podem vir a resultar em danos materiais, imateriais e até mesmo físicos.

Tais danos podem incluir a perda total de controle sobre os dados, a limitação de direitos dos titulares, discriminação, roubo de identidade, danos para a reputação pessoal, perda de confidencialidade de dados protegidos pelo sigilo profissional, perdas financeiras, dentre outras situações capazes de violar os direitos e liberdades dos titulares.

Diante da possível gravidade ocasionada pela violação de dados, o RGPD obriga o responsável pelo tratamento a notificar a violação à autoridade de controle, a menos que seja muito improvável que da violação resultem riscos que possam causar efeitos adversos. Quando verificado um elevado risco de ocorrência de efeitos danosos, o responsável pelo tratamento também deve comunicar a ocorrência da violação para as pessoas afetadas, ou seja, para o titular do dado.

A importância de se identificar uma violação e avaliar o possível risco que possa acarretar aos titulares dos dados e terceiros e proceder com consequente a notificação é ressaltada no Considerando nº 87 do RGPD, que nos remete à necessidade de verificar a aplicação de todas "[...]as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular. [...]."[63].

O mesmo dispositivo também preleciona que a comprovação de que a notificação foi enviada sem demora justificada, leva em consideração a gravidade e a natureza da violação e as consequências que o titular dos dados poderá vir a enfrentar. Sendo que, tal notificação pode resultar em uma intervenção da autoridade de controle.

[63] REGULAMENTO (UE) 2016/679 - **Jornal Oficial da União Europeia**, considerando nº 87.

Ainda, na Secção 4 do RGPD nos deparamos com mais algumas orientações acerca da avaliação dos possíveis efeitos adversos para os titulares. De modo que, se os responsáveis pelo tratamento deixarem de notificar a autoridade de controle ou os titulares de dados de uma violação, mesmo que os requisitos presentes nos artigos 33º e/ou 34º do RGPD tenham sido observados, é facultado à autoridade de controle a imposição de medidas corretivas, por exemplo, a imposição de coimas que podem ser de até 10.000.000 euros ou até 2% do volume de negócios anual da pessoa jurídica.

Não se pode deixar de ressaltar que, em determinadas situações, a ausência de notificação de uma violação de dados pode revelar a não observância ou inadequação das medidas de segurança adotadas por parte do responsável pelo tratamento.

A autoridade de controle também pode emitir sanções tanto pela ausência de comunicação ou notificação da violação (conforme artigos 33º e 34º do RGPD), bem como, pela ausência de adoção de medidas de segurança que se mostrem adequadas (conforme artigo 32º do RGPD), uma vez que se tratam de infrações completamente distintas.

No âmbito de aplicabilidade de tais normas no direito interno de Portugal é imperioso salientar que a autoridade responsável pela realização do controle de dados é a Comissão Nacionalidade de Proteção de Dados (CNPD), a qual foi instituída pela Lei nº 58/2019 de 08 de agosto, que garante a execução do RGPD na ordem jurídica interna.

De acordo com a aludida norma, a CNPD é a autoridade de controle nacional de Portugal, de forma que, toda violação de dados que seja de competência do direito português deve ser notificada à tal órgão[64].

Ainda, os artigos 57º do RGPD e 6º da Lei 58/2019 elencam as atribuições da CNPD, dentre todas as responsabilidades atribuídas ao órgão, damos especial ênfase para a fiscalização do cumprimento do RGPD e demais normas que regulam a proteção de dados pessoais, realizar investigações e impor meios de correção, os quais podem incluir na aplicação advertências, repreensões, ordenar e impor medidas, e até mesmo aplicar coimas.

Portanto, além de ser o órgão responsável por abarcar as questões que envolvem a proteção de dados em todo o território de Portugal, a CNPD também deve ser notificada da ocorrência de violação de dados, sempre que exigido pela norma.

[64] Lei nº 58/2019 - **Diário da República, Série I. Nº 151** (08/08/2019), artigo 3º

2.4.1 A necessidade de notificação à autoridade de controle

Feitas as considerações acerca das medidas que devem ser adotadas pelo responsável pelo tratamento, passaremos ao estudo dos requisitos legais que devem ser observados pelo responsável no momento da formulação da notificação destinada à autoridade de controle, de modo a analisar os fatores internos e externos que devem ser observados na realização de tal comunicação.

O artigo 33º do RGPD determina que, diante de qualquer violação de dados pessoais, o responsável pelo tratamento deve notificar – no prazo de até 72 horas - a autoridade de controle competente da ocorrência da violação, a menos que tal violação não represente um risco aos direitos e liberdades de seus titulares.

Se tal notificação não for encaminhada à autoridade de controle dentro do prazo de 72 horas, deverá ser encaminhada em um momento posterior, juntamente com a justificativa do atraso no envio da comunicação.

Nesse sentido, o Grupo de Trabalho do Artigo 29º[65] para a Proteção de Dados levantou um importante questionamento, que diz respeito ao momento exato em que o responsável pelo tratamento passar a ter conhecimento da existência da ocorrência da violação de dados.

Concluindo que, apenas as circunstancias que envolvem uma determinada violação é que podem esclarecer as exatas condições em que se pode considerar que o responsável pelo tratamento tenha o conhecimento desta violação.

De modo que, podem haver casos que permitam que tal avaliação seja feita de forma extremante simples e fácil, por exemplo, diante da ausência de energia elétrica que acarreta em uma imediata indisponibilidade dos dados, ao passo que em outros casos poderá se levar algum tempo para apurar se efetivamente houve algum tipo de violação que tenha afetado os dados.

Fato é que, deve se dar devida ênfase à necessidade de se tomar uma ação imediata para investigar o incidente. Sendo necessário verificar, em um primeiro momento, se efetivamente houve alguma violação aos dados e, em caso positivo, adotar medidas imediatas de reparação e notificar a autoridade se controle, se assim se fizer necessário. Tendo sempre como objetivo primordial, conferir segurança e amparo aos dados e, consequentemente, aos seus titulares.

Ainda, o Grupo de Trabalho acima mencionado[66], nos ensina que, após ter o conhecimento de uma possível e potencial violação acarretada por um ato de terceiro ou ao

[65] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. **Parecer nº 03/2014 relativo à notificação da violação de dados pessoais**, p. 16

[66] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. *Op. Cit.*, p. 20

detectar um incidente de segurança que até então era desconhecido, pode o responsável pelo tratamento realizar, durante um breve período de tempo, uma investigação com o objetivo de se certificar se de facto houve ou não uma violação. Sendo que, durante este período investigatório, "[...] o responsável pelo tratamento não deve ser considerado como tendo conhecimento. [...]"[67].

Todavia, espera-se que a investigação se inicie com a maior brevidade possível, de forma a permitir que seja apurado com determinado grau de certeza a ocorrência concreta de uma violação.

Portanto, ocorrendo uma violação de dados, o responsável pelo tratamento deverá se certificar de que todas as medidas de proteção e organização restaram devidamente observadas e informar a autoridade de controle de forma breve, preferencialmente, dentro do prazo de 72 horas.

De acordo com o disposto no Considerando nº 87 do RGPD: "[...] Para comprovar que a notificação foi enviada sem demora injustificada importa ter em consideração, em especial, a natureza e a gravidade da violação dos dados pessoais e as respetivas consequências e efeitos adversos para o titular dos dados. [...]". Ou seja, o responsável pelo tratamento deverá analisar o provável risco para os titulares dos dados, com o objetivo de determinar se irá ou não proceder com notificação da autoridade de controle e das demais medidas necessárias.

Nesse aspecto, não se pode esquecer da figura do subcontratante, que é um terceiro que atua no tratamento de dados sob orientações do responsável pelo tratamento. Apesar do responsável pelo tratamento deter responsabilidade global pela proteção de dados, o subcontratante desempenha um papel fundamental para que o responsável pelo tratamento possa cumprir com as suas obrigações, uma vez que atua no processo de tratamento como uma espécie de suporte para o primeiro.

O nº 2 do artigo 33º do RGPD dispõem que, se o responsável pelo tratamento recorrer a um subcontratante para auxílio no desempenho de suas funções e, se o mesmo tomar conhecimento da ocorrência de uma violação de dados que o subcontratante está tratando em nome do responsável pelo tratamento, deverá notificar este último " sem demora injustificada".

Esta obrigação do subcontratante informar ao responsável pelo tratamento permite que este último avalie a situação ocorrida em todas as suas vertentes e, tome as medidas necessárias para o cumprimento das normas de proteção de dados pessoais.

[67] *Idem*.

Ainda, o RGPD não determina um prazo limite para que o subcontratante comunique o responsável pelo tratamento, a norma tão somente assevera que este o deve fazer "sem demora justificada". Nesse sentido, o Grupo de Trabalhos do Artigo 29º[68], anteriormente citado, recomenda que o subcontratante realize a notificação imediatamente, de modo a disponibilizar informações sobre a violação, possibilitando que o responsável pelo tratamento venha a cumprir com o prazo de notificação da autoridade de controle dentro do prazo de 72 horas.

A notificação a realizada para a Autoridade de Controle poderá acarretar em uma intervenção do órgão, seja para impor novas medidas, realizar investigações e, se necessário aplicar meios corretivos com o objetivo de evitar que novos episódios semelhantes venham a se repetir ou se tornem comuns.

Importante salientar que a notificação deverá conter alguns requisitos mínimos, os quais encontram-se elencados no nº 3 do artigo 33º do RGPD, devendo obrigatoriamente " [...] a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa; b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; c) Descrever as consequências prováveis da violação de dados pessoais; d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;".

Da leitura do aludido diploma legal podemos verificar que a norma não define categorias de registros de dados pessoais ou de titulares de dados. Diante disso, o Grupo de Estudos do Artigo 29º[69] sugere que as denominadas categorias de dados pessoais digam respeito aos diversos tipos de pessoas singulares que tiveram seus dados afetados pela violação, por exemplo, trabalhadores, clientes, idosos, crianças, dentre outros.

Enquanto que, as categorias de registros de dados pessoais podem se referir aos tipos de registros que foram objetos do tratamento, por exemplo, dados de saúde, dados financeiros, registros realizados no âmbito escolar, dentre outros.

[68] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. *Op. Cit.*, p. 22

[69] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. *Op. Cit.*, p. 23

De acordo com o disposto no Considerando nº 85 o RGPD, um dos objetivos que levou à criação da obrigatoriedade da notificação consiste em limitar os danos que podem afetar as pessoas singulares, titulares dos dados.

Portanto, se os tipos de dados pessoais ou tipos de titulares identificarem um risco específico de dano decorrente de uma violação, é extremamente necessário que a notificação indique tais categorias, o que permite avaliar as prováveis consequências decorrentes da violação.

Ainda, o nº4 do artigo 33º do RGPD prevê a possibilidade de fornecer as informações por fases à autoridade de controle, sendo que tal medida apenas se verifica nos casos em que não for possível fornecer todas as informações ao mesmo tempo.

Nesse sentido, ressaltamos as análises realizadas sobre o artigo no Grupo de estudos do artigo 29[70º], no sentido de que tal norma evidencia que o RGPD reconhece que nem sempre os responsáveis pelo tratamento estarão na posse de todas as informações que dizem respeito à violação no prazo de 72 horas. Por este motivo, é que se permite que a notificação seja efetivada em partes.

É muito provável que tal situação possa ser verificada em violações que se mostrem mais complexas como, por exemplo, a necessidade de se realizar uma investigação forense para determinar qual a exata natureza da violação e o alcance dos danos ocasionados aos dados pessoais.

Nos casos em que há disponibilização de informações por fases, a autoridade de controle deverá dispor sobre quando e como serão apresentadas as informações suplementares. O que não pode impedir que o responsável pelo tratamento forneça informações suplementares em qualquer outra fase, desde que tenha conhecimento de informações adicionais sobre a violação e que se mostrem relevantes.

Feitos os breves apontamentos acerca da necessidade de notificação da autoridade de controle, não podemos deixar de tratar dos casos de violações que encontram respaldo no nº 1 do artigo 33º do RGPD, e que não precisam ser notificados à autoridade de controle pois não apresentam qualquer capacidade de resultar em algum "risco para os direitos e liberdades das pessoas singulares".

Tomamos o exemplo a ocorrência de uma violação de dados que se encontram encriptados, em que se verificou a ocorrência da quebra de confidencialidade. Ou seja, houve a violação de informações que se encontram armazenadas em formato de códigos.

[70] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. *Op. Cit.*, p. 25

Em um primeiro momento, parece-nos evidente que tal situação se trata de uma efetiva violação e, por isso, deve ser notificada à autoridade de controle. Todavia, a questão posta deve ser analisada com cautela sobretudo, por se tratarem de dados que se encontram ininteligíveis para terceiros que não fazem parte da operação de tratamento.

Assim, se a chave não estiver comprometida e não puder ser descoberta por terceiros através dos meios eletrônicos disponíveis, os dados pessoais são completamente ininteligíveis. Por isso, a probabilidade da violação ocorrida afetar negativamente as pessoas em causa é extremamente baixa e, de acordo com os ensinamentos emitidos pelo Grupo de Trabalho do artigo 29º[71], nesses casos, não é necessário emitir notificação para as autoridades de controle, uma vez que não se verifica chances de danos aos titulares dos dados.

Assim, pode-se sustentar a ideia de que, se a violação ocorrida envolver dados pessoais tornados ininteligíveis para terceiros não autorizados, ou seja, dados encriptados, a notificação à autoridade de controle pode não ser necessária porque a violação ocorrida não coloca em risco os direitos e liberdades dos titulares.

Contudo, é importante salientar que, se os dados não tiverem sido objeto de um encriptamento seguro, poderá causar riscos quanto à sua disponibilização a terceiros não autorizados, ocasião em que, evidentemente, estaremos diante de um incumprimento RGPD, havendo a efetiva necessidade de ser reportado à autoridade de controle.

Por fim, resta evidente que o responsável pelo tratamento tem a obrigação de comunicar a autoridade de controle sempre que houver uma violação de dados que coloque em risco os direitos e liberdades dos titulares. Ao passo que, caberá a autoridade de controle analisar a situação e tomar as medidas que se mostrem necessárias, podendo solicitar esclarecimentos, dar aconselhamentos, determinar medidas que devem ser adotadas para minimizar os danos e riscos e até mesmo, a aplicação de coimas.

2.4.2 A necessidade de comunicação ao titular de dados

A ocorrência de uma violação de dados pessoais não acarreta apenas na necessidade de notificação da autoridade de controle, ao passo em que o artigo 34º do RGPD determina a obrigatoriedade de haver a comunicação da violação ao titular dos dados, vejamos: "1.Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e

[71] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. *Op. Cit.*, p. 26

liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada. [...]".

Assim, alguns casos de violação exigem, para além da notificação direcionada à autoridade de controle, a existência da comunicação da ocorrência da violação para todas as pessoas afetadas.

Da leitura do diploma legal podemos concluir que a comunicação ao titular de dados deve ser realizada sempre que verificada que a violação ocorrida pode acarretar em um elevado risco para os direitos e liberdades dos titulares dos dados violados.

Também é possível auferir que a comunicação deve ser realizada "sem demora injustificada", entendemos aqui que o objetivo do legislador foi determinar que a comunicação seja realizada da forma mais rápida possível, uma vez que os direitos e liberdades dos titulares dos dados encontram-se em risco.

Igualmente, o Considerando nº 86 do RGPD evidencia que o objetivo principal da notificação aos titulares, advêm da necessidade de prestação de informações acerca das medidas que estas pessoas devem tomar para se protegerem das possíveis consequências negativas que a violação pode acarretar.

Ressaltamos que o legislador tomou o cuidado de discriminar a forma como a comunicação deverá ser feita ao titular de dado, ao mencionar no nº 2 do já mencionado artigo 34º que a comunicação deverá conter uma descrição da natureza da violação, o nome e os contatos do encarregado da proteção de dados ou de outro suporte de contato, uma descrição das prováveis consequências oriundas da violação e a descrição das medidas propostas ou adotadas para reparar a violação ou atenuar os efeitos negativos.

De acordo com o disposto no Grupo de Trabalho do artigo 29º[72], o responsável pelo tratamento não se encontra restrito ao disposto no RGPD, de modo que, sempre será possível que forneça informações para além das exigidas pela norma.

Em regra, as violações devem ser comunicadas diretamente aos titulares de dados, a menos que isto acarrete em um esforço desproporcional, ocasião em que deverá ser realizada uma comunicação pública ou outra medida semelhante que seja capaz de dar conhecimento da violação aos titulares de uma forma eficaz.

Tal possibilidade detém amparo legal no artigo nº 34º, nº 3, alínea c), que preleciona: "[...]3.A comunicação ao titular dos dados a que se refere o n.o 1 não é exigida se for preenchida uma das seguintes condições: [...] c) Implicar um esforço desproporcionado. Nesse caso, é feita

[72] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. *Op. Cit.*, p. 27

uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz. [...]".

A comunicação com os titulares de dados deve ser realizada através de um meio que maximize a possibilidade de se comunicar com todas as pessoas afetadas de forma adequada e facilitada, como, por exemplo, SMS, correio eletrônico, postais, *etc*. É permitido que o responsável se utilize de vários métodos de comunicação e busque mais de um meio de contato, não se restringindo à apenas uma forma para contato com os titulares.

Também é muito importante que a comunicação seja realizada de forma acessível, utilizando-se de linguagem apropriada e permitindo que as pessoas sejam capazes de entender as informações que estão sendo prestadas, bem como, compreendem a natureza da violação ocorrida as medidas de que podem ser tomadas para sua proteção individual.

O Considerando nº 86 do RGPD dispõe que "Essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação".

Portanto, o responsável pelo tratamento pode recorrer à cooperação da autoridade de controle para cumprimento do dever de comunicar os titulares de dados acerca da violação. A autoridade por sua vez, para além de atuar em regime de cooperação poderá emitir orientações ao responsável pelo tratamento acerca das comunicações, objetivando evitar maiores danos aos titulares.

Questão extremamente interessante diz respeito ao fato de que o responsável pelo tratamento também poderá contar com a cooperação das autoridades de polícia. Isso porque, o Considerando nº 88 do RGPD determina que a notificação da violação deverá levar em consideração "os legítimos interesses das autoridades de polícia nos casos em que a divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias da violação de dados pessoais".

Ou seja, existe a hipótese de o responsável pelo tratamento atrasar a comunicação da violação aos titulares de dados se tal fato possa a vir prejudicar o trabalho das investigações, na medida em que tal atraso apenas se justifica mediante o aconselhamento da autoridade de polícia.

O mesmo ocorre com a notificação que deve ser dirigida à autoridade de controle, ao passo em que, o artigo 34º, nº 3 do RGPD prevê as condições que não exigem a notificação às pessoas singulares. A primeira condição que dispensa a comunicação, refere-se às situações em que o responsável pelo tratamento tiver adotado as medidas organizativas e técnicas adequadas observando proteger os dados pessoais antes mesmo da violação, sobretudo medidas que tornem os dados incompreensíveis para terceiros não autorizados. Como ocorre, por exemplo, com os dados encriptados.

A comunicação ao titular também é desnecessária nos casos em que, após a ocorrência da violação, o responsável pelo tratamento tome medidas que asseguram que os riscos aos direitos e liberdades dos titulares já não são mais suscetíveis de ocorrerem.

E ainda, há desobrigação de comunicar a ocorrência aos titulares dos dados da ocorrência da violação, se esta exigir do responsável pelo tratamento um esforço completamente desproporcional.

Nesses casos, o responsável pelo tratamento deverá comprovar para a autoridade de controle que a comunicação da violação aos titulares não foi realizada porque se encontra preenchida uma ou mais das condições legais que eximem tal comunicação.

Ainda, a autoridade de controle pode exigir que o responsável pelo tratamento comunique a violação de dados aos titulares se considerar que a violação pode acarretar em um elevado risco para os direitos e liberdades das pessoas singulares.

Igualmente, se tal autoridade verificar que as razões levantadas pelo responsável pelo tratamento de dados que justificam a não notificação dos titulares não for bem fundamentada, poderá utilizar de seus poderes e até mesmo aplicar as sanções disponíveis.

Diante de todo o exposto, pode-se verificar que as operações de tratamento de dados contribuem para o desenvolvimento e aprimoramento do direito da saúde. Ao mesmo tempo é necessário olhar para o regime de segurança de dados como uma peça central de todo o RGPD e que deve sempre estar alinhado às operações de tratamento.

As operações de tratamento de dados da saúde, por seu turno, devem ser realizadas com observância às regras que determinam os direitos e deveres dos responsáveis pelo tratamento e subcontratantes e ainda, deverá observar as normas deontológicas de sigilo profissional que é imposto a todos aqueles que desenvolvem atividades de cuidados de saúde.

A observância destas leis no processo de tratamento e diante ocorrência de uma violação destes dados é essencial para resguardar os direitos e interesses dos titulares de dados, que podem ser prejudicados e, futuramente recorrer a reparação dos danos sofridos em decorrência da responsabilização civil dos envolvidos.

3. A RESPONSABILIDADE CIVIL PELA VIOLAÇÃO DE DADOS PESSOAIS DA SAÚDE À LUZ DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

É notória a existência de diversas normas no âmbito do direito interno e da União Europeia que regulam o processo de tratamento de dados, impondo uma série de princípios e deveres que devem ser seguidos para que se possa assegurar aos titulares a mínima segurança aos seus dados pessoais.

Assim como, também é evidente que, apesar da existência deste respaldo e cuidado legal com a operação de tratamento, há situações em que se pode verificar a efetiva ocorrência de violação de dados pessoais.

Conforme sustentado no parágrafo anterior, diante da ocorrência da violação de dados, tanto as autoridades de controle como os responsáveis pelo tratamento devem avaliar os impactos que podem advir da violação e devem, imediatamente, agir em conformidade com as previsões legais contidas no RGPD acerca da matéria.

Nesse contexto da efetiva ocorrência de danos em desfavor de terceiros em virtude da violação de dados, é que se verifica os primeiros traços de uma possível responsabilização civil, a qual nos propomos desenvolver no presente estudo. O qual tem como objetivo analisar o alcance da responsabilidade civil diante da ocorrência de uma violação de dados da saúde, apontando os seus principais limites e o amparo legal para tanto.

Portanto, passaremos ao estudo do instituto da responsabilidade civil voltando-se à uma análise que leva em consideração o disposto não apenas na norma civilista, mas também no disposto no RGPD, uma vez que estamos diante de uma matéria que envolve tanto o ramo do Direito Civil como o regimento que diz respeito à proteção de dados.

No âmbito da responsabilidade civil em decorrência da violação de dados, as figuras do responsável pelo tratamento e o subcontratante são peças essenciais, tal reconhecimento se dá pela mais atual legislação europeia que regula o tema.

Isso se dá porque há uma série de normas que regulam as atividades daqueles que controlam ou executam operações de tratamento de dados, na medida em que, as normas que regulam a proteção de dados incumbem ao responsável pelo tratamento e ao subcontratante a observância de diversos deveres quando se está diante da realização de operações de tratamento de dados.

