DEPARTAMENTO DE DIREITO

MESTRADO EM DIREITO

ESPECIALIDADE EM CIÊNCIAS JURÍDICAS

UNIVERSIDADE AUTÓNOMA DE LISBOA

"LUÍS DE CAMÕES"

OS RISCOS DA DEFINIÇÃO DE PERFIS PARA A PRIVACIDADE DA PESSOA HUMANA: PROTEÇÃO DOS DADOS PESSOAIS SENSÍVEIS

Dissertação para a obtenção do grau de Mestre em Direito

Autor: Luiz Henrique Xavier Gomes

Orientadores: Professora Me. Patrícia Cardoso Dias e Professor Doutor Pedro Trovão Rosário

Número do candidato: 30001916

Janeiro de 2024

Lisboa

Dedicatória

Para àqueles que valorizam a proteção dos dados pessoais e lutam por um equilíbrio justo entre a definição de perfis e a preservação da privacidade.

Agradecimentos

A minha amada esposa Marcela, pela compreensão, apoio incansável e paciência durante todo o processo de elaboração desta dissertação. Você é minha fonte inesgotável de apoio, carinho e inspiração.

Ao meu filho Henrique, aquele que um mero sorriso levava todo o cansaço das noites insones de leitura e redação, que este trabalho seja um exemplo para você, mostrando a importância de buscar conhecimento e perseguir seus sonhos.

Aos meus pais, meus primeiros educadores, sem a confiança e o incentivo de vocês, eu não estaria aqui hoje, cada noite debruçados sobre a mesa, fazendo atividades de casa valeram a pena.

Aos meus orientadores, pelas dedicadas lições, pelo conhecimento compartilhado e pelos insights valiosos que contribuíram imensamente para o desenvolvimento deste trabalho.

Aos amigos e colegas de turma, pelas discussões enriquecedoras, pelo apoio mútuo e pela troca de ideias ao longo dessa jornada.

Agradeço também a todos aqueles que, de alguma forma, contribuíram para este trabalho, seja por meio de sugestões, críticas construtivas ou apoio moral.

Resumo

A coleta, tratamento e transferência de dados de maneira automatizada e manual tem modificado a concepção do que é a sociedade, resultando em uma ruptura nas tradicionais relações econômicas e sociais, afetando, inclusive, alguns direitos fundamentais, como a privacidade. Nessa esteira, a discussão acerca de como salvaguardar a vida privada e a intimidade do titular dos dados nunca esteve tão evidenciada, principalmente dentro do contexto do *profiling*, que envolve a construção de perfis por meio da análise automatizada de grandes quantidades de dados coletados sobre indivíduos ou grupos, com o objetivo prever comportamentos e a partir dessas predições, tomar decisões automatizadas. A técnica definição de perfis, apesar de apresentar alguns benefícios aos usuários e processadores dos dados, pode resultar em efeitos prejudiciais no desenvolvimento da vida privada dos indivíduos, principalmente em cenários onde o tratamento de dados brutos possa resultar, através do *profiling*, na geração de dados sensíveis. Desta feita, este estudo tem como escopo principal expor de que forma o direito a proteção de dados pessoais se desdobra para garantir a privacidade diante da definição de perfis que podem resultar na criação de dados sensíveis, traçando os limites legais para tratamento dos dados pessoais em casos de *profiling* e quando do tratamento dos dados sensíveis. Assim, busca-se demonstrar como a legislação relativa à proteção de dados pessoais no cenário europeu (RGPD) e brasileiro (LGPD) estabelecem mecanismos de controle sobre dados em diversos níveis, a fim de garantir efetiva privacidade e evitar a discriminação dos indivíduos cujos dados são utilizados na definição de perfis que resulta em dado sensíveis.

Palavras-chave: Privacidade. Proteção de dados pessoais. Profiling. Dados sensíveis.

Abstract

The collecting, processing, and transferring of data, both automated and manual, have reshaped the concept of society, resulting in a disruption of traditional economic and social relationships, impacting fundamental rights such as privacy. Within this context, the discussion on how to safeguard the private life and intimacy of data subjects has become increasingly prominent, particularly in the context of profiling, which involves the construction of profiles through automated analysis of large amounts of data collected about individuals or groups, with the aim of predicting behaviors and making automated decisions based on these predictions. Although profiling presents some benefits to users and data processors, it can have detrimental effects on the development of individuals' private lives, especially in scenarios where the processing of raw data through profiling may generate sensitive data. Therefore, this study aims to expose how the right to personal data protection unfolds to ensure privacy in the face of profiling that may lead to the creation of sensitive data, establishing legal boundaries for the processing of personal data in cases of profiling and the treatment of sensitive data. Thus, it seeks to demonstrate how legislation regarding the protection of personal data, such as the European General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (LGPD), establishes control mechanisms at various levels to ensure effective privacy and prevent discrimination against individuals whose data is used in profiling that results in sensitive data.

***Keywords*:** *Privacy. Protection of personal data. Profiling. Sensitive data*.

SUMÁRIO

Siglas

Art.- Artigo;

CRP- Constituição da República Portuguesa;

CF/88- Constituição da República Federativa do Brasil

CC- Código Civil;

DUDH- Declaração Universal dos Direitos do Homem;

CDHLF- Convenção dos Direitos do Homem e das Liberdades Fundamentais;

RGPD- Regulamento Geral da Proteção de Dados;

LGPD – Lei Geral de Proteção de Dados;

TEDH – Tribunal Europeu dos Direitos Humanos;

TJUE – Tribunal de Justiça da União Europeia

CEDH- Convenção Europeia dos Direitos do Homem;

CDFU – Carta dos Direitos Fundamentais da União Europeia;

CNPD- Comissão Nacional de Proteção de Dados;

TUE – Tratado da União Europeia;

TFUE- Tratado de Funcionamento da União Europeia;

UE- União Europeia;

CEPD- Comité Europeu para a Proteção de Dados;

WP 29- Grupo de Trabalho do Artigo 29º;

CJUE- Corte de Justiça da União Europeia.

INTRODUÇÃO

A rápida evolução da tecnologia e o crescente aumento da coleta, fluxo e tratamento de dados pessoais têm levantado preocupações significativas sobre o direito fundamento à privacidade da pessoa humana, exigindo-se dos legisladores e operadores do direito que se mantenham em estado de permanente alerta, com o intuito de observar quais as medidas necessárias para proteção desta prerrogativa.

De fato, no mundo que se torna cada vez mais virtual, os indivíduos desfrutam de acesso fácil a uma vasta quantidade de informações, enquanto suas atividades realizadas por meios digitais deixam um rastro de dados. Em razão desse comportamento, empresas e governos têm a possibilidade de coletar grandes volumes de dados sobre os sujeitos, utilizando essas informações para obter conhecimentos íntimos dos titulares dos dados.

É nesse contexto que surge o fenômeno da "definição de perfis" (*profiling*), a qual envolve a categorização de perfis dos titulares dos dados, através da análise automatizada de grandes quantidades de dados coletados sobre um indivíduo, com o objetivo de tomar decisões relacionadas ao perfilado ou prever seus comportamentos.

Esta dissertação tem como objetivo analisar os mecanismos de tutela previstos no Regulamento Geral de Proteção de Dados e na Lei Geral de Proteção de Dados para salvaguardar a privacidade quando a definição de perfis resulta no surgimento de dados pessoais sensíveis. Os dados sensíveis, que envolvem informações sobre a origem racial ou étnica, opiniões políticas, crenças religiosas, orientação sexual, entre outros aspectos íntimos, merecem uma proteção especial devido ao potencial de discriminação e violação da dignidade humana que podem resultar de seu tratamento inadequado.

Para aprofundar o estudo em questão, será adotada uma abordagem de pesquisa exploratória. Nesse sentido, os conhecimentos a serem trabalhados serão aprimorados e desenvolvidos por meio dos métodos dedutivo e dialético, assim como pelos procedimentos histórico, comparativo e estudo de caso. A pesquisa será embasada em fontes bibliográficas e documentais, que englobam tanto documentos de fontes primárias quanto secundárias, como livros, revistas, artigos científicos e documentos oficiais, como leis e provimentos.

Assim, no primeiro capítulo, serão explorados os conceitos e evolução histórica do direito à privacidade e do direito à proteção dos dados pessoais, bem como suas normativas de proteção. Serão analisadas as diferenças entre esses dois direitos fundamentais, assim como as limitações legítimas impostas ao direito à proteção dos dados pessoais, considerando as

ingerências justificadas à luz da Convenção Europeia sobre os Direitos Humanos e da Carta dos Direitos Fundamentais da União Europeia, bem como em face de outros direitos.

Já o segundo capítulo abordará o tratamento dos dados pessoais, explorando as bases legais para o seu processamento, incluindo o consentimento, o legítimo interesse e outras bases legais estabelecidas pela legislação. Serão apresentados os princípios fundamentais que regem o tratamento de dados pessoais, como a licitude, lealdade e transparência, a limitação das finalidades, a minimização dos dados, a exatidão, a conservação, a integridade e confidencialidade, bem como a responsabilidade. Além disso, será discutida a distinção entre o tratamento de dados pessoais automatizados e não automatizados.

No terceiro capítulo, o foco será na definição de perfis e nos dados pessoais sensíveis. Serão apresentados os benefícios e riscos associados à definição de perfis, destacando-se os mecanismos de tutela existentes para mitigar os seus efeitos negativos. Em relação aos dados pessoais sensíveis, serão exploradas sua definição e características, bem como os mecanismos de tutela específicos previstos nas legislações vigentes. Será dada ênfase ao consentimento qualificado como requisito essencial para o tratamento desses dados, assim como às demais hipóteses autorizativas.

Desta feita, após entendimento dos riscos associados à definição de perfis para a privacidade da pessoa humana, com ênfase na proteção dos dados pessoais sensíveis, bem como depois de feita a análise dos marcos normativos e as diferentes abordagens adotadas, demonstra-se como os atuais mecanismos de tutela de proteção de dados já consagrados pelos diplomas normativos atuais, no Brasil e na Europa, podem ser utilizados resguardar o direito fundamental à privacidade.

1. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O direito à privacidade e a proteção de dados pessoais, como restará demonstrado neste capítulo, apesar de apresentarem pontos de contato, não se confundem, havendo evidente diferenciação quanto sua regulamentação e âmbito de aplicabilidade das normas inerentes aos institutos.

Desta feita, será abordada nas próximas linhas, a origem e evolução da privacidade e da proteção dos dados pessoais, a diferença entre estes direitos e seu *status* atual no ordenamento jurídico português e brasileiro.

1.1. Do direito à privacidade: evolução histórica, conceito e proteção normativa

A ideia de vida privada está presente desde comunidades humanas primitivas, representando uma necessidade inerente a qualquer espécie. Neste ensejo, já foi observado que a maioria dos animais procuram, em algum momento, um período individual de reclusão ou limita sua vivência à pequenos grupos, havendo então uma verdadeira necessidade orgânica de espaço privado para sobrevivência[1].

No aspecto social humano, um conceito de vida privada também não é algo recente. É ululante que os seres humanos são gregários, depende das relações sociais para sobrevivência, pois é dentro de um ambiente social que desenvolve sua personalidade e costumes.[2] As primeiras discussões acerca da intimidade, ainda não como um direito, surgem na Antiguidade clássica, época na qual Aristóteles já diferenciava a esfera privada ("oikos"), encontrada no respeito à família, às questões económicas, e biológicas; da esfera pública ("polis"), traduzida no respeito à liberdade política dos cidadãos[3].

Contudo, conforme observa Diogo Leite Campos, durante um longo período a publicidade caracterizava a vida dos indivíduos, não havia de se falar em uma salvaguarda à privacidade, pois o direito só tutelava as violações mais graves da sociedade. Assim, defende que até o século XIX, "cada ser humano representava-se como um espaço aberto a todos os outros, solidário para com estes, comunicando incessantemente", razão pela qual o direito à uma vida privada era impensável neste período.[4]

---

[1] WESTIN, Alan F. – **Privacy and Freedom**, p. 8.
[2] VASCONCELOS, Pedro Pais de – **Direito de Personalidade**, p. 22.
[3] ARISTÓTELES – **Politique, I, II**, p. 30.
[4] CAMPOS, Diogo Leite – O Direito e os Direitos da Personalidade, p. 207-209.

Com efeito, a vida era pública, pois era inerente à sociedade o controle acerca do que se passava com cada um dos seus integrantes, fosse este um súdito, guerreiro ou até um soberano. A publicidade do comportamento era essencial em uma sociedade que moldava sua conduta no comportamento do próximo, razão pela qual, quanto maior era a posição do indivíduo, maior era também a divulgação dos seus comportamentos, para servir de exemplo e pautar a conduta das demais pessoas da sociedade.[5]

Mais a frente, com a crescente ideia de um individualismo, que tem como base as seitas cristãs reformadoras, onde se defendia a possibilidade de uma salvação singular, em detrimento de uma ascensão coletiva ao reino dos céus, é que o direito passa a tutelar uma liberdade negativa, a ser contraposta ao soberano e a terceiros, "cada homem segue seu caminho solitário".[6]

Neste momento, o indivíduo enxerga-se como um elemento independente da sociedade na qual convive, privatiza-se, de modo que o que faz ou deixa de fazer, o modo como se relaciona dentro do seu seio familiar, suas ideias, não dizem respeito aos demais membros da ordem social, denota-se uma esfera privada, protegida por um direito de exclusão.[7]

Assim, com o surgimento dos direitos da personalidade, também foi construído um conceito de privacidade como algo próprio do que era íntimo do agente, ou seja, seu círculo familiar e seu lar. Ademais, fazia também parte da definição da intimidade, "à esfera protegida ou à dimensão de ação e responsabilidade, em que os indivíduos podem agir dentro de um caminho que é independente das decisões e das influências da esfera pública, do Estado, das instituições, e da sociedade"[8].

Através da evolução da acepção da vida privada e intimidade, foi no Iluminismo, que se desenhou uma tutela da privacidade com definições mais condizentes com a noção atual, sendo-lhe outorgado um tratamento especial do direito. É neste momento que há uma mudança na percepção da pessoa humana e sua relação com a sociedade e o Estado. O indivíduo é visto como um sujeito detentor não só de deveres, mas também de direitos que pode contrapor aos seus pares e ao soberano, dentre estes direitos, destaca-se para o nosso estudo, a privacidade[9].

---

[5] CAMPOS, Diogo Leite – Lições de Direitos da Personalidade, p. 209.
[6] *Idem* – O Direito e os Direitos da Personalidade, p. 210.
[7] *Idem* – Lições de Direitos da Personalidade, p. 2011.
[8] CORREIA, Victor – **Sobre o direito à privacidade**, p. 2.
[9] CANCELIER, Mikhail Vieira de Lorenzi – **O Direito a Privacidade hoje: perspectiva histórica e o cenário brasileiro**, p. 2.

O paradigma europeu demonstrou a importância de cada pessoa como um ser único detendo de uma esfera de sua vida privada que merece proteção e resguardo contra interferências externas. Logo, admite-se que cada cidadão teria direito a algum grau de privacidade, sendo uma prerrogativa inerente ao homem o resguardo a exposição pública injustificada[10], tudo isto como verdadeiro corolário do direito de liberdade do indivíduo.

Estes primeiros passos se caracterizaram por um individualismo exacerbado do da privacidade, que se externava como a prerrogativa do sujeito de ser deixado só, sem sofrer a interferência do Estado e de terceiros em sua esfera privada. Tratava-se aqui do direito descrito por Brandeis e Warren como *the right to be alone*[11]. Este aspecto negativo de enxergar a privacidade, é considerado pela doutrina como o marco inicial para o estudo e compreensão do tema.

Uma das principais contribuições da doutrina de Brandeis e Warren foi vincular o desenvolvimento da personalidade individual a privacidade, afastando-se da concepção anterior que unia a vida privada a aspetos de proteção da propriedade. Neste ensejo, dentro da definição do direito de estar só resta compreendido os direitos dos indivíduos de terem respeitada sua intimidade frente a utilização tecnologia intrusivas, há época, máquinas fotográficas e artigos de jornais, que desde antigamente já devassavam a intimidade das pessoas públicas.

Destarte, as primeiras decisões judiciais que reconhecem a intimidade, reconhecem um direito à privacidade reservado apenas a garantia da intimidade das personalidades de grande relevo social, configurando o que Doneda, após narrar celebres casos da jurisprudência, alcunhou de "privacidade com caráter elitista"[12].

Há época, revelava-se que a defesa da intimidade dos indivíduos apenas seria digna da tutela do Estado nas hipóteses em que houvesse a defenestração dos segredos das celebridades e pessoas públicas. O homem médio e sua vida medíocre estariam fora do interesse da sociedade e, em razão disso, exilado também do resguardo jurídico fornecido pela privacidade em face das referidas tecnologias intrusivas.