Ao considerar que o conceito atribuído ao tratamento de dados é extremamente amplo, uma vez que abrange diversas operações, desde a coleta de informações até a sua armazenagem e destruição, pode-se auferir que tanto o responsável pelo tratamento como subcontratante

devem observar as normas de proteção de dados durante todo a persecução do processo, que pode perdurar por anos, o que os mantém como responsáveis durante todo este período.

A autora Mafalda Miranda Barbosa[73] nos ensina que no âmbito da proteção de dados estão presentes duas noções de liberdade distintas. A denominada *role responsability*, que diz respeito à responsabilidade que é imputada em virtude da função, cargo ou papel que uma pessoa ocupa, que torna obrigatória a observância de determinados deveres. Por exemplo, em virtude das atividades desempenhadas pelo responsável pelo tratamento, este está adstrito à observância de uma série de deveres legais que são impostos pelo RGPD.

Enquanto que a *liability responsability* implica em uma aceitação sobre o mérito da conduta, em que a responsabilidade é vista como o resultado de uma ação, permitindo que o indivíduo seja responsabilizado pelos atos praticados por terreiros.

Portanto, a figura do responsável pelo tratamento de dados nos remete à ideia de responsabilidade em virtude de lhe ser atribuído especial encargo que implica em deveres inerentes à atividade desenvolvida. Neste mesmo contexto, verificamos a presença da *liability* quando se está diante da violação de um ou mais deveres que são impostos ao responsável.

A violação de dados pode acarretar em duas responsabilidades: a que se dá pelo tratamento de dados, no âmbito do exercício de uma atividade de tratamento propriamente dita e a responsabilidade civil em decorrência da violação de dados.

Sendo que, há uma linha de continuidade entre elas, uma vez que, a responsabilidade pelo tratamento se encontra associada a uma esfera de deveres de cuidados, o que permite – em um momento posterior – apurar quem deve ser responsabilizado na esfera civil.

Nesse sentido, é imperioso tratarmos sobre o conceito atribuído ao responsável pelo tratamento para compreendermos alguns dos limites enfrentados pela responsabilidade civil. O Grupo de Trabalho do Artigo 29º[74], sustenta que o conceito atribuído ao responsável pelo tratamento é funcional, pois objetiva atribuir uma série de responsabilidades aos que exercem uma influência sobre os dados pessoais.

As disposições legais que estabelecem condições para o tratamento de dados são atribuídas ao responsável pelo tratamento, por este motivo ele é o responsável pelos prejuízos decorrentes do tratamento ilícito, ou seja, do próprio conceito de responsável pelo tratamento pode-se retirar a atribuição da responsabilidade.

---

[73] BARBOSA, Mafalda Miranda - **Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil**, p. 424

[74] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA - **Parecer nº 1/2010 sobre os conceitos imputados ao subcontratante e ao responsável pelo tratamento**, p. 12.

Portanto, a lesão de um direito ou interesse que detém proteção legal, resulta da convolação de uma esfera primitiva responsabilidade pelo outro em uma esfera de responsabilidade diante do outro, sendo que é esta primeira que nos oferece o embrião da imputação que irá ser estabelecida.

Conforme restou salientado anteriormente, o RGPD nos apresenta a concretização da denominada "*role responsability*" na medida em que imputa uma série de deveres que devem ser observados pelos responsáveis e subcontratantes. Todavia, não basta pensar em uma esfera de responsabilidade para que a imputação possa se afirmar, tanto é que ela é definida pelo legislador de forma abstrata.

Cabe-nos estudar em que medida a lesão ocorrida se liga ao dever imputado pela norma. Para tanto, é de suma importância compreender as relações entre o responsável pelo tratamento e demais responsáveis ou subcontratante.

O artigo 82º do Regulamento Geral da Proteção de Dados prevê que qualquer indivíduo que tenha sofrido danos em virtude de uma violação na proteção de dados tem o direito de ser indenizado pelo responsável pelo tratamento ou subcontratante pelos danos sofridos, vejamos: "1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. […]".

Em continuidade, o nº 2 do supracitado artigo legal acrescenta que o responsável pelo tratamento que se encontra envolvido em um processo de tratamento que não observe o regulamento de proteção de dados é responsável se dele resultar danos. Sendo que, o subcontratante apenas será responsabilizado se não tiver seguido as orientações lícitas do responsável pelo tratamento ou se não tiver cumprido as obrigações legais são aqueles que desenvolvem a função de subcontratante.

Há também a possibilidade do total afastamento da responsabilidade nos casos em que é possível ao responsável pelo tratamento a efetiva comprovação de que este não contribuiu com a ocorrência do efeito danoso e que atuou em conformidade com as regras e princípios que norteiam o regime de proteção de dados.

Também devemos considerar os casos em que há mais de um responsável pelo tratamento ou de um subcontratante, em que ambos são considerados como responsáveis pelos danos causados em virtude do tratamento.

Tal situação encontra amparo legal no artigo 82º do RGPD que preleciona: " […] 4. Quando mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam, nos

termos dos n.os 2 e 3, responsáveis por eventuais danos causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados. 5.Quando tenha pago, em conformidade com o n.o 4, uma indemnização integral pelos danos sofridos, um responsável pelo tratamento ou um subcontratante tem o direito de reclamar a outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento a parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com as condições previstas no n.o 2.".

Portanto, cada um será responsável pela totalidade dos danos, havendo a possibilidade do exercício do direito de regresso em relação à parte da indenização que corresponde à respectiva parte do dano causado.

Existindo uma solidariedade obrigacional entre o responsável e o subcontratante ao mesmo tempo em há a possibilidade de inversão do ônus da prova na medida em que se verifica a violação das obrigações impostas pela norma.

Assim, o sujeito que atua na condição de responsável pelo tratamento e que, no exercício da sua função lida com dados alheios, assume uma esfera de risco, o que implica na necessidade de adoção das medidas de cuidado e proteção que são instituídas pelo legislador, com o objetivo de prevenir uma possível responsabilização.

Conforme verificado anteriormente, a ocorrência de uma violação dos dados em virtude da inobservância das normas que exprimem o dever de cuidado, parte da sua esfera primitiva (que corresponde à responsabilidade pelo outro, ou seja, pelos dados do outro) passando para uma esfera mais ampla de responsabilidade, que se configura na responsabilidade perante o outro, sobre a qual passam a ser conduzidos os danos e lesões que poderiam ser evitados se cumpridos os deveres legais impostos.

Todavia, para que a responsabilidade seja afirmada não basta a existência deste nexo de imputação decorrente da observância das normas, também devem ser associados os requisitos imputáveis à pretensão indenizatória, ou seja, a ilicitude, o dano e a culpa.

Para que possamos aprofundar os estudos de modo a tratar das diversas modalidade de responsabilidade civil, importa em um primeiro momento, fazer um breve panorama acerca da função exercida pelo responsável pelo tratamento e pelo subcontratante, uma vez que a modalidade de responsabilidade civil em concreto depende diretamente da posição que estas duas figuram assumem em relação ao tratamento de dados.

3.1 AS FUNÇÕES EXERCIDAS PELO RESPONSÁVEL PELO TRATAMENTO E PELO SUBCONTRATANTE E A SUA INTERLIGAÇÃO COM A RESPONSABILIZAÇÃO NA ESFERA CIVIL

O artigo 4º, nº 7 do RGPD determina que o responsável pelo tratamento de dados pode ser uma pessoa coletiva ou singular, sob a qual é incumbida a tarefa de determinar os meios e as finalidades sob os quais se dará toda a operação de tratamento. Ou seja, trata-se da pessoa responsável por decidir quais meios e procedimentos que serão utilizados para a realização da recolha e tratamento dos dados, bem como o motivo que justifica a efetivação da operação de tratamento.

De acordo com o Grupo de Trabalho do artigo 29º[75], as funções que são atribuídas ao responsável podem advir de três vias distintas: por meio de uma competência legal expressa, de uma competência tácita que é verificada no âmbito contratual ou de uma competência de fato.

Sendo que, o desenvolvimento e a prática das atividades realizadas pelo responsável pelo tratamento não podem advir de uma relação de informalidade, de modo que, é indispensável que exista uma nomeação formal do indivíduo que irá ser responsável pelo desempenho da atividade de tratamento, uma irá exercer o controle efetivo sobre os dados.

Igualmente, nas demais vias do controle que é exercido pelo responsável pelo tratamento, deve-se ter especial atenção às cláusulas de um eventual contrato que preveja o grau e nível de controle que será realizado[76].

A determinação de cláusulas contratuais que tenham como objetivo prever o grau de nível do controle a ser realizado, além de conferir maior segurança jurídica em relação aos dados, servirá como apoio nos casos de uma eventual responsabilização civil nos casos em que há violação de dados, conforme trataremos a seguir, em capítulo destinado ao estudo da matéria.

Portanto, o responsável pelo tratamento assume um papel crucial nos procedimentos de tratamento de dados, o qual é responsável pode determinar as os meios e as finalidades que irão reger todo o procedimento e além disso, é incumbido da observância de uma série de deveres impostos pelo RGPD durante o exercício da sua função.

---

[75] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA - **Parecer nº 1/2010 sobre os conceitos imputados ao subcontratante e ao responsável pelo tratamento**, p. 15 e seguintes.
[76] *Idem*.

É permitido ao responsável pelo tratamento que se recorra ao auxílio de terceiros para realização das operações de tratamento de dados, os quais irão exercer suas funções de acordo com as determinações deste primeiro.

A figura do terceiro descrito acima, corresponde ao papel desempenhado pelo subcontratante, o qual também é apto a atuar no processo de tratamento de dados, porém sua atuação encontra-se adstrita às orientações do responsável pelo tratamento. De modo que, em regra, não é permitido que o subcontratante venha a tomar decisões que possam interferir ativamente no processo de tratamento.

Todavia, há casos em que pode-se verificar a existência de uma exceção à tal regra, a qual se dá em virtude de fatores supervenientes, em que o subcontratante passa a determinar quais são os meios ou finalidades do tratamento. Ocasião em que passa a assumir uma tarefa que cabe ao responsável pelo tratamento.

Para melhor elucidar a questão colocada, tomamos o próprio exemplo utilizado pelo Parecer nº 1/2010 do Grupo de Trabalho do artigo 29º[77], o qual nos apresenta a situação hipotética em que a empresa X presta serviços para o público em geral.

Sendo que, no momento em que tal empresa celebra um contrato ela faz a recolha de dados dos clientes e os disponibiliza para uma outra entidade, a qual armazena, digitaliza e cataloga todas as informações que forem relevantes para X, de acordo com as instruções específicas pré disponibilizadas por ela, a qual exerce a função de responsável pelo tratamento de dados.

Todavia, se X contratar uma empresa para lhe auxiliar com a promoção de seus serviços junto de seus clientes, a qual presta serviços de marketing a diversas outras empresas. Ao passo em que, com o decorrer do tempo a mencionada empresa de marketing decide utilizar a base de dados de X para promover produtos de outros clientes, assumindo uma nova finalidade para os dados, a empresa de marketing deixa de ser subcontratante e passa a ser a responsável pelo tratamento dos dados.

Esta mudança na figura do responsável pelo tratamento se dá em virtude do disposto no artigo 28º, nº 10 do RGPD que preleciona: "o subcontratante que, em violação ao presente regulamento, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão".

[77] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. *Op. Cit.*, p. 09

No mesmo sentido, o aludido Parecer nº 1/2010 preleciona que "a determinação da finalidade do tratamento está reservada ao responsável pelo tratamento"[78], portanto, sempre que o subcontratante determinar uma nova finalidade para o tratamento, irá assumir a posição de responsável pelo tratamento.

Assim, podemos sustentar que a figura do responsável pelo tratamento dos dados é completamente dinâmica, uma vez que o exercício desta função não se encontra adstrita às determinações estipuladas em um primeiro momento e, o seu desenvolvimento dentro das operações de tratamento de dados encontra-se intimamente ligada ao controle real e efetivo sobre as finalidades e aos meios que irão reger o tratamento.

Por outro lado, fica evidente que a determinação legal que trata dos casos em que o subcontratante venha a eleger uma nova finalidade para o tratamento dos dados, colocando-o em posição de igualdade ao real responsável pelo tratamento de dados, pretende conferir maior segurança jurídica em relação às garantias dos titulares de dados.

Para a autora Mafalda Miranda Barbosa, o disposto no artigo 28, nº 10 do RGPD, apenas faz sentido nos casos em que a utilização dos dados com a nova finalidade não tenha "em vista uma violação dos direitos que subjazem a proteção de dados"[79].

Inclusive, nos casos em que a "estrutura organizacional"[80] do subcontratante passa a ser substituída pela figura do responsável pelo tratamento, em virtude da nova finalidade, é possível "antever uma utilização dos dados em termos de efetivo controlo factual sobres eles e em termos de utilização consentânea com o regulamento"[81], situação esta, que vai muito além da questão da ilegitimidade da utilização dos dados em virtude da ausência do consentimento do seu titular.

Não se pode deixar de mencionar que há casos em que o tratamento de dados pode contar com mais de um responsável. Tal possibilidade encontra respaldo legal nos artigos 4º, nº 7 e 26º, ambos do RGPD, o qual preleciona: "quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento"[82].

Igualmente, o artigo 82º do RGPD reconhece a possibilidade de responsabilização de mais de um responsável, vejamos: "[...] Quando mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam, nos termos dos n.os 2 e 3, responsáveis por eventuais danos

[78] *Ibidem*.
[79] BARBOSA, *Op. Cit.*, p. 444.
[80] *Idem*.
[81] *Ibidem*.
[82] REGULAMENTO (UE) 2016/679 - **Jornal Oficial da União Europeia**, artigo 26º.

causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados.".

Nesse sentido, é importante ressaltar que nem todas as situações de tratamento de dados que envolvem uma pluralidade de responsáveis pelo tratamento, convolam necessariamente para uma pluralidade de responsabilidade, conforme verificaremos a seguir.

Para que se possa falar na existência de controle conjunto é indispensável que haja a partilha de meios e das finalidades, sendo que, sempre que não exista esta conjunção não se pode falar na responsabilização conjunta.

Ou seja, o controle conjunto pressupõe o domínio dos dados por ambos os controladores (responsáveis pelo tratamento). Uma vez que esta conjunção pressupõem o desenvolvimento direto de ambas as partes, as quais devem desempenhar suas funções em observância das obrigações previstas nas normas de segurança dos dados pessoais.

Estaremos diante de um controle conjunto nas hipóteses em que "os mesmos dados são partilhados por mais do que uma entidade, unidas pela prossecução de uma finalidade comum ou pela utilização de meios definidos em conjunto, de tal modo que só conseguimos antever uma atividade de tratamento de dados"[83].

Assim, a distinção que existe entre o controle comum (também denominado de controle paralelo) e o controle conjunto de dados é evidente, na medida em que o primeiro não envolve a partilha de meios e finalidades.

Para melhor elucidar a questão colocada, levamos em consideração a seguinte situação hipotética: uma empresa que vende produtos alimentares faz a recolha e tratamento dos dados de seus funcionários, com o objetivo de gerir os salários e, em um momento posterior, compartilha tais dados com a autoridade tributária. Neste caso, apesar de haver o compartilhamento de dados, não se pode falar na existência de um controle conjunto pois não há uma unicidade entre os meios e as finalidades destes dois responsáveis pelo tratamento.

Portanto, é imputado à figura do responsável pelo tratamento o dever de determinar as finalidades e os meios pelos quais se darão o tratamento. Sendo que, devemos sempre considerar a hipótese da existência de mais de um responsável pelo tratamento, ocasião em que, deverá ser analisado se há um controle paralelo ou conjunto de dados, o qual é definido com base na instituição dos critérios de determinação dos meios e das finalidades do respectivo tratamento.

[83] BARBOSA, *Op. Cit.*, p. 447.

O subcontratante, por sua vez, exerce as atividades por conta de outro sujeito (responsável pelo tratamento), o que faz com que as finalidades do tratamento não possam ser definidas por este, que apenas atua em nome de outrem.

Inclusive, a atual legislação em vigor trata destas situações em que o subcontratante – mesmo em desrespeito às normas – determina uma nova finalidade e/ou meio, passando a ocupar a condição de responsável pelo tratamento, o que acarreta no aumento dos deveres e obrigações que devem ser observados.

3.2 MODALIDADES CLÁSSICAS DO RESSARCIMENTO - ESPÉCIES DE RESPONSABILIZAÇÃO

Feita uma análise acerca das estruturas problemáticas que podem advir do exercício das funções desempenhadas pelos responsáveis pelo tratamento e pelo subcontratante, faz-se necessário aprofundarmos os estudos de modo a tratar das modalidades clássicas de ressarcimento no âmbito da proteção de dados.

Para a concretização do presente estudo, iremos adotar a posição dualista a qual distingue a responsabilidade civil em duas grandes modalidades: a responsabilidade aquiliana e a responsabilidade obrigacional, as quais apresentam diferenças significativas entre si.

Ao passo em que a primeira pode ser entendida como uma resposta do ordenamento jurídico face ás violações de direitos com eficácia *erga omnes*, enquanto que segunda modalidade de responsabilidade advém do "incumprimento de uma obrigação em sentido técnico, independentemente da fonte onde brotou"[84].

A realização de tal distinção permite uma melhor compreensão do alcance da responsabilização civil quando se está diante de um dano causado em virtude da violação de dados, conforme verificaremos a seguir.

3.2.1 A responsabilidade civil aquiliana

Também pode ser conhecida como extracontratual, encontra-se prevista no artigo 483º do CC, a qual se caracteriza pelo descumprimento de um dever legal que acarreta na ocorrência de um ou mais danos que afetam à terreiros. Vejamos a disposição legal que regula a matéria: "1. Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer

[84] BARBOSA, Mafalda Miranda – **Proteção de dados e direitos de personalidade**: uma relação de interioridade constitutiva, p. 13.

disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação. 2. Só existe obrigação de indemnizar independentemente de culpa nos casos especificados na lei. ".

Assim, podemos afirmar que esta modalidade de responsabilização civil sempre estará presente nos casos em que a prática de um determinado ato, em violação de uma disposição legal ou do direito de terceiros, acarreta em danos para com terceiros.

Para complementar o conceito deste tipo de modalidade e clarificar o tema, tomamos como exemplo os ensinamentos exarados pelo Tribunal do Porto, em que trata do conceito atribuído à responsabilidade civil extracontratual, asseverando que "[...] advém da violação de direitos absolutos (violação de deveres genéricos de respeito, violação de normas gerais destinadas à proteção de outrem) ou da prática de certos atos que, embora lícitos, causam prejuízo a outrem [...]."[85]

Portanto, de acordo com o Tribunal supracitado, ainda que a ação praticada pelo agente tenha cunho lícito, pode-se fazer em responsabilidade civil aquiliana, uma vez que há a efetiva ocorrência de um dano em face de terceiros.

De modo que, a aplicabilidade do regime de responsabilização civil também depende a verificação da presença de alguns requisitos mínimos que são determinantes para que se possa falar em responsabilidade. Tais requisitos correspondem à ocorrência de um fato, na ilicitude da conduta, na culpa do agente, na efetiva ocorrência do dano e no nexo de causalidade.

O primeiro pressuposto pode ser facilmente visualizado, uma vez que corresponde à uma ação humana que advém da vontade do indivíduo, a qual pode ocorrer por ação ou omissão. Na medida em que, neste ultimo deve estar presente o dever do agente de praticar determinado fato, conforme dispõem o artigo 486º do CC: "As simples omissões dão lugar à obrigação de reparar os danos, quando, independentemente dos outros requisitos legais, havia, por força da lei ou de negócio jurídico, o dever de praticar o acto omitido.".

Uma questão que, no passado, foi objeto de discussão doutrinária e jurisprudencial, mas que atualmente há um consenso bem estabelecido, diz respeito a saber se interessa mais a conduta efetivamente praticada pelo agente ou o resultado danoso.

De forma sucinta, pode-se sustentar que, se estivermos diante de uma situação em que há violação imediata ao bem jurídico tutelado, importa levar em consideração apenas o resultado. Todavia, diante de uma situação de violação do dever de cuidado ou de negligência, é imperioso levar em consideração a conduta do agente lesante.

[85] TRIBUNAL da Relação do Porto - **Acórdão do processo nº 274/17.8T8AVR.P1**, de 08 de fevereiro de 2021. Relatora Eugénia Cunha.

Neste ínterim, também convém tratar das pessoas inimputáveis, as quais não detém capacidade suficiente para compreender e realizar o fato lesivo. Para que um fato possa ser imputável aos agente, exige-se que o indivíduo tenha a plena capacidade de realizar e entender a sua conduta, ou seja, se detém condições suficientes para compreender o efetivo significado da sua atuação.

O artigo 488º do CC trata deste assunto ao asseverar que "Não responde pelas consequências do facto danoso quem, no momento em que o facto ocorreu, estava, por qualquer causa, incapacitado de entender ou querer, salvo se o agente se colocou culposamente nesse estado, sendo este transitório.".

Assim, pode-se afirmar que, em regra, presume-se, em um primeiro momento, que todas as pessoas são imputáveis. Justamente, por se tratar de uma presunção, esta é ilidível, até mesmo porque a atribuição da característica de inimputabilidade á alguém deve ser feita de forma extremamente cuidadosa e restritiva.

A ocorrência da ilicitude na conduta realizada pelo agente é um fator indispensável para que se possa falar em responsabilização civil extracontratual. A presença deste elemento é marcado pela existência de uma norma jurídica de proteção dos direitos e interesses ou de direitos de outrem que deixam de ser observadas pelo agente.

De acordo com ilustre Tribunal Central Administrativo Sul, a ilicitude da conduta pode ser vista como um "[…]juízo de inobservância do direito objetivo, por violação de um direito subjetivo alheio ou de normas de proteção de interesses alheios, sem que haja causa de justificação. […]"[86].

A autora Ana Mafalda Miranda Barbosa[87] nos remete à existência de três modalidades distintas de ilicitude no âmbito da responsabilização civil extracontratual, as quais contribuem de forma significativa para melhor compreensão do tema sob exame.

A primeira modalidade tratada pela autora diz respeito à violação de direitos alheios, a qual resulta do artigo 483º, nº 1º do CC, a qual se concretiza pelo resultado jurídico que acarreta. Enquanto a segunda modalidade ilicitude se dá pela "quebra de uma norma legal de proteção de interesses alheios", onde a culpa diz respeito única e exclusivamente à violação da norma, não havendo a preocupação quanto ao resultado da ação.

[86] TRIBUNAL Central Administrativo Sul - **Acórdão do processo nº 116/16.1BECTB**, de 28 de junho de 2018. Relator Paulo Pereira Gouveia.
[87] BARBOSA, Ana Mafalda Castanheira Neves de Miranda – **Lições de Responsabilidade Civil**, p. 146-202.

Por fim, a terceira modalidade de ilicitude diz respeito ao direito subjetivo e, de forma simples pode ser traduzida na "violação dolosa dos bens costumes"[88].

Há na doutrina diversas teorias acerca do abuso de direito, todavia não iremos adentar ao estudo destas teorias por duas razões, primeiro porque a análise e estudo destas teorias não interfere de forma transversal com o que se busca com o presente trabalho que corresponde ao estudo da responsabilização civil pela violação de dados, permitindo o aprofundamento no tema central sem a necessidade de adentar nos entendimentos acerca da ilicitude ocasionada em decorrência do abuso de direito. Em segundo lugar, porque acreditamos que as duas primeiras modalidades são as que mais interessam e colaboram com a consecução do presente estudo.

Em sede de proteção de dados pessoais, pode-se afirmar que a responsabilização aquiliana advém de uma "relação de interioridade constitutiva entre a proteção de dados e diversos direitos de personalidade"[89]. Ou seja, a responsabilização civil sempre estará presente nos casos de tratamento de dados pessoas que em há o desrespeito aos direitos fundamentais do titular.

O artigo 82º do RGPD preleciona que qualquer indivíduo que tenha sofrido prejuízo ocorrido em razão da violação das disposições legais de proteção de dados ou do tratamento ilícito tem o direito de obter a reparação dos danos sofridos, vejamos: "Artigo 82.º 1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.".

Assim, o aludido dispositivo legal apresenta um campo de aplicação aparentemente irrestrito, uma vez que permite a responsabilização civil diante de toda e qualquer violação às normas e princípios que se encontram dispostos no RGPD.

Avançando a leitura do artigo supracitado, a responsabilização dos responsáveis pelo tratamento se dá apenas nos tratamentos em que eles se encontrem envolvidos e ainda, a responsabilidade do subcontratante só se verifica em duas situações concretas: pelo incumprimento das instruções do responsável pelo tratamento ou em virtude do incumprimento de obrigações normativas, no âmbito do tratamento de dados.

Portanto, partindo-se de uma leitura mais aprofundada deste dispositivo, fica evidenciado que nem todas as violações ao RGPD permitem a responsabilização civil aquiliana, mas tão somente, as violações que são decorrentes daquela operação de tratamento de dados.

---

[88] BARBOSA, *Op. Cit.*, p. 183.

[89] BARBOSA, Mafalda Miranda - **Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil**, p. 450.

O autor Menezes Cordeiro[90] nos apresenta uma interpretação mais alargada deste dispositivo legal ao assinalar que "[…] o artigo 82.º abrange tratamentos ilícitos, bem como violações de direitos, de obrigações ou de proibições legais que estejam indiretamente relacionadas com as atividades desenvolvidas pelos responsáveis e pelos subcontratantes.".

Podemos afirmar que a responsabilização civil aquiliana é muito ampla e vai além dos casos de violação do RGPD, vez que inclui todos os demais tratamentos que violem os atos de execução, e ainda as normas jurídicas estabelecidas pelos Estados-Membros que conferem execução interna às regras estabelecidas no RGPD.

De modo que, todos aqueles que em algum momento figurarem como lesados no âmbito da operação de tratamento de dados, não têm o seu direito de reparação restrito unicamente ao âmbito do artigo 82º do RGPD. Havendo a possibilidade de pleitear a responsabilização em virtude da violação de outras normas legais, para além do RGPD, e ainda, há a possibilidade de responsabilização contratual que será abordada em capítulo próprio.

Esgotados os estudos acerca da ilicitude da conduta, passaremos à análise da culpa em sede de responsabilização civil, a qual permite a justificação dos mecanismos da responsabilidade civil, sobretudo no que diz respeito à sua aplicabilidade no âmbito da proteção de dados.

Da leitura do artigo 483º, nº 2º do CC, podemos auferir que a regra geral é que não se pode falar em responsabilidade civil sem que haja culpa. Todavia, há uma exceção para tal regra, que é a responsabilidade objetiva, onde não há necessidade de provar a culpa do agente.

De acordo com os ensinamentos de Ana Mafalda Barbosa[91] a culpa pode ser visualizada como um "juízo de censura ético-jurídica", a qual traduz um desvalor na conduta realizada pelo agente, o qual poderia e deveria ter agido de forma diversa, mas não o fez, acarretando na ocorrência de um dano.

A culpa pode ser dividida em duas modalidades distintas, o dolo e a negligência. Este primeiro diz respeito a intenção do agente em praticar o ato, enquanto a negligência pode ser traduzida na violação de um dever de cuidado.

No âmbito do tratamento de dados, a negligência pode ser facilmente percebida, por exemplo, quando se está diante de uma violação de dados ocasionado pela inobservância dos deveres que são imputados pelo RGPD ao responsável pelo tratamento e ao subcontratante. Ou seja, existem normas que impõem um dever de cuidado, mas por agir com negligência durante

[90] CORDEIRO, A. Barreto Menezes – **Direito da proteção de dados:** à luz do RGPD e da Lei nº 58/2019, p. 383.
[91] BARBOSA, Ana Mafalda Castanheira Neves de Miranda – **Lições de Responsabilidade Civil**, p. 228.

o desempenho de suas atividades o responsável pelo tratamento deixa de cumprir com o que lhe é determinado.

Situação completamente diferente se verifica, por exemplo, quando o responsável pelo tratamento, mesmo sabendo da existência de uma norma expressa que proíba a conduta de divulgação de dados que permitam a identificação do seu titular, procede com a divulgação dos aludidos dados, com o objetivo de ocasionar um evento com resultado danoso ao titular dos dados.

Outra questão que merece especial atenção no que diz respeito à presunção da culpa e o seu aspeto probatório tange ao afastamento da culpa do responsável pelo tratamento. O CC em seu artigo 487, nº 1 impõem ao lesado o dever de provar que o autor do facto agiu com culpa, salvo disposição legal ao contrário. Vejamos a disposição normativa citada: "É ao lesado que incumbe provar a culpa do autor da lesão, salvo havendo presunção legal de culpa. […]".

Para a autora Ana Mafalda Barbosa[92], esta norma se encontra em "consonância com a regra em matéria de repartição do ónus da prova", uma vez que a culpa pode ser visualizada como o pressuposto do direito do indivíduo em obter uma indenização. Todavia, conforme já restou salientado, esta norma pode sofrer desvios, em que o lesado não terá de provar a ocorrência da culpa se houver disposição legal neste sentido.

Dá-se a merecida evidência ao disposto no artigo 82º, nº 3 do RGPD, o qual também exonera a responsabilidade do responsável pelo tratamento e do subcontratante se comprovado que estes não foram responsáveis pelo fato causador que originou o dano.

A imputabilidade registrada no aludido dispositivo se assemelha muito com o disposto no artigo 799º, nº 1º do CC: "1. Incumbe ao devedor provar que a falta de cumprimento ou o cumprimento defeituoso da obrigação não procede de culpa sua.".

Contudo, não pode haver confusão entre o disposto no CC com o disposto no RGPD, uma vez que a presunção prevista no aludido artigo 799º, nº 1, não se consubstancia apenas em uma presunção da culpa, além disso o alcance da norma do RGPD "não se circunscreve a este universo"[93].

Portanto, a não responsabilização no âmbito do Regulamento Geral da Proteção de dados pode ser verificada sempre que o subcontratante ou o responsável pela proteção de dados conseguirem encontrar fundamentos capazes de afastar a culpa e a ilicitude dos seus atos ou ainda, comprovarem que os atos praticados durante o desenvolvimento da sua atividade não contribuíram para a ocorrência do dano.

[92] BARBOSA, *Op. Cit.*, p. 238.
[93] CORDEIRO, A. Barreto Menezes - **O Consentimento do Titular dos Dados no RGPD**, p. 15.

Por seu turno, o dano pode ser caracterizado na esfera civilista como "[…] a perda in natura que o lesado sofreu, em consequência de um certo facto, nos interesses materiais, espirituais ou morais que o direito tutelado ou a norma infringida visam tutelar."[94]. Assim, o dano pode ser visualizado como uma consequência negativa do comportamento, sendo que tal repercussão pode ocorrer na esfera material e moral.

Todavia, em sede de proteção de dados nos deparamos com outra situação, uma vez que o RGPD não apresenta qualquer definição que possa ser atribuída ao conceito de dano. De acordo com Menezes Cordeiro[95] tal ausência foi alvo de discussão no âmbito do Conselho de criação da norma, em que os Estados-Membros questionaram se tal conceito já havia sido analisado e consolidado no âmbito do Direito da União Europeia.

Na discussão levantada foram manifestadas duas posições distintas. A primeira considerava que cabe ao direito interno de cada um dos países estabelecer o conceito que deve ser atribuído ao dano. Enquanto, a outra posição sustentava que é dever do TJUE analisar e interpretar a aplicação do disposto no artigo 82º do RGPD e, consequentemente o conceito que deve ser atribuído ao dano.

Ainda segundo o autor supra mencionado[96], a ausência de um consolidado conceito de dano deve ser acrescida há outros dois fatores que dificultam a aplicação do artigo 82º do RGPD, que correspondem à complexidade de quantificar os danos efetivamente causados, e ainda, a atribuição da competência aos tribunais dos Estados-Membros para dirimir os conflitos deste gênero, nos termos do artigo 82º, nº 6 do RGPD.

Da análise do Considerando nº 146 do RGPD podemos chegar à conclusão que pode-se atribuir ao dano o conceito que é "interpretado em sentido lato à luz da jurisprudência" do TJUE, não podendo deixar de refletir fielmente os princípios e os objetivos primordiais do RGPD.

Tratando-se da responsabilização na esfera civil, pode-se observar que o TJUE impõe aos Estados-Membros a observância de dois princípios: o da efetividade e da equivalência. Em que este primeiro, diz respeito a não tornar impossível ou a dificultar o exercício dos direitos que são reconhecidos pelo direito europeu, enquanto o segundo impede que os aplicadores do direito coloquem os sujeitos lesados em uma posição menos favorável do que estariam se houvesse a aplicação de uma norma interna análoga.

---

[94] VARELA, João de Matos Antunes – **Das obrigações em geral**, p. 598.
[95] CORDEIRO, A. Barreto Menezes – **Direito da proteção de dados:** à luz do RGPD e da Lei nº 58/2019, p. 384-386.
[96] *Idem*.

Com o objetivo de esclarecer o tema, colacionamos parte da decisão proferida pelo TJUE no julgamento do Acórdão nº C-494/16[97]:

> […] ao princípio da equivalência, importa recordar que o mesmo assenta na ideia de que os indivíduos que invocam os direitos conferidos pela ordem jurídica da União não devem ser desfavorecidos em relação aos que invocam direitos de natureza puramente interna.[…] No que respeita, por outro lado, ao princípio da efetividade, decorre da jurisprudência do Tribunal de Justiça que a questão de saber se uma disposição processual nacional torna, na prática, impossível ou excessivamente difícil o exercício dos direitos conferidos aos particulares pelo direito da União deve ser analisada tendo em conta o lugar que essa disposição ocupa no processo visto como um todo, a tramitação deste e as suas particularidades perante as várias instâncias nacionais.

Portanto, a aplicação prática do disposto no RGPD, a título de responsabilidade civil, deve levar em consideração a existência de uma norma interna que regule situação análoga e ainda, o exercício dos direitos conferidos pela norma europeia não pode ser obstado ou ter acesso dificultado por meio de mecanismos ou disposições nacionais.

Nesse sentido, o TJUE também é uníssono ao sustentar que a fixação da indenização deve ser adequada ao prejuízo que a vítima sofreu e ainda deverá ter o cunho de compensar os danos sofridos em sua integralidade[98]. Esta mesma conclusão pode ser auferida a partir da leitura do disposto no Considerando nº 146 do RGPD, no qual o legislador evidenciou que "Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido". Não poderíamos deixar de tratar da natureza dos danos, que pode ser dividida entre danos materiais (patrimonial) e imateriais (não patrimonial ou moral).

De acordo com os ensinamentos de Ana Mafalda Barbosa[99], uma sucinta distinção da natureza do dano reside no fato de que, o dano material pode ser avaliado em dinheiro, enquanto o imaterial não pode ser mensurado ou avaliado em quantia monetária.

Os danos materiais encontram previsão normativa no artigo 483º do CC, que evidencia que verifica-se a presença dos danos materiais em todas as situações em que, tudo o que for afetado pelo dano e pode ser trocado por dinheiro.

Enquanto os danos imateriais encontram subsídio legal nos artigos 70º e 496º, ambos do CC. Esta modalidade de ressarcimento não permite que os danos sofridos sejam trocados por dinheiro, porém podem ser avaliáveis em dinheiro.

No que diz respeito à natureza dos danos no âmbito da Proteção de dados é perfeitamente possível falar-se em dano material (patrimonial) e imaterial (moral), apesar de, a

---

[97] TRIBUNAL DE JUSTIÇA, Primeira Secção - **Acórdão do processo nº C-494/16**, de 07 de março de 2018.
[98] Conforme preleciona o Acórdão do TJUE nº C-46/93 e c-48/93 e ainda acerca da compensação à integralidade dos danos causados: acórdão do TJUE nº C-407/14.
[99] BARBOSA, *Op. Cit.*, p. 300.

primeira vista parecer mais fácil imaginar questões práticas que envolvem os danos imateriais, podemos tomar como exemplo o despedimento ou a não contratação de um trabalhador em virtude de uma informação ou dado obtido ou divulgado de forma ilícita.

Nomeadamente, a visualização da ocorrência do dano moral, em sede de responsabilização pela violação de dados é muito mais simples, pode-se levar em consideração a violação da intimidade da vida privada, a exposição não pretendida, a discriminação, dentre outros diretos da personalidade que podem vir a ser diretamente feridos.

Por fim, o nexo de causalidade é um requisito essencial para a imputação da responsabilização civil, principalmente quando se será diante de alguma violação do RGPD.

Da leitura do disposto no artigo 82º do aludido diploma legal, podemos verificar que apenas poderá haver responsabilização se entre a violação de dados e os danos produzido houver um nexo de causalidade. Tal conclusão pode ser alcançada a partir da leitura das expressões "devido a", "causados pelo" e ainda, "em virtude de", as quais evidenciam a necessidade de um nexo causal.

Para o autor Menezes Cordeiro[100], em que pese o Considerando nº 146 do RGPD apenas somente tratar do dano, o conceito a ser atribuído à causalidade também deve ser interpretado à luz da jurisprudência do Tribunal de Justiça, refletindo os objetivos primordiais do regulamento.

O TJUE no julgamento do processo C-557/12[101] ressaltou que, sem excluir as competências dos tribunais locais, evidencia a rejeição da necessidade de haver um nexo causal direito entre o dano e a violação ao RGPD.

Feita a análise acerca dos elementos constitutivos da responsabilidade civil cumpre-nos afunilar ainda mais o tema sob exame de moro a tratarmos da responsabilização aquiliana voltada aos casos que envolvem a violação de dados pessoais, bem como, tratando dos sujeitos que podem ser responsabilizados civilmente.

3.2.1.1 Os sujeitos envolvidos com o tratamento e a possibilidade de responsabilização civil aquiliana

A responsabilização civil ocorrida no âmbito da operação de tratamento de dados, que advém da violação do disposto no RGPD poderá ter seu surgimento a partir de um controle realizado de forma conjunta, paralela ou por meio da subcontratação.

[100] CORDEIRO, *Op. Cit.*, p. 387.
[101] TRIBUNAL DE JUSTIÇA, Quinta Secção – **Acórdão do processo nº C-557/12**, de 05 de junho de 2014.

Considerando o amplo leque de possibilidades de responsabilização nesta esfera, iremos desenvolver o presente trabalho de modo a levar em consideração diversas hipóteses de responsabilização. Todavia, devemos nos lembrar que, na prática, certamente, poderemos nos deparar com questões e casos hipotéticos completamente diferentes das que serão aqui abordadas, o que acarreta na necessidade de avaliação individual da casuística.

Conforme explicamos em momento posterior, o controle conjunto ocorre quando dois ou mais sujeitos realizam o tratamento de dados, de modo que compartilham a mesma finalidade e meios.

Havendo a violação de dados de um controle realizado em conjunto nos deparamos com a possível responsabilização de todos os envolvidos no tratamento, de forma solidária. Tal solução advém do disposto no artigo 82º, nº 2 do RGPD bem como do artigo 497º do CC. O que nos permite auferir que, um único tratamento de dados pode convergir em duas ou mais esferas de responsabilidade subjetiva.

A infinidade de possibilidades que podem acarretar na responsabilização dos envolvidos com o tratamento é enorme, inclusive, como verificamos anteriormente, podemos nos deparar com situações que envolvem mais de um responsável pelo tratamento em sede de controle paralelo.

Para melhor esclarecer o tema tratado, leva-se em consideração o seguinte caso hipotético: a empresa "X" faz a recolha de dados de seus clientes, em seguida partilha estes dados com a empresa "Y", de modo que os tratamentos realizados pelas empresas não possuem a mesma finalidade e meios.

A autora Mafalda Miranda Barbosa[102], ao analisar situação semelhante, nos ensina que cada uma das empresas deverá ser responsabilizada pelo dano que advir do tratamento realizado.

Todavia, conforme salientamos anteriormente, o tratamento de dados é extremamente amplo e envolve inúmeras operações, inclusive a partilha (transmissão) de dados ocorrida entre as duas empresas, integra o conceito de tratamento.

Portanto, se "X", qualidade de 1º responsável pelo tratamento, não assegura o cumprimento do disposto no RGPD pelo 2º responsável, ou seja, "Y" poderá ser alvo da responsabilização civil. Deve-se salientar que esta responsabilização pode ser afastada se levarmos em conta a ideia da confiança existente entre as partes[103].

---

[102] BARBOSA, Mafalda Miranda - **Data controllers e data processors**: da responsabilidade pelo tratamento de dados à responsabilidade civil, p. 454-457.
[103] *Idem*.

Ainda, deve ser levada em consideração da hipótese da empresa "y" se encontrar sediada em local fora da União Europeia, pelo que somente poderá se falar em tratamento dos dados se existirem garantias suficientes para cumprimento de um nível de proteção à tais dados que seja idêntica ao que o RGPD dispõe. Inclusive, é possível que se impute a responsabilidade solidária para "X", nos termos do artigo 82º, nº 4º do RGPD: "4.Quando mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam, nos termos dos n.os 2 e 3, responsáveis por eventuais danos causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados.".

Por outro lado, o artigo 82º, nº 1 do RGPD prevê a hipótese de isenção da responsabilização civil, que pode ser invocada pelo Responsável pelo Tratamento, eximindo-o da responsabilidade, desde que prove que em momento algum agiu de forma danosa, não sendo o responsável pela origem dos danos ocorridos.

Também devemos levar em consideração o caso hipotético posto acima, em que a empresa "Y", ao receber os dados fornecidos por "X", passa a assumir uma nova finalidade para os dados, passando a ser o 2º responsável. Este último, pode ser visto em relação à "X" como a figura de comissário, aplicando-se as regras de responsabilização disposta no artigo 500º do CC, que preleciona:

> Artigo 500.º
> 1. Aquele que encarrega outrem de qualquer comissão responde, independentemente de culpa, pelos danos que o comissário causar, desde que sobre este recaia também a obrigação de indemnizar.
> 2. A responsabilidade do comitente só existe se o facto danoso for praticado pelo comissário, ainda que intencionalmente ou contra as instruções daquele, no exercício da função que lhe foi confiada.
> 3. O comitente que satisfizer a indemnização tem o direito de exigir do comissário o reembolso de tudo quanto haja pago, excepto se houver também culpa da sua parte; neste caso será aplicável o disposto no n.º 2 do artigo 497.º

Trata-se da denominada responsabilidade pelo risco, na qual uma pessoa é obrigada a ressarcir outrem em virtude de um dano, independentemente de o ter originado, na qual estaremos diante de uma situação de responsabilidade objetiva.

Assim, para que "X" possa ser responsabilizado é indispensável que o ato tenha sido praticado no exercício das suas funções, atendendo-se aos pressupostos da responsabilidade e verificando-se a existência da relação de comissão entre ambos.

Quando se está diante da responsabilização pelo mencionado artigo do CC, é imperioso saber se realmente há uma efetiva ligação entre o comitente e o comissário, a existência de

danos causados pelo comissário, que os danos tenham ocorrido no exercício da função e ainda, se a atribuição as funções aumentaram o risco da lesão ou se ela teria ocorrido da mesma forma, ainda que não houvesse a comissão, que não passou de uma mera ocasião do aparecimento da violação.

Portanto, no caso hipotético, mesmo que "Y" tenha efetivamente violado as instruções de "X", elegendo uma nova finalidade para o tratamento de dados, não o poderia ter feito sem os meios disponibilizados pela empresa "X".

As questões acerca da responsabilidade civil do responsável pelo tratamento parecem menos complexas quando se trata da violação de dados ocasionada pelo subcontratante.

A contratação de um subcontratante que não apresente garantias suficientes de execução de medidas técnicas e organizativas necessárias, pode acarretar na responsabilização direta subjetiva do Responsável pelo tratamento.

O simples facto de o subcontratante demonstrar o cumprimento adequado do código de conduta ou comprovar que passou por um procedimento de certificação, podem ser utilizados como elementos que demonstram o cumprimento das obrigações por parte do responsável pelo tratamento. Também é possível se falar em responsabilidade civil objetiva, conforme explicitado anteriormente.

Diante de todo o exposto, pode-se concluir que no âmbito da aplicação do RGPD, existem inúmeras possibilidades de responsabilização na esfera civil, sendo que, cabe ao aplicador da norma avaliar a situação em concreto de forma cuidadosa, sempre levando em consideração que todo o dano deve ser reparado e ao mesmo tempo evitando a responsabilização indevida, sob pena de haver enriquecimento ilícito.

3.2.2 A responsabilidade civil obrigacional

É sabido que, no âmbito da proteção de dados, existem duas modalidades completamente distintas de responsabilização na esfera civil, as quais compreendem, a já estudada responsabilidade extracontratual e a responsabilidade contratual ou obrigacional, que será objeto de estudo do presente capítulo.

Como o próprio nome indica, a denominada responsabilidade contratual pressupõe a existência prévia de um contrato, portanto esta modalidade de responsabilização apenas se verifica no âmbito da proteção de dados quando o tratamento realizado tenha fundamento em uma base negocial.

Ainda que o contrato firmado entre as partes não tenha o objetivo direto de conferir proteção aos dados pessoais, o princípio da boa-fé contratual pode impor deveres de cuidado que podem acarretar na responsabilização na esfera civil[104].

A responsabilização contratual no âmbito do controle conjunto não oferece grandes obstáculos. Uma vez que, por se tratar de um contrato celebrado por mais de um sujeito, cada um dos contratantes pode ser alvo de uma futura responsabilização, na medida em que incorre em culpa.

No âmbito do controle conjunto, ou seja, um contrato que é celebrado por mais de um sujeito. Parece-nos que tal situação é relativamente simples, na medida em que cada um dos contratantes poderá ser alvo da responsabilização civil, na medida em que tiverem contribuído com culpa para a ocorrência do evento danoso.

Todavia, a questão da responsabilização contratual pode ser mais complexa se levarmos em consideração os casos que há controle paralelos dos dados, relação na qual, de acordo com Mafalda Miranda Barbosa[105] é necessário analisar tal situação sob o aspecto do artigo 800º do CC, o qual preleciona "O devedor é responsável perante o credor pelos actos dos seus representantes legais ou das pessoas que utilize para o cumprimento da obrigação, como se tais actos fossem praticados pelo próprio devedor.".

Portanto, o responsável pelo tratamento que se utiliza de um terceiro para auxiliar na atividade de tratamento de dados, irá responder pelos atos dos auxiliares como se tais atos houvessem sido praticados por si mesmo.