Entretanto, com o aumento do fluxo, colheita e processamento dos dados, bem como em razão da mudança no paradigma da relação entre o indivíduo e o Estado, restou evidenciado que a tutela do direito à privacidade deveria se aplicar a todo e qualquer cidadão,

---

[10] FORTES, Vinicius – **O direito fundamental à privacidade: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil**, p. 98.

[11] *But if privacy is once recognized as a right entitled to legal protection, the interposition of the courts cannot depend on the particular nature of the injuries resulting*. WARREN, Samuel; BRANDEIS, Louis – **The right to privacy**, p. 14.

[12] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 8.

haja vista ser indissociável do direito fundamental de liberdade que detém toda pessoa humana.

Observou-se uma ampliação do campo de proteção da privacidade para todas as pessoas da sociedade. Agora, não apenas as figuras públicas poderiam ter sua intimidade violada, mas qualquer pessoa, resultando essas ingerências não quistas em temerários movimentos contra a liberdade dos indivíduos, principalmente em uma sociedade que coleta e trata informações de forma massiva[13]. A privacidade encontrava-se direcionada para uma dimensão individual e negativa, isto é, baseada em quais informações o indivíduo poderia esconder do conhecimento de terceiros.[14]

Contudo, esta inicial concepção negativa da privacidade (*right to be alone*) não mais atendia aos anseios sociais, não mais se afigurava como suficiente evitar as interferências externas na privacidade do cidadão, não era mais compatível com as provocações enfrentadas pela intimidade face o desenvolvimento de novas tecnologias.

Desta feita, em resposta as aspirações da sociedade, da necessidade do indivíduo de ter influência acerca das suas informações pessoais, desenvolveu-se uma face positiva do direito do direito à privacidade, a qual permite ao sujeito, além de titularizar os dados pessoais, controlar as informações lhe sejam atinentes[15]. Neste sentido, Rodotà ensina que à privacidade deixa de se estruturar em torno do fundamento 'pessoa-informação-segredo', ou seja, em uma noção que defendia apenas o impedimento das interferências na vida privada, passando também a se centrar no eixo 'pessoa-informação-circulação-controle." [16].

O paradigma histórico desta mudança é o julgamento realizado pelo Tribunal Constitucional Alemão, originalmente denominado "Volkszählungsurteil" (1983), em que foi considerada inconstitucional uma lei que determinava recenseamento geral da população e tinha por objeto a coleta de dados pessoais de todos os cidadãos. No caso em tela, reconhecendo-se uma cláusula geral de privacidade, alargou-se o conceito do instituto, através do reconhecimento do direito dos indivíduos de controlar seus dados e informações pessoais (autodeterminação informativa)[17].

Portanto, percebe-se dessa caminhada histórica, que a definição de privacidade não pode ser explicitada pelo legislador de maneira típica e fechada, mas configura-se em

[13] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 8.
[14] RODOTÀ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje**, p. 102.
[15] PILATI, Jose; OLIVO, Mikhail – **Um Novo Olhar sobre o Direito à Privacidade: caso Snowden e pós-modernidade jurídica**, p. 10.
[16] RODOTÀ, Stefano – ***Op. Cit.***, p. 102.
[17] FORTES, Vinicius – **O direito fundamental à privacidade: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil**, p. 133-134.

verdadeira cláusula geral, que terá seu conteúdo preenchido e modificado de acordo com os aspectos históricos, sociais e até geográficos, sendo que a conjuntura da sociedade é que irá delimitar um maior ou menor enfrentamento no que toca tutela deste instituto.

Apesar da impossibilidade de se traçar de maneira exaustiva um conceito do que é o direito à privacidade, doutrinariamente tem-se compreendido o instituto sob dois aspectos: (i) negativo, onde a privacidade é o direito do sujeito de se insurgir contra indevida interferência do Estado ou de terceiros na sua vida privada; (ii) positivo, que resulta no controle das informações de caráter pessoal, autorizando ou não a publicidade destes dados por terceiros[18].

Canotilho e Moreira ao tratar da privacidade optaram por dividi-la em direitos menores, inicialmente definindo-a como a faculdade de impedir estranhos de tomarem conhecimento acerca de informações da própria vida privada e familiar; e posteriormente, estabelecendo se tratar do direito que impede os dados pessoais de serem publicizados por estranhos[19].

O doutrinador Paulo Mota Pinto, ao conceituar a tutela à privacidade, aduz se tratar do interesse do sujeito em retirar-se da atenção alheia, limitando o acesso das informações a si próprio ou à regulando a publicidade de informações pessoais; bem como, traz a privacidade como o direito de se contrapor fundamentalmente ao interesse em conhecer e em divulgar informação própria e a ter acesso ou controlar os movimentos do indivíduo[20].

Já o ilustre José Afonso da Silva, define o direito à privacidade como o poder que detém o titular acerca do próprio conjunto de informações pessoais, restando ao sujeito do direito a decisão acerca da manutenção das informações pessoais sob seu exclusivo domínio, ou pela transferência temporária de tais dados a terceiros, definindo igualmente as condições e forma de publicidade[21].

Em razão do exposto, a privacidade pode ser conceituada como o poder do titular da informação de não permitir a ingerência do Estado ou de Particulares em sua esfera íntima, demandando uma conduta negativa de tais agentes no que se refere aos elementos mais pessoais da vida. Para além, consiste outrossim em um direito de titularidade e controle acerca da divulgação dos aspectos pessoais, ficando ao detentor de tais dados estabelecer, em condições de normalidade, os casos que irá permitir a divulgação de suas informações.

---

[18] PIRES, Lucas – **Direito à Privacidade no Âmbito da Sociedade da Informação: reflexões em torno da questão nos inícios do século XXI**, p. 32.
[19] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**, p. 467.
[20] PINTO, Paulo Mota – **O direito à reserva sobre a intimidade da vida privada**, p. 505.
[21] SILVA, José Afonso da – **Curso de direito constitucional positivo**, p. 206.

Voltando o estudo ao aspecto normativo, a privacidade é um direito humano de caráter supranacional, sendo objeto de diversas previsões neste sentido, merecendo destaque o assentado a previsão do art. 12º da Declaração Universal dos Direitos do Homem, adotada pela Organização das Nações Unidas (ONU), em 1948, onde se estabelece proteção legal para que não ocorram intromissões arbitrárias na vida privada.

Ainda no panorama normativa, apresenta-se a privacidade como um Direito Fundamental plenamente reconhecido por diversos diplomas, como fazem a Convenção Europeia dos Direitos Humanos, em seu artigo 8º; a Declaração Universal dos Direitos Humanos, em seu artigo 12º; a Constituição da República Portuguesa (CRP), no artigo 26º, '1'; e a Constituição da República Federativa do Brasil (CF/88), no artigo 5º, inciso X.

Para além, no arcabouço jurídico português, o direito à privacidade é expressamente listado como um direito da personalidade pelo Código Civil, havendo previsão no art. 80.º, nos termos que segue: "1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem. 2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas". Percebe-se que o código substantivo luso ao positivar o direito à privacidade como um direito da personalidade, não faz alusão expressa ao termo "privacidade", mas sim, trata acerca do direito à "intimidade da vida privada".

As referidas alcunhas não se sinônimos, sendo a privacidade um gênero do qual fazem parte a intimidade e a vida privada. Logo, não foi a esmo a opção de texto normativo feita pelo legislador quando da edição do Código Civil[22]. O precitado entendimento é corroborado por Cabral, a qual destaca ser necessário diferenciar o que de fato seria íntimo, daquilo que na verdade não se constitui propriamente em um segredo[23].

Assim, a intimidade consiste em sentimentos, comportamentos, segredos que o indivíduo guarda apenas para si, ou tão somente compartilha com pessoas do seu círculo de confiança, não sendo na maioria das vezes visível ou perceptível para estranhos ou até pessoas do convívio social, trata-se de questões ligadas a afetividade, saúde, sexualidade, fatos do passado, por exemplo, que apenas os mais íntimos compartilham, as vezes, nem mesmo estes[24]. Por outro lado, a vida privada, detém um escopo mais amplo, traduzindo-se em aspectos pessoais do agente que são de conhecimento por aqueles do seu convívio, trata-se de

[22] Em sentido contrário ao aqui exposto, Pinto, Canotilho e Moreira sustentam que o legislador português não diferenciou as esferas da vida privada e da intimidade. PINTO, Paulo Mota – **A Protecção da Vida Privada e a Constituição**, p. 162-163. CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**, p. 468.
[23] CABRAL, Rita Amaral – **O direito à intimidade da vida privada: breve reflexão acerca do art. 8.º do Código Civil. Separata dos Estudos em memória do Prof. Doutor Paulo Cunha**, p. 25.
[24] PIRES, Lucas – **Direito à Privacidade no Âmbito da Sociedade da Informação: reflexões em torno da questão nos inícios do século XXI**, p. 44-45.

informações como, o estado civil, trabalhos desempenhados, escolaridade, time de futebol favorito, são dados que apesar de pessoais não invadem a intimidade do agente[25].

Corroborando com o exposto, Vieira de forma sucinta expõe que, enquanto a intimidade é mais "fechada", tendo o condão de trazer a luz os pensamentos do indivíduo, suas ideias e emoções, sendo assim algo mais restrito da pessoa, àquilo que deseja manter em sigilo por revelar suas convicções e desejos mais íntimo; a vida privada é mais "aberta", caracterizada pelas ocorrências do convívio pessoal e familiar, o que pode ser de ciência daqueles que desfrutam de sua convivência, mesmo sem qualquer exteriorização pelo sujeito.[26]

Em comum, os aspectos da intimidade e da vida privada, se apresentam como espécies da cláusula geral do direito à privacidade, dizendo respeito as informações e dados que já são de conhecimento do sujeito, porém que este prefere manter reservado para si ou deseja compartilhar apenas com pessoas do seu círculo social. Plenamente justificável esta ampla tutela de proteção reconhecida à privacidade, haja ser esta é essencial para o desenvolvimento da personalidade e da própria dignidade da pessoa humana. O direito à privacidade está entrelaçado ao direito de liberdade, ambos se apresentam como um elemento indispensável na formação da própria personalidade e autodeterminação dos indivíduos. Ora, somente um sujeito detentor de uma esfera inviolável de intimidade tem o condão de agir com liberdade, ou seja, a privacidade apresenta-se então como pré-requisito para diversas outras liberdades fundamentais formadoras da própria personalidade, como a liberdade sexual, de expressão e religião[27].

Ocorre que, dentro de um contexto em que os indivíduos se encontram cada vez mais demandados a entregar uma grande quantidade de informações em troca de serviços ou produtos fornecidos por agentes públicos e privados, verificou-se uma falta de controle sobre a coleta, circulação e tratamento dos dados pessoais. Nessa esteira, como forma de salvaguardar as informações pessoais exsurge uma nova arquitetura de proteção aos dados pessoais, que será objeto de estudo nas linhas seguintes.

---

[25] PIRES, Lucas – **Direito à Privacidade no Âmbito da Sociedade da Informação: reflexões em torno da questão nos inícios do século XXI**, p. 44-45.
[26] VIEIRA, Tatiana Malta – **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**, p. 28.
[27] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 7.

1.2. Do direito à proteção dos dados pessoais: evolução histórica, conceito e proteção normativa

Passados esses apontamentos iniciais, onde se traçou um panorama histórico acerca do direito à privacidade, bem como sua evolução como direito, para encerrar trazendo uma definição e parte de seu arcabouço legislativo, faz-se necessário traçar um panorama acerca do surgimento e positivação da proteção dos dados pessoais.

De início, cumpre destacar que enquanto ocorriam as discussões acerca da regulamentação ou não de determinadas condutas perpetradas pelos governos, empresas e cidadãos, a coleta e processamento das informações pessoais evoluía, havendo um aumento significativo na quantidade de dados armazenados e uma enorme evolução nos mecanismos de tratamento, toda essa mutação avançava sem que houvesse sido estabelecido o arcabouço jurídico necessário para pacificação social.

Nesse ínterim, destaca Bobbio, que a constante evolução da tecnologia, mais precisamente no ramo das telecomunicações, resultava em transformações tão relevantes na vida, organização e relações sociais dos indivíduos, que nasciam situações típicas resultando em novas demandas de liberdade e de poderes demandando uma positivação.[28] Já Rodotà, verifica que hodiernamente se observa um distanciamento entre a velocidade da inovação e a regulação de novas matérias, provocando uma rápida obsolescência das previsões normativas que tem como escopo regular a um único dado ou problema.[29] Finalmente, Giannotti advoga que esta tardança em regular os fatores sociais indicou uma inversão de valores, pois foram os fatos que desenharam o dever ser.[30]

Para o Grupo de Trabalho 29, a proteção de dados pessoais evoluiu do direito a privacidade, previsto no art. 8º da Convenção Europeia Sobre Direitos Humanos, haja vista que o aumento das novas tecnologias e das novas formas de vigilância, tanto no setor público quanto no privado, configurou a necessidade de uma proteção adicional para os indivíduos contra terceiros (particularmente o Estado) quando diante da manipulação dos seus dados pessoais.[31]

Portanto, com o fito de evitar a dominação do Direito pelas tecnologias e arquiteturas de rede, percebeu-se a necessidade de se estabelecer diretrizes éticas para embasar e

[28] BOBBIO, Norberto – **A Era dos Direitos**, p. 53.
[29] RODOTÀ, Stefano – **A vida na sociedade de vigilância: A privacidade hoje**, p. 42.
[30] GIANNOTTI, Edoardo – **A tutela constitucional da intimidade**, p. 17.
[31] 29 DATA PROTECTION WORKING PARTY – Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, p. 3.

direcionar o processamento dos dados pessoais, assim, como resposta aos anseios da sociedade, o direito procurando o controle jurídico da revolução tecnológica que se observava, principalmente, com o surgimento da internet, da coleta e tratamento massivo de dados, passou a positivar a autodeterminação informativa por intermédio de leis de proteção de dados, que parcela da doutrina divide em quatro gerações[32].

No que se refere a primeira geração, Rodotà aduz que o escopo das leis estava em obtemperar às ansiedades sobre abusos da intimidade individual que surgiram em razão dos avanços da tecnologia.[33] São exemplos desta geração normativa, a Lei de Dados da Suécia (1973), o *Privacy Act* Norte-americano de 1974 e a Lei Federal de Proteção de Dados da Alemanha (1977)". Segundo Doneda, a característica marcante dessas normas é o estabelecimento de princípios de proteção amplos focado primordialmente no processamento de dados.[34] No mais, o Estado era o principal destinatário da regulamentação, pois já era comum se utilizar de grandes bancos de dados, normalmente extraído de censos realizados pelos entes estatais, para obter informações sobre os indivíduos[35].

A geração primeva tornou-se antiquada, pois o avanço tecnológico no tratamento de dados deixou de ser apenas estatal, sendo feito também por entes privados. Esse cenário ensejou a segunda geração de leis que, ciente da maior automatização da coleta e processamento de dados também por agentes privados, eleva os direitos de consentimento e liberdade de escolha do titular das informações como princípios fundamentais a proteção dos dados pessoais[36].

Como clara evolução das leis até então existentes, a terceira geração apresenta como escopo uma proteção maior ao direito à privacidade, abrangendo não somente a liberdade de ceder ou não os dados, mas sim uma preocupação legítima de garantia da eficácia a proteção da vida privada dos indivíduos. A ingerência do titular dos dados pessoais é ampliada para todas as fases (da coleta ao processamento), firmando-se as normas no princípio da autodeterminação informativa. Conforme Doneda, a tutela da informação passa por um processo mais complexo que o mero consentimento, prevendo faculdades para a efetiva participação do agente dentro do contexto no qual lhe é requerido os seus dados, inclusive,

---

[32] BIONI, Bruno Ricardo – **Proteção de dados pessoais: a função e os limites do consentimento**, p. 113-117.
[33] RODOTÀ, Stefano – **A vida na sociedade de vigilância: A privacidade hoje**, p. 49.
[34] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 208.
[35] LUGATI, Lys Nunes; DE ALMEIDA, Juliana Evangelista – **Da Evolução das Legislações sobre a Proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**, p. 4.
[36] BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo – Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso, p. 13.

prevendo e regulando hipóteses em que a liberdade de concessão dos dados é cerceada, estabelecendo para estes casos um maior controle do titular dos dados.[37]

Todavia, a terceira geração tinha como principal objetivo tutelar direitos individuais dos titulares dos dados pessoais, mostrando-se rapidamente como uma camada de proteção insuficiente para resguardo da proteção das informações.[38] Assim, foi natural o surgimento de uma quarta geração de normas de abrigo, vigente até hoje.