A estrutura normativa do artigo 800º do CC não pode ser confundida com o já estudado artigo 500º da mesma lei. Neste primeiro, desaparece a dupla imputação, na medida em que o devedor responde pelos atos dos auxiliares que utilizar para cumprimento da obrigação, como se os atos realizados fossem apenas seus.

Ao tratar do tema, o autor Carneiro da Frada também realiza tal diferenciação, ressaltando que a há distinção na técnica da norma: "O que ela faz é projetar logo a conduta do auxiliar na pessoa do devedor para verificar se desse modo o devedor incorreria ou não em responsabilidade" [106].

A inaplicabilidade do disposto no artigo 500º do CC, nos casos que envolvem a responsabilidade civil obrigacional, também se justifica pelo fato de que, quando estamos

[104] BARBOSA, *Op. Cit.*, p. 462.
[105] BARBOSA, *Op. Cit.*, p. 464.
[106] FRADA, Manuel A. Carneiro da - **A responsabilidade objectiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana**, p. 301.

diante da realização de um contrato há uma ideia de que se estabelece uma espécie de confiança entre as partes contratantes, independentemente da culpa pelos danos que podem decorrer da contratação. Portanto, o contratante encontra-se em uma posição que o coloca como responsável diante da ocorrência do incumprimento contratual.

Enquanto que, no artigo 800º do CC, se reconhece que o devedor não pode deixar de ser responsável pelo incumprimento da obrigação simplesmente porque se utilizou de terceiros que prestaram auxílio à este primeiro para o cumprimento da obrigação.

Para melhor compreensão, tomamos os exemplos de Mafalda Miranda Barbosa[107], que sustenta a existência de duas situações semelhantes, mas que se distinguem em ralação à aplicabilidade do artigo 800º do CC.

É evidente que o artigo 800º do CC não tem a intenção de alargar o âmbito de responsabilização do devedor, mas sim, de fazer com que o devedor responda civilmente como se ele mesmo estivesse atuando. Ou seja, irá ser responsabilizado independentemente da ideia de culpa em virtude da ideia da confiança contratual estabelecida entre os contratantes.

Da leitura do disposto no artigo 800º do CC podemos vislumbrar que a pretensão indenizatória pela violação do aludido dispositivo legal deverá observar quatro requisitos: a existência de uma obrigação, a existência de uma relação entre o devedor e o terceiro que será utilizado para cumprimento da obrigação, a efetiva atuação do terceiro no cumprimento da obrigação e por fim, a atuação do auxiliar.

Inclusive, de acordo com Mafalda Miranda Barbosa[108] o posicionamento adotado por grande parte da doutrina vai de encontro à necessidade de preenchimento de tais requisitos, sustentando que o devedor apenas pode ser responsabilizado pelos atos que são praticados no âmbito do cumprimento da obrigação.

Por este motivo, o problema central da questão colocada não diz respeito à ocorrência da violação dos deveres de prestação, mas sim, diante da ocorrência da violação dos deveres de conduta e deveres acessórios.

Nesse aspecto, levanta-se também o questionamento se o pressuposto da culpa deve ser entendido sob esta luz, de modo que, se a responsabilidade do terceiro é vista como a responsabilidade do próprio devedor, então se excluída a responsabilidade do primeiro, consequentemente não há que se falar na responsabilidade do segundo.

Portanto, a responsabilização do devedor no âmbito do artigo 800º do CC será demarcada no âmbito da obrigação que é previamente assumida pelo devedor, sendo

[107] BARBOSA, *Op. Cit.*, p. 466-467.
[108] BARBOSA, *Op. Cit.*, p. 470-471.

imprescindível que se trate de uma obrigação em sentido técnico. Portanto, a existência da responsabilidade contratual pela violação de dados, apenas será viável quando a legitimação para a realização do tratamento de dados seja negocial.

Neste âmbito pode-se falar na responsabilização do responsável pelo tratamento pelos atos praticados pelos subcontratantes, porém não se garante a responsabilização do contratante. Todavia, poder-se-á falar em responsabilização contratual, quando se estiver diante de um contrato celebrado entre o responsável pelo tratamento e o subcontratante, com eficácia de proteção para terceiros.

Inclusive, o artigo 28º do RGPD dispõe que "o tratamento em subcontratação é regulado por contrato ou ato normativo ao abrigo do direito da União ou dos Estados Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoas e as categorias dos titulares de dados, e as obrigações e direitos do responsável pelo tratamento".

3.2.3 A responsabilidade contratual e extracontratual e o concurso

Existem duas modalidades distintas de responsabilização civil, que compreendem a responsabilidade aquiliana, a qual advém do incumprimento de uma disposição legal e a responsabilidade obrigacional que tem como fundamento um contrato, que restou violado.

Assim, importa saber qual dos regimes deve ser aplicado nos casos em que uma única situação acarreta no dano que gera possibilidade de haver a responsabilização aquiliana e obrigacional ao mesmo tempo.

A distinção entre estes dois tipos de responsabilidade civil é essencial para responder ao questionamento acima. Assim, a responsabilidade aquiliana, encontra previsão normativa no artigo 483º e seguintes do CC, e surge como uma consequência da violação direitos absolutos.

Enquanto que a responsabilidade obrigacional possui campo normativo completamente diferente, prevista nos artigos 798º e seguintes do CC, e pressupõe a existência de uma relação contratual, se apresentando como uma consequência da violação de um dever que advém de tal relação.

Conforme restou exposto anteriormente, tal diferenciação permite a existência de situações em que se verifica o concurso destas modalidades. Casos estes que não exigem o concurso de ações, ou seja, uma única ação que poderá incorrer na responsabilidade contratual e extracontratual.

Os ensinamentos de, Rui de Alarcão[109] corroboram com o entendimento acima exarado, na medida em que sustenta que "o mesmo facto humano pode provocar um dano simultaneamente contratual e extracontratual". Ou seja, o mesmo fato pode representar tanto uma violação de um contrato como um fato ilícito, no mesmo momento.

O Tribunal da Relação do Porto[110], por meio de Acórdão tratou do tema sob estudo, ressaltando que, nos casos em que se verifica a dupla responsabilização, o lesado se depara com duas situações distintas no que diz respeito ao ingresso de ação de responsabilidade.

A primeira situação permite que o lesado intente uma única ação, socorrendo-se das normas de responsabilidade contratual e extracontratual, enquanto que, a segunda admite o ajuizamento de ações autônomas.

Em continuidade, o aludido Acórdão preleciona que aos adeptos da teoria da existência de concurso destas duas modalidades de responsabilização civil, é possível configurar o concurso como de ações ou de normas.

Ao aceitar-se a existência de um concurso de ações, a causa de pedir será, de um lado, o contrato e de outro o dever jurídico de não lesar outrem. Quando se tratar de uma única ação deverá haver um concurso de pretensões, compostas pelo dever contratual e pelo dever de não causar ofensas aos bens e direitos alheios, como obrigações jurídicas independentes colocados conjuntamente, "não sendo proibido ao autor invocar em grau posterior do processo, uma norma diversa da que alegara"[111].

O Tribunal da Relação de Lisboa[112] também tratou de analisar questão semelhante, na ocasião, sustentou que quando um único fato vem a causar danos de naturezas diversas, não se pode considerar a existência de distintas pretensões, ou seja, haverá apenas uma pretensão, que é o dano, sendo que a qualificação delitual ou contratual não tem o poder de alterar a identidade do pedido.

Todavia, Superior Tribunal de Justiça apresentou um posicionamento completamente distinto, ao se deparar com situação semelhante[113], em que há a ocorrência de um dano decorrente uma única ação, o qual acarreta no incumprimento de uma relação obrigacional

[109] ALARCÃO, Rui de - **Direito das Obrigações**, p. 210.
[110] TRIBUNAL da Relação do Porto - **Acórdão do processo nº 274/17.8TAVR.P1**, de 08 de fevereiro de 2021. Relatora Eugénia Cunha.
[111] *Idem*.
[112] TRIBUNAL da Relação de Lisboa - **Acórdão do processo nº 512/10.8TCFUN.L1-2**, de 27 de setembro de 2012. Relatora Teresa Albuquerque.
[113] SUPREMO Tribunal de Justiça, primeira Secção - **Acórdão do processo nº 4444/03.8TBVIS.C1.S1**, de 07 de fevereiro de 2017. Relator: Helder Roque.

previamente estipulada (contrato) e também acarreta no incumprimento da observância de uma norma de dever de cuidado e proteção.

Para o STJ, para além do dever de cumprimento das obrigações contratuais, existem, na relação contratual, determinados deveres acessórios de conduta, de cuidado e de prestação, independentemente da existência de direitos primários. Assim, deve-se alargar a esfera da responsabilidade contratual em relação à aquiliana, uma vez que se entende que o dever genérico é absorvido sempre que se está em causa comportamentos que se ligam com o objetivo contratual, devendo-se falar em concurso aparente entre as duas modalidades de responsabilidade.

Diante da situação de coexistência de dois tipos de responsabilidades distintas, em virtude da ocorrência de um único fato que provoque um dano que possibilite ao lesado a tutela contratual e de um fato ilícito no âmbito extracontratual, não haverá cumulação de responsabilidade, quando esta acarretar na duplicidade da indenização.

Ainda, de acordo com a decisão supracitada, há uma situação completamente distinta quando um mesmo fato danoso, acarrete na possibilidade de responsabilização contratual em relação à uma determinada pessoa que firmou o contrato e na responsabilidade extracontratual de terceiro alheio ao ato negocial. Na medida em que verifica que, no caso narrado, há um concurso real entre a responsabilidade aquiliana e obrigacional.

Por fim, o STJ sustenta que havendo apenas um dano, que é resultado de um único fato e uma só conduta, com amparo em dois regimes legais de proteção ao lesado, os quais tem como objetivo a reparação de danos, porém cada regime possui sua própria teologia, não há justificativa que sustente a concorrência de pretensões.

Assim, diante da existência de tal concurso, há uma diversificação de pedidos que dependem da mesma situação factual, estando-se diante de um pedido de indenização com duplo fundamento, em que case ao lesado optar pelo regime que se mostrar mais favorável às suas pretensões.

Recentemente o Tribunal da Relação de Lisboa[114], exarou decisão que vai de encontro ao dito acima, na medida em que ressaltou que o concurso entre a responsabilidade contratual e extracontratual é aparente, na medida em que, verificando-se a ocorrência de apenas um dano, que é resultado de um único fato, a duplicidade de ações ou a concorrência da pretensão não se justificam, não havendo que se falar no sistema de cúmulo.

[114] TRIBUNAL da Relação de Lisboa - **Acórdão do processo nº 9773/16.8T8LSB.L1-7**, de 24 de setembro de 2019. Relator José Capacete.

O acórdão reconhece a omissão legislativa existente quanto à matéria e, sustenta que o lesado deverá procurar a solução mais adequada para a solução deste impasse, sempre levando em consideração os valores e interesses contrapostos. Ressaltando que, o CC confere maior proteção jurídica ao lesado quando se está diante da responsabilidade contratual.

O Acórdão justifica tal afirmação, sustentando que se houverem danos em decorrência de um vínculo negocial, o pedido de indenização deverá ser pautado nas regras de responsabilidade contratual. A mesma solução impere nos casos em que o fato que acarreta na violação do negócio simultaneamente preenche os requisitos da ação extracontratual.

Portanto, atualmente, não há legislação que regule as situações em que um único evento danos pode acarretar na responsabilização pela via contratual e extracontratual. O que acarreta na existência de decisões e posicionamentos completamente antagônicos sobre a solução do impasse, na medida em que, há quem defenda o sistema do cúmulo, sob o pretexto de que se tratam de pretensões completamente distintas e que não se confundem, não havendo que se falar na existência de concurso de normas.

Enquanto que, há quem sustente a existência de um concurso aparente de normas, uma vez que há apenas um dano, não havendo que se falar na aplicação cumulativa das duas modalidades de responsabilidade em uma única situação.

3.3 O ALCANCE DA RESPONSABILIDADE CIVIL PELA VIOLAÇÃO DE DADOS RELATIVOS À SAÚDE

Os estudos anteriormente realizados acerca dos dados relativos à saúde permitiram a identificação do atual conceito que é atribuído a estes dados, levando-se em consideração o seu desenvolvimento histórico e social, permitindo a visualização de todas as nunces que encontram-se diretamente ligadas ao procedimento de tratamento e segurança de dados e a sua representatividade para a sociedade atual.

Ao passo que, a pesquisa desenvolvida acerca da responsabilização civil em virtude da ocorrência da violação de dados pessoais à luz do RGPD evidenciou a existência de diferentes hipóteses de responsabilização dos envolvidos com o tratamento de dados.

Nesse sentido, é imperioso tratar do alcance e limites existentes no âmbito desta responsabilização civil, sobretudo no que diz respeito à violação dos dados relativos à saúde, permitindo a compreensão dos limites existentes nas situações em que se verifica a necessidade de responsabilização civil.

Conforme salientamos anteriormente, tanto a Constituição da República portuguesa como o direito positivo Europeu e de inúmeros países, reconhecem a proteção à saúde como um direito fundamental.

Tal reconhecimento advém da essencialidade que este direito-dever apresenta para o desenvolvimento e aprimoramento social, portanto é indispensável que o Estado garanta o direito e acesso à saúde para todos os indivíduos que compõem a sociedade, sem qualquer tipo de discriminação ou seletividade.

Na medida em que a efetivação deste direito poderá se dar por meio de diversas vias, sejam elas de cunho público ou particular por meio de instituições que prestam serviços de cuidados à saúde, profissionais da saúde, laboratórios, aplicativos e *softwares* que se destinam a armazenar dados para acompanhamento da saúde e do bem-estar, dentre outros meios de coleta e tratamento de dados.

Nesse sentido, não se pode deixar de levar em consideração que o desenvolvimento tecnológico pode ser visualizado como um fator contributivo para o desenvolvimento e aprimoramento das ferramentas da saúde, garantindo a expansão deste direito e facilitando o seu desenvolvimento diário.

É notório que tal avanço tecnológico é um contributo para o desenvolvimento da saúde humana, todavia há uma questão que também sofreu um grande desenvolvimento e que merece especial atenção, tal questão se trata dos dados pessoais relativos à saúde.

A coleta e tratamento deste tipo de dado é essencial para o desenvolvimento da grande maioria das atividades de cuidados à saúde, as quais permitem que, por meio da disponibilização de tais informações, o profissional da área da saúde possa analisar as especificidades colocadas por seus pacientes e, com base nas informações e dados coletados, possam desenvolver suas atividades profissionais com maestria.

A coleta, tratamento e armazenamento de tais dados também permitem o acompanhamento do histórico de saúde de seu titular e pode estar diretamente ligado com a qualidade de vida e bem-estar buscada pelo seu titular, por exemplo, nos casos que o indivíduo se utiliza de um aplicativo, *software* ou sistema computacional que acompanha o consumo e gasto de calorias diárias ou a oscilação dos batimentos cardíacos.

Portanto, pode-se afirmar que recolha e o tratamento de dados se encontram diretamente ligadas ao desenvolvimento da grande maioria de atividades relacionadas aos cuidados de saúde, estando cada vez mais presente e enraizado na atual sociedade.

Todavia, esta facilidade na recolha, tratamento e conservação destes dados devem ser vistos com cuidado, sobretudo no âmbito jurídico, uma vez que tais informações dizem respeito

á questões extremamente íntimas de seus titulares, encontrando importantes limites na esfera do direito da reserva da vida privada.

Evidente que tal preocupação se tronou cada vez mais intensa, principalmente nos últimos anos, em que houve um maior desenvolvimento tecnológico e social, o qual permitiu que a recolha e o compartilhamento de informações e dados se tronassem cada vez mais rápidas, fáceis e acessíveis.

Na medida em que, a coleta de dados relativos à saúde deixou de ser realizada apenas em locais onde se prestam serviços relacionados com a saúde, ampliando-se de uma forma exponencial diante da criação de incontáveis aplicativos, sistemas e dispositivos que registram tais informações, como por exemplo, um aplicativo que controla os batimentos cardíacos que pode ser conectado a um relógio de pulso e ao celular ou aos aplicativos que tem o objetivo de acompanhar o ciclo menstrual ou o desenvolvimento gestacional.

Diante disso, a realização das operações de tratamento dos dados relativos à saúde devem sempre observar as normas e princípios legais que os regulam, a qual apenas é possível se verificar-se que o tratamento é uma condição necessária e acessória para o desenvolvimento de atividades de cuidados com a saúde.

Assim, existem diversas normas que tutelam e reconhecem a necessidade de haver a preservação da esfera íntima dos indivíduos, sobretudo quando se esta diante de dados que se disponibilizados de uma forma que permita a identificação do seu titular são capazes de causar imensa dor, desconforto, sofrimento e até mesmo colocar sue titular em situações discriminatórias.

As informações relativas à saúde podem dizer respeito à uma série de acontecimentos da vida civil do indivíduo e, justamente por este motivo, é que o legislador optou pela criação de normas que conferissem maios amparo jurídico no âmbito do tratamento de tais dados.

Diante da significância que os dados relativos à saúde apresentam, o seu tratamento deve seguir um regime especial, que se encontra consagrado no artigo 9º do RGPD. Este regime especial apresenta um agravamento dos requisitos legais para o tratamento destes dados, se o compararmos com o regime comum.

Em regra, o artigo supracitado proíbe o tratamento de dados relativos à saúde, elencando em seu nº 2, uma série de situações em que o referido tratamento passa a ser permitido. Tal proibição advém da justificativa da importância que estes dados apresentam para o seu titular, sobretudo para a reserva de sua intimidade e vida privada.

A primeira exceção legal permite a realização do tratamento de tais dados desde que haja o consentimento expresso do seu titular, verifica-se aqui a presença latente do direito à

autodeterminação informacional. Na medida em que, parte-se do prossuposto de que o titular dos dados deve ter pleno conhecimento e ciência de quais dados relativos à sua saúde são objetos de tratamento e a finalidade utilizada como meio justificador, caso contrário, não poderá se falar em tratamento.

Todavia, há possibilidade de ocorrer o afastamento da necessidade do consentimento expresso do titular, nos casos em que houver a criação de uma norma pela União ou Estados-Membros que afastem o direito do titular de dados a autorizar o tratamento de seus próprios dados. Apesar de que, atualmente, não existem normas que permitam tal afastamento, nem no direito interno de Portugal, nem no direito da União Europeia.

O tratamento de dados sensíveis também é permitido nos casos em que estes se mostrem necessários para o cumprimento de obrigações e do exercício de direitos que dizem respeito às obrigações laborais, ou seja, situações diretamente relacionadas com a legislação laboral, segurança social e de proteção social.

Portanto, para aplicação desta exceção devem estar presentes dois requisitos distintos. Na medida em que, o primeiro corresponde a existência de um suporte legal e, o segundo diz respeito à necessidade de haver uma relação direta entre o cumprimento das obrigações ou o exercício de um direito e o tratamento de dados.

O tratamento destes dados apenas será considerado necessário se não houver qualquer outro meio hábil que possibilite o exercício do direito ou cumprimento da obrigação por outra forma que não se encontre diretamente ligada à esfera privada do titular dos dados.

Também pode-se falar em tratamento dos dados sensíveis nos casos em que este se mostrar necessário para proteger os interesses vitais do seu titular ou de terceiro, nos casos em que o titular de dados se encontra incapacitado de exteriorizar seu consentimento expresso.

A aplicação desta exceção pode ser visualizada, por exemplo, nos casos em que a vida ou a integridade física estejam em perigo e a realização do tratamento de dados se faz necessária para evitar a ocorrência de eventos gravosos.

Assim, este requisito abarca todos os casos em que não é possível obter o consentimento do seu titular como, por exemplo, nos casos que o titular se encontra acometido por doença grave, tenha sofrido algum tipo de acidente ou até mesmo, nos casos de desaparecimento. Sendo que, na prática deve-se sempre buscar e considerar a possibilidade de haver um representante legal do titular de dados, que possa suprir a ausência de consentimento.

A quarta situação que permite o tratamento dos dados sensíveis diz respeito ao exercício da atividade de tratamento por fundações, associações ou outro organismo que não tenha fins lucrativos e que tenha objetivos filosóficos, políticos, sindicais ou religiosos.

Neste âmbito, o tratamento poderá ser realizado desde que seja realizado com observância e respeito ao exercício das atividades legítimas da entidade. Os dados devem pertencer aos seus membros, antigos membros ou aos terceiros que tenham contato direto com a entidade, não estão abrangidos os dados que dizem respeito às demais pessoais que podem ser visualizadas como terceiros no processo, como por exemplo, os fornecedores ou entidades comerciais[115]. Sendo que, em momento algum estes dados podem ser disponibilizados á terceiros sem o consentimento de seus titulares.

Também é possível se falar no tratamento de dados sensíveis que tenham se tornados públicos pelo seu próprio titular, ou seja, o titular dos dados que por sua livre e espontânea vontade opta por tornar público seus dados. Portanto, evidente que a justificativa existente por trás desta exceção consiste no fato de que o próprio titular reconhece que o tratamento destes dados não o incomoda ou prejudica.

O mesmo ocorre com os dados que se mostrarem necessários para a declaração ou defesa e um direito no âmbito judicial ou no âmbito do exercício das funções de um tribunal. Portanto, poderá haver tratamento dos dados quando se está diante da cooperação, desenvolvimento e administração da justiça.

Há também a exceção do tratamento de dados sensíveis para satisfazer os interesses públicos importantes, desde que, haja previsão expressa no Direito da União ou dos Estados Membros. O tratamento deverá ser proporcional ao interesse público e ainda, devem haver medidas específicas e adequadas que salvaguardem os interesses e os direitos fundamentais dos titulares.

Nesse aspecto, salientamos que o RGPD em momento algum atribui um conceito à palavra ‘importante’, causando diversos questionamentos acerca do alcance da norma. Para o autor Menezes Cordeiro[116], a inclusão deste adjetivo evidencia a natureza peculiar dos dados sensíveis, bem como os riscos inerentes ao seu tratamento. Na medida em que, não basta sustentar que o tratamento é necessário para a garantia do interesse público, dever-se-á comprovar tal importância por meios quantitativos e qualitativos como, por exemplo, o número de indivíduos beneficiados e as consequências que o não tratamento pode acarretar.

A alínea ‘h’ do artigo 9º do RGPD apresenta a exceção que julgamos muito importante para a persecução do presente estudo, sob o qual se justifica o tratamento realizado no âmbito da medicina preventiva ou do trabalho, com o objetivo de avaliar a capacidade de trabalho, a

[115] CORDEIRO, *Op. Cit.*, p. 245.
[116] CORDEIRO, *Op. Cit.*, p. 248.

realização do diagnóstico médico, a prestação de serviços de cuidados da saúde ou de seu tratamento e ainda, a gestão de serviços e sistemas de saúde ou de ação social.

Nesse contexto, o tratamento destes dados podem se fundar no direito da União ou dos Estados-Membros, quando da criação de normas que assim o reconheçam ou em virtude da existência de uma relação jurídica existente com o profissional da saúde, o qual encontra-se obrigado á observar o dever de sigilo.

No âmbito da saúde pública, é permitido o tratamento dos dados sensíveis sempre que este se mostre necessário e haja previsão expressa no âmbito do direito da União-Europeia ou dos Estados-Membros.

Esta exceção distingue-se da anteriormente tratada na medida em que a primeira diz respeito a proteção de interesses individuais, na medida em que a presente exceção trata de interesses coletivos.

Para compreensão do alcance deste dispositivo legal, é importante levarmos em consideração o conceito de saúde pública à Luz do artigo 3º, 1, c) do Regulamento nº 1338/2008 de 16 de dezembro: "Todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidade de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade.".

Assim, quaisquer elementos acima enunciados podem servir como causa justificadora do tratamento dos dados relativos à saúde, desde que, tal tratamento seja motivado pela persecução do interesse público, não bastando a persecução do interesse individual como meio justificador.

Por fim, a última hipótese do RGPD que permite o tratamento de dados sensíveis diz respeito as informações de arquivo que demonstrem interesse público, com o objetivo de investigação histórica, científica e fins estatísticos.

Neste caso, o tratamento apenas poderá ocorrer se houver previsão normativa - no âmbito do direito da União ou dos Estados-Membros - que assim permita. Ainda, o tratamento deve se mostrar proporcional aos interesses visados e observar o respeito à autodeterminação informacional dos seus titulares e, estar abarcado por medidas que salvaguardem os direitos e interesses dos titulares.

Portanto, no âmbito do RGPD, a regra é a de que não pode haver o tratamento dos dados relativos à saúde, com exceção dos requisitos acima estudados, que justificam a realização do seu tratamento e o legitimam.

Todavia, as regras e condições especiais para realização do tratamento dos dados relativos à saúde não se esgotam apenas no âmbito do RGPD. Diante da necessidade de haver uma especial regulamentação interna sobre o tema, Portugal estabeleceu no artigo 29º da Lei nº 58/2019 uma série de requisitos internos que legitimam e que devem ser observados quando se está diante do tratamento de dados relativos à saúde e dados genéticos.

O nº 1º da lei interna supracitada sustenta que, o acesso aos dados pessoais da saúde "rege-se pelo princípio da necessidade de conhecer a informação.". O autor Menezes Cordeiro[117] nos ensina que o disposto na norma é um reflexo do princípio do *need to know*, em que todos aqueles que auxiliam os responsáveis pelo tratamento ou o subcontratante apenas podem ter acesso aos dados pessoais relativos à saúde se necessário para o desenvolvimento de suas funções, o que pode ser visto como uma medida que busca implementar maior segurança aos dados.

Em continuidade, o nº 2 do mesmo dispositivo legal preleciona que o tratamento de dados realizado por motivos de interesse público no âmbito da saúde pública e realizado no âmbito da medicina preventiva ou do trabalho, dever ser realizado por um profissional que se encontre "obrigado a sigilo ou por outra pessoa sujeita a dever de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação.".

Sendo que, o acesso aos tais dados deve ser feito exclusivamente de forma eletrónica, havendo exceção à regra nos casos em que se verifica a impossibilidade técnica ou há expressa indicação do titular de dados, sendo completamente proibia a divulgação ou transmissão posterior dos dados.

Igualmente, os artigos 4º e 5º do diploma legal acima mencionado, também tratam do dever de sigilo, que pode ser dividido em três grandes grupos, os quais consistem em: estudantes e investigadores da área da saúde e genética; os trabalhadores, prestadores de serviços e encarregados da proteção de dados e responsáveis que tratam do tratamento de dados genéticos e relativos à saúde e, por fim, "os titulares de órgãos e trabalhadores" que no âmbito do acompanhamento, fiscalização ou financiamento da atividades de prestação de cuidados da saúde, tenham acesso aos dados de saúde.

Nesse sentido, salientamos a ponderação realizada por Menezes Cordeiro, o qual sustenta que o disposto nestes artigos não pode ser visualizado como "uma porta aberta ao tratamento de dados"[118], mas deverá ser visto como uma imposição do dever de sigilo e confidencialidade de todas as classes de sujeitos enumeradas.

[117] CORDEIRO, *Op. Cit.*, p. 253.
[118] CORDEIRO, *Op. Cit.*, p. 254.

Por fim, o aludido artigo 29º determina a criação de portarias que estabeleçam os requisitos de segurança mínimos para o tratamento dos dados relativos à saúde, os quais deveriam tratar da permissão de acesso, autenticação précia e o registro eletrónico dos dados. Todavia, até o presente momento, não houve a edição de qualquer portaria neste sentido, carecendo de norma complementar neste sinto.

Em que pese a inexistência de portarias que venham a regular a matéria, este preceito deve ser conjugado com a obrigação que o responsável pelo tratamento e o subcontratante possuem de adotar e implementar medidas organizativas e técnicas que objetivem assegurar a segurança dos dados em virtude do risco que tais dados apresentam.

Portanto, é evidente que tanto a União-Europeia como as normas internas do direito português reconhecem a necessidade de aplicação de um regime específico para o tratamento dos dados relativos à saúde, em virtude da significância que a natureza destes dados apresentam para com a esfera individual e privada de seus titulares.

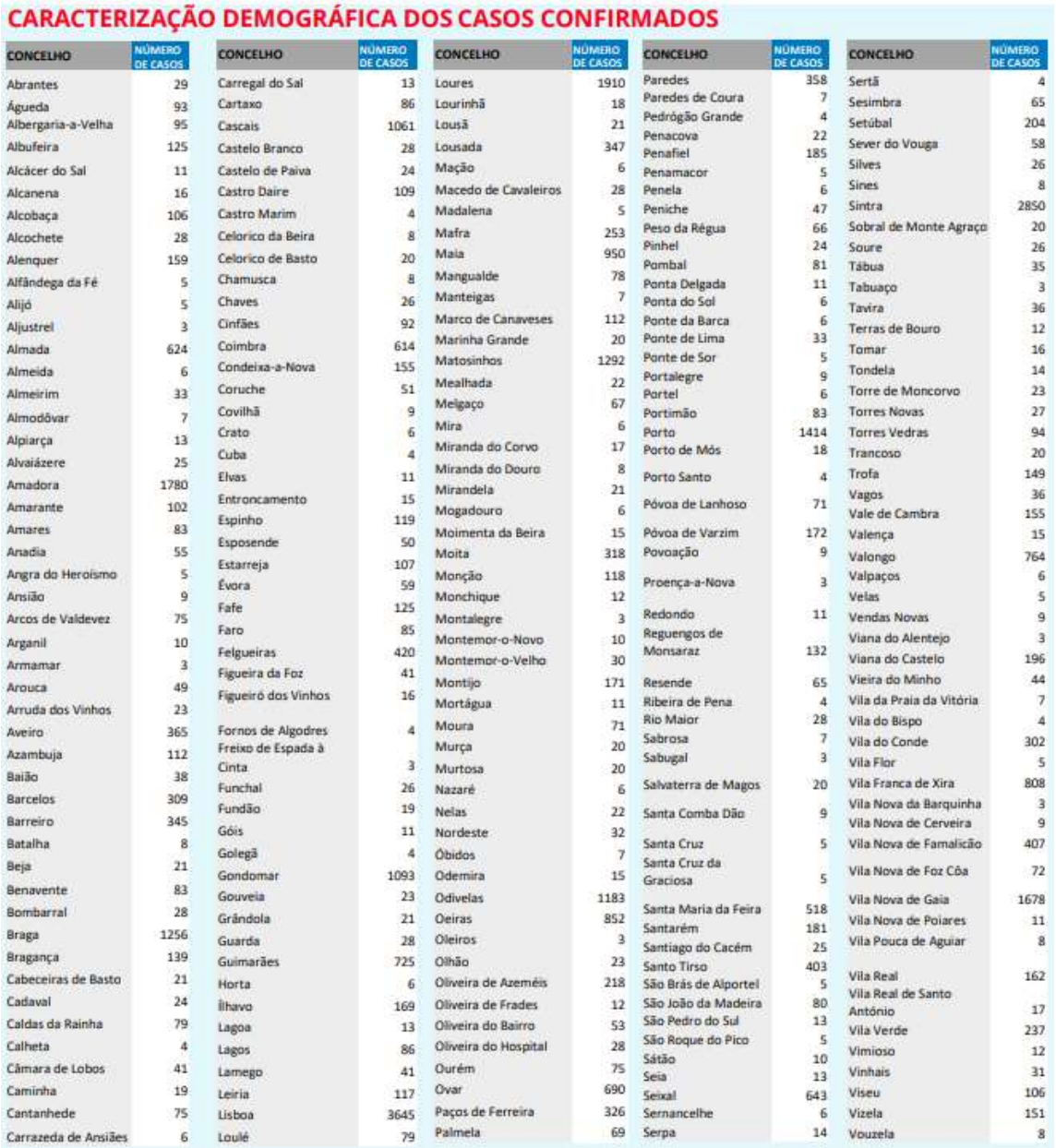
Ainda no âmbito da possibilidade de ocorrência de violação de dados relativos à saúde, é de suma importância para o desenvolvimento do presente trabalho e compreensão prática do desenvolvimento do tema, considerar o posicionamento da CNPD emitido em 22 de abril de 2020[119], o qual sugere orientações acerca do tratamento e da divulgação de dados de saúde.

A breve análise das orientações emitidas pela CNPD permite a compreensão de uma das formas em que pode se verificar a ocorrência da violação de dados relativos à saúde na vida prática e cotidiana, evidenciando a linha tênue que separa o tratamento realizado em conformidade com as normas de proteção de dados e o tratamento que acarreta na violação de tais normas, acarretando em enormes danos aos seus titulares.

Em virtude da pandemia no setor da saúde mundial que decorreu da propagação do Covid-19, a Autoridade Nacional de Saúde e a Direção-Geral de Saúde (DGS) passaram a emitir informações públicas, destinadas à toda a sociedade, que dizem respeito ao número total nacional de casos suspeitos, confirmados, óbitos e recuperados, e ainda, a distribuição regional do número de óbitos. Sendo que, no sítio da DGS era possível se obter a informação do número de óbitos e infectados por concelho, conforme pode-se observar a partir da imagem abaixo[120]:

[119] COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS - **Orientações: Sobre divulgação de informação relativa a infetados por Covid-19**.

[120] DGS, Novo Coronavírus, Covid-19, **Relatório de situação nº 124 de 04/07/2022**. Disponível em: https://covid19.min-saude.pt/relatorio-de-situacao/>.



CARACTERIZAÇÃO DEMOGRÁFICA DOS CASOS CONFIRMADOS

CONCELHO	NÚMERO DE CASOS
Abrantes	29
Águeda	93
Albergaria-a-Velha	95
Albufeira	125
Alcácer do Sal	11
Alcanena	16
Alcobaça	106
Alcochete	28
Alenquer	159
Alfândega da Fé	5
Alijó	5
Aljustrel	3
Almada	624
Almeida	6
Almeirim	33
Almodôvar	7
Alpiarça	13
Alvaiázere	25
Amadora	1780
Amarante	102
Amares	83
Anadia	55
Angra do Heroísmo	5
Ansião	9
Arcos de Valdevez	75
Arganil	10
Armamar	3
Arouca	49
Arruda dos Vinhos	23
Aveiro	365
Azambuja	112
Baião	38
Barcelos	309
Barreiro	345
Batalha	8
Beja	21
Benavente	83
Bombarral	28
Braga	1256
Bragança	139
Cabeceiras de Basto	21
Cadaval	24
Caldas da Rainha	79
Calheta	4
Câmara de Lobos	41
Caminha	19
Cantanhede	75
Carrazeda de Ansiães	6
Carregal do Sal	13
Cartaxo	86
Cascais	1061
Castelo Branco	28
Castelo de Paiva	24
Castro Daire	109
Castro Marim	4
Celorico da Beira	8
Celorico de Basto	20
Chamusca	8
Chaves	26
Cinfães	92
Coimbra	614
Condeixa-a-Nova	155
Coruche	51
Covilhã	9
Crato	6
Cuba	4
Elvas	11
Entroncamento	15
Espinho	119
Esposende	50
Estarreja	107
Évora	59
Fafe	125
Faro	85
Felgueiras	420
Figueira da Foz	41
Figueiró dos Vinhos	16
Fornos de Algodres	4
Freixo de Espada à Cinta	3
Funchal	26
Fundão	19
Góis	11
Golegã	4
Gondomar	1093
Gouveia	23
Grândola	21
Guarda	28
Guimarães	725
Horta	6
Ílhavo	169
Lagoa	13
Lagos	86
Lamego	41
Leiria	117
Lisboa	3645
Loulé	79
Loures	1910
Lourinhã	18
Lousã	21
Lousada	347
Mação	6
Macedo de Cavaleiros	28
Madalena	5
Mafra	253
Maia	950
Mangualde	78
Manteigas	7
Marco de Canaveses	112
Marinha Grande	20
Matosinhos	1292
Mealhada	22
Melgaço	67
Mira	6
Miranda do Corvo	17
Miranda do Douro	8
Mirandela	21
Mogadouro	6
Moimenta da Beira	15
Moita	318
Monção	118
Monchique	12
Montalegre	3
Montemor-o-Novo	10
Montemor-o-Velho	30
Montijo	171
Mortágua	11
Moura	71
Murça	20
Murtosa	20
Nazaré	6
Nelas	22
Nordeste	32
Óbidos	7
Odemira	15
Odivelas	1183
Oeiras	852
Oleiros	3
Olhão	23
Oliveira de Azeméis	218
Oliveira de Frades	12
Oliveira do Bairro	53
Oliveira do Hospital	28
Ourém	75
Ovar	690
Paços de Ferreira	326
Palmela	69
Paredes	358
Paredes de Coura	7
Pedrógão Grande	4
Penacova	22
Penafiel	185
Penamacor	5
Penela	6
Peniche	47
Peso da Régua	66
Pinhel	24
Pombal	81
Ponta Delgada	11
Ponta do Sol	6
Ponte da Barca	6
Ponte de Lima	33
Ponte de Sor	5
Portalegre	9
Portel	6
Portimão	83
Porto	1414
Porto de Mós	18
Porto Santo	4
Póvoa de Lanhoso	71
Póvoa de Varzim	172
Povoação	9
Proença-a-Nova	3
Redondo	11
Reguengos de Monsaraz	132
Resende	65
Ribeira de Pena	4
Rio Maior	28
Sabrosa	7
Sabugal	3
Salvaterra de Magos	20
Santa Comba Dão	9
Santa Cruz	5
Santa Cruz da Graciosa	5
Santa Maria da Feira	518
Santarém	181
Santiago do Cacém	25
Santo Tirso	403
São Brás de Alportel	5
São João da Madeira	80
São Pedro do Sul	13
São Roque do Pico	5
Sátão	10
Seia	13
Seixal	643
Sernancelhe	6
Serpa	14
Sertã	4
Sesimbra	65
Setúbal	204
Sever do Vouga	58
Silves	26
Sines	8
Sintra	2850
Sobral de Monte Agraço	20
Soure	26
Tábua	35
Tabuaço	3
Tavira	36
Terras de Bouro	12
Tomar	16
Tondela	14
Torre de Moncorvo	23
Torres Novas	27
Torres Vedras	94
Trancoso	20
Trofa	149
Vagos	36
Vale de Cambra	155
Valença	15
Valongo	764
Valpaços	6
Velas	5
Vendas Novas	9
Viana do Alentejo	3
Viana do Castelo	196
Vieira do Minho	44
Vila da Praia da Vitória	7
Vila do Bispo	4
Vila do Conde	302
Vila Flor	5
Vila Franca de Xira	808
Vila Nova da Barquinha	3
Vila Nova de Cerveira	9
Vila Nova de Famalicão	407
Vila Nova de Foz Côa	72
Vila Nova de Gaia	1678
Vila Nova de Poiares	11
Vila Pouca de Aguiar	8
Vila Real	162
Vila Real de Santo António	17
Vila Verde	237
Vimioso	12
Vinhais	31
Viseu	106
Vizela	151
Vouzela	8

Figura 1. Tabela retirada do Relatório de Situação nº 124 emitido pela DGS. Demonstra o número de casos confirmados de contágio do COVID-19 por concelho de Portugal "Reimpressa de https://covid19.min-saude.pt/relatorio-de-situacao/" por DGS, 04/07/2020, Portugal, p. 01.

Ocorre que, tal divulgação periódica acarretou diversas queixas da população em geral, sustentando, sobretudo o incômodo com a divulgação de dados da saúde. Tais reclamações foram diretamente dirigidas à CNPD que, oficialmente, emitiu o documento intitulado: "Orientações sobre a divulgação de informação relativa a infetados por Covid-19", o qual quedou-se a analisar a situação de divulgação de dados pelas autoridades públicas com base na legislação atual existente sobre o assunto.

Resumidamente, a CNPD sustentou que os dados publicados pelas autoridades públicas devem ser devem ser visualizados como "fonte da informação para os órgãos de comunicação

social e para as entidades púbicas e privadas que entendem dar-lhe visibilidade […] para dar tranquilidade às suas populações […]". Sendo que, a divulgação de tais dados não pode, em momento algum, identificar os seus titulares, devendo sempre haver a observância ao regime jurídico de proteção de dados.

Em continuidade, a aludida Comissão considerou casos hipotéticos em que há identificação do titular de dados, utilizando-se como justificativa principal o fato de que tal divulgação se mostraria é necessária para garantir a saúde e proteção de toda a população.

Após análise aprofundada, chegou-se à conclusão de que a realização de tal tratamento dependeria da existência de uma norma legal que o regulasse e que, ao mesmo tempo, acautelasse os interesses e direitos dos seus titulares, porém esta legislação não existe o que torna esta situação completamente ilegítima e ilegal.

Também foi levada em consideração a eventual hipótese de realização do tratamento, com identificação dos titulares, mediante a existência do consentimento expresso dos titulares quanto a tal situação.

Ocasião em que, a CNPD concluiu não se verificam as condições necessárias para a emissão de um consentimento livre, vez que há uma evidente situação de vulnerabilidade das pessoas contaminadas pelo vírus ainda, há a situação de dependência de intervenção das autoridades Estatais.

Diante das hipóteses e conclusões levantadas pela Comissão, pode-se auferir que a divulgação de dados da saúde com a identificação dos infectados será sempre desproporcional, em virtude do impacto negativo que pode causa na vida dos indivíduos.

As orientações emitidas pela CNPD também trataram de um particular assunto que merece ser mencionado no presente estudo, nomeadamente no que diz respeito à publicação de dados sem a identificação do seu titular em uma circunscrição territorial com pequena dimensão populacional, que permita que, mesmo sem qualquer informação relativa à pessoa do titular, seja possível realizar a identificação dos contaminados.

É evidente que, quando se está diante de uma região de pequena dimensão territorial com poucos cidadãos residentes se torna muito fácil identificar as pessoas infectadas. Portanto, tal situação se enquadra nos casos em que os titulares podem ser facilmente identificados, estando sujeita às regras do regime jurídico de proteção de dados, havendo falta de legitimidade do Estado para a publicação de tais dados.

Em que pese as orientações emitidas pela CNPD serem voltadas para uma situação em específico, nomeadamente a divulgação de dados diretamente ligados à pacientes com Covid-

19, sabemos que tal orientação pode e deve ser observadas em diversas situações que envolvem o tratamento de dados relativos à saúde.

Portanto, o tratamento dos dados relativos à saúde deve ser realizado com base em técnicas e medidas de organização que visem proteger os dados dos titulares. Sendo que, diante da necessidade de divulgação de tais dados, deve-se levar em consideração o cuidado de evitar a possível identificação dos seus titulares.

Apesar da existência de diversas normas tanto no âmbito da União Europeia como no âmbito do direito interno de Portugal, que conferem extrema proteção jurídica aos dados de saúde, os quais atravessam o sistema de tratamento de forma transversal, na tentativa de evitar a ocorrência da violação de tais dados. É necessário considerarmos que sempre há a real e efetiva possibilidade da ocorrência da violação que acarrete em danos aos direitos, liberdades e interesses dos seus titulares.

Ao passo em que, todo cidadão que estiver diante da situação de violação de seus dados, seja por meio da divulgação indevida, pelo compartilhamento ou dentre tantas as outras possibilidades de ocorrência de violação, tem o direito de buscar a responsabilização do causador do dano e a consequente pretensão indenizatória, conforme disposto nos já estudados artigos 79º e 82º do RGPD.

É de suma importância para o presente estudo ressaltar que, apesar dos dados relativos à saúde serem considerados dados sensíveis e, por isso, contarem com um regime de tratamento especial - que se mostra mais rigoroso se comparado ao regime aplicado aos demais dados -, não há qualquer legislação especial que regule a responsabilização civil em virtude da violação de dados pessoais relativos à saúde.

De forma sucinta, podemos afirmar que os limites impostos pela responsabilidade civil para aqueles que, por exemplo, expõem dados da saúde é o mesmo para aqueles que violam dados que não possuem a característica de dados sensíveis.

Assim, sempre que houver a efetiva violação de tais dados, deverá haver a aplicação do regime geral, estudado anteriormente, sem qualquer distinção por se tratar de dados sensíveis. Apesar do legislador reconhecer a natureza valiosa que os dados sensíveis representam para os seus titulares, a proteção normativa se esgota na existência da diferenciação quanto ao tratamento de tais dados, em que as operações de tratamento são mais rigorosas quando se está diante destes dados especiais.

Esta dualidade existente na norma, nos conduz diretamente à reflexão da necessidade da discussão acerca da busca de mecanismos que apresentem um sistema de responsabilização civil mais rígido, sobretudo quando se está diante de dados relativos à saúde de seus titulares,

o que inevitavelmente também conduz à necessidade de refletir acerca da pretensão indenizatória decorrente da responsabilização pela violação de dados sensíveis.

Todavia, antes de adentrarmos propriamente na reflexão suscitada acima, é imperioso relembrar os limites impostos no âmbito da responsabilização civil, verificada nos casos em que há efetiva violação de dados relativos à saúde.

É sabido que, no âmbito da violação de dados, há possibilidade de se verificar a ocorrência de duas formas distintas de responsabilização na esfera civil, as quais correspondem à responsabilidade obrigacional e a aquiliana.

Esta última modalidade de responsabilidade advém do incumprimento de uma norma, da violação a um preceito legal, o qual acarreta na ocorrência de danos em desfavor de terceiros. No âmbito da proteção de dados relativos à saúde, tal responsabilização advém da violação dos preceitos dispostos no RGPD e das normas internas que regulam a matéria.

Podemos afirmar que tal prerrogativa, advém sobretudo do disposto nos artigos 79º e 82º, nº 1, do RGPD, os quais reconhecem que todos os titulares de dados têm o direito de ingressar com ação judicial sempre que houver violação aos seus direitos no âmbito da realização do tratamento de dados, podendo receber uma indenização do responsável pelo tratamento ou subcontratante pelos danos materiais ou imateriais sofridos.

A delimitação do alcance da responsabilização civil aquiliana não apresenta grandes óbices quando se está diante da violação de dados relativos à saúde que advém da realização de um tratamento realizado por um único responsável pelo tratamento, sem que haja a subcontratação.