Atualmente, o quarto ciclo estende seu escopo para além do controle individual dos dados, tendo como incipiente uma tutela difusa, buscando proteger a coletividade de tratamentos de dados frente a imparável evolução tecnológica. Neste ponto, se criou mecanismos que visam um padrão coletivo de proteção, reconhecendo o evidente desiquilíbrio que existe entre o titular dos dados pessoais e o controlador destas informações. Desta maneira, se positivou métodos de restrição dos usos de dados sensíveis, se elevou o direito ao acesso como instituto fundamental na proteção de dados, exsurgindo obrigações de transparência a serem observadas pelo poder público e pelas instituições privadas que coletam e processam informações.[39]

Na precitada quarta geração, as regras nacionais sobre proteção de dados são suplementadas por regramentos setoriais, como o Regulamento Geral sobre Proteção de Dados que entrou em vigor em 2018. O desenvolvimento destas normas protetivas busca evoluir no mesmo passo das potências de processamento de dados atuais, adotando, para isto conceitos jurídicos indeterminados, consagrando normas de maneira aberta, para que possa o intérprete e aplicar do direito adaptar as novas tecnologias as previsões normativas já estabelecidas.[40]

Passada esta evolução histórica e todas as gerações de normas que buscam a proteção dos dados pessoais, percebe-se que houve uma ampliação da tutela e por consequência do conceito do direito a proteção dos dados pessoais. Hoje é possível conceituar o instituto como um direito fundamental dos indivíduos de controlar suas informações pessoais e decidir como terceiros, sejam organizações ou governos, as coletam, usam, armazenam e compartilham.

---

[37] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 97.
[38] LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de – **Da Evolução das Legislações sobre a Proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**, p. 6.
[39] BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo – Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso, p. 14.
[40] CAMURÇA, Lia Carolina Vasconcelos – **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário**, p. 148.

Quanto a proteção normativa, conforme os ensinamentos de Menezes, as fontes do direito de proteção de dados na Europa, podem ser classificadas como: paraconstitucionais, legislativas e infralegislativas.[41]

Como fonte paraconstitucional primordial tem-se a Carta dos Direitos Fundamentais da União Europeia, que em seu artigo 8º estabelece as diretrizes e princípios (como a licitude, lealdade e limitação das finalidades) que irradiam sobre todo arcabouço legislativo atinente a matéria, elevando a proteção dos dados pessoais ao status de direito fundamental e universal. Para além, ressalta o consentimento como premissa para o tratamento de dados pessoais e determina a criação de um órgão independente de fiscalização.[42] Ainda no âmbito europeu, diversas são as fontes legislativas, sendo merecedoras de destaque o Regulamento (UE), 2018/1807; o Regulamento (UE) 2018/1725; Regulamento da (UE) nº 611/2013 e a Diretriz (UE) 2016/680 do Parlamento Europeu e do Conselho. Enfim, no que toca as fontes infralegislativas, estas decorrem das recomendações, diretrizes e melhores práticas emanadas do Comite Europeu para a Proteção de Dados, conforme previsto no art. 70 do RGPD.

No que tange as fontes do direito português, a regulamentação da proteção dos dados pessoais encontra-se consagrada na Constituição, onde no art. 35º, desde sua origem, já contemplava o direito dos cidadãos a retificação e atualização dos dados, tendo após alterações alargado ainda esta tutela. Em escala infraconstitucional, apresentam-se atualmente como fontes ordinárias a Lei de Execução do RGPD, as Leis 59/2019, Lei 41/2014, Lei 12/2005, Lei 26/2016 e a Lei 1/2005. Por fim, como fontes infralegislativa, cabe apontar a atuação da Comissão Nacional da Proteção de Dados, através da produção de pareceres, orientações e recomendações genéricas.[43]

Dentro do ordenamento jurídico brasileiro, a Constituição Federal, após a emenda constitucional 115/2022, passou a assegurar a proteção dos dados pessoais, inclusive nos meios digitais, listando o referido instituto dentro dos direitos fundamentais das pessoas. Em esfera infraconstitucional, antes da emenda a Constituição, já era possível se observar alguns passos na proteção dos dados pessoais. Inicialmente, com o Código de Defesa do Consumidor, diploma que estabelece a proteção dada ao titular dos dados frente a bancos de dados e cadastros, em seu artigo 43. Posteriormente, em 2011, através da Lei 12.414/2011, consagrou-se a concepção da autodeterminação informativa, ao fincar o prévio consentimento do titular dos dados para o compartilhamento e processamento das informações. Mais à

[41] CORDEIRO, António Barreto Menezes – **Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019**, p. 68.
[42] LEITE, Beatriz da Costa Gomes – **Proteção de dados e privacidade em linha**, p. 19.
[43] *Idem* – ***Op. Cit.***, p. 21.

frente, o através do Marco Civil da Internet (Lei 12.965/2014), buscou-se regulamentar o uso da rede mundial de computadores, prevendo prerrogativas ao cidadão nas relações travadas no meio virtual. Contudo, o ordenamento jurídico brasileiro ainda necessitava de lei que tutelasse diretamente a proteção de dados, o que só veio a ocorrer no ano de 2018, através da Lei de Proteção de Dados (Lei 13709/2018).[44]

1.3. Diferenças entre o direito à privacidade e a proteção aos dados pessoais

Conforme tecido nas linhas iniciais, o conceito de privacidade traz consigo uma carga negativa, uma garantia de não ingerência (ou opacidade) em questões ligadas a vida privada do indivíduo. A privacidade, nesta concepção negativa, protege o indivíduo contra interferências em sua intimidade, seja em razão de condutas perpetradas pelo governo ou por um agente privado. Consiste, então, em um direito fundamental com viés de limitação de poderes.[45]

Para doutrina mais abalizada, em sua concepção positiva, a privacidade é o direito que permite ao agente ser livre, ser quem é, é o direito que possibilita ao cidadão ter suas escolhas a respeito de sexualidade, saúde e comportamento, respeitadas e mantidas dentro de sua esfera privada, sem ingerências estatais ou de entidades privadas. Corroborando com o exposto, De Hert e Gutwirth trazem a ideia de que o cidadão ao ser observado, ao ter sua privacidade dilacerada, não se comporta livremente, sendo incapaz de fazer suas mais íntimas escolha ou se o fizer, terá o risco de violar normas sociais e aceitar o risco de sua conduta. Trata-se do papel da privacidade na construção da personalidade do agente.[46]

Em outras palavras, a tutela da privacidade se inicia com o direito de ser deixado só (*right to be left alone*), passando para uma salvaguarda contra eventuais abusos perpetrados pelos Governos e outras instituições diante da possibilidade de ingerência na vida privada do sujeito. Logo, verifica-se um direito de abstenção geral de intromissões na intimidade do titular da informação.

Assim, apesar de consagrada como um direito fundamental, características de individualismo permeiam a privacidade. Não poderia se esperar nada diferente, até pelo seu potencial de evidenciar as individualidades do titular do direito. Aliás são estas

---

[44] LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de – **Da Evolução das Legislações sobre a Proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**, p. 12.
[45] GUTWIRTH, Serge; DE HERT, Paul – **Privacy, data protection and law enforcement. Opacity of the individual and transparency of power**, p. 83.
[46] *Ibidem*.

individualidades, permanentemente ameaçadas em razão do potencial crescimento do fluxo de informações, que iluminam um outro aspecto do caráter da privacidade: a importância para a própria sociedade democrática como pré-requisito para diversas outras liberdades fundamentais.[47]

Desta feita, a privacidade se apresenta como o direito do cidadão de ter seus comportamentos e pensamentos íntimos opacos diante do mar de informações que é navegado por agentes públicos e privados, constituindo verdadeiro véu que cobre e esconde a vida privada de ingerências não quistas, sendo negativo na concepção de que não admite interferências e positivo na ideia de possibilitar ao titular do direito ser quem o deseja ser, sem que se sinta vigiado ou controlado.

Em reflexão acerca da noção atual do direito à privacidade, Rodotà aduz que o conceito inicial, qual seja, o direito a ser deixado só cede o lugar à faculdade de manter controle sobre os dados pessoais, de modo que larga-se o sigilo e procura-se o controle sobre as informações pessoais. Afora isso, sustenta que a busca pela privacidade se confunde com a busca a autodeterminação informativa, passando o direito em cotejo a servir como uma salvaguarda de não-discriminação.[48] Nestas linhas, já é possível observar que dentro desse novo contexto há na verdade o descolamento dos elementos da privacidade para constituição de um novo direito fundamental, o da proteção dos dados pessoais.

Contudo, diferente da privacidade, a proteção dos dados pessoais não é proibitiva, não busca mascarar informações ou dados do seu titular, mas sim dar controle ao indivíduo sobre todas as etapas de manejo dos seus dados, da coleta ao processamento final. A circulação dos dados não pode ser negado, pois em uma sociedade da informação é natural que tanto Estados, quanto agente privados, se utilizem dos elementos coletados para pautarem suas políticas públicas ou ações de mercado.

Assim, o principal objetivo da proteção dos dados pessoais consiste em consagrar uma arquitetura de controle para resguardar a privacidade dos cidadãos (quando for este o caso) e trazer mecanismos de responsabilização dos agentes que realizam o tratamentos das informações que são coletadas.[49] A tutela dos dados pessoais se configura como um direito do titular de obstar o processamento e coleta indiscriminado e/ou não desejado, ao mesmo tempo promovendo um arcabouço legal que traz responsabilidade civil para aqueles que agem em contrário as disposições legais ou sem o consentimento na coleta e tratamento dos dados.

---

[47] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 91.
[48] RODOTÀ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje**, p. 102.
[49] GUTWIRTH, Serge; DE HERT, Paul – **Privacy, data protection and law enforcement. Opacity of the individual and transparency of power**, p. 93.

Percebe-se que a busca do legislador é pela transparência dos processos em que informações pessoais serão tratadas, e não em empregar uma opacidade como ocorre quando positivadas normas a respeito da vida privada e intimidade. Enquanto a privacidade é regulamentada com escopo de afastar a intrusão dos agentes públicos e privados na esfera íntima do cidadão, a proteção de dados trabalha com a premissa de que o tratamento de dados não só é possível, mas necessário, contudo, precisa ser regulado para evitar abusos que podem findar por violar outros direitos, como a autonomia da vontade, a liberdade e a própria privacidade do titular das informações.

No panorama atual do mercado, é inevitável que haja tratamento dos dados, portanto, impossível regulamentar essas condutas apenas pelo viés da privacidade, que findaria por proibir todo e qualquer processamento, inclusive nas hipóteses em que não houvesse uma efetiva violação a privacidade do sujeito. Ora, em razão da insuficiência da privacidade e de outros institutos para a regulamentar o processamento das informações pessoais, é natural que haja uma autonomização do direito a proteção dos dados pessoais, que por necessário a manutenção das operações financeiras e governamentais na sociedade atual, elevou-se a um direito fundamental autônomo para resguarda o cidadão do tratamento não autorizado.

Doutrinariamente, os autores têm se dividido em três correntes que discorrem acerca da relação entre a proteção dos dados pessoais e a privacidade.

Para a primeira linha de pensamento, a privacidade seria o gênero do qual decorreria a espécie proteção de dados pessoais. A tutela dos dados pessoais seria o estágio atual de evolução do direito à privacidade e apenas um dos instrumentos para resguardo da vida privada, no sentido de possibilitar o controle informacional. É conceito da privacidade informacional, adotado majoritariamente nos Estados unidos, onde não há uma separação entre privacidade e proteção de dados.[50]

De outra linha, há posicionamentos que defendem a privacidade e a proteção de dados como institutos distintos, mas complementares, que atuam de maneira conjunta para a proteção da dignidade da pessoa humana. Aqui firma-se uma ideia de autodeterminação informativa, no sentido que os referidos direitos quando garantidos possibilitam o desenvolvimento e autonomia dos indivíduos.[51]

Já a última corrente, que prevalece no cenário jurídico europeu, consagra a tutela dos dados como um direito autônomo com múltiplas funções, não se limitando apenas a tutela da

[50] SCHWARTZ, Paul – **The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. The American Journal of Comparative Law**, p. 686.
[51] MENDES, Laura Schertel – **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**, p. 34.

privacidade. Nesta senda, mesmo se adotando uma acepção ampla de privacidade, o atual cenário do processamento de dados e sua respectiva regulação, como as regras que dispõe da transferência de dados entre países ou a segurança da informação, não estariam abrangidos pelo escopo da opacidade que caracteriza o referido direito. Assim, é natural a existência de um direito autônomo que sirva além dos interesses da dignidade da pessoa humana, também para regulamentar os interesses econômicos ligados ao tratamento dos dados pessoais, buscando garantir um desenvolvimento econômico sustentável. Aliás, para o Grupo de Trabalho 29, a autonomia do direito a proteção dos dados pessoais foi reconhecida como um direito separado pela primeira vez na Convenção do Conselho da Europa para a proteção de indivíduos no que diz respeito ao tratamento automatizado de dados pessoais (Convenção 108), que também constituiu uma importante fonte de inspiração na Diretiva 95/46/CE.[52]

Então, os argumentos de que a proteção de dados surgiu inicialmente da concepção positiva da privacidade[53] (baseando-se principalmente na autodeterminação informativa), confundindo-se com este direito e sendo apenas um desdobramento deste, não se sustentam. No ordenamento jurídico brasileiro e português, aliás, referidos institutos encontram-se atualmente positivados de maneira separada dentro das respectivas cartas magnas, logo, constitucionalmente já se reconhece a autonomia destes direitos.

Com efeito, dentro do contexto das normas que restaram positivadas ao longo dos anos, é plenamente possível se verificar uma autonomização da proteção de dados pessoais, de modo que apenas parcela do que se é protegido teria também o escopo da privacidade (mais precisamente quando falamos de dados pessoais sensíveis), servindo a tutela das informações pessoais também para salvaguardar outros direitos e, como aqui já dito, principalmente a transparência e controle sobre a circulação dos dados pessoais.

Neste sentido, Dias dispõe que "o direito à reserva sobre a intimidade da privada e o direito à proteção de dados pessoais distinguem-se na sua formulação e alcance porquanto o primeiro consiste numa proibição genérica de ingerência que apenas poderá ser legitimada por critérios de interesse geral superior (sempre sujeitos a ponderação), e o segundo num mecanismo de segurança e proteção para o titular dos dados sempre que estes sejam objeto de tratamento, considerando-se um direito moderno e dinâmico".[54]

---

[52] 29 DATA PROTECTION WORKING PARTY – Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, p. 3.
[53] RODOTÀ, Stefano – **A vida na sociedade de vigilância: a privacidade hoje**, p. 15.
[54] DIAS, Patrícia Cardoso – **Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública**, p. 4.

Diante do exposto, estabelecida a evolução histórica, o conceito, o sistema normativo e as diferenças entre o direito a privacidade e a proteção de dados pessoais, no capítulo seguinte iremos abordar uma das questões mais relevantes no âmbito dos direitos fundamentais: o das suas limitações.

1.4. Limitações ao direito à proteção de dados pessoais

Como exposto, a proteção aos dados pessoais é direito fundamental e autônomo já plenamente reconhecido nesses termos pela CRP e pela CF/88. Contudo, é comezinho que os direitos fundamentais não são ilimitados ou ilimitáveis.

Aliás, na vida em sociedade, limitar os direitos fundamentais é um dos modos de proteger os outros direitos fundamentais de terceiros ou de garantir outros bens jurídicos relevantes, como a segurança pública e o interesse público. Com efeito, os direitos devem ser organizados em uma existência harmoniosa com o intuito de que nenhuma garantia ou direito possa ser reconhecido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros".[55]

Deste modo, não obstante serem os direitos fundamentais universais e inalienáveis, da sua interdependência e em razão do contexto em que são aplicados, decorre a necessidade de estabelecer limites.[56]

Nos tópicos seguintes serão estudadas de forma sucinta essas limitações, discorrendo acerca das ingerências previstas na CEDH, as limitações previstas na CDFU e, finalmente, as limitações lícitas em face de outros direitos.

1.4.1. Ingerências justificadas à luz da Convenção Europeia sobre os Direitos Humanos

A Convenção Europeia Sobre os Direitos Humanos (CEDH) prevê em seu artigo 8º, 1, que qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. Portanto, o direito a privacidade resta expressamente consagrado no referido diploma e reconhecido assim como um direito humano.