Ocasião em que se verifica que, sempre que houver alguma violação de dados o seu titular poderá acionar o poder judiciário em face do responsável pelo tratamento para pleitear a sua responsabilização civil em decorrência do incumprimento do disposto no RGPD.

Nesse sentido, acreditamos que, a inversão do ônus da prova contida no nº 3, do artigo 82º pode ser visualizada como uma ferramenta limitadora do exercício do direito que é consagrado aos titulares que tiveram seus dados violados, sobretudo quando se tratam dos dados relativos à saúde.

O aludido dispositivo legal determina que o subcontratante ou o responsável pelo tratamento podem ficar isentos da responsabilização civil se provarem que não são responsáveis pelo evento que originou os danos.

Portanto, nas situações em que se o titular tiver seus dados pessoais violados poderá ingressar com a respectiva ação judicial para pleitear a responsabilização civil do responsável pelo tratamento e do subcontratante, com o consequente direito de ressarcir os danos sofridos.

Todavia, o responsável pelo tratamento e o subcontratante podem eximir-se da responsabilidade se detiverem provas hábeis a comprovar que não são responsáveis pelo evento que originou os danos.

Ao trazermos esta discussão para o âmbito dos dados pessoais sensíveis, os quais detém normas de tratamento diferenciadas em virtude de sua natureza e da extensão dos danos que podem acarretar aos seus titulares, cabe-nos o questionamento se a inversão do ônus da prova se mostra como uma medida proporcional aos riscos e danos que podem advir da violação dos dados relativos à saúde.

Ao nosso ver, não há razoabilidade normativa na criação de um sistema diferenciado, que tem como objetivo conferir maior segurança ao sistema de tratamento de um grupo de dados sensíveis, e não garantir aos titulares destes dados o direito de exercerem a responsabilização civil plena, diante da violação de tais dados.

Inclusive, devemos nos lembrar que, tanto o responsável pelo tratamento como o subcontratante assumem riscos que são inerentes ao exercício de sua atividade e, por isso devem sempre adotar métodos e medidas que reduzem tais riscos.

Portanto, acreditamos que, a solução mais plausível a ser tomada, levando em consideração a natureza e a extensão dos possíveis danos morais e patrimoniais que podem advir da violação de dados, seria mitigar a aplicação da inversão do ônus da prova apenas às situações que envolvem o tratamento de dados sensíveis.

Todavia, tal mitigação do ônus probatório dependeria da criação de uma norma em específico, no âmbito da União Europeia. Não havendo que se falar em tal possibilidade em decorrência de uma decisão judicial, uma vez que, se assim o fosse, a própria decisão estaria ferindo os princípios do RGPD, o que a tornaria completamente questionável.

O alcance da responsabilidade civil aquiliana também deve ser visto sob uma perspectiva mais ampla, de modo a englobar as situações em que há o controle conjunto e paralelo destes dados.

A questão não apresenta grandes óbices quando se está diante da ocorrência do controle conjunto, na medida em que, podemos sustentar que esta possibilidade se encontra prevista no próprio RGPD (art. 82º, nº 2) ao delimitar as linhas em que se pode falar na responsabilidade do subcontratante e do responsável pelo tratamento, vejamos: “[...] Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente

regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.”.

Conforme já restou dito anteriormente, o responsável pelo tratamento sempre será responsabilizado diante da ocorrência da violação de dados ocasionada em decorrência da não observância dos preceitos dispostos no RGPD, enquanto que o subcontratante tem sua responsabilidade limitada ao não cumprimento das obrigações que a ele são imputadas pelo RGPD ou por não seguir as instruções emitidas pelo responsável pelo tratamento.

As operações de tratamento realizadas em regime conjunto por um subcontratante e por um responsável, geralmente e em regra (porque existem exceções conforme veremos adiante) são realizadas de forma em que há o compartilhamento de meios e finalidades, por isso, estaremos diante da responsabilidade solidária.

De acordo com o artigo 497º do CC, sempre que houverem diversas pessoas responsáveis pelos danos, a responsabilidade será solidária. Assim, presume-se que todos os envolvidos com o evento que gerou o dano devem ser responsabilizados.

O alcance da responsabilização civil aquiliana se torna um pouco mais complexa quando se está diante de um tratamento paralelo de dados, ou seja, quando tais dados são compartilhados por mais de um indivíduo, em que não há a efetiva partilha das finalidades e meios.

Em um primeiro momento, parece-nos evidente que, por não haver a mesma finalidade e meios de tratamento, cada responsável pelo tratamento exerce a atividade de forma individual, respondendo pelos danos que advém do próprio tratamento.

Todavia, há importantes ponderações que devem ser realizadas neste âmbito, para que assim seja possível auferir com precisão o alcance da responsabilidade civil neste sentido. Inicialmente, relembramos que o conceito de tratamento de dados é muito amplo e a própria atividade de tratamento envolve diversas situações, por exemplo, a recolha, o registro, a estruturação, a alteração, a manutenção, a recuperação, a destruição, dentre outros.

Inclusive, não podemos deixar de mencionar que o próprio compartilhamento de dados com terceiros, no âmbito do controle e tratamento paralelo, também consiste em uma operação que se encontra englobada no conceito de tratamento de dados, sendo assim considerado.

Justamente por este motivo é que sempre que houver o compartilhamento de dados, o responsável pelo tratamento deverá se certificar e assegurar que o segundo, com o qual compartilha os dados, agirá em conformidade com as regras e princípios do RGPD e da Legislação interna do país que regula a proteção de dados.

Situação semelhante ocorre nos casos quem há o compartilhamento e envio de dados para um país que não faz parte da União Europeia, ocasião em que o responsável pelo tratamento que realiza a operação de tratamento deve se certificar da existência de garantias suficientes de cumprimento do RGPD e em um nível idêntico a da União Europeia, sob pena de incorrer em responsabilização civil nos termos do artigo 82º, nº 4 do RGPD.

A autora Mafalda Miranda Barbosa nos ensina que, sempre que houver mais de uma esfera de responsabilidade civil em relação à um único conjunto de dados pessoais, sob os quais se verifica a ocorrência de um efeito danoso, todos os envolvidos com o tratamento devem ser responsabilizados solidariamente, nos termos do artigo 82º, nºs 3 e 4 do RGPD. Salvo se, a "[...] esfera de responsabilidade de um agente consome a do outro." [121].

Portanto, o alcance da responsabilidade civil este aspecto é muito amplo, principalmente no que diz respeito ao responsável pelo tratamento, o qual será responsabilizado, bastando que se encontre envolvido com o tratamento.

Ao mesmo tempo, se considerarmos que o compartilhamento de dados faz parte do tratamento de dados, o primeiro responsável poderá isentar-se da responsabilidade se comprovar que observou as normas de proteção de dados e não contribuiu para com a ocorrência do evento danoso.

Outra situação que merece ser debatida e que amplia o respaldo legal para a responsabilização civil diz respeito à situação em que o responsável pelo tratamento contrata um terceiro, o qual confere uma nova finalidade para os dados.

Para melhor elucidar a questão, tomamos o seguinte caso hipotético, o hospital X, contrata a empresa de *marketing* Y para divulgar seus produtos, dando acesso à todos os dados de seus clientes para que a empresa Y possa exercer a função contratada.

Todavia, a empresa de marketing Y, decide utilizar esta mesma base de dados para difundir produtos de outros clientes, definindo uma nova finalidade para estes dados. Ainda que, Y passe a ocupar o lugar de responsável pelo tratamento ao definir uma nova finalidade, ainda há que se falar na responsabilização de X.

De acordo com Mafalda Miranda Barbosa[122], a empresa Y pode ser vista nesta relação como comissário, uma vez que foi contratada por X, a situação posta pode ser analisada sob a perspectiva do artigo 500º do CC, o qual preleciona: " [...]Aquele que encarrega outrem de qualquer comissão responde, independentemente de culpa, pelos danos que o comissário causar, desde que sobre este recaia também a obrigação de indemnizar.".

[121] BARBOSA, *Op. Cit.*, p. 456.
[122] BARBOSA, *Op. Cit.*, p. 457.

Para que se possa falar na responsabilização civil em decorrência do artigo 500º do CC é indispensável que a relação de comissão exista efetivamente também estejam presentes os já estudados pressupostos da responsabilidade civil e ainda, o ato deve ser praticado durante o exercício das funções.

O dano ocorrido deve ser visualizado como a efetiva concretização do risco que advém do exercício da função, "[...] Do que se trata, afinal, é de saber se a atribuição daquelas funções aumentou o risco de surgimento da lesão ou se ela poderia ter lugar de igual modo, ainda que não existisse a comissão que foi, assim, mera ocasião (como poderia haver outras) de surgimento da violação." [123].

Portanto, no caso hipotético sob análise, mesmo que a empresa de *marketing* Y tenha contrariado as instruções emitidas pelo hospital, no momento em que decidiu eleger uma nova finalidade para o tratamento, é evidente que a Y jamais poderia ter o feito sem os meios que foram disponibilizados por X.

Avançando os estudos, não podemos deixar de tratar das situações em que a violação de dados ocorre em virtude de um ato praticado pelo subcontratante. Neste caso, é possível verificar uma significativa atenuação da responsabilidade que é incumbida ao responsável pelo tratamento.

Estar-se-á diante da responsabilidade subjetiva, apenas se comprovado que o responsável pelo tratamento violou a obrigação de recorrer ao auxílio de subcontratantes que demonstrem possuir medidas técnicas e organizativas que conferem proteção aos dados.

A comprovação deste requisito pode ser realizada por meio da comprovação de que o subcontratante cumpre com um código de conduta aprovado ou por meios de procedimentos de certificação. Ou seja, o responsável pelo tratamento deverá comprovar que buscou o apoio de um profissional capacitado e que segue as regras de proteção de dados.

No que diz respeito à responsabilidade objetiva, a mesma poderá ocorrer nos termos do artigo 500º do CC conforme explicado anteriormente. Sendo que, a responsabilização do responsável pelo tratamento não irá afastar a responsabilidade do subcontratante.

Diante de todas as considerações realizadas acerca da responsabilidade aquiliana em decorrência da violação de dados da saúde, podemos auferir que, apesar de o RGPD ter uma abrangência muito grande quanto às pessoas que podem exercer o direito de indenização e responsabilidade, ao utilizar-se da expressão "qualquer pessoa que tenha sofrido danos", não

[123] *Idem*.

podemos deixar de mencionar que tal regra impõem algumas limitações quanto a parte que cometeu o ato lesante.

Conforme tratamos anteriormente, o nº1 do artigo 82º do RGPD, reconhece o direito do indivíduo que sofreu danos no âmbito dos processos de tratamento de dados de receber uma indenização atribuída a título de responsabilidade civil. Todavia, podemos afirmar que tal responsabilização encontra três situações distintas que podem ser visualizadas como fatores que limitam o alcance da responsabilidade pela violação dos dados relativos à saúde.

A primeira situação limitante diz respeito ao fato de que a norma apenas reconhece a possibilidade de responsabilização civil pelos danos que advém de uma violação ao RGPD, ou seja, se houver uma violação de dados a qual não viola os preceitos estabelecidos no aludido Regulamento, não há que se falar em indenização, nem responsabilização civil como base nesta lei.

Concordamos que, o RGPD apresenta um largo rol de deveres impostos á todos aqueles que se encontram envolvidos com o processo de tratamento de dados, com o objetivo de manter a segurança dos dados e conferir proteção jurídica aos direitos e interesses de seus titulares. Porém, não podemos concordar que a norma esgota todas as possibilidades fáticas que podem ocorrer no cotidiano social, para além disso, temos que levar em consideração que há um crescente desenvolvimento tecnológico que tem apresentado diversos métodos, ferramentas e meios que envolvem as situações de tratamento de dados, criando novos mecanismos que a própria lei não teria como prever, porque seu surgimento se deu antes mesmo da existência destas tecnologias atuais e futuras.

A segunda situação que acreditamos que pode ser vista como uma limitação para a responsabilização aquiliana diz respeito ao fato da segunda parte do nº 1 do artigo 82º do RGPD reconhecer que apenas o responsável pelo tratamento e o subcontratante tem o dever de indenizar. Portanto, nos casos em que houver a violação de dados relativos à saúde, a qual decorra da inobservância dos preceitos estabelecidos no RGPD, haverá o direito a receber uma indenização, a qual é dirigida apenas ao responsável pelo tratamento e ao subcontratante.

Não podemos deixar de relembrar que o nº 2 do art. 82 do RGPD reconhece que todo e qualquer responsável pelo tratamento que esteja envolvido em tal processo é responsável pelos danos que violem o aludido Regulamento, sendo que, o subcontratante apenas será responsabilizado se não tiver cumprido com as obrigações contidas no RGPD que são impostas aos subcontratantes ou se não tive seguido as instruções do responsável pelo tratamento.

Assim, é possível verificar uma pequena limitação da norma no que diz respeito ao alcance da responsabilidade civil quanto à figura do subcontratante, o qual, apesar de se

encontrar inserido no processo de tratamento tem sua responsabilidade limitada no âmbito do RGPD, podendo se falar também - ocasionalmente e conforme descrito acima - a sua responsabilização solidária, com base no artigo 500º do CC.

Por fim, não podemos deixar, mais uma vez, de mencionar que, ao nosso ver, o nº 3 do artigo 82º do RGPD também deve ser visto como uma importante situação em que há efetiva limitação do alcance da responsabilidade civil pela violação de dados, sobretudo, no que diz respeito ao responsável pelo tratamento e ao subcontratante, os quais podem ser utilizar de provas para ver sua responsabilidade totalmente ou parcialmente afastadas.

Realizadas as considerações acerca da responsabilidade aquiliana em decorrência da violação de dados relativos à saúde, as quais possibilitaram uma análise acerca dos fatores que, ao nosso ver, podem ser visualizados como limites para a imposição da responsabilização civil aquiliana, diante da ocorrência da violação de dados, passaremos, neste momento, a aprofundar os estudos em relação à responsabilidade contratual ou obrigacional.

A aplicabilidade da responsabilização civil obrigacional no âmbito da violação de dados advém da pré-existência de um contrato firmado entre as partes. Ou seja, advêm de uma relação negocial e obrigacional, a qual foi discutida, negociada e firmada entre as partes contratantes, as quais assumem direitos e deveres para a persecução da finalidade estipulada no próprio contrato.

Apesar de se tratar de uma modalidade de responsabilidade que advém de uma relação negocial, não podemos limitar o alcance da responsabilidade, de forma genérica, ás cláusulas contratuais que compõem a manifestação de vontade das partes. O próprio princípio da boa-fé contratual pode impor alguns deveres de cuidado, os quais, se forem violados, podem acarretar na responsabilização obrigacional em virtude da ocorrência da violação dos deveres de conduta[124].

Na relação obrigacional firmada a título de controle conjunto, em que há um contrato firmado por mais de um sujeito, não há maiores dúvidas acerca da responsabilização diante da ocorrência da violação de danos, na medida em que todos aqueles que firmaram o contrato podem ser responsabilizados, seja com base em uma cláusula contratual firmada entre as partes ou em observância ao princípio da boa-fé, conforme sustentado acima.

Todavia, a responsabilização em virtude da violação aos dados pessoais, ocorrida no âmbito do controle paralelo não nos parecer ser tão simples assim, principalmente nas situações em que o responsável pelo tratamento – que firmou um contrato com terceiro para realização

[124] BARBOSA, *Op. Cit.*, p. 462.

de tratamento de dados, por exemplo – recorre à pessoa do subcontratante para cumprimento do objeto do contrato.

No âmbito da responsabilização em virtude de um ato cometido pelo subcontratante, tomamos as lições de Mafalda Miranda Barbosa[125] para delimitar o alcance da responsabilização civil tanto do subcontratante como do responsável pelo tratamento.

De acordo com a autora supracitada, ás situações em que há uma efetiva violação em decorrência de um fato causado pelo subcontratante podem ser visualizadas sob o disposto no artigo 800º do CC, o qual preleciona: " 1. O devedor é responsável perante o credor pelos actos dos seus representantes legais ou das pessoas que utilize para o cumprimento da obrigação, como se tais actos fossem praticados pelo próprio devedor.".

Deste modo, o responsável pelo tratamento passará a responder por todos os comportamentos danosos praticados pelo subcontratante ou terceiros que vier a utilizar com o objetivo de cumprir a obrigação contratual contraída.

Não havendo que se falar em dupla imputação, como ocorre com a aplicação do artigo 500º do CC no âmbito da responsabilização civil aquiliana, uma vez que apenas o responsável pelo tratamento irá responder pelos atos dos seus auxiliares como se tivessem sido praticados por ele.

Assim, ainda que o responsável pelo tratamento não atue com culpa, mas há um efetivo dano ocasionado por um terceiro auxiliar (subcontratante) verifica-se a possibilidade de aplicação do artigo 800º do CC, trata-se da responsabilidade objetiva por fato alheio de terceiro.

A aplicação de deste dispositivo legal também se justifica pelo fato de o próprio contrato que estabelece as obrigações e direitos convencionados entra as partes é que firma a responsabilidade e, consequentemente, define quem é o obrigado. Também, não seria razoável a perda da imputação dos danos porque o contratante se utilizou de terceiros para cumprimento de uma obrigação firmada por ele próprio.

Para que se possa falar na procedência da pretensão indenizatória pelo artigo 800º do CC é necessário a presença de alguns requisitos que constituem na existência de uma obrigação decorrente de um ato negocial, a existência da relação entre o contratante e o terceiro que é utilizado para cumprimento da obrigação negocial, a efetiva atuação de terceiro no tratamento, na qualidade de auxiliar.

Todavia, devemos levar em consideração que a responsabilidade sob estudo decorre de uma relação contratual, por isso a aplicabilidade do dispositivo normativo acima identificado

[125] BARBOSA, *Op. Cit.*, p. 463-469.

deve levar em consideração algumas situações peculiares, nomeadamente o contrato que é firmado entre o responsável pelo tratamento e o subcontratante.

Assim, pode-se afirmar que o fato delimitador que abarca a responsabilização diz respeito ao âmbito da relação que é previamente assumida pelo responsável pelo tratamento, devendo ser estabelecida uma obrigação em sentido técnico. De modo que, tal responsabilização apenas se faz possível quando a legitimação para a realização da operação de tratamento se trate de um objeto negocial.

É de suma importância que o contrato estabelecido entre o subcontratante e o responsável pelo tratamento tenha eficácia de proteção para terceiros. Assim, não seria permito que os terceiros exigissem a prestação (cumprimento do contrato principal) do subcontratante, mas poderiam se tornar credores de uma possível pretensão indenizatória deste último.

Para tanto, o artigo 28º, nº 3, do RGPD apresenta-se como um grande contributo neste sentido, ao afirmar que o tratamento de dados realizados em regime de subcontratação de ser "[...] regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento", devendo fazer referência ao preceito tratado acima.

Superficialmente, podemos afirmar que o alcance e os limites da responsabilidade civil obrigacional decorrente da violação de dados da saúde encontram-se diretamente limitada às disposições contidas na base negocial firmada entre as partes, que acarreta na constituição de um contrato, eivado de direitos e deveres sob os quais as partes se obrigam ao cumprimento.

Entendemos que, a visualização da questão acima tratada que diz respeito à aplicação do princípio da boa-fé contratual utilizada como fator justificativo para aplicação da responsabilidade civil pode ser visualizada como um alargamento do direito que o lesado possui em relação à sua pretensão indenizatória. Uma vez que, presume-se que, nestes casos, o lesado não tomou o cuidado de prever contratualmente a ocorrência da violação de dados, havendo um alargamento na interpretação e alcance o próprio contrato para que seja possível que se fale em responsabilização na esfera civil.

No que diz respeito aos casos em que o responsável pelo tratamento utiliza-se de subcontratantes para a execução e cumprimento da obrigação contraída por este primeiro, acreditamos que é possível afirmar que, em regar a responsabilização do subcontratante poderá ser limitada ou até mesmo reduzida, uma vez que este atua no processo de tratamento apenas

como terceiro, contratado pelo responsável pelo tratamento e, justamente, por isso, há a responsabilização do responsável pelo tratamento como se este tivesse praticado o ato lesivo.

Nesse aspecto, é importante ressaltar que esta limitação em relação ao subcontratante pode ser facultativa, ou seja, o subcontratante poderá ser responsabilizado se, no contrato firmado diretamente com o responsável pelo tratamento para execução do tratamento, houver tal previsibilidade contratual.

Podemos afirmar que sempre que se está diante da efetivação de um contrato que envolva o tratamento de dados pessoais da saúde, deve-se atentar à necessidade e importância de se estabelecer cláusulas contratuais que confiram maior segurança e proteção jurídica aos seus titulares e à todos aqueles que se encontram envolvidos na operação de tratamento.

Tal necessidade ainda é aumentada quando se está diante de dados que dizem respeito à saúde de seu titular, que em virtude de sua natureza e da significância destas informações, a sua violação pode vir a causar danos aos direitos e interesses de seus titulares.

Assim, na tentativa de incluir possíveis situações comuns e corriqueiras que podem advir do tratamento, sempre buscar estabelecer cláusulas contratuais penais que prevejam a possibilidade de aplicação de multa em virtude da violação e tais dados, bem como, a obrigatoriedade de tronar os dados criptografados, evitando que, terceiros que não fazem parte do processo de tratamento que eventualmente tenham acesso aos dados não consigam compreende-los.

Há ainda uma particular situação que nos conduz à verificação da delimitação do alcance da esfera da responsabilidade civil diante da ocorrência da violação de dados relativos à saúde. No capítulo anterior, nos dedicamos à análise de situações que envolvem a prática de uma única ação danosa que, ao mesmo tempo, deixa de observar as cláusulas de um contrato de tratamento estabelecido entre as partes e acaba por ferir uma norma de proteção, ou seja, nas situações que se pode falar em responsabilidade aquiliana e obrigacional.

Nesse sentido, podemos afirmar que existem duas posições antagônicas que tornam o alcance da responsabilização civil questionável. Assim, quando estamos diante da aplicabilidade da teoria do sistema do não cúmulo, em que o lesado deve verificar qual das duas espécies de responsabilidade se mostra mais favorável aos seus interesses individuais, podemos afirmar que há uma evidente limitação ao alcance da responsabilidade civil, uma vez que o lesado deve optar se pretende pleitear a responsabilidade aquiliana ou obrigacional.

Não nos parece ser possível concordar com tal posicionamento, uma vez que, se estaria restringindo o direito do lesado de exercer os seus direitos que encontram respaldo tanto na legislação quanto no contrato firmado entre as partes.

Também, a distinção entre as espécies de responsabilidade é evidente, o conceito de ilicitude subjacente à responsabilidade aquiliana não envolve a necessidade de existência prévia de uma obrigação em sentido técnico e implica na preterição de um direito absoluto, não é possível se estabelecer uma relação de especialidade entre estas modalidades.

Nesse sentido, salientamos os ensinamentos de Mafalda Miranda Barbosa (2017, p. 20) sobre o assunto, a qual sustenta que a simultaneidade da ocorrência da responsabilização na esfera aquiliana e obrigacional diante uma mesma situação factual danosa, nos leva a acreditar que "existe um concurso de títulos de fundamentação de uma mesma pretensão indenizatória [...]" em que é possível combinar as normas que regulam as duas hipóteses de responsabilidade civil.

Portanto, acreditamos que, a aplicação do sistema do não cúmulo nos casos em que há um único fato ilício que provocou o dano gerando duas possibilidades e indenização, apresenta-se como uma posição limitante do direito do lesado.

Por este motivo, defendemos o posicionamento doutrinário e jurisprudencial que acata a adoção do sistema do cúmulo, em que não há que se falar na existência de concurso de normas, havendo a possibilidade de o lesado ingressar com uma única ação a pleitear ambas as hipóteses de responsabilização ou o ingresso de ações autónomas.

Inequívoco que, o posicionamento por nós defendido, apresenta um âmbito de alcance da responsabilidade civil muito mais amplo, uma vez que se pode falar na responsabilização de ambas as modalidades, não sendo exigido ao lesado que opte pela que lhe parecer mais conveniente.

Realizadas as ponderações necessárias para compreensão da dimensão e alcance da responsabilidade civil diante da ocorrência da violação dos dados relativos à saúde, passaremos a fazer breves considerações acerca da pretensão indenizatória, que deve ser vista aqui como uma consequência da responsabilização na esfera civil.

Apesar de não haver uma unanimidade entre os juristas acerca do objetivo da fixação da obrigação de ressarcir, pode-se afirmar que esta tem como objetivo promover a reparação do dano causado, a prevenção a ocorrência de situações que possam acarretar em prejuízos e a sanção pelo comportamento causado.

Assim, uma das consequências advindas da efetiva responsabilização civil é a obrigação do agente causador do dano em indenizar o lesado. Ou seja, a indenização tem como objetivo reconstituir a situação original que existiria se não houvesse o evento que causou o dano lesivo, conforme dispõe o artigo 562º do CC.

A reparação do dano civil, voltando-se ao estado *a quo* se mostra evidente quando se está diante de danos de cunho meramente patrimoniais, onde é possível mensurar quantitativamente os danos causados e, consequentemente repará-los. Todavia, tal situação se inverte ao tratarmos da ressarcibilidade dos danos que não detém cunho patrimonial, ou seja, os danos morais que afetam a moral do lesado.

Em virtude da natureza pela qual os danos morais se encontram revestidos, não é possível realizar a reparação completa dos danos sofridos. Todavia, é sempre preferível que o lesante receba uma quantia em dinheiro na tentativa de compensar o dano ou, ao menos, atenuar ou minorar a lesão sofrida, do que deixa-lo sem nada obrigando-o a suportar os danos que lhe foram causados.

Nestes casos, não há que se falar em ressarcimento do dano efetivamente, porque não é possível mensurar quantitativamente os danos sofridos e compensá-los monetariamente, logo pode-se falar na existência de uma espécie de compensação que se mostre aparentemente proporcional aos danos sofridos.

O autor Antunes Varela[126], seguindo o entendimento partilhado pela maior parte da doutrina, tratou do tema com muita propriedade ao revelar a função satisfatória e compensatória da responsabilidade civil, sustentando que "Entre a solução de nenhuma indemnização a atribuir ao lesado, a pretexto de que o dinheiro não consegue apagar o dano, e a de se lhe conceder uma compensação […] ou satisfação adequada, ainda que com certa margem de discricionariedade na sua fixação, é incontestavelmente mais justo e criteriosa a segunda orientação […], sabendo-se que a composição pecuniária pode servir para satisfação das mais variadas necessidades.".

Portanto, a indenização pecuniária que favorece o lesado, não tem o objetivo de reparar, mas sim, de tentar satisfazer as dores morais suportadas por ele. A própria jurisprudência é uníssona quanto ao fato de que "a reparação de tais danos não constitui uma verdadeira indemnização, mediante a qual se visa reconstituir a situação preexistente."[127]. Objetiva-se de algum modo, compensar os danos sofridos, não propriamente de indenizar o lesado pelo ocorrido.

Podemos dizer que as funções preventivas e sancionatórias se encontram interligadas quando estamos diante da responsabilidade civil, pois como ficará claro a seguir podemos sustentar que há uma relação de dependência entre elas.

---

[126] VARELA, *Op. Cit.*, p. 603-604.
[127] SUPREMO Tribunal de Justiça - **Acórdão do processo nº 070011**, de 01 de junho de 1982. Relator: Joaquim Figueiredo.

A presença da finalidade preventiva se dá em virtude de havendo uma obrigação indenizatória diante da ocorrência de um dano, o agente sempre tenderá a observar os deveres de cuidado, evitando a ocorrência do dano na esfera alheia.

Sabemos que o indivíduo que é obrigado a indenizar estará sendo punido por ter causado uma lesão, todavia, ao mesmo tempo também se busca prevenir que o próprio lesante ou terceiros, utilizem o ocorrido como exemplo a não ser seguido, e não venham a produzir situações semelhantes. De acordo com Júlio Gomes (1989, p. 106) chama-se "preventivo-punitiva porque, no fundo, prevenção e punição são duas faces de uma mesma medalha, expressões de um único princípio".

Justamente diante deste contexto da pretensão indenizatória é que defendemos que, quando estamos diante da ocorrência da violação de um dado pessoal sensível, que é a situação na qual se encontra inserida os dados relativos à saúde, é evidente que o titular dos danos pode vir a sofrer danos materiais, os quais podem ser facilmente quantificáveis.

Todavia, a questão mostra mais complexidade quando há a efetiva ocorrência dos danos morais, que acreditamos que a dor e o sofrimento que a violação de dados da saúde pode causar são imensos. Por isso, acreditamos que o aplicador da lei deverá sempre levar em conta uma indenização justa quando se está diante da violação de dados da saúde, a qual não se pode comprar à uma violação de dados que não se encontram inseridos no rol de dados sensíveis.

O próprio RGPD reconhece a importância dos dados sensíveis, tanto é que determina regras diferentes de tratamento para este tipo de dados, uma vez que se está diante de dados e informações que dizem respeito ao mais íntimo do seu titular.

Portanto, verifica-se uma evidente necessidade de implementação, seja em nível do Regulamento Europeu ou regulamento local, de normas que conferem maior proteção jurídica aos titulares de tais dados principalmente no que diz respeito à responsabilização civil em decorrência da violação destes dados. Além disso, ressaltamos que, o intérprete e aplicador da lei deverá fixar uma indenização levando em consideração diversos fatores, mas sempre ponderando pela significância de tais dados.

É imperioso que diante da responsabilização civil em decorrência da violação de dados pessoais da saúde, haja a observância dos fundamentos da responsabilidade civil, nomeadamente a finalidade ressarcitória, preventiva e sancionatória. Cabendo ao Estado regular tal situação de forma extremamente rígida, evitando que a violação de dados sensíveis aconteça ou se repita e, fazendo com que aqueles que se viram lesados tenham uma compensação legítima dos danos sofridos.

CONCLUSÃO

Para alcançar o principal objetivo do presente estudo, que consiste em estudar qual os limites e o alcance da responsabilidade civil diante da ocorrência da violação de dados pessoais da saúde, partiu-se do estudo acerca do desenvolvimento histórico do direito à privacidade e da proteção de dados, o que permitiu o alcance do atual conceito atribuído aos dados pessoais, nomeadamente dos dados relativos à saúde.

De forma muito sucinta, podemos afirmar que o desenvolvimento e aprimoramento da esfera pessoal do indivíduo na sociedade acarretaram no surgimento do direito à reserva da vida privada.

Tal direito, encontra-se diretamente ligados e correlacionados com o direito à proteção de dados, que pode ser visto como o resultado da somatória do desenvolvimento tecnológico com a necessidade de preservação da vida privada e da intimidade.

Assim, podemos sustentar que os regimes legais que visam a proteção de dados, podem ser visualizados como uma resposta do Estado para as adversidades que possam surgir diante das operações de tratamento de dados pessoais, bem como, podem ser vistos como uma tutela estatal que objetiva preservar os mais profundos interesses e direitos dos titulares de dados.

Diante desta necessidade de proteção é que o ordenamento jurídico europeu, por meio do RGPD, estabeleceu normas e diretrizes que objetivam assegurar a segurança de dados, as quais podem ser visualizadas como um instrumento essencial e indispensável para a realização do tratamento de dados pessoais.

O mesmo diploma legal reconhece a existência de dados pessoais sensíveis, os quais detém especial cuidado em relação ao tratamento, em virtude da natureza que tais dados apresentam, que dizem respeito às informações da vida mais íntima de seu titular e ainda, levando-se em consideração que, a ocorrência da violação de tais dados pode acarretar em enormes prejuízos morais e materiais aos seus titulares.

É neste contexto de dados sensíveis que se englobam os dados relativos à saúde, os quais encontram-se elencados nesta categoria especial porque tratam de informações que dizem respeito à saúde e à esfera mais íntima da vida de seus titulares. Ou seja, tratam-se de dados e informações, que por vezes, o próprio titular opta por mantê-los em sigilo até mesmo de seus familiares e pessoas mais próximas.

A coleta e o tratamento desta modalidade de dados sensíveis se verificam, sobretudo, no âmbito da prestação de cuidados da saúde, que utilizam destes dados para o exercício de funções especiais e características.

Podemos afirmar que, neste âmbito as operações de tratamento de dados encontram uma dupla proteção normativa, uma vez que, tais operações devem ser realizadas de acordo com as normas que regulam a segurança de dados, mas também, há a necessidade de observância das normas deontológicas por parte daqueles que realizam a coleta de dados no exercício da profissão como ocorre, por exemplo, com os médicos e enfermeiros.

Todavia, também devemos salientar que as operações de tratamento de dados relativos à saúde não se esgotam no âmbito da prestação de cuidados para com a saúde, uma vez que, o crescente desenvolvimento tecnológico tem nos apresentado diversos meios e formas de recolha e tratamento destes dados, como acontece, por exemplo, com os aplicativos de celular que acompanham a queima de calorias diárias, o nível de oxigênio no sangue, *etc*.

Justamente neste âmbito de tratamento de dados sensíveis é que nos deparamos com o questionamento da possibilidade de divulgação destes dados e quando estaremos de fato, diante de uma violação.

De acordo com o RGPD, estaremos diante de uma violação de dados sempre que houver uma transgressão na segurança de dados que possa vir a provocar a destruição, perda, a alteração, a divulgação ou o acesso sem autorização dos dados pessoais.

Sendo que, a ocorrência de uma violação de dados que enseja no dano ao seu titular pode ser vista como os primeiros passos para a caracterização da responsabilidade civil neste âmbito.

De modo que, na prática, sempre que o responsável pelo tratamento se deparar com qualquer situação de violação de dados, este deverá em um primeiro momento, avaliar os impactado que tal violação acarretou ou poderá acarretar e, em seguida, deverá tomar as medidas legais cabíveis. Se necessário, deverá comunicar e notificar o titular dos dados e a Autoridade de Controle sobre a ocorrência da violação, expondo os possíveis riscos.

Havendo uma efetiva violação de dados que tenha causado danos ao seu titular, é defeso aos lesados a invocação da responsabilidade civil, com o intuito de ver-se ressarcido pelos danos sofridos.

Esta responsabilização pode ocorrer diante de duas vertentes, ou seja, pode-se falar na responsabilização civil aquiliana, que advém do incumprimento do RGPD e demais normas de proteção de dados. Bem como, da responsabilização obrigacional, que se encontra diretamente ligada ao incumprimento contratual.

O aprofundamento dos estudos, sobretudo no tocante à responsabilização pela violação de dados pessoais permitiu que, no âmbito da responsabilidade obrigacional, a visualização dos limites da responsabilização se mostram mais evidentes, na medida em que aquele que assume

uma obrigação através de um contrato deve cumpri-la e, mesmo que, no instrumento contratual firmado entre as partes, não exista qualquer previsão acerca da violação de dados, o devedor pode ver-se obrigado à indenizar em virtude do princípio da boa-fé contratual.

Tal espécie de violação apresenta uma pequena discussão no que diz respeito aos casos em que há mais de um contratante, ao passo em que, quando se está diante da ocorrência de um controle conjunto, onde há dois responsáveis pelo tratamento que compartilham a mesma finalidade ou os mesmos meios, cada um deverá responder na medida de sua culpa, uma vez que ambos atuam na qualidade de responsáveis pelo tratamento.

Todavia, a solução não pode ser a mesma nos casos em que há controle paralelo, em que não há a partilha das finalidades e dos meios, ocasião em que o responsável pelo tratamento irá responder pelos danos como se ele mesmo os tivesse praticado, nos termos do artigo 800º do CC.

Portanto, podemos afirmar que a responsabilidade civil aquiliana apresenta limites muito bem delimitados quando se está diante de um contrato firmado apenas entre duas partes, em que o contratante será responsabilizado na medida em que concorreu para o descumprimento contratual e ocorrência do dano. Sendo que, o mesmo aplica-se aos casos em que há controle conjunto.

Todavia, tal questão apresenta maior complexidade quando se está diante da realização de um controle paralelo, em que os limites da responsabilidade civil se esgotam na pessoa do responsável pelo tratamento, o qual responde pelos atos de terceiros em sua totalidade.

No que tange à responsabilidade aquiliana, é importante lembrar que o limite de responsabilidade do responsável pelo tratamento e do subcontratante pode deve ser verificado de acordo com a situação em concreto, uma vez que o tema apresenta diversas possibilidades de responsabilização, principalmente quando se refere à tratamentos realizados por mais de uma pessoa.

Enquanto que, poderemos falar na existência da responsabilidade civil aquiliana nas situações em que se verificar a ocorrência de um dano material ou imaterial, que advenha do incumprimento das normas e preceitos que regulam a proteção de dados, no âmbito do direito interno ou da UE.

Nesse sentido, ressaltamos que o RGPD nos remete à responsabilização civil objetiva do responsável pelo tratamento e do subcontratante, uma vez que a aludida norma determina que sempre que houver uma violação de dados ocasionada pela inobservância das regras de tratamento o lesado poderá pleitear uma indenização do responsável pelo tratamento ou do subcontratante.

Todavia, a mesma norma prevê a hipótese de afastamento da responsabilização nos casos em que responsável pelo tratamento ou o subcontratante comprovem que em momento algum contribuíram com a ocorrência do dano.

Portanto, em um primeiro momento, o alcance da responsabilidade civil aquiliana parece ser extremamente amplo, pois imputa a responsabilização objetiva ao subcontratante e ao responsável pelo tratamento. Porém, tal responsabilização se limita à efetiva comprovação de observância das normas que regulam as operações de tratamento e à comprovação da contribuição com o dano.

O alcance da responsabilidade civil aquiliana não se esgota nos termos acima mencionados, de modo que, é indispensável realizar o estudo e análise desta modalidade de responsabilização no âmbito da realização do controle conjunto e paralelo.

O controle conjunto de dados pressupõe a existência do compartilhamento de meios e finalidades e, por isso, a análise da responsabilidade civil nesta esfera não apresenta maiores dificuldades, de modo que, evidente a existência da responsabilidade solidária, uma vez que os envolvidos nas operações de tratamento de dados compartilham dos mesmos escopos para desenvolvimento de suas atividades.

Todavia, o alcance da responsabilidade civil aquiliana ocorrido no âmbito do controle paralelo de dados exige atenção e cuidado, uma vez que estamos diante de uma situação em que não há o compartilhamento de finalidades e dos meios que conduzem o tratamento.

Incialmente, parece-nos prudente concluir que cada um dos responsáveis pelo tratamento deverá ser responsabilizado nos limites dos tratamentos que realizou, vez que estamos diante de uma situação que envolve o exercício individual das atividades de tratamento.

Porém, o conceito que é atribuído às operações de tratamento de dados é amplo e, envolve diversas operações, dentre elas o próprio compartilhamento de dados. Assim, o responsável pelo tratamento deverá se certificar de que aquele com que compartilha os dados desempenha suas atividades em observância às regras e princípios do RGPD.

Ocasião em que, evidentemente nos deparamos com a esfera de responsabilidade solidária, uma vez que o artigo 82º, nº 4 do RGPD determina que, nos casos em que há mais de um responsável pelo tratamento ou subcontratante que se encontrem envolvidos no mesmo tratamento, cada um é responsável pela totalidade dos danos.

Verificando-se, nesse caso, a possibilidade de isenção da responsabilidade do primeiro, se este comprovar que agiu em observância às normas de proteção de dados e não contribuiu para a ocorrência do evento danoso, nos termos do artigo 82º, nº 3 do RGPD.

Também levamos em consideração a hipótese do responsável pelo tratamento contar com o auxílio de um subcontratante para realização de uma operação de tratamento de dados, em que este segundo, no desempenho de suas funções, passa a determinar uma nova finalidade para o tratamento.

Acreditamos que, no caso supracitado faz-se necessária a aplicação do artigo 500º do CC, de modo a estender a responsabilidade ao responsável pelo tratamento, uma vez que, o subcontratante pode ser visto como comissário nesta relação, pois foi contratado pelo responsável para operar o tratamento.

Portanto, o estudo realizado permite a compreensão da responsabilização civil em decorrência da violação dos dados pessoais da saúde, de modo que, a definição do alcance e dos limites impostos nesta esfera devem ser analisados de forma muito cuidadosa, sempre se levando em consideração as situações mais minuciosas que dizem respeito à operação de tratamento e os limites contratuais estabelecidos.

As pesquisas realizadas encontram certa limitação no que diz respeito à existência da escassa jurisprudência local que trate diretamente sobre o tema investigado. Todavia, embora a existência desta limitação, foram utilizadas jurisprudências análogas, que apresentam similitude com o abordado e que contribuíram de forma significativa para sua persecução.

Verifica-se a possibilidade de complementação e continuação do estudo realizado, nomeadamente no que diz respeito à avaliação da efetiva necessidade de ampliação da responsabilidade civil quando se está diante de dados sensíveis. Incluindo-se, por exemplo, a verificação da possibilidade de inaplicabilidade no disposto no artigo 82º, nº 3, uma vez que se tratam de riscos de advém do exercício da atividade desempenhada.

Por fim, é evidente a necessidade de amparo jurídico que se coloca sobre a proteção dados da saúde, a qual tem se intensificado a cada dia em virtude da facilidade de compartilhamento de dados que se verifica no mundo atual aliada à especial atenção que tem se dado à saúde nos últimos anos.

Tais facilidades nem sempre se apresentam como fatores benéficos para a sociedade, uma vez que, deve-se levar em consideração a possível ocorrência da violação destes dados, que poderá acarretar na exposição indevida de seus titulares, causando danos imensuráveis.

Por este motivo, é muito importante que as ciências jurídicas se dediquem ao estudo destas situações, com o intuito de buscar meios efetivos de buscar a devida reparação aos titulares lesados, levando-se em consideração as limitações impostas pela norma nesse sentido.

REFERÊNCIAS

AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA E CONSELHO DA EUROPA – **Manual da Legislação Europeia sobre Proteção de Dados**. [Em linha]. 2014, p. 216. Disponível na internet: < https://www.echr.coe.int/Documents/Handbook_data_protection_Por.pdf>. ISBN 978-92-871-9939-3.

AGOSTINI, Leonardo Cesar de - **A intimidade e a vida privada como expressões da liberdade humana**. Porto Alegre: Núria Fabris Editora, 2011. ISBN: 9788560520787.

ALARCÃO, Rui de - **Direito das Obrigações:** Lições Policopiadas, Coimbra, 1983.

ALERTA SECURITY - **Os Pilares da Segurança da Informação**. [Em linha]. [Consult. 28 out. 2020]. Disponível em WWW: <URL:https://alertasecurity.com.br/blog/31-base-capitulo-1-os-pilares-da-seguranca-da-informacao>.

ARENDT, Hannah - **A condição humana.** Tradução de Roberto Raposo.10. ed. Rio de Janeiro: Forense Universitária, 2001. ISBN: 978-85-218-0255-6.

ARENDT, Hannah - **Entre o passado e o futuro**. 5. Ed. São Paulo: Perspectiva, 2000. ISBN: 9788527301176.

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DE INFORMAÇÃO – **Glossário da Sociedade da Informação** [Em linha]. Lisboa, 2022, atual. 2022 [Consult. 27fev.2022]. Disponível em WWW: <https://apdsi.pt/glossario/>.

BARBOSA, Ana Mafalda Castanheira Neves de Miranda – **Lições de Responsabilidade Civil**. Cascais: Princípia Editora, Lda. 2017, ISBN: 978-989-716-156-8.

BARBOSA, Mafalda Miranda - Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. **Revista de Direito Comercial**. [Em linha]. (2018), p. 423-494. [Consult. 26 dez. 2020]. Disponível em WWW: <URL:

https://www.revistadedireitocomercial.com/data-controllers-e-data-processors>. ISSN 2183-9824.

BARBOSA, Mafalda Miranda – Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade Civil. **Revista do Instituto do Conhecimento AB**. [Em linha]. Nº 7, Ano V (2017), p. 13-47 [Consult. 13 mai. 2022]. Disponível em WWW: <https://abreuadvogados.com/wp-content/uploads/2021/03/protecao-de-dados-e-direitos-de-personalidade.pdf>. ISSN 9780218294972.

BERNARDO, Frei - **Pessoa: saúde e ética**. Porto: Edição dos amigos do Fr. Bernardo, O.P: 1988.

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. **Civilistica.com** [Em linha]. Ano 9, nº 3 (2020) [Consult. 10 abr. 2022]. Disponível em WWW: <http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/>. ISSN: 2316-8374.

CACHAPUZ, Maria Cláudia - **Intimidade e vida privada no novo Código Civil brasileiro:** uma leitura orientada no Discurso Jurídico. Porto Alegre: Sergio Antonio Fabris Editora, 2006. ISBN: 8575253484.

CACHAPUZ, Maria Claúdia Mércio - Privacidade, proteção de dados e autodeterminação informativa. **Revista Jurídica da Presidência.** [Em linha]. V. 15, Nº 107 (2014), p. 823-848 [Consult. 19 out. 2020]. Disponível em WWW: <URL:https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/126/118>.

CANCELIER, Mikhail Vieira de Lorenzi **- Infinito Particular:** Privacidade no Século XXI e a Manutenção do Direito de estar só. Rio de Janeiro: Lumen Juris, 2017. ISBN: 9788551903391.

CANCELIER, Mikhail Vieira; PILATI, José Isaac - Privacidade, Pós-Modernidade Jurídica E Governança Digital: O Exemplo Do Marco Civil Da Internet Na Direção De Um

Novo Direito. **Espaço Jurídico.** [Em linha]. V**.** 18, nº 1 (2017), p. 65-82 [Consult. 03 ago. 2022]. Disponível em WWW: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/7252.> ISSN 1519-5899.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS - **Deliberação nº 51/2001.** [Em linha]. [Consult. 25 Out. 2020]. Disponível em WWW: <https://www.cnpd.pt/home/orientacoes/DEL51-2001-ACESSO-DADOS-SAUDE.pdf>.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS - **Orientações: Sobre divulgação de informação relativa a infetados por Covid-19.** [Em linha]. [Consult. 03 Set. 2020]. Disponível em WWW: <https://www.cnpd.pt/home/orientacoes/Orientacoes_divulgacao_informacao_infetados_Covid-19.pdf>.

CORDEIRO, A. Barreto Menezes – **Direito da proteção de dados: à luz do RGPD e da Lei nº 58/2019**. Coimbra: Edições Almedina, 2020. ISBN 978-972-40-8304-9.