Importante destacar, que não há no referido instrumento normativo menção expressa à proteção aos dados pessoais, contudo, o TEDH emprega um conceito elástico de privacidade

[55] SUPREMO TRIBUNAL FEDERAL – **Acórdão proferido n.º MS 23.452**, [em linha].
[56] NOVAIS, Jorge Reis – **As restrições aos direitos fundamentais não expressamente autorizadas pela constituição**, p. 193.

para, quando possível e principalmente diante de dados sensíveis, abarcar também a proteção aos dados pessoais, como aconteceu nos casos Leander v Sweden (1987), Amann v Switzerland (2000), Rotaru v Romania (2000), Copland v United Kingdom (2007) e Wieser and Bicos Beteiligungen GmbH v Austria (2007), demostrando que a privacidade é um conceito mais vasto do que parece.[57]

Contudo, e não podia ser diferente, não se trata de um direito absoluto, razão pela qual o art. 8º, 2 da CEDH estabelece expressamente as hipóteses em que é admitida ingerência da autoridade pública sobre a vida privada, ou seja, casos em que será afastado o véu que cobre a vida privada e poderão ser publicizados aspectos íntimos do indivíduo.

Assim, a própria convenção estabelece que poderá haver ingerências na vida privada quando estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

O TEDH por vezes é chamado a identificar se houve ou não violação ao direito à privacidade e se esta ingerência observou ou não os pressupostos contidos no art. 8º, 2, da Convenção, neste casos o Tribunal analisa, de início, se houve violação da vida privada ou familiar; posteriormente, se tal limitação estava legalmente autorizada por norma habilitante do local em que foi praticada; e, por último, se há proporcionalidade na medida, ou seja, se foi razoável a ingerência para satisfazer uma necessidade social ou democrática.[58]

Desta feita, importante ter a noção dos elementos indicados no art. 8º, 2 da Convenção para verificar se a ingerência realizada estaria conforme ou não. Nesse diapasão, o Manual da Legislação Europeia sobre Proteção de Dados e o Grupo de Trabalho 29, ao interpretar o referido dispositivo, aduzem que as hipóteses trazidas são cumulativas e se resumem em: (i) conformidade com a lei; (ii) legítimo interesse e (iii) necessidades de uma sociedade democrática.[59,60]

No que toca a primeira condição, conformidade com a lei, para que seja possível limitação ao direito fundamental de privacidade, a medida deve além de estar legalmente prevista no ordenamento jurídico, ser também compatível com o Estado de Direito, com fulcro no disposto no Preâmbulo da Convenção, que orienta os objetivos e propósitos do

[57] MENDES, Paulo de Sousa – **A privacidade digital posta à prova no processo penal**, p. 227.
[58] *Idem* – ***Op. Cit.,*** p. 228.
[59] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data Protection Law**, p. 37.
[60] 29 DATA PROTECTION WORKING PARTY – Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, p. 5.

precitado artigo 8º. No mais, na hipótese de limitações a direitos por meio da lei, o ato normativo deve prever regulamentações específicas e abrangentes que recaiam sobre os aspectos essenciais das restrições, excluindo assim a possibilidade de regulamentos independentes ou autônomos.[61]

Quanto ao tema, o Tribunal Europeu de Direitos Humanos (TEDH) em diversas hipóteses analisou as limitações legais impostas pelos Estados Membros com relação ao direito à privacidade, estabelecendo alguns parâmetros a serem observados pela Autoridade Pública, vejamos alguns desses julgados abaixo.

No caso S. and Marper v. the United Kingdom, julgado pela Corte Europeia, decidiu-se que as leis de restrição devem ser previstas de maneira claras e detalhadas, bem como devem prever garantias mínimas destacando, entre outras coisas, à duração, armazenamento, uso, acesso de terceiros, procedimentos para preservar a integridade e confidencialidade dos dados e procedimentos para sua destruição, fornecendo assim garantias suficientes contra o risco de abuso e arbitrariedade.[62]

Já no caso Kopp v. Switzerland, firmou-se o entendimento de que a expressão "em conformidade com a lei", prevista no Artigo 8º, 2, exige, em primeiro lugar, que a medida impugnada tenha base na legislação nacional; tratando também da qualidade da lei em questão, exigindo que a legislação nacional deve ser suficientemente clara em seus termos para fornecer aos cidadãos uma indicação adequada sobre as circunstâncias e as condições sob as quais as autoridades públicas têm o poder de recorrer a tais medidas.[63]

Em uma interpretação sistemática dos julgados acima, é possível apontar que não basta a edição de uma lei para que se permita a ingerência sobre o direito à privacidade. A lei deve ser acessível e previsível, ou seja, formulada com precisão suficiente para permitir que o indivíduo, se necessário com aconselhamento apropriado, regule sua conduta. Para que a lei interna atenda a esses requisitos, ela deve fornecer proteção jurídica adequada contra arbitrariedade e indicar com clareza suficiente a extensão da discricionariedade conferida às autoridades competentes e a maneira de exercê-la. Além disse, as informações coletadas não

---

[61] CANOTILHO, José Joaquim Gomes – **Direito Constitucional e Teoria da Constituição**, p. 1278.

[62] CONSEIL DEL'EUROPE – **S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 8 December 2008**, [em linha].

[63] No mesmo sentido, conforme citação contida no caso Kopp v. Switzeland, vários julgados adotaram o exposto: "Kruslin v. France, 24 April 1990, § 27, Series A no. 176-A; Huvig v. France, 24 April 1990, § 26, Series A no. 176-B; Lambert v. France, 24 August 1998, § 23, Reports of Judgments and Decisions 1998-V; Perry v. the United Kingdom, no. 63737/00, § 45, ECHR 2003-IX (extracts); Dumitru Popescu v. Romania (no. 2), no. 71525/01, § 61, 26 April 2007; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, § 71, 28 June 2007; Liberty and Others v. the United Kingdom, no. 58243/00, § 59, 1 July 2008).".

poderiam ser armazenadas de forma perene, deve haver uma temporalidade da retenção dessas informações e seu uso apenas para aquilo no que foi proposto no dispositivo legal.

Quanto ao segundo requisito, o legítimo interesse, consiste na salvaguarda dos interesses públicos ou dos direitos e liberdades de outras pessoas. De acordo com o art. 8, 2, da Convenção, haverá legítimo interesse nas seguintes hipóteses: os interesses da segurança nacional, a segurança pública ou o bem-estar econômico de um país, a prevenção de distúrbios ou crimes, a proteção da saúde ou moralidade.[64]

Nestes casos, não se analisa uma medida legislativa restritiva, mas sim é feita uma ponderação entre o direito à privacidade que está sendo restringido e o legítimo interesse que no caso concreto justificou a restrição.[65] Por exemplo, no caso Sérvulo v Portugal (2015), que envolvia buscas por documentos em escritórios de advocacia e apreensão de ficheiros e dados nos computadores da sociedade, o TEDH considerou que a ingerência na privacidade visava um fim legítimo, pois autorizadas no âmbito de um inquérito relativo à prática de crimes de corrupção, participação económica em negócio, branqueamento e prevaricação e, por conseguinte, tinham em vista a repressão de infrações penais.[66] Fez-se uma ponderação entre o direito de sigilo/privacidade das informações que estavam guardadas e o interesse da segurança pública de combater os delitos em cotejo e, diante deste aparente conflito, afastou-se episodicamente o direito da privacidade para permitir a investigação e persecução dos criminosos no caso em cotejo.

Finalmente, no que toca as necessidades de uma sociedade democrática, trata-se de elemento que caminha muito próximo ao legítimo interesse. No caso, o vocábulo "necessidade" já foi discutido em diversos julgados do TEDH[67], tendo se decidido que necessidade não significa indispensabilidade, ou seja, que se trata da única medida possível, contudo, tampouco a ingerência não pode ser utilizada de forma ordinária e corriqueira, deve limitação corresponder a um imperativo social premente e, em particular, que seja proporcional ao objetivo legítimo buscado. Se examina a restrição para verificar se esta é justificada em razão de relevante interesse social e mais, se a limitação ainda foi adequada, ou seja, se não passou dos limites da razoabilidade.

Para isso, o Grupo de Trabalho 29 estabeleceu que, inicialmente deve-se identificar qual o tipo específico de problema ou delito, posteriormente, deve ser estabelecido a

[64] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data Protection Law**, p. 39.
[65] MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**, p. 376.
[66] MENDES, Paulo de Sousa – **A privacidade digital posta à prova no processo penal**, p. 230.
[67] Por exemplo, Gillow v. The United Kingdom, Leander v. Sweden, Handyside v. United Kingdom.

gravidade do problema (como afetam a sociedade) e as evidências que suportam este posicionamento. Estabelecida a necessidade da limitação ao direito à privacidade, nos termos acima, deve se levar em conta o tempo, isto é, deve-se ponderar se as medidas a serem tomadas são proporcionais e ainda relevantes em razão do período que decorreu o problema, e mais, se forem relevantes, por quanto tempo irá durar a ingerência, que igualmente não podem ser mantidas por um tempo desarrazoado quando comparado com a justificativa inicialmente apresentada.[68]

A título exemplificativo, se uma autoridade de segurança pública deseja realizar uma vigilância eletrônica em uma área pública para prevenir atos de terrorismo, essa atividade está sendo realizada em busca de um objetivo legítimo, ou seja, a prevenção de crimes graves. É evidenciado que há um interesso social a ser atendido, contudo, não pode essa vigilância se estender de forma perene, tampouco, podem os dados que foram coletados, caso não se demonstre a razão, serem armazenados de forma eterna, sob pena de ser considerada uma interferência indevida nos direitos de privacidade, como definido no Artigo 8(2) da Convenção Europeia dos Direitos do Homem.

1.4.2. Limitações lícitas à luz da Carta dos Direitos Fundamentais da União Europeia

O art. 7º da Carta dos Direitos Fundamentais da União Europeia, prevê que: "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.", consagrando, igualmente, o direito a privacidade como um direito fundamental do ser humano. Já em seu art. 8º, prevê que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.", positivando o direito fundamental à privacidade e o direito a proteção de dados em artigos diferentes, já reconhecendo a autonomia deste.

Por óbvio, os direitos fundamentais inscrito na Carta também não são absolutos[69], de modo que o presente diploma normativo, estabelece uma cláusula geral de limitação dos

[68] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE**, p. 8-9.

[69] Neste sentido, o Advogado Geral do caso Volker v. Markus Schecke (C-92/09) opinou que: "Como um certo número de outros direitos clássicos da CEDH, o direito à privacidade não é um direito absoluto. O artigo 8.°, n.° 2, CEDH reconhece expressamente a possibilidade de excepções a este direito, tal como faz o artigo 9.° da Convenção n.° 108 em relação ao direito à protecção dos dados pessoais. Da mesma forma, o artigo 52.° da Carta define (em termos gerais) critérios semelhantes que, caso estejam preenchidos, permitem excepções (ou derrogações) aos direitos consagrados pela Carta". CONCLUSÕES da Advogada-geral Eleanor Sharpston apresentadas em 17 de Junho de 2010: Processos apensos C-92/09 e C-93/09 Volker und Markus Schecke GbR (Processo C-92/09) contra Land Hessen, [em linha].

direitos e liberdades que reconhece, em seu art. 52, dispondo que qualquer limitação lícita ao exercício de direitos fundamentais deverá observar os seguintes requisitos: (i) ser prevista em lei, que deve respeitar o conteúdo essencial desses direitos; (ii) a restrição deve ser necessária e proporcional; (iii) observar o interesse público ou os direitos fundamentais de terceiros.

A primeira condição, previsão legal, possui as mesmas características já descritas quando comentando as ingerências previstas na CEDH. Neste sentido, o Advogado Geral do caso C-203/15, opinou no sentido de que segundo decisões reiteradas do TJUE, a expressão *prevista por lei* indica que o fundamento legal deve ser acessível e previsível ao indivíduo, de modo que sua redação tenha precisão suficiente que permita ao cidadão (por vezes com a devida assistência de um advogado), moldar o seu comportamento. E mais, as autoridades não podem tomar decisões arbitrárias ou agir sem justificação sólida ao limitar um direito fundamental. Isso está de acordo com o princípio do primado do direito, que significa que a lei é superior e prevalece sobre a vontade arbitrária do Estado ou de suas autoridades.[70]

Ademais, a lei mesmo que observe o exposto acima, não poderá desvirtuar o objeto jurídico que pretende o direito fundamental resguardar, isto é, as limitações não podem ser tão extensas e intrusivas que tenham o condão de afastar o conteúdo essencial do direito positivado, sob pena de serem consideradas irregulares. Por conseguinte, a restrição deve estar em conformidade com os fins que motivaram a sua adoção, não podendo esgotar o direito fundamental que está limitando[71]. Se por acaso, for verificada que a lei objeto de análise resulta na afetação da essência do direito, a medida adota já é ilegal e não é necessário prosseguir com a avaliação de sua compatibilidade com as regras estabelecidas no Artigo 52(1) da Carta.[72]

De fato, no caso Schrems v. Estados Unidos da América (2015), a Corte de Justiça da União Europeia (CJUE) anulou o *Safe Harbor*, que permitia a transferência de dados pessoais entre a União Europeia e os Estados Unidos, após constatar que o regime de tutela das informações norte americano não garantias medidas adequadas da salvaguarda dos dados pessoais e da privacidade dos cidadãos europeus[73]. Neste julgado o TJUE reconheceu que a legislação americana, em particular a Lei de Vigilância de Inteligência Estrangeira (FISA) e o programa PRISM, permite que as autoridades dos EUA acessem dados pessoais de cidadãos

[70] CONCLUSÕES do Advogado Geral Henrik Saugmandsgaard Øe, apresentadas em 19 de julho de 2016: Processos apensos C-203/15 e C-698/15 Tele2 Sverige AB contra Post- och telestyrelsen (C-203/15), [em linha].
[71] ARCHANJO, Daniela Resende – **O princípio da proporcionalidade na solução de colisões de direitos fundamentais**, p. 163.
[72] EUROPEAN DATA PROTECTION SUPERVISOR – **Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit**, p. 2.
[73] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 6 de outubro de 2015 (Grande Secção), Schrems (C-362/14, EU:C:2015:650)**, [em linha].

da UE de maneira inadequada e em larga escala, sem garantias efetivas de proteção do direito à privacidade e da proteção aos dados pessoais, de modo que, mesmo havendo previsão legal, havia um evidente desrespeito ao conteúdo mínimo dos direitos em cotejo.

Aliás, este foi o entendimento esposado no parecer dado pelo Advogado Geral, o qual firmou que: "tendo em conta as condições previstas para poder admitir restrições ao exercício dos direitos e liberdades protegidos pala Carta, duvido profundamente que se possa considerar que as restrições em causa no presente processo respeitam o conteúdo essencial dos artigos 7.° e 8.° da Carta. Com efeito, o acesso dos serviços de informação americanos aos dados transferidos parece estender-se ao conteúdo das comunicações eletrónicas, o que viola o conteúdo essencial do direito fundamental ao respeito da vida privada e de outros direitos consagrados no artigo 7.° da Carta.", expressando posteriormente que, "a aplicação do conjunto dos princípios de porto seguro, pode considerar-se que essas limitações afetam o conteúdo essencial do direito fundamental à proteção dos dados pessoais".[74]

Em relação ao segundo pressuposto, vamos dividir o seu estudo. De início, quanto a necessidade, a limitação só é cabível quando for a melhor e/ou única maneira viável para a obtenção da finalidade pretendida, sendo também a ferramenta que trará o menor custo aos direitos do indivíduo, que sempre deve ser preservado no máximo possível.[75] Em outras palavras, a medida não há de exceder os limites indispensáveis à conservação do fim legítimo que se almeja. Pela necessidade não se questiona a escolha operada, mas o meio empregado e que este deve ser dosado para chegar ao fim pretendido. Assim, de todas as medidas que igualmente servem à obtenção de um fim, cumpre eleger aquela menos nociva aos interesses do cidadão.

Nesta senda, no acórdão do caso C-293/12, o TJUE ao tratar das limitações e preocupações relacionadas à Diretiva 2006/24, que se refere à retenção de dados de comunicações eletrônicas para fins de segurança pública, firmou o posicionamento de que a falta de critérios objetivos para limitar o acesso e uso dos dados significa que não há uma avaliação clara da necessidade de reter e acessar determinados dados para alcançar os objetivos de prevenção ou investigação de crimes graves. A ausência de limites claros torna difícil demonstrar que a retenção de dados é de fato necessário necessária. Portanto, firmou-se a conclusão de que a Diretiva 2006/24 comporta uma limitação nos direitos fundamentais de privacidade e proteção dos dados pessoais, de grande amplitude e particular gravidade na

[74] CONCLUSÕES do Advogado-geral Yves Bot, apresentadas em 23 de setembro de 2015: Processo C-362/14 Maximillian Schrems contra Data Protection Commissioner, [em linha].
[75] STUMM, Raquel Denize – **Princípio da proporcionalidade no direito constitucional brasileiro**, p. 79.

ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário.[76]

Por outro lado, a proporcionalidade consiste em verificar se há mais vantagens em se admitir o instrumento restritivo utilizado do que desvantagens na limitação do direito. Para reduzir desvantagens e riscos ao exercício dos direitos à privacidade e proteção de dados, é importante que as limitações contenham salvaguardas necessárias e proporcionais. Com efeito, o princípio da proporcionalidade em sentido estrito, no contexto do Direito, está ligado à ideia de impedir que o Estado exceda seus limites em relação aos direitos individuais das pessoas. Isso significa evitar tanto a omissão excessiva do Estado ao não cumprir obrigações positivas em benefício das pessoas quanto, de forma mais comum, prevenir a imposição de encargos excessivos ou intervenções desproporcionadas na esfera jurídica dos cidadãos.[77]

A jurisprudência do TJUE é pacífica no reconhecimento do uso da proporcionalidade como baliza para aferir a legitimidade da limitação. Neste sentido, em diversos casos[78], já se firmou o entendimento de que o princípio da proporcionalidade demanda que os atos das instituições sejam adequados à realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário à realização desses objetivos.

Mais especificamente, restou firmado no Acórdão de 8 de abril de 2014 (Grande Secção), Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238), que a proporcionalidade se reveste de um caráter especial no contexto da Carta, empregando um significado diferente do estabelecido no artigo 5.°, n.° 4, do Tratado da União Europeia (TUE). Na hipótese, a proporcionalidade não se apresenta como um princípio geral que guia a atuação da União, mas como uma regra, uma proporcionalidade *stricto sensu,* apresentando-se como um requisito fundamental para qualquer restrição aos direitos fundamentais.[79]

Por fim, como última condição, temos a observância dos interesses públicos e direitos de terceiros. Não poderia ser diferente, pois por diversas vezes o direito à privacidade e à

---

[76] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 8 de abril de 2014 (Grande Secção), Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238).** [em linha].

[77] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel – **Curso de direito constitucional**, p. 214.

[78] Acórdãos Afton Chemical, C-343/09, EU:C:2010:419, n.° 45; Volker und Markus Schecke e Eifert, EU:C:2010:662, n.° 74; Nelson e o., C-581/10 e C-629/10, EU:C:2012:657, n.° 71; Sky Österreich, C-283/11, EU:C:2013:28, n.° 50; e Schaible, C-101/12, EU:C:2013:661, n.° 29).

[79] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 8 de abril de 2014 (Grande Secção), Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238)**, [em linha].

proteção de dados pessoais irá interagir com outros direitos fundamentais, havendo concessões e limitação de ambos os lados, como será demonstrado no tópico seguinte.

Já em relação ao interesse público, conforme ensinamentos de Celso Antônio Bandeira de Mello, este é definido como o interesse resultante do conjunto de interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da Sociedade e pelo simples fato de o serem[80], como exemplos trazidos pela doutrina, temos a promoção da paz, do bem-estar dos indivíduos, segurança pública, dentro outros.[81]

Desta feita, podemos conceituar o interesse público como a fusão qualificada dos interesses individuais, isto é, o instituto que dá publicidade as vontades de uma coletividade. Não é caracterizado, de maneira autônoma, independente dos esforços de cada um, pelo contrário, é a face difusa dos interesses de cada indivíduo.

Não obstante a definição acima, é evidente que na maioria dos casos de restrição, o titular das informações, não desejaria que fosse limitado o seu direito à privacidade ou restringida a proteção de seus dados pessoais. Contudo, compreenderá que é impossível salvaguardar a harmonia social e a segurança pública, sem a prevalência do interesse público de um modo geral, desde que presente ainda as demais condições acima delineadas.

Logo, é de suma importância explicar e definir detalhadamente o escopo do interesse público que se busca proteger através da limitação à proteção dos direitos pessoais. Isto porque, a necessidade desta restrição será medida levando em consideração o contexto em que é aplicada. Nesses termos, uma descrição detalhada do objetivo da limitação e das medidas propostas é essencial para permitir a avaliação quanto à sua previsão legal, necessidade e proporcionalidade.

1.4.3. Limitações lícitas em face de outros direitos

Como exposto no tópico anterior, o art. 52, 1 da Carta estabelece as restrições lícitas ao exercício de direito fundamental a proteção dos dados pessoais, destacando a necessidade de uma previsão legal que respeite o conteúdo essencial da proteção de dados, acompanhada de uma limitação necessária e proporcional aos fins buscados, devendo sempre observar ao final o interesse público ou os direitos fundamentais e liberdade de terceiros.

[80] MELLO, Celso Antônio Bandeira – **Curso de Direito Administrativo**, p. 59.
[81] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data Protection Law**, p. 42.

Desta feita, como já esposado neste trabalho, não obstante serem direitos fundamentais, os direitos à privacidade e a proteção dos dados pessoais não podem ser compreendidos como prerrogativas absolutas a salvaguardarem todo e qualquer tratamento de dados pessoais, sendo parte de um sistema normativo harmonioso a compreensão de que sofrem, como outros direitos fundamentais, limitações.

Logo, a depender do caso concreto e do aparente conflito de interesses, outros direitos fundamentais poderão funcionar como balizas limitadoras do direito à proteção aos dados pessoais, sendo necessária uma ponderação de valores, para que possa se chegar a conclusão de qual direito prevalecerá na hipótese.

A ponderação de valores é o método utilizado para solucionar os conflitos aparente entre normas, sem soluções apriorísticas, quando não é possível a utilização das formas hermenêuticas clássicas[82]. De início, verifica-se a intensidade da intervenção, ou seja, quanto o direito necessita ser limitado para harmonia entre os diferentes valores. Posteriormente, devem ser demonstradas as justificativas que sustentam a limitação. Por último, é feita a ponderação no sentido restrito, analisando os aspectos do caso concreto para identificar qual direito fundamental deve ser aplicado.[83]

Por exemplo, um conflito aparente comum é o decorrente entre a proteção dos dados pessoais e a liberdade de expressão e de acesso da informação[84]. Na hipótese em que haja aparente confronto entre a liberdade de expressão e/ou acesso de informação e a proteção aos dados pessoais, a mencionada técnica de ponderação dos conflitos deverá ser utilizada, sempre observando se há ou não efetivo interesse público na divulgação e ou acesso da informação, como principal critério para afastamento episódico do direito fundamental a proteção dos dados pessoais.

Doutrinariamente, tem-se traçado algumas diretrizes para resolver esses eventuais conflitos, observando em primeiro lugar qual à natureza dos dados envolvidos (se são sensíveis ou não) e o potencial dano à privacidade que o acesso ou divulgação pública resultaria. Nesses termos, se reconhece que o grau de ingerência no direito à proteção de dados irá variar caso se trate de informações meramente identificativas ou dados pessoais sensíveis.[85]

---

[82] BARCELLOS, Ana Paula de – **Ponderação racionalidade e atividade jurisdicional**, p. 23.
[83] ALEXY, Robert – **Teoria dos Direitos Fundamentais**, p. 68.
[84] Direito consagrado expressamente na Constituição Portuguesa, em seu artigo 37 e na Constituição Brasileira, em seu artigo 5º, inciso IX.
[85] ÁLVAREZ, José Luis Rodríguez – **Transparencia y protección de datos personales: criterios legales de conciliación**, p. 52.

A relação entre a liberdade de expressão e a proteção de dados pessoais esta consagrada no Regulamento Geral de Proteção de Dados, em seu art. 85, que consubstancia que os Estados-Membros devem compatibilizar o direito à proteção de dados pessoais com o direito à liberdade de expressão e informação. Em particular, a depender do caso concreto, podem ser feitas derrogações para fins jornalísticos, de expressão acadêmica, artística ou literária, na medida em que sejam necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e informação.[86]

Quantos as ingerências feitas pelas autoridades públicas, o Grupo de Trabalho 29, apresentou algumas orientações a serem seguidas, com a finalidade de limitações que vão de encontro com a carta. Em suma do que foi apresentado, destacou-se como primeira condição a identificação da necessidade social premente que justifique a limitação, considerando a gravidade do problema e o tempo decorrido desde a ocorrência do problema. Quanto à proporcionalidade, firmou-se ser fundamental definir claramente os objetivos a serem alcançados para determinar quais categorias de dados são necessárias, como eles serão processados e a qualidade dos dados requerida. O acesso aos dados de terceiros deve ser limitado por salvaguardas adequadas. Como terceira condição, dispõe que é necessário garantir que a coleta e retenção de dados sejam adequadas e relevantes, sem excessos, levando em consideração o direito à privacidade individual. Cada medida deve ser avaliada separadamente em relação à sua duração e impacto. Finalmente, as propostas devem ser baseadas em evidências sólidas, incluindo pesquisas, estatísticas e previsões, para garantir que haja razões relevantes e suficientes que justifiquem a limitação do direito à proteção de dados pessoais.[87]

Feitas as presentes considerações acerca do direito à privacidade e a proteção dos dados pessoais, passando por sua evolução histórica, conceito, diferenças e limitações, passamos no capítulo seguinte a uma visão geral do tratamento dos dados pessoais nos termos do RGPD e da LGPD.

[86] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data Protection Law**, p. 54.
[87] 29 DATA PROTECTION WORKING PARTY – Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, p. 5.

2. DO TRATAMENTO DOS DADOS PESSOAIS

No presente capítulo será abordado a forma de tratamento dos dados pessoais (automatizados e não automatizados), dispondo acerca dos mecanismos previstos no Regulamento Geral de Proteção de Dados Europeu e na Lei Geral de Proteção de Dados brasileira.

Prima facie, cumpre destacar que há forte influência do RGPD sobre a lei brasileira, de maneira que muitos dos dispositivos de ambos os diplomas se equivalem, apenas apresentando pequenas diferenças[88]. Assim, na presente dissertação a abordagem se firmará inicialmente no regime consagrado pelo Regulamento Europeu, sendo tecidos comentários pontuais quando houver previsão diversa ou complementar na LGPD.

O Regulamento Geral de Proteção de Dados Europeu (RGPD) consagra um conjunto harmonizado de normas aplicáveis a qualquer processamento de dados da pessoa física que ocorra no âmbito da União Europeia, estabelecendo desde os seus considerandos que qualquer tratamento de dados deverá ser concebido para servir as pessoas e não como um fim em si próprio.

Nessa esteira, com o escopo de esclarecer de imediato as condutas que serão tipificadas, o RGPD em seu art. 4º traz uma definição pormenorizada e exemplificativa de tudo aquilo que é considerado como "tratamento", conceituando o instituto como uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a 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.

Além de estabelecer um conceito exemplificativo, cheio de condutas que são caracterizadas como tratamento de dados, o modelo europeu ainda estabelece condicionantes a este processamento, positivando hipóteses legais tanto de autorização do tratamento (havendo proibição legal de tratamento quando não se encaixar na hipótese normativa), quanto de limitação do tratamento, mesmo que já autorizado, estabelecendo a medida, especificação meio e finalidade do tratamento.[89]

---

[88] Esta similitude decorre de imposições estabelecidas no regulamento para tratamento e transferência de dados para países que não façam parte da União e que pretendam estabelecer um fluxo de dados com nações europeias ou realizar o tratamento de dados de cidadãos europeus.

[89] GUIDI, Guilherme Berti de Campos – **Proteção de Dados Pessoais: a composição de sistemas pelo Direito Internacional**, p. 101.

De igual forma, a Lei Geral de Proteção de Dados, em seu art. 5º, X, afastando-se do costume dos diplomas legais brasileiros que normalmente não estabelecem conceitos para os institutos abrangidos, também optou por definir de maneira exemplificativa o que seria o "tratamento dos dados pessoais", consignando ser: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Outrossim, na Lei Geral de Proteção de Dados brasileira, também seguindo o paradigma europeu, foi consagrado no artigo 1º que o tratamento de dados, seja por pessoa física ou jurídica, no âmbito público ou privado, prescinde de uma base legal como fundamento para o processamento das informações pessoais, também limitando o tratamento, mesmo aqueles permitidos pelo titular dos dados e/ou autorizados legalmente, aos princípios previstas no art. 6º do diploma normativo.

Dentro do arcabouço de ambos os diplomas normativos, portanto, não sendo uma hipótese de exclusão, deverá ocorrer o encaixe do tratamento realizado em pelo menos uma das hipóteses legais para que ele seja considerado legítimo e lícito, sendo possível inclusive necessidade cumulação de bases legais para licitude do tratamento.

As referidas bases foram estipuladas de forma geral e variada, no presente estudo nos limitaremos a abordar de maneira suscinta: o consentimento, o legítimo interesse e o cumprimento de obrigação legal. Além das hipóteses legais que autorizam o tratamento dos dados pessoais, serão também objeto de análise os princípios relacionados ao tratamento dos dados pessoais.

2.1. Das bases legais para o tratamento dos dados pessoais

A licitude do tratamento dos dados pessoais deverá se amoldar a uma ou até mais de uma das bases legais consagradas na RGPD e na LGPD quando houver o processamento de dados pessoais para que possa se considerar lícita, conforme restará demonstrado.

Aliás, excetuado o consentimento, estudado no próximo tópico, as demais bases legais previstas pelos diplomas normativos supracitados, estarão vinculadas ao princípio da necessidade do processamento dos dados pelo controlador, razão pela qual indispensável o estudo dos referidos institutos.

2.1.1. Consentimento

O consentimento é a primeira base legal positivada para o tratamento dos dados pessoais, repetindo-se esta previsão normativa no RGPD (em seu art. 6º, 1, a) e na Lei Geral de Proteção de Dados brasileira (art. 7º, I). Logo, caso o titular dos dados pessoais permita que suas informações sejam acessadas, coletadas e tratadas, tem-se atendida a primeira condicionante legal que permite o tratamento.

Ao estabelecer o consentimento como um dos fundamentos legais a permitir o tratamento dos dados pessoais, homenageia-se a autonomia privada do titular dos dados, ou seja, é reconhecida a capacidade que o titular do direito de estabelecer relações jurídicas com outros, inclusive, relativo aos seus dados pessoais, de forma a consagrar uma das mais importantes manifestações que o ser humano pode realizar como ente autodeterminado que é reconhecido pelo direito[90]. Em igual sentido, Tepedino e Teffé, advogam que ao se estabelecer o consentimento como um dos fundamentos legais para o processamento de dados, consagra-se a autonomia da vontade como um mecanismo que promove a autodeterminação e a construção livre da esfera privada.[91]

Quanto a sua definição, de acordo com os ensinamentos de Doneda, o consentimento pode ser conceituado como a ferramenta da manifestação da autonomia do indivíduo, faculdade esta que possibilita ao titular dos dados pessoais modificar a esfera de tutela dos seus direitos tendo como base uma expressão de vontade que tenha exteriorizado. No mais, expõe que dentro de um contexto de proteção de dados, apesar de estarmos diante de uma relativização de elementos tocantes ao próprio direito de personalidade, a anuência no processamento dos dados não importará em renúncia a tutela legal ou falta de interesse em sua proteção, mas em real exercício dessa faculdade consagrando um ato de exercício de autodeterminação informativa daquele que é o titular dos dados.[92]

Aliás, o referido autor ainda destaca que tomando por base a maneira como é disciplinado o consentimento dentro do arcabouço legal, se faz possível verificar a natureza do sistema de proteção de dados pessoais. Considera-se de cunho patrimonialista, quando a anuência do titular tiver uma função legitimadora de inserção destas informações no mercado, transformando os dados pessoais em verdadeira *comodity*. Por outro lado, quando a proteção de dados está firmada nos direitos da personalidade, o consentimento passa a consagrar a

[90] CAMPOS, Diogo Leite – Lições de Direitos da Personalidade, p. 216.
[91] TEPEDINO, Gustavo; TEFFÉ, Chiata Spadaccini de – **O Consentimento na circulação De Dados Pessoais**, p. 83.
[92] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 377-380.

impossibilidade de cessão definitiva dos dados pessoais, condicionando o uso dos dados a uma específica disposição legislativa ou a um instrumento designado em lei, com o fito de resguardar autodeterminação ao indivíduo sobre a sua esfera privada.[93]

Não obstante o exposto, independente da acepção adotada pelo sistema normativo, o estabelecimento do consentimento como uma das premissas legais para o ulterior processamento dos dados é essencial em um cenário de coleta massiva e mercantilização de dados, pois coloca o controle do tratamento dos dados pessoais na mão do titular dos dados desde o início do processo, refletindo em uma maior salvaguarda legal.

Os diplomas normativos em comento também não se olvidam em trazer sua própria definição para o consentimento dentro do panorama da proteção dos dados pessoais. Nos termos do artigo 4º, 11 do Regulamento Geral de Proteção de Dados, o consentimento decorre de uma manifestação de vontade, **livre, específica, informada e explícita**, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Seguindo a mesma linha, a Lei Geral de Proteção de Dados Brasileira, em seu artigo 5º, XII, define o consentimento como a manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Ademais, a convenção 108+, em seu artigo 5, 2., que o tratamento dos dados deve ser efetuado com base em um **consentimento livre, específico, informado e inequívoco** do titular dos dados.

Como pode se perceber, os vocábulos "livre, específico, informado e inequívoco*"* se repetem na definição trazida pelo Regulamento Geral de Proteção de Dados e na Convenção 108+, merecendo, assim, serem objeto de um estudo mais aprofundado.

Ao se dispor expressamente que o consentimento deve correr de uma manifestação **livre**, o legislador de imediato infere que o sujeito tutelado terá a faculdade de fornecer ou não sua anuência para o tratamento dos dados pessoais, vedando expressamente a possibilidade de processamento das informações quando estivermos diante de uma manifestação de vontade viciada objetiva ou subjetivamente. Portanto, o consentimento deve ser dado voluntariamente, sem coerção, pressão ou influência indevida. Isso significa que a pessoa deve ter a liberdade de escolher se deseja ou não permitir o tratamento de seus dados pessoais. Se houver qualquer forma de coerção, os dados não podem ser considerados legalmente consentidos.

Ainda quanto a liberdade do consentimento, o considerando 42 do RGPD, dispõe que não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados

[93] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 390.

não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado. Assim, a revogabilidade do consentimento, ou seja, a possibilidade de o titular dos dados retirar o seu consentimento sem ser objeto de qualquer penalidade é um dos elementos que caracterizam o consentimento como livre.

Quanto ao consentimento **específico**, a permissão é limitada a finalidade para a qual foi outorgada, de modo que o indivíduo deve ser informado sobre como seus dados serão usados e consentir explicitamente para cada finalidade. Portanto, para ser específico, deve o consentimento ser dado de forma explícita para propósitos precisos e bem definidos pelo controlador, antes do início do tratamento dos dados.[94] Por exemplo, se uma empresa deseja usar seus dados para enviar newsletters e para processar pagamentos separadamente, você deve dar consentimento separadamente para cada uma dessas finalidades.

Em consonância com a definição positivada no art. 5º, XII da LGPD e a recomendação 32 da RGPD, advoga-se por uma interpretação restritiva do consentimento, que se abstenha a finalidade para o qual foi anuída, restando proibido o controlador dos dados pessoais de ampliar a anuência que lhe foi albergada, não podendo ir além dos termos que foram pactuados, postergar o tratamento dos dados para momento um posterior ou utilizar os dados com fins diversos.[95] Assim, deverá a anuência outorgada compreender todas etapas do processamento que se busca com aquela finalidade e, na hipótese em que haja múltiplas finalidades, múltiplos também devem ser os consentimentos.

Neste diapasão, a *European Data Protection Board* traz um caso prático onde uma instituição financeira solicita anuência dos seus usuários para utilização dos dados de pagamentos que são coletados para finalidades ligadas a publicidade, não relacionadas ou necessárias a execução dos serviços bancários em si. Nessa hipótese, por óbvio, não poderá a negativa do usuário em autorizar o tratamento de seus dados para fins de marketing resultar também na negativa da prestação dos próprios serviços bancários.[96]

Ademais, para uma manifestação **informada**, deve o titular dos dados pessoais ter disponibilizado para si todos os elementos necessários e suficientes para ponderar de maneira escorreita e precisa acerca da situação e a forma de como seus dados serão processados. E mais, na hipótese de ser necessário o prévio processamento das informações para o fornecimento de serviço ou compra de um produto, o titular será informado com destaque sobre esse aspecto e sobre os instrumentos pelos quais poderá exercer seus direitos. Em

[94] SOMBRA, Thiago – **Fundamentos da regulação da privacidade e proteção de dados pessoais**, p. 137.
[95] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario – **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**, p. 6.
[96] EUROPEAN DATA PROTECTION BOARD – **Guidelines on Consent under Regulation 2016/679**, p. 11.

outras palavras, deve ser dado publicidade ao titular dos dados pessoais de maneira clara e compreensível sobre o que está sendo pedido e sobre os detalhes do tratamento de dados. Isso inclui informações sobre quem está coletando os dados, para que finalidade, por quanto tempo os dados serão armazenados e quem terá acesso a eles. As informações fornecidas devem ser suficientes para permitir que a pessoa tome uma decisão informada sobre se deve ou não dar o consentimento.

Não mais se admite uma lógica binária, onde o usuário ou permite todos os termos do serviço ou não poderá utilizá-lo. Muito pelo contrário, conjugando os preceitos de um consentimento livre e informado, surge a possibilidade de manifestação do consentimento de forma granular, no sentido de incentivar configurações de privacidade personalizáveis e termos de uso que contenham cláusulas específicas para cada hipótese de tratamento de dado que está sendo consentido.[97]

Finalmente, **inequívoco** é o consentimento dado sem ambiguidade, ou seja, onde o titular dos dados pessoais expressa sua concordância de maneira clara e sem deixar margem para interpretações dúbias. Geralmente, isso é feito por meio de uma ação afirmativa, como marcar uma caixa de seleção ou clicar em um botão de "Aceitar". Nos termos do art. 5º, 42, da Convenção 108+, deve o consentimento consubstanciar a livre expressão de uma escolha intencional, dada por uma declaração (que pode ser escrita, inclusive por meios eletrónicos, ou oral) ou por uma ação positiva clara e que indique inequivocamente, neste contexto específico, a aceitação da proposta de tratamento de dados pessoais.

Nesse diapasão, a maneira pela qual é dada a anuência não precisa ser necessariamente escrita, outras formas também podem ser adotadas, desde que o indivíduo detenha elementos suficientes para a tomar de maneira inequívoca a decisão. Sobre o tema, um parecer do Grupo de Trabalho *29* traz o seguinte exemplo: deslizar o dedo na tela do aparelho celular pode ser uma forma de externa permissão para o tratamento dos dados pessoais. Para isto, as informações sobre a maneira de externar a concordância devem ter sido informadas de maneira clara para o sujeito.[98]

[97] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario – **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**, p. 8-9.
[98] EUROPEAN DATA PROTECTION BOARD – **Guidelines on Consent under Regulation 2016/679**, p. 13.

2.1.2. Legítimo interesse

Trata-se da hipótese legal que possibilita o tratamento dos dados independente do consentimento do seu titular, com base na natureza e objetivo da atividade econômica ou pública que é desempenhada pelo controlador dos dados, que finda por justificar um necessário processamento de informações. Como se prescinde do consentimento do titular dos dados, deve ser especialmente considerada a finalidade, necessidade e proporcionalidade da utilização das informações coletadas, de modo que processamentos mais genéricos e invasivos são normalmente considerandos ilegítimos.[99]

O legítimo interesse encontra-se positivado na Lei de Proteção Geral de Dados, em seu artigo 10º, onde se estabelece que apenas será possível fundamentar o processamento de dados para objetivos legítimos do controlador, sempre se considerando o fato concreto, traçando, posteriormente, algumas hipóteses não exaustivas em que se presume esse interesse legítimo, como: (i) no apoio e promoção de atividades do controlador; (ii) tratamento realizado para proteção em relação ao titular dos dados, incluído aí, prestação de serviços que o beneficiem ou que decorram de exercício regular de um direito do controlador.

O Regulamento Geral de Proteção de Dados (RGPD), também consagra o interesse legítimo como salvaguarda para o tratamento de dados, nos termos do art. 6º, 1, 'f', o qual estabelece a possibilidade de processamento de dados quando necessários para atendimento do legítimo interesse do controlador dos dados, excetuado este embasamento quando o tratamento possa resultar em violação a direitos ou liberdades fundamentais do titular dos dados pessoais, principalmente se o titular dos dados for uma criança.

"Legítimo" são os objetivos do responsável pelo tratamento ou o controlador dos dados que vão ao encontro da lei, seja em matéria de proteção de dados ou demais legislação aplicáveis. Por outro lado, tem-se entendido o "interesse" como o escopo mais amplo que o processador dos dados tem ao realizar o tratamento das informações, ou o benefício que o responsável pelo processamento possa obter em razão da operação realizada. Como visto, a natureza do interesse pode variar e irá ser diferente a depender da atividade (pública ou privada) que é desempenhada pelo controlador ou responsável pelo tratamento dos dados. Por vezes, o interesse pode ser considerado público, se preponderante for os benéficos para a sociedade, por exemplo, a liberdade de impressa, a segurança nacional; em outras hipóteses,

[99] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario – **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**, p. 14.

pode ser particular daquele que realizada o tratamento dos dados, como nas empresas de marketing digital.[100]

Ademais, a demonstração do legítimo interesse não pode se basear unicamente em declaração do controlador dos dados neste sentido, deverá haver demonstração prática de que o processamento dos dados é indispensável ou traz relevante benefício a atividade desempenhada pelo controlador, de modo que não há como perquirir essa atividade sem um mínimo processamento das informações pessoais dos seus usuários.

Nesse diapasão, a doutrina lista algumas hipóteses em que se entende haver legítimo interesse para o processamento de dados, por exemplo: (i) quando a falta de consentimento do titular obstar o manuseio dos seus dados em confronto com finalidades legítimas vinculadas a atividades realizadas pelo controlador[101]; (ii) quando o processamento das informações pessoais faz-se necessário para traçar perfis do consumo com o objetivo de evitar fraudes em sistemas de cartão de crédito ou conta corrente *on line;*[102] *(*iii) fornecimento de imagens de segurança;[103] (iv) transferência dos dados entre empresas do mesmo grupo econômico para fins administrativos internos, incluindo aí as informações relativas a clientes e funcionários.

Parcela da doutrina critica a previsão legal do "legítimo interesse" como um dos fundamentos para o tratamento dos dados pessoais. A intenção do legislador em trazer uma permissão aberta, consagrada em um conteúdo jurídico indeterminado, foi para encaixar atividades econômicas futuras, legítimas ou socialmente relevantes de processamento de dados, que não poderiam ser dispostas ou não eram de conhecimento geral quando foi editado o Regulamento.[104]

Com efeito, nos diplomas normativos acima listados, o legítimo interesse é positivado como um conceito jurídico indeterminado, a ser preenchido dependendo do contexto, tempo e lugar que está sendo feito o processamento dos dados. A intenção dos legisladores foi de flexibilizar o sistema, objetivando consagrar também hipóteses que não pudessem de maneira apriorística serem regulamentadas, permitindo então que a norma extraída compactue com novos usos e finalidades que sejam estabelecidos para o tratamento de dados pessoais.

Entretanto, a referida flexibilidade finda por arrastar essa base legal para o cerne das discussões das autoridades de controle e tribunais, que corriqueiramente decidem sobre a

---

[100] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE**, p. 36-37.
[101] BIONI, Bruno – **Proteção de dados pessoais: a função e os limites do consentimento**, p. 232.
[102] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario – **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**, p. 15.
[103] *Ibidem.*
[104] MARCACINI, Augusto Tavares Rosa – **Regras aplicadas ao tratamento de dados pessoais**, p. 153.

razoabilidade e existência de fato do legítimo interesse no processamento dos dados, sempre buscando a manutenção da máxima de que os titulares não sejam injustiçados pelo processamento.

A título exemplificativo, uma companhia de publicidade pode coletar as informações pessoais de usuários para fins de publicidade direcionada. A empresa, pode sustentar sua conduta em um "legítimo interesse" de processar esses dados para mostrar anúncios mais relevantes e personalizados aos usuários. No entanto, esse questionamento é extremamente questionável, pois os indivíduos podem considerar invasivo o rastreamento de suas atividades sem que tenham dado consentimento.

No TJUE, quando do julgamento dos processos apensos C-468/10 e C-469/10, restou firmado o entendimento de que não havendo anuência do titular dos dados, o interesse legítimo prosseguido pelo responsável por esse tratamento, demanda, a salvaguarda dos direitos fundamentais dos indivíduos e, ainda, que as informações apareçam em fontes acessíveis ao público, não se permitindo o processamento de dados que não apareçam em tais fontes.[105]

Em razão do referido julgado, ocorreu uma limitação do embasamento do legítimo interesse, criando uma maior barreira para o uso indiscriminado desta justificativa legal. Com efeito, da consagração de que as informações utilizadas devem estar acessíveis de forma pública, decorre uma efetiva restrição a utilização, obstando que o interesse legítimo venha a ser desvirtuado.

Afora isso, a Opinion 06/2004 do Grupo de Trabalho 29, aponta que o legítimo interesse do controlador dos dados não se afigura como suficiente para permitir o tratamento dos dados, trata-se de um ponto de partida, devendo ainda ser realizada a ponderação entra o interesse do controlador e o direito fundamental a proteção de dados e a privacidade do titular das informações.[106]

Neste sentido, aplica-se um teste de ponderação, colocando de um lado da balança, os direitos do titular dos dados e do outro lado, o direito de quem faz o processamento das informações. Neste cenário, são observados alguns parâmetros para verificar a configuração

[105] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 24 de novembro de 2011 (Terceira Secção), C-468/10 e C-469/10)**, [em linha].
[106] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE**, p. 39.

de um legítimo interesse, como o impacto do processamento sobre o titular dos dados e sobre as salvaguardas legais desenhadas para proteger o titular dos dados.[107]

Formuladas essas considerações, na linhas dos ensinamentos de Teffé e Viola, chega-se as seguintes premissas para reconhecimento de um tratamento de dados baseado no legítimo interesse: (i) na hipótese em que for mais adequado, desde que utilizado de forma proporcional e limitada, caso haja benefício evidente e certo para o controlador; (ii) quando não ocorrer impacto relevante aos direitos e garantias do sujeito dos dados; (iii) quando o titular dos dados já espera que seus dados sejam tratadas em razão das atividades ou de um exercício regular do direito do controlador dos dados; (iv) quando não há possibilidade de se contactar o titular dos dados para o consentimento ou presume que o consentimento seria dado pelo titular, tendo em vista a natureza da atividade. [108]

Assim, quando estivermos diante de um tratamento de dados baseados no legítimo interesse, caberá o processamento dos dados apenas dentro do estritamente necessário a finalidade do controlador, que deverá adotar medidas de transparência no tratamento para que possa este ser objeto de controle pelo titular dos dados pessoais.

E mais, para que o interesse seja de fato considerado legítimo, deve-se ponderar de maneira cuidadosa, se o sujeito que teve seus dados pessoais recolhidos pode razoavelmente antecipar, com base no contexto e fase em que as informações são coletadas, que essas poderão vir a ser tratados com essa finalidade, ou seja, com base no interesse legítimo do controlador, dispensando, assim, o consentimento do titular dos dados pessoais.

Todavia, diante da insegurança que a justificativa apenas do legítimo interesse traz, o que se observa no dia a dia é que, mesmo empresas que encontram justificativa na natureza das suas atividades para o tratamento de dados, tendo assim uma base legal para seu processamento, procuram sempre outras condicionantes legais de tratamento, principalmente o consentimento do titular dos dados, de modo que resulte ao controlados dos dados uma maior salvaguarda de eventual responsabilização pelo manuseio das informações pessoais de terceiros.[109]

---

[107] PEREIRA DE SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius – **Considerações iniciais sobre os interesses legítimos do controlador na lei geral de proteção de dados pessoais**, p. 121.
[108] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario – **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**, p. 17.
[109] VOIGT, Paul; BUSSCHE, Axel von dem – **The EU General Data Protection Regulation (GDPR). A Practical Guide**, p. 101.

2.1.3. Outras bases legais

Conforme disposto no art. 6º do Regulamento Geral de Proteção de Dados, além do consentimento e do interesse legítimo, há ainda outros fundamentos legais que possibilitam o tratamento do dado pessoal, como: (i) necessidade de execução de um contrato do qual o titular dos dados pessoais é parte, ou para diligências pré-contratuais a pedido do titular dos dados; (ii) obrigações jurídicas imputadas ao responsável pelo tratamento; (iii) interesses vitais do titular dos dados pessoais ou de outra pessoa; (iv) exercício de funções públicas ou exercício de autoridade pública, for necessário o tratamento dos dados.

Já o art. 7º da Lei Geral de Proteção de Dados brasileira é mais descritivo, além do consentimento e interesse legítimo, lista uma série de previsões legais em que se considerará lícito o processamento dos dados pessoais, merecendo destaque as seguintes previsões: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) tratamento e uso compartilhado de dados pela administração pública para implementação de políticas públicas; (iii) para exercício regular de direitos, em processos judiciais, administrativos ou arbitrais; (iv) para proteção do crédito.

Desta maneira, o RGPD e a LGPD, de maneira correta e adequada consubstanciam outras hipóteses legais que autorizam o processamento de dados, independente de que haja o consentimento do titular dos dados. Exemplos nos próprios diplomas normativas e na doutrina não faltam, como nos casos dos tratamentos baseados em cumprimento a uma obrigação legal, as hipóteses de serviços de saúde e/ou proteção à vida do titular dos dados, dentro do exercício regular de um direito e para a execução ou preparação de um contrato.[110]

A pertinência dessas bases legais diversas é gigantesca, haja vista que nestes fundamentos consolidados ora expostos, não é relevante questionar a possibilidade da anuência pelo titular dos dados. Muito pelo contrário, evidencia-se que seria irrazoável e inadequado exigir o consentimento em casos que a contraparte, processadora das informações, terá obrigações legais no tratamento dos dados, por exemplo; ou, ainda, exigir a anuência de uma pessoa que está inconsciente, para poder acessar suas informações médicas e prosseguir com um tratamento de urgência.

Ademais, não há óbice para que o responsável pelo processamento dos dados pessoais se utilize de mais de um dos embasamentos legais para que sem o consentimento proceda ao manuseio das informações, muito pelo contrário, caso a atividade desempenhada se encaixe

[110] GUIDI, Guilherme Berti de Campos – **Proteção de Dados Pessoais: a composição de sistemas pelo Direito Internacional**, p. 96.

com mais de um dos fundamentos, é medida de cautela do controlador apontar expressamente todas as hipóteses legais autorizativas do tratamento. Em outra via, defendem Teffé e Viola, contudo, ainda que se possa utilizar mais de um fundamento, a escolha deve recair sobre aquele que se demonstre mais adequado e seguro diante de uma situação concreta.[111]

Dentro do âmbito da regulamentação europeia também se entende que seria permitido ao controlador fundamentar o manuseio dos dados indicando mais de uma base legal. Com efeito, tomando por base o art. 17, (1), b da RGPD, o qual estabelece que o tutelado pela proteção dos dados poderá revogar o consentimento no qual se baseia o processamento dos dados, caso não exista outra base legal para o precitado tratamento.[112]

O panorama onde consagra-se um fundamento adequado com a base legal como necessidade para o processamento das informações pessoais, consiste em característica própria da escola de proteção de dados europeias, fonte de inspiração para a regulamento do tratamento de dados no Brasil, razão pela qual também adotada pela LGPD. Por outro lado, para a escola americana, como pontua Solove, a regra é a do tratamento geral dispensando um embasamento legal, podendo as informações serem coletadas, manuseadas e apagadas livremente, a menos que exista lei específica que proíba a conduta.[113]

Pois bem, nas hipóteses em que o contrato é a base legal que irá fundamentar o processamento de dados pessoais, verifica-se que o legislador estabeleceu dois cenários diferentes, uma previsão pré-contratual, ainda quando da fase de deliberação acerca do negócio jurídico; e outra pós-contratual, em razão da necessidade execução de um contrato do qual o titular dos dados pessoais é parte.

Na fase pré-contratual, o tratamento de dados justifica-se na medida em que, a pedido do titular dos dados, o responsável pelo processamento das informações irá diligenciar perseguindo os elementos necessários para formalização do negócio jurídico pretendido. Por exemplo, uma empresa poderá coletar os dados pessoais dos candidatos a emprego, como seus currículos, informações de contato... tudo com o objetivo posterior de formalizar o contrato de trabalho. Neste caso, apenas os dados necessários à contratação podem ser coletados, não podendo esta base legal ser utilizada para, por exemplo, posteriormente, servir

[111] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario – **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**, p. 15.
[112] MENKE, Fabiano – **A possibilidade de cumulação de bases legais nas operações de tratamento de dados pessoais**, p. 3.
[113] SOLOVE, Daniel J. – **Introduction: Privacy Self-Management and the Consent Dilemma**, p. 1887.

para encaminhamento de publicidade da empresa, fim diverso para o qual foi coletada a informação.[114]

Já o tratamento realizado na fase de execução do contrato, abrange a coleta de informações necessárias a efetivação daquilo que foi negociado, como tratamento dos dados relacionados ao endereço (para entrega e/ou eventual cobrança), relativos ao cartão de crédito (para pagamento), enfim, tudo que seja necessário para dar eficácia ao negócio. Cabe ressaltar, que neste caso a interpretação do que pode ser coletado também é restrita àquilo que for necessário para viabilizar a execução do negócio, de modo que é preciso de ponderar qual a razão do contrato, para se vislumbrar quais dados necessariamente precisam ser tratados.[115]

Quando o fundamento jurídico para o tratamento for uma "obrigação legal", estamos diante de uma determinação prevista em lei, que deve preencher todos os requisitos para que a obrigação seja válida, devendo ainda o respeito as normas atinentes a proteção dos dados pessoais, e observância os princípios da finalidade, proporcionalidade e necessidade. O Parecer 06/2014, do Grupo de Trabalho 29, ao tratar sobre o tema, ainda traz uma série de considerações acerca desta base legal, como: (i) as obrigações decorrentes de lei de países terceiros não estão abrangidas; (ii) a obrigação tem de ser vinculativa, não pode haver discricionariedade em seu cumprimento; (iii) a obrigação legal deve ser clara quanto ao tratamento dos dados pessoais que exige.[116]

O fundamento para tratamento com base na "obrigação legal", por vezes se confunde com a base legal prevista para o "exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento", haja vista que as obrigações legais por vezes vão buscar o interesse público.

O interesse público aqui tratado, se refere aos objetivos pretendidos pela União Europeia ou um Estado-Membro, já a expressão "autoridade pública" abrange os agentes públicos ligados a União ou a um Estado-Membro, de modo que autoridades de países estrangeiros não tem o condão de se utilizar deste embasamento legal para o tratamento de dados. Aqui também se vislumbra dois cenários, (i) quando o próprio responsável pelo tratamento seja uma autoridade pública, sendo o tratamento necessário para exercício dessa autoridade ou em obrigação legal; (ii) quando o responsável pelo tratamento é um particular, mas lhe é feita a solicitação dos dados por uma autoridade pública. O presente embasamento

---

[114] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE**, p. 28.
[115] *Idem* – ***Op. Cit.***, p. 26.
[116] *Idem* – ***Op. Cit.***, p. 30.

tem um âmbito de aplicação muito amplo, o que requer uma interpretação estrita e uma identificação clara do interesse público, a depender do caso que está sendo tratado.[117]

Finalmente, a última base legal que ainda não foi tecida considerações é o "interesse vital" do titular dos dados pessoais ou de outra pessoa singular. Nesta hipótese, resta evidenciada a necessidade de uma situação em que o próprio titular ou o terceiro não estejam em condições de consentir com o processamento de seus dados, de modo que para salvaguardar o bem maior, que é a vida do indivíduo, permite a norma o tratamento dos dados pessoais que forem encontrados. O Grupo de Trabalho 29 considera que este embasamento legal deve ser interpretado de maneira estrita, ou seja, quando for possível conseguir o consentimento válido, este deve ser tentado, entende também que apenas é possível utilizar esta base em questões de vida ou morte ou, no mínimo em casos que acarretem riscos para a saúde da pessoa em causa[118].

2.2. Princípios relativos ao tratamento dos dados pessoais

Os princípios aplicáveis na tutela das informações pessoais estão expressamente previstos no art. 5º do Regulamento Geral de Proteção de Dados, classificando-os da seguinte forma: (i) licitude, lealdade e transparência; (ii) limitação das finalidades; (iii) minimização dos dados; (iv) exatidão; (v) limite da conservação; (vi) integridade e confidencialidade; (vii) responsabilidade.

Igualmente, a Lei Geral de Proteção de Dados brasileira também lista expressamente os princípios que lhe são aplicáveis, destacando a necessidade de observância da boa-fé e das seguintes normas: (i) finalidade; (ii) adequação; (iii) necessidade; (iv) livre acesso; (v) qualidade dos dados; (vi) transparência; (vii) segurança; (viii) prevenção; (ix) não discriminação; (x) responsabilização e prestação de contas.

Os princípios expostos servem como mais uma salvaguarda na proteção dos dados pessoais, haja vista que somente será lícito o processamento que observar as máximas acima declinadas, conforme previsto no diploma europeu e brasileiro.

Desta feita, não se aufere suficiente o consentimento, o interesse legítimo ou a adequação em algum dos outros fundamentos legalmente previstos, para que se configure a

[117] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE**, p. 33-35.
[118] *Idem* – ***Op. Cit.***, p. 32.

licitude deve o manuseio dos dados respeitar e se orientar pelos referidos princípios. Dada essa importância, passamos a análise sucinta de cada princípio previsto no RGPD.

2.2.1. Licitude, lealdade e transparência

A licitude demanda que previamente aos tratamentos dos dados pessoais é necessário investigar qual o embasamento legal para o processamento e se esta atividade observa os princípios orientadores da proteção dos dados pessoais. Em outras palavras, os controladores apenas poderão tratar as informações caso exista autorização e base legal para tal objetivo, principalmente levando em conta o que estiver delimitado pelos diplomas gerais, como o RGPD e a LGPD, e diplomas específicos, como aqueles que tratam de direito a saúde ou a proteção do crédito.[119]

Aliás, quando do tratamento das categorias especiais de dados pessoais, a RGPD não impede que os Estados-Membros estabeleçam situações específicas de tratamento, ou seja, circunstâncias especiais, dentre estas, há a possibilidade de estabelecer condições diversas de licitude para o tratamento.[120]

No que toca a lealdade, o manuseio das informações deve ser dar de maneira justa, no sentido de que quando for necessária a autorização do titular dos dados, a linguagem deva ser simples e acessível, indicando claramente as circunstâncias e instrumentos utilizados, para que se possa tomar uma decisão informada e consciente acerca da permissão para processamento. Ademais, dentro deste senso de justiça, também se pondera como o tratamento dos dados afeta diretamente o seu titular, e se este resultado é equitativo diante do embasamento legal que permitiu o manejo dos dados, *verbis gratia*, quando se faz o rastreio dos dados de navegação do usuário com o objetivo de verificar seu interesse e posteriormente lhe oferecer passagens ou serviços de hospedagem mais caro do que está sendo ofertado para outros consumidores.[121] A deslealde, neste caso, salta aos olhos, sendo evidente a ilicitude do tratamento empregado.

Dentro ainda da jurisprudência do Tribunal Europeu de Direitos Humanos, encontra-se o processo 61496/08, onde resta claro a necessidade de se comunicar ao titular dos dados pessoais qual será o tratamento das informações que serão coletadas. Na demanda em cotejo, discutiu-se a possibilidade de monitoramento do computador dos trabalhadores, tendo se

[119] BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentário ao GDPR**, p. 157.
[120] CONCLUSÕES do Advogado-geral Manuel Campos Sánchez-Bordona apresentadas em 27 de abril de 2023: Processo C-807/21 Deutsche Wohnen SE contra Staatsanwaltschaft Berlin, [em linha].
[121] BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentário ao GDPR**, p. 116.

decidido que faz-se necessário uma prévia comunicação ao empregado acerca do monitoramento dos dados durante o trabalho, sob pena de violação a privacidade do trabalhador.[122]

Por último, quanto ao princípio da transparência, o RGPD em seu considerando (58) aduz que as informações direcionadas ao titular dos dados ou ofertadas ao público devem se apresentar fácil compreensão e acesso, serem concisas, simples clara, possibilitando a visualização quando disponível. Ademais, conforme o relatório explicativo da Convenção 108+, por força do art. 8, o responsável é obrigado a agir de forma transparente, com a finalidade de garantir um tratamento leal, que possibilite ao titular dos dados compreender e exercer os seus direitos no contexto de tratamento dos dados pessoais. Para isto, deve ser publicizado de forma obrigatória algumas informações, como nome e endereço pelo do responsável pelo tratamento, o fundamento jurídico, as finalidades do tratamento, a categoria e o destino dos dados tratados.[123]

Assim, a transparência deve ser, ainda, proporcional ao potencial de processamento que possui o controlador no manejo dos dados e a capacidade dos titulares entenderem as novidades dos produtos e serviços que estão sendo ofertados. Nesse diapasão, deve o controlador dos dados presumir a vulnerabilidade quanto as possibilidades infinitas de manuseio das informações que foram coletadas, o que resulta em se empregar os termos e meios mais claros e acessíveis o possível para os usuários.[124]

Este foi o entendimento do TJUE no processo C-487/21, ao dispor que: "em conformidade com o princípio da transparência..., qualquer informação destinada ao titular dos dados deve ser concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples.".[125] A conclusão do Advogado Geral não foi diferente, acrescentando ainda que: (i) a facilidade de entendimento da informação (que denota a transparência) é necessária, inclusive, para o exercício dos direitos de acesso garantido pela RGPD; (ii) a transparência é uma condição prévia para o exercício integral dos direitos garantidos ao titular pelo RGPD.[126]

---

[122] EUROPEAN COURT OF HUMAN RIGHTS. COUR EUROPÉENNE DES DROITS DE L'HOMME –**Case of Barbulescu v. Romania No. 61496/08**, [em linha].
[123]COUNCIL OF EUROPE. COMMITTEE OF MINISTERS – **Convenção para proteção das pessoas relativamente ao tratamento de dados de carácter pessoal**, p. 24.
[124] BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentário ao GDPR**, p. 126.
[125] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – Acórdão de 4 de maio de 2023 (Primeira Secção) Processo 487/21, [em linha].
[126] CONCLUSÕES do Advogado-geral Giovanni Pitruzzella apresentadas em 15 de dezembro de 2022: Processo C-487/21 F.F. sendo intervenientes: Österreichische Datenschutzbehörde, CRIF GmbH, [em linha].

Diante do exposto, fácil perceber a razão pela qual o princípio da transparência é uma das pedras anulares para o tratamento lícito dos dados, estando reiterado em diversos pontos do RGDP, como no art. 1, (a) e art. 13.

2.2.2. Limitação das finalidades

Pela limitação das finalidades, resta legalmente consagrado no RGPD que os dados devem ser coletados com escopo específico, expresso e legítimo, obstando que sejam processados no futuro de uma maneira incompatível com a finalidade pelo qual foi primeiramente coletado. Em igual sentido, ao tratar do princípio da finalidade, a LGPD consubstancia que o processamento dos dados deve ser realizado com motivos legítimos, específicos, explícitos e informados ao titular, não havendo possibilidade de processamento em momento posterior que seja incompatível com as finalidades previamente estabelecidas. Logo, o processamento destas informações com outros objetivos que não os pré-determinados quando da coleta dos dados pessoais, somente poderia ser autorizado se houver compatibilidade com as finalidades iniciais, hipótese na qual não se fará necessário readequar o embasamento legal para o manuseio dos dados pessoais.

Esta limitação deve ser específica, no sentido de que os motivos para colheita das informações devem ser além de precisos, já identificados, isto antes mesmo que se proceda com a coleta, pois assim será possível identificar se o tratamento está dentro do propósito que foi apresentado. Fala-se em limitação expressa ou explícita, com o fito de salvaguardar que todos os envolvidos no procedimento de tratamento de dados, seja o titular dos dados ou o controlador, possuam a mesma compreensão acerca de qual é a finalidade do tratamento. Enfim, a legitimidade se consubstancia na formação do contexto jurídico pelo qual estão sendo tratados os dados, não limitado apenas pela base legal que o permite, mas também e eventualmente, em outros diplomas normativos que tratem da matéria[127].

Assim, nos termos do considerando (50) do RGPD um eventual tratamento secundário para o dado que foi coletado, poderá ser realizado caso se identifique as seguintes condições: (i) relações prévias do titular dos dados com o responsável pelo tratamento fazem presumir que há possibilidade de uma posterior utilização; (ii) o perfil das informações coletadas; (iii) as consequências que o processamento posterior apresenta para o tutelado; (iv) o estabelecimento de garantias adequadas para o processamento inicial e demais operações

[127]BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentário ao GDPR**, p. 236.

realizadas. Para além, o tratamento posterior para fins diversos pelo qual houve o recolhimento, é também possibilitado caso seja feito para arquivo de interesse público, com finalidade estatística ou de pesquisa acadêmica.

No mais, em uma adaptação do princípio a um mundo onde a circulação e o multiprocessamento de dados fazem parte de diversos modelos de negócios, principalmente dentro de um contexto em que as informações coletadas são indispensáveis para a prestação do serviço, fornecimento do produto[128], Moerel e Prins expõe ter ocorrido uma flexibilização da limitação a finalidade, possibilitando o tratamento posterior, com finalidades diversas das iniciais, em hipóteses que existam legítimo interesse do controlador dos dados ou para salvaguardar interesse público.[129]

2.2.3. Minimização dos dados

O processamento de dados pessoais deverá ser limitado as hipóteses em que é imperativo devido a natureza do produto ou da prestação do serviço ofertado, não se permitindo a coleta e manejo de informações para casos em que não haja real necessidade. No mais, sendo necessário, o controlador dos dados pessoais deve limitar o tratamento apenas aquilo que é relevante e imperioso para atingir a finalidade pretendida quando da coleta, mantendo as informações, igualmente, somente pelo tempo necessário para cumprimento do escopo pretendido. No mais, são encorajadas medidas que possibilitam desvincular os dados da pessoa que os produziu, como ocorre através da pseudonimização.[130]

O princípio em cotejo é de fundamental importância para o sistema, tendo em vista que nos dias atuais há uma tendência dos controladores de realizarem uma coleta cada vez maior das informações pessoais dos seus clientes e usuários, motivados pelo aumento na capacidade de processamento, na redução dos custos de armazenamento e na esperança que no futuro próximo os dados armazenados possam servir para viabilizar novos produtos e serviços.

Logo, a norma se apresenta como uma limitadora de condutas desde a coleta, resguardando que a manutenção dos dados se dará pelo período razoável e imperativo a sua

[128] Como ocorre em monitores/relógios da internet das coisas e dos dados fornecidos pelo usuário para prestar monitoramento de saúde, horas de sono, passos...
[129] MOEREL, Lokke e PRINS Corien – **On the Death of Purpose Limitation**, p. 10.
[130] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data Protection Law**, p. 15.

finalidade, tendo como fundamento também a salvaguarda dos direitos e liberdades individuais do titular dos dados.[131]

2.2.4. Exatidão

As informações pessoais coletadas deverão ser precisas e atualizadas, sendo obrigatório que se estabeleçam procedimentos para que os dados imprecisos, levando em consideração o escopo pelo qual está sendo processado, sejam apagados ou retificados em um prazo razoável. A LGPD traz uma definição legal para esta máxima vinculando a uma ideia de qualidade dos dados, no sentido de ser uma verdadeira salvaguarda do titular de que os dados coletados sejam exatos, claros, relevantes e atualizados.

Quanto a atualização dos dados, haverá casos em que não poderá o responsável promovê-la, haja vista que o abrigo da informação está sendo utilizada dentro de um contexto de resguardo dos acontecimentos históricos, como ocorre, por exemplo, em dados de saúde e cirurgia listados em prontuários médicos. Por outro lado, haverá situações em que é imperativo a atualização dos dados pessoais, bem como a verificação contínua de sua permanência, *verbis gratia*, o estado civil dos proprietários dos imóveis nos registros públicos, os quais devem ser objeto de conferência e eventual atualização antes da disponibilidade do bem pelo detentor do direito real.[132]

Portanto, afora tutelar a privacidade dos sujeitos, preocupa-se o princípio em mote em resguardar a identidade e estado do titular dos dados, haja vista que informações desatualizadas, incompletas ou imprecisas podem revelar, principalmente perante terceiros e aquele que realiza o tratamento dos dados pessoais, um alongamento do equívoco quanto ao status e identidade daquele que está tendo seus dados processados. Esta inexatidão e desatualização pode, inclusive, ter resultado danoso para o titular dos dados, como em casos de profiling, *scoring* ou histórico de saúde baseados em premissas que não mais se sustentam.[133]

O direito exatidão dos dados pessoais, aliás, está expressamente previsto no art. 18 do Regulamento Geral, onde consagra a possibilidade de o titular contestar o conteúdo dos dados armazenados com o objetivo de esclarecer as informações. Este direito já encontrava-se também previsto na Convenção 108+, no artigo 9, alínea (a), onde se prevê a possibilidade de

[131] BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentário ao GDPR**, p. 377.
[132] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data Protection Law**, p. 17.
[133] BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentário ao GDPR**, p. 408.

contestação de decisões puramente automatizadas com o objetivo de questionar, por exemplo, a inexatidão dos dados utilizados para a tomada de decisão.[134]

2.2.5. Conservação

Os dados pessoais deverão ser apagados ou anonimizados a partir do momento em que não tenham mais utilidade, baseando-se o prazo para o tratamento na finalidade pela qual foi realizado o acolhimento dos dados.[135] Em outras palavras, as informações apenas devem ser mantidas durante o prazo imperativo para finalizar o processamento com base no motivo pelo qual se fundamentou a coleta; findo este prazo, devem se promover o apagamento ou anonimização.

Ao tratar sobre o tema, o Tribunal Europeu de Direitos Humanos já definiu que as leis nacionais devem garantir que apenas sejam armazenados os dados relevantes ao tratamento que será realizado e que a identificação do titular dos dados (com base na informação armazenada) deve ser limitada ao período do tratamento.[136] Trata-se de salvaguardas previstas na jurisprudência para minimizar o processamento dos dados pessoais.

Assim, caso seja a manutenção dos dados implique na vinculação direta ao seu titular, urge ao responsável pelo tratamento deletar as informações coletadas. Contudo, caso haja a possibilidade de desentrelaçar o dado coletado da pessoa que o produziu, urge a manutenção das informações através da anonimização.

No mais, permite o RGPD que as informações pessoais coletadas possam ser conservadas em maior longevidade, desde que o processamento dos dado ser der com a finalidade exclusiva de investigação científica ou histórica, para arquivo de interesse público. Dentro do interesse público, estão incluídos, dentre outros, a proteção da segurança nacional, a investigação e repressão de infrações penais, a aplicação de sanções penais, a proteção do titular dos dados e a proteção dos direitos e liberdades fundamentais de terceiros.

---

[134] COUNCIL OF EUROPE. COMMITTEE OF MINISTERS – **Convenção para proteção das pessoas relativamente ao tratamento de dados de carácter pessoal**, p. 30.
[135] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data Protection Law**, p. 18.
[136] CONSEIL DEL'EUROPE – **S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 8 December 2008**, [em linha].

2.2.6. Integridade e confidencialidade

Os responsáveis pelos dados pessoais devem tomar medidas preventivas e saneadoras para impedir que ocorram violações dos bancos de dados, seja de modo proposital ou acidental, garantindo a segurança das informações armazenadas em face de acessos não autorizados ou ilícitos, destruição ou danificação acidental.

A integralidade e confidencialidade são máximas chaves para prevenir a perda ou o acesso não autorizado dos dados, de modo que o controlador dos dados deverá levar em conta os mecanismos atuais, os custos e a natureza da implementação dessas medidas preventivas, baseando-se na finalidade do tratamento, riscos que detém a atividade e a gravidade que decorrerá da perda ou eventual vazamento dos dados.

Com base neste premissa, é que o Conselho Nacional de Justiça, por exemplo, implementou o provimento 74/2018, dispondo sobre os padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil, formulando políticas mínimas de investimento pelas serventias extrajudiciais, baseando-se principalmente no faturamento e quantidade de processamento de dados pessoais realizados pelos cartórios.

2.2.7. Responsabilidade

A responsabilidade exige que seja implementado de forma ativa e contínua medidas para promover e salvaguardar a proteção de dados em suas atividades de processamento, bem como que o responsável possa demonstrar as medidas que são tomadas para observância da proteção dos dados pessoais. Nesse sentido, dispõe a Lei Geral de Proteção de Dados brasileira que o agente deve demonstrar a utilização de meios eficazes e capazes à proteção de dados, além disto deve comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Nesse ínterim, os controladores e processadores são responsáveis civilmente pela conformidade de suas operações de processamento com as leis de proteção de dados e suas respectivas obrigações, devendo ser capazes de demonstrar conformidade com as disposições de proteção de dados aos titulares dos dados, ao público em geral e às autoridades de supervisão a qualquer momento. Os processadores também devem cumprir algumas obrigações estritamente ligadas à prestação de contas (como manter um registro das operações de processamento e nomear um Encarregado da Proteção de Dados).

2.3. Tratamento de dados pessoais automatizados e não automatizados

Conforme exposto, o tratamento de dados pessoais consiste em qualquer operação realizada, seja de coleta, gravação, organização, estruturamento, classificação, guarda, adaptação, transmissão, uso, enfim, toda e qualquer etapa contida dentro do processamento das informações pessoais.

No art. 4º, 2 da RGPD, a expressão "tratamento" denota uma intervenção ou um conjunto de intervenções realizadas sobre dados pessoais ou sobre conjuntos de dados pessoais, de maneira automatizada ou não, tais como a recolha, a estruturação, a conservação, a alteração, a recuperação. O uso do vernáculo "tais como", na definição de tratamento, traduz uma enumeração não taxativa das formas de coleta e processamento apresentadas no dispositivo.[137]

Assim, sob a proteção do RGPD, observam-se, três níveis de automatização dos meios de tratamento: não automatizados (corresponde a um processamento manual dos dados), parcialmente automatizados (envolve uma intervenção humana apenas limitada) e totalmente automatizados (ocorre sem qualquer intervenção humana direta).

O tratamento não automatizado consiste no procedimento manual de categorização e armazenamento através de folhas soltas (ficheiros) ou livros manuscritos de dados pessoais de usuários de um serviço particular ou público. O Regulamento Geral de Proteção de Dados, no art. 4º, 6, dispõe que ficheiros são qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico. Por vezes, o tratamento manual é necessário e antecede o tratamento automatizado.

Nesta senda, no Processo C-25/17 (Tietosuojavaltuutettu x Jehovan todistajat — uskonnollinen yhdyskunta), o advogado geral concluiu que o agrupamento de informações pessoais não automatizada que tenha sido recolhida por membros de uma comunidade religiosa, no âmbito de uma atividade de pregação de porta em porta, em que seja estabelecida uma divisão geográfica desses dados, para posterior utilização em visitas, constitui-se em um ficheiro, logo, um tratamento de dados manual, resultando na responsabilidade da comunidade religiosa, mesmo que não tenha acesso aos dados pessoais que tenham sido recolhidos pelos seus membros.[138]

---

[137] CORREIA, Sergio Miguel – **Direito de Oposição à Definição de Perfis**, p. 190.

[138] CONCLUSÕES do Advogado-geral Paolo Mengozzi apresentadas em 1 de fevereiro de 2018: Processo C-25/17 Tietosuojavaltuutettu contra Jehovan todistajat — uskonnollinen yhdyskunta, [em linha].

De outro lado, o tratamento automatizado não tem uma definição positivada no RGPD, utilizando-se o diploma da técnica legislativa de conceito jurídico indeterminado, para que o aplicador do direito, no caso concreto e de acordo com o avanço da tecnologia da sua época, possa delimitar o que se entende ao seu tempo como um tratamento automatizado. Mas, apesar de não trazer um conceito definido, estabelece no art. 2º, ao dispor sobre o âmbito de aplicação material da RGPD, a tutela de proteção dos dados pessoais tratados de forma total ou parcialmente automatizada.

A Convenção 108+, o legislador fez a opção de trazer uma definição legal, referindo-se ao tratamento automatizado de dados como "qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, tais como a recolha, armazenamento, preservação, alteração, recuperação, divulgação, disponibilização, supressão, destruição ou execução de operações lógicas e/ou aritméticas sobre esses dados". Pode se perceber que diferencia do tratamento manual em razão da aplicação das precitadas operações lógicas ou aritméticas sobre os dados coletados.[139]

Nesta toada, a doutrina tem conceituado o tratamento automatizado como o processamento de informações realizada de forma completa ou parcial através de meios de automatização, como computadores, celulares, roteadores, podendo as referidas ferramentas utilizarem de diversos instrumentos, como algoritmos, big data e inteligência artificial.[140] Já o Grupo de Trabalho 29 define as decisões automatizadas como o processamento baseado em qualquer tipo de dado (fornecido, observado ou inferido) em que há a capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana.[141]

De fato, as formas de tratamento automatizado dos dados são as mais diversas e mais comuns. À título exemplificativo, o TJUE decidiu no Acórdão de 6 de novembro de 2003 (Grande Secção), Lindqvist (C-101/01, EU:C:2003:596), que referências contidas em um website, onde seja publicizado dados das pessoas, como nome, telefone, informações relativas às suas condições de trabalho e seus hobbies, configura-se como um tratamento de dados pessoais por meios total ou parcialmente automatizados.[142]

Dentro do tratamento automatizado é comum a utilização do algoritmo, seja qual a plataforma (computadores, tabletes, celulares, relógios inteligentes) que está sendo utilizada.

---

[139] COUNCIL OF EUROPE. COMMITTEE OF MINISTERS – **Convenção para proteção das pessoas relativamente ao tratamento de dados de carácter pessoal**, p. 30.
[140] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data protection law**, p. 97
[141] 29 DATA PROTECTION WORKING PARTY – **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**, [em linha].
[142] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 6 de novembro de 2003 (Grande Secção), Lindqvist (C-101/01, EU:C:2003:596)**, [em linha].

Por algoritmo se entende o conjunto de códigos lógicos e matemáticos que detalham como um computador processará informações para realizar uma tarefa ou alcançar um determinado resultado. Assim, um algoritmo será o procedimento informatizado que objetiva resolver problemas e/ou atingir objetivos, traduzindo-se em uma sequência de instruções que informam ao computador o que fazer para atingir um objetivo, modificando as informações de entrada em resultados que possam ser compreendidos por humanos.[143]

Em relação ao funcionamento, os algoritmos se dividem em: (i) programados, ou seja, os que seguem as operações definidas pelo programador, logo, após coleta da informação (*input*), o dado é processado nos termos que foram definidos pelo programador, para depois apresentador o resultado (*output*); (ii) não programados, as informações e o resultado planejado são coletados (*input)*,com base nestes dados, o algoritmo produz outro algoritmo, de modo que a programação também é feita de forma automatizada.[144] Assim, para construção de um algoritmo são necessários dados (informações a serem analisadas) e o resultado pretendido (definição de sucesso), razão pela qual O'Neil define o algoritmo como opiniões traduzidas em códigos.[145]

No processamento de dados pessoais, um algoritmo pode ser utilizado para automatizar o tratamento e a análise dessas informações, podendo ser utilizado em diversas etapas, como na coleta de dados pessoais; preparação das informações; análise e processamento (extraindo contextos, identificando correlações, realizando classificações, traçando perfis); e na tomada de decisões (recomendando produtos, avaliando riscos, personalizando conteúdos). Os algoritmos já ocupam parcela relevante da nossa vida, nos influenciando na tomada de diversas decisões cotidianas como, por exemplo, na seleção de empregados, na concessão de empréstimos, para cálculo de risco nos seguros, para recomendação de filmes e séries.[146]

Outra forma listada pela doutrina de tratamento automático é a utilização de *big data*. A referida expressão possui um conceito polissêmico, pode se referir ao conjunto de dados coletados em uma escala gigantesca, com múltiplas fontes e suportes; ou se referir a técnica de processamento de informações para resultar em um conhecimento altamente específico e direcionado do que foi manuseado. Ao se utilizar as técnicas empreendidas, dados brutos que

[143] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS – **Big data: discrimination in data-supported decision making**, p. 4.
[144] DOMINGOS, Pedro – **The master algorithm: how the quest for the ultimate machine learning will remake our world**, p. 2-6.
[145] O'NEIL, Cathy – **The era of blind faith in big data must end. TEDIdeas**, [em linha].
[146] COSTA, Diego Carneiro – **A Discriminação Algorítmica e as Novas Perspectivas Sobre o Tratamento De Dados Pessoais Sensíveis**, p. 165.

isoladamente não teriam qualquer valor, após lapidados através de algoritmos, resultam em grandes ativos. O implemento da análise de dados conforme modelos *big data* possui grande público, haja vista ser uma medida com custo reduzido e promessa de eficiência no tratamento da informação.[147]

No que pese na grande maioria dos casos se verificar uma análise pelo sistema *big data* adotando um modelo descritivo, chama a atenção do mercado os resultados que demonstram a capacidade preditiva (com a antecipação de comportamentos e acontecimentos) e prescritiva (com previsão da solução mais adequada para determinada questão). Os resultados produzidos são normalmente empregados através de decisões automatizadas.[148]

Afora o uso do sistema *big data,* hodiernamente, o processamento dos dados passou a ser realizado com a utilização de algoritmos que, através da experiência de tratamentos anteriores e tomando por base os dados históricos disponíveis, tem a capacidade de melhorarem automaticamente, ou seja, passaram a ter a habilidade de tomar decisões sem que haja uma programação expressa neste sentido. O referido processo de aprendizagem algorítmica autônoma é denominado de *machine learning*.[149]

Com efeito, a utilização de programas de aprendizado de máquina possibilita aos computadores a capacidade de desenvolvimento empírico e de tomada autônoma de decisões, dispensando, inclusive, qualquer intervenção humana após o desenvolvimento inicial do algoritmo, ao ponto de os próprios desenvolvedores terem dificuldade de entender como ou o porquê a decisão foi tomada pela máquina.[150] Nestes casos, podemos chegar ao ponto em que todo o procedimento seria automatizado, não havendo intervenção humana em mais nenhum dos momentos de tomada de decisões.

No mais, dentro desta evolução algorítmica que envolve o *machine learning* surge a "inteligência artificial", que pode ser definida como uma tecnologia que constrói a si mesma; o algoritmo é alimentado com uma série de casos, hipóteses e exemplos de dados de treino. Com esta informação, são identificados