CORDEIRO, A. Barreto Menezes - **O Consentimento do Titular dos Dados no RGPD**.[Em linha]. Universidade de Lisboa. Lisboa: Centro de Investigação de Direito Privado, 2018. [Consult. 15 jul. 2021] Disponível em WWW: <https://blook.pt/publications/publication/e772e2d8f7b4/>.

CORDEIRO, António Barreto Menezes – **Direito das obrigações**. 2º Vol. Coimbra: AAFDL, 2001. ISBN 5606939000576.

COSTA JUNIOR, Paulo José da - **O direito de estar só: tutela penal da intimidade**. 2ª ed. São Paulo: RT, 1995. ISBN: 9780786162635.

COSTA, Mário Júlio de Almeida – **Direito das Obrigações**. 12 ed. Coimbra: Edições Almedina, 2010, ISBN 9789724040332.

CUNHA, Carolina – Proteção de dados e aplicações móveis na área da saúde: um diagnóstico sumário. **Banca, bolsa e seguros**. [Em linha]. Nº 3 (2018), p. 31-50. [Consult. 13 mar. 2021]. Disponível em WWW: < https://www.fd.uc.pt/bbs/revista/>. ISSN 2183-5586.

DEODATO, Sérgio - A proteção da informação da Saúde. **Fórum de Proteção de Dados** [Em linha]. Nº 04 (2017), p. 62-71 [Consult. 20 Set. 2020]. Disponível em WWW: <https://www.cnpd.pt/home/revistaforum/forum2017_1/files/assets/basic-html/page-I.html#>. ISSN 2183-5977.

DEODATO, Sérgio – **A proteção dos dados pessoais de Saúde.** Lisboa: Universidade Católica, 2016. ISBN 978-972-54-0578-9.

DEODATO, Sérgio - **Direito da Saúde: colectânea de legislação anotada**. Coimbra: Almedina, 2012. ISBN: 978-972-40-4750-8.

DEODATO, Sérgio – Segurança da Informação em Saúde. **X Seminário de Ética: Segurança da Informação**. [Em linha]. Nº 34 (2010), p. 41-46 [Consult. 18 mai. 2021]. Disponível em WWW: <https://www.flipsnack.com/ordemenfermeiros/roe34/full-view.html>. ISSN 1646-2629.

DIREÇÃO-GERAL DA SAÚDE - **Relatório de Situação nº 124** [Documento icónico]. [Em linha]. Portugal: Direção-Geral da Saúde, 2020 [Consult. 06 nov. 2022]. Disponível em WWW: < https://covid19.min-saude.pt/relatorio-de-situacao/>.

DONEDA, Danilo - **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006. ISSN 9788571475625.

DRE – **Lexionário**. [Em linha]. Lisboa: Diário da República Eletrónico, atual. 2022. [Consult. 20 Nov. 2020]. Disponível em WWW: <https://dre.pt/dre/lexionario/termo/dados-relativos-a-saude-acesso-dever-notificacao>.

ESTORNINHO, Maria João; MACIEIRINHA, Tiago – **Direito da Saúde**. Lisboa: Universidade Católica Editora, 2014. ISBN 9789725404034.

FARIA, Jorge Ribeiro de; VASCONSELOS, Miguel Pestana de; PEDRO, Rute Teixeira. **Direito das obrigações.** 2ª Ed. Reimpressão. Coimbra: Edições Almedina, 2020. ISBN: 9789724086538.

FAZENDEIRO, Ana – **Regulamento Geral Sobre a Proteção de Dados**. 3ª ed. Coimbra: Edições Almedina, 2018. ISBN 978-972-40-7629-4.

FRADA, Manuel A. Carneiro da - A responsabilidade objectiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana. **Direito e Justiça In**. Lisboa: Universidade Católica Editora, 1998. ISSN 0871-0336. Vol. XII: tomo I, p. 297-311.

GOMES, Júlio - Uma função punitiva para a responsabilidade civil e uma função reparatória para a responsabilidade penal?. **Revista de Direito e Economia**. ISSN 0870-8835. Ano 15 (1989), p. 106-144.

GONÇALVES, Anabela Susana de Sousa – O tratamento de dados pessoais no Regulamento Geral de Proteção de Dados. **Scientia Iuridica.** ISSN 0870-8185, tomo LXVIII, Nº 350 (2019), p. 165-190.

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. **Parecer nº 4/2007** sobre o conceito de dados pessoais, 2004. 11750/02/PT WP 89. [Em linha]. [Consult. 12 ago. 2021]. Disponível em WWW: <https://www.gpdp.gov.mo/index.php?m=content&c=index&a=print_news&catid=153&id=16>.

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. **Parecer nº 1/2010** sobre os conceitos de responsável pelo tratamento e subcontratante, adotado em 16 de fevereiro de 2010. 00264/10/PT WP 169. [Em linha]. [Consult. 12 ago. 2021]. Disponível em WWW: <https://www.gpdp.gov.mo/file/Documents%20of%20European%20Union/PT/%E7%AC%AC1_2010%E8%99%9F%E6%84%8F%E8%A6%8B%E6%9B%B8_PT.pdf>.

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTECÇÃO DOS DADOS DA COMISSÃO EUROPEIA. **Parecer nº 03/2014** relativo à notificação da violação de dados pessoais, adotado em 25 de março de 2014. 693/14/PT/WP 213. [Em linha]. [Consult. 12 ago. 2021]. Disponível em WWW: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf >.

HABERMAS, Jürgen - **Mudança estrutural da esfera pública:** investigações sobre uma categoria da sociedade burguesa. Tradução de Denilson Luís Werle. São Paulo: Editora Unesp, 2014. ISBN: 9788539305131.

INSTITUTO INFORMATION MANAGEMENT - **Vazamentos mostram importância da governança de dados no setor de saúde.** [Em linha]. São Paulo, 2019 [Consult. 20 set. 2020]. Disponível em WWW: < https://docmanagement.com.br/12/17/2019/vazamentos-mostram-importancia-da-governanca-de-dados-no-setor-de-saude/>.

LOUREIRO, João [*et al*.] - **Direito da saúde: estudos em homenagem ao Prof. Doutor Guilherme de Oliveira.** Volume V. Coimbra: Edições Almedina, S.A., 2016. ISBN 978-972-40-6603-5.

LOURENÇO, Paula Meira - **A Função Punitiva da Responsabilidade Civil**. Coimbra: Coimbra Editora, 2006. ISBN: 9789723214215.

MAGALHÃES, Ana Filipa; PEREIRA, Maria Leitão – **Regulamento Geral da Proteção de dados: manual prático**. 2ª ed. Porto: Vida Económica – Editorial, SA, 2018. ISBN 978-989-768-445-6.

MANDIM, David. Diário de notícias - **Infetados queixam-se da divulgação de dados pessoais por autarquias.** [Em linha]. Lisboa, 2020. [Consult. 22 set. 2020]. Disponível em WWW: <https://www.dn.pt/pais/infetados-queixam-se-da-divulgacao-de-dados-pessoais-por-autarquias-12110324.html>.

MARQUES, Márcia Cristina Alexandre de Magalhães – **O regulamento geral sobre a proteção de dados.** Porto: Librum Editora, 2019. ISBN 978-989-54605-0-2.

MELO, Augusto. **Proteção de dados pessoais na era da informação: a privacidade e intimidade em face do avanço tecnológico**. 1ª Ed. Porto: Juruá, 2019. ISBN 978-989-712-656-7.

MOREIRA, Sónia – A proteção das pessoas singulares no novo Regulamento Geral de Proteção de Dados Pessoais. **Direito na Lusofonia. Direito e novas Tecnologias In.** Braga: Escola de Direito da Universidade do Minho, 2018. ISBN: 978-989-99766-5-8. P, 485-492.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra - **Responsabilidade Civil na LGPD: Problemas e Soluções** [Em linha]. V. 6, Nº 1, p. 158-174 (2020). [Consult. 11 nov. 2021]. Disponível em WWW: <https://indexlaw.org/index.php/conpedireview/article/view/7024>. e-ISSN: 2448-3931.

NUNES, Rui - Justiça Distributiva e Direito à Saúde. **Direito à Saúde: dilemas atuais In**. Lisboa: Editorial Juruá, 2017, p. 9-31. ISBN 978-989-712-414-3.

OLIVEIRA, Egon Rafael dos Santos - Direito à saúde: dilemas atuais. **Cadernos Ibero-Americanos De Direito Sanitário** [Em linha]. V. 9, Nº 2, p. 228–234 (2020). [Consul. 13 mai. 2021]. Disponível em WWW: <https://doi.org/10.17566/ciads.v9i2.636>. ISSN 2358-1824.

PEEK, Niels; RODRIGUES, Pedro Pereira – Three controversies in health data Science. **International Journal of Data Science and Analytics** [Em linha]. Nº 6, p. 261-269 (2018). [Consult. 05 jan. 2021]. Disponível em WWW: < https://doi.org/10.1007/s41060-018-0109-y>.

PINHEIRO, Alexandre Sousa - **Privacy e Proteção de dados pessoais: a construção dogmática do direito à identidade informacional**. Lisboa: AAFDL Editora, 2015. ISBN:9786120002605.

PIRES, Lucas de Almendra Freitas - **Direito à Privacidade no âmbito da sociedade de informação: reflexões em torno da questão nos inícios do século XXI.** Dissertação de mestrado apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do Mestrado Científico, Coimbra, 2014.

POÇAS, Luís – Problemas e dilemas do setor segurador: o RGPD e o tratamento de dados de saúde. **Banca, bolsa e seguros**. [Em linha]. Nº 3 (2018), p. 217-302. [Consult. 13 mar. 2021]. Disponível em WWW: < https://www.fd.uc.pt/bbs/revista/>. ISSN 2183-5586.

REBOLLO DELGADO, Lucrecio – **Protección de datos em Europa. Origen, evolución y regulación actual.** Madrid: Editorial Dykinson, 1º Ed., 2018. ISBN 978-8491486558.

REBOLLO DELGADO, Lucrecio **– Vida privada y protección de datos em la Unión Europea**. Madrid: Editorial Dykinson, 1ª Ed., 2008. ISBN 978-8498493337.

REDE EUROPEIA DE COOPERAÇÃO CIENTIFICA, Medicina e direitos do homem da Federação europeia das Redes Científicas - **A Saúde face aos direitos do homem, à ética e às morais**. Trad. Maria Teresa Serpa. Lisboa: Instituto Piaget, 2001. ISBN:972-771-404-8.

REGENTE, Diuliane Ellen Ribeiro. **A proteção de dados pessoais e privacidade do utilizador no âmbito das comunicações eletrónicas**. Dissertação de mestrado apresentada na Universidade Autónoma de Lisboa, 2015.

RENAUD, Isabel Carmelo Rosa - Conferência Inicial: A confiança. **A Revista da Ordem dos Enfermeiros**: Segurança da Informação [Em linha]. Número 34 (2010), páginas 9-17. Jun. [Consult. 23 ago. 2021]. Disponível em WWW: <https://www.ordemenfermeiros.pt/roe/>.

REUTERS, Kacper Pempel. O Jornal Económico **- Portugal sem Meios de Proteção de Dados Pessoais, CNPD Alerta o Agravamento da Situação**. [Em linha]. Lisboa, 2018. [Consult. 26 out. 2020]. Disponível em WWW: <https://jornaleconomico.sapo.pt/noticias/portugal-sem-meios-de-protecao-de-dados-pessoais-cnpd-alerta-o-agravamento-da-situacao-375383>.

ROSA, Diogo Miguel Alcaçarenho – **Proteção de Dados Pessoais em saúde e hospitais E.P.E.: Responsabilidade civil do responsável pelo tratamento.** Dissertação de mestrado apresentada à Faculdade de Direito da Universidade de Lisboa no âmbito do Mestrado Profissionalizante em ciências jurídico-empresariais, Lisboa, 2018.

SANTOS, Sofia Berberan; GABRIEL, João – **Regulamento Geral de Protecção de Dados: Legislação e Algumas Notas**. 1ª ed. Lisboa: Edição GPA academy, 2017. ISBN 978-989-691-625-1.

SILVA, Heraclides Sequeira dos Santos – **A proteção de dados pessoais na era global: o caso Schrems.** Dissertação de mestrado apresentada à Universidade Nova de Lisboa no âmbito do Mestrado em Ciências Jurídicas Forenses, Lisboa, 2017.

TEIXEIRA, Sílvia Gabriel; FREITAS, Carolina Rodrigues - A Responsabilidade Civil na Proteção de Dados: um Estudo Comparado entre Brasil e União Europeia. **Direito civil e tecnologia [Recurso eletrônico on-line] organização I Congresso de Tecnologias Aplicadas ao Direito**. [Em linha], p. 109-116. [Consult. 26 Dez. 2020]. Disponível em WWW: < www.conpedi.org.br>. ISBN 978-85-5505-658-1.

TELLES, Inocêncio Galvão – **Direito das Obrigações.** Reimpressão da 7. Ed. Coimbra: Coimbra Editora, 2010. ISBN:9789723207712.

THIBES, Mariana Zanata - **As formas de manifestação da privacidade nos três espíritos do capitalismo: da intimidade burguesa ao exibicionismo de si nas redes sociais**. Sociologias [Em linha]. Volume 19, nº 46 (2017), p. 316-343. [Consult. 16 Jan. 2021]. Disponível na internet: <http://www.scielo.br/pdf/soc/v19n46/1517-4522-soc-19-46-00316.pdf>. ISSN 1807-1337.

VARELA, João de Matos Antunes – **Das obrigações em geral**. Coimbra: Almedina, 2005. ISBN: 972-40-1389-8.

VILLAS-BÔAS, Maria Elisa - O direito-dever de sigilo na proteção ao paciente. **Revista Bioética**. [Em linha], vol. 23, nº 3 (2015), pp. 513-523. [Consult. 24 Set. 2020]. Disponível em WWW: <https://www.scielo.br/pdf/bioet/v23n3/1983-8034-bioet-23-3-0513.pdf>. ISSN 1983-8034.

WACHOWICZ, Marcos – **Proteção de Dados Pessoais em Perspectiva: LGPD e RGPD na ótica do direito comparado** [Em linha]. Curitiba: Gedai, 2020. [Consult. 05 nov. 2022]. Disponível em WWW: <https://www.gedai.com.br/wp-content/uploads/2020/11/Protecao-de-dados-pessoais-em-perspectiva_ebook.pdf >. ISBN 978-86233-51-3.

REFERÊNCIAS LEGAIS

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2016/C 202/02) - **Jornal Oficial da União Europeia**. [Em linha]. (07/06/2016) C202/389-C202/405 [Consult. 05 Set. 2020]. Disponível em WWW: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>.

CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA - **Diário da República, Série I**. Nº 86/1976 (10/04/1976). [Em linha]. [Consult. 28 out. 2020]. Disponível em WWW: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

CONVENÇÃO EUROPEIA DOS DIREITOS DO HOMEM - **Tribunal Europeu dos Direitos do Homem**. [Em linha]. (02/10/2013), p. 3-64. [Consult. 20 Set. 2020]. Disponível WWW: <https://www.echr.coe.int/d/ocuments/convention_por.pdf>.

CONVENÇÃO PARA A PROTECÇÃO DO HOMEM E DA DIGNIDADE DO SER HUMANO FACE ÀS APLICAÇÕES DA BIOLOGIA E DA MEDICINA: CONVENÇÃO SOBRE OS DIREITOS HUMANOS E BIOMEDICINA - **Conselho da Europa**, 2001. [Em linha]. Disponível em: <https://www.ministeriopublico.pt/instrumento/convencao-para-proteccao-dos-direitos-do-homem-e-da-dignidade-do-ser-humano-face-22>.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948 - **Assembleia Geral da ONU.** 217 [III] A, Paris. [Em linha]. [Consult. 05 Set. 2020]. Disponível em WWW: <https://dre.pt/dre/geral/legislacao-relevante/declaracao-universal-direitos-humanos>.

DECRETO-LEI Nº 47344/66 - **Diário do Governo, Série I**. Nº 274/1966 (25/11/1966). [Em linha]. [Consult. 13 Out. 2021]. Disponível em WWW: <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=775A0066&nid=775&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo>.

DECRETO-LEI Nº 59/2019 - **Diário da República, Série I**. Nº 88 (05/08/2019). [Em linha]. [Consult. 13 Out. 2020]. Disponível em WWW: <https://dre.pt/dre/detalhe/decreto-lei/59-2019-122242530>.

DIRECTIVA 97/66/CE DE 15 DE DEZEMBRO DE 1997 - **Jornal Oficial das Comunidades Europeias.** [Em linha]. (30/01/1998), p. L24/1-L24/8 [Consult. 12 ago. 2021]. Disponível em WWW: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31997L0066>.

LEI n.º 95/2019 - **Diário da República, Série I.** N.º 136 (16-07-2012) [Em linha]. p. 55-66. Disponível em: <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1668&tabela=leis&ficha=1&pagina=1>.

LEI Nº 12/2005 - **Diário da República, Série I-A**. Nº 18 (26/01/2005) [Em linha]. [Consult. 13 Out. 2020]. Disponível em WWW: <https://dre.pt/dre/detalhe/lei/12-2005-624463?_ts=1662076800034>.

LEI Nº 58/2019 - **Diário da República, Série I**. Nº 151 (08/08/2019). [Em linha]. [Consult. 13 Out. 2020]. Disponível em WWW: <https://dre.pt/pesquisa/-/search/123815982/details/maximized>.

REGULAMENTO (CE) Nº 1338/2008 - **Jornal Oficial da União Europeia**. [Em linha]. (31/12/2008), p. L354/70-L354/81 [Consult. 12 ago. 2021]. Disponível em WWW: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008R1338&from=LV>.

REGULAMENTO (CE) Nº 45/2001 - **Jornal Oficial das Comunidades Europeias.** [Em linha]. (12/01/2001), p. L8/1-L8/22 [Consult. 12 ago. 2021]. Disponível em WWW: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32001R0045>.

REGULAMENTO (UE) 2016/679 - **Jornal Oficial da União Europeia**. [Em linha]. (04/05/2016), p. L119/1-L119/88 [Consult. 05 Set. 2020]. Disponível em WWW: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>.

REGULAMENTO Nº 707/2016. **Diário da República, Série II**. Nº 139/2016 (21/07/2016). [Em linha]. [Consult. 05 Set. 2020]. Disponível em WWW:

<https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2649&tabela=leis&ficha=1&pagina=1&so_miolo=>.

REFERÊNCIAS JURISPRUDENCIAIS

SUPREMO Tribunal de Justiça - **Acórdão do processo nº 070011,** de 01 de junho de 1982. Relator: Joaquim Figueiredo. [Em linha]. [Consult. 21 mai. 2021]. Disponível em WWW: <
http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/69765ddd515ffd13802568fc003ab69c?OpenDocument>.

TRIBUNAL DE JUSTIÇA – **Acórdão dos processos apensos nºs C-46/93 e C-48/93**, de 05 de março de 1996. [Em linha]. [Consult. 03 abr. 2022]. Disponível em WWW: <https://curia.europa.eu/juris/showPdf.jsf?text=&docid=81389&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=29742>.

TRIBUNAL DE JUSTIÇA, Grande Secção - **Acórdão do processo nº C-28/08 P,** de 29 de junho de 2010. [Em linha]. [Consult. 23 set. 2021]. Disponível em WWW: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=84752&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=8063333>.

TRIBUNAL da Relação de Lisboa - **Acórdão do processo nº 512/10.8TCFUN.L1-2,** de 27 de setembro de 2012. Relatora Teresa Albuquerque. [Em linha]. [Consult. 30 jan. 2022]. Disponível em WWW: <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/378f8f0cf358eec180257afc00400bba?OpenDocument&Highlight=0,512%2F10.8TCFUN.L1-2>.

TRIBUNAL DE JUSTIÇA, Terceira Secção - **Acórdão do processo nº C-342/12,** de 30 de maio de 2013. [Em linha]. [Consult. 23 set. 2021]. Disponível em WWW: <https://curia.europa.eu/juris/liste.jsf?num=C-342/12&language=PT>.

TRIBUNAL DE JUSTIÇA, Quinta Secção – **Acórdão do processo nº C-557/12**, de 05 de junho de 2014. [Em linha]. [Consult. 16 mai. 2021]. Disponível em WWW: <https://curia.europa.eu/juris/liste.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=

C-
557%252F12&for=&jge=&dates=&language=pt&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lg=&page=1&cid=801953>.

TRIBUNAL DE JUSTIÇA, Quarta Secção – **Acórdão do processo nº C-212/13, de** 11 de dezembro de 2014. [Em linha]. [Consult. 23 set. 2021]. Disponível em WWW: <https://curia.europa.eu/juris/liste.jsf?language=pt&num=C-212/13 aos 20/11/2021>.

TRIBUNAL da Relação do Porto - **Acórdão do processo nº 1359/15.0T8MAI-A.P1,** de 28 de outubro de 2015. Relatora Anabela Dias da Silva. [Em linha]. [Consult. 26 nov. 2021]. Disponível em WWW: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/55ca523cb8284d0880257f1f00509496?OpenDocument&Highlight=0,1359%2F15.0T8MAI-A.P1>.

TRIBUNAL DE JUSTIÇA, Quarta Secção – **Acórdão do processo nº C-407/14**, de 17 de dezembro de 2015. [Em linha]. [Consult. 30 abr. 2022]. Disponível em WWW: < https://curia.europa.eu/juris/document/document.jsf?text=&docid=173120&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=297425>.

SUPREMO Tribunal de Justiça, Primeira Secção - **Acórdão do processo nº 4444/03.8TBVIS.C1.S1,** de 07 de fevereiro de 2017. Relator: Helder Roque. [Em linha]. [Consult. 21 mai. 2021]. Disponível em WWW: < http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/52aafc0211430543802580c1003b6f13?OpenDocument>.

TRIBUNAL DE JUSTIÇA, Primeira Secção - **Acórdão do processo nº C-494/16,** de 07 de março de 2018. [Em linha]. [Consult. 05 mai. 2021]. Disponível em WWW: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=200013&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=10169451>.

TRIBUNAL Central Administrativo Sul - **Acórdão do processo nº 116/16.1BECTB,** de 28 de junho de 2018. Relator Paulo Pereira Gouveia. [Em linha]. [Consult. 30 jan. 2022].

Disponível em WWW: <http://www.dgsi.pt/jtca.nsf/-/B1E9739F0FF115DC802582C2003ADAB1>.

TRIBUNAL da Relação de Lisboa - **Acórdão do processo nº 9773/16.8T8LSB.L1-7,** de 24 de setembro de 2019. Relator José Capacete. [Em linha]. [Consult. 26 jan. 2022]. Disponível em WWW: < http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/5acee3d4bfcb142e8025848800457c30?OpenDocument>.

TRIBUNAL da Relação do Porto - **Acórdão do processo nº 274/17.8TAVR.P1,** de 08 de fevereiro de 2021. Relatora Eugénia Cunha. [Em linha]. [Consult. 25 mai. 2022]. Disponível em WWW: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/1af045e0f3a44cd6802586960055018b?OpenDocument>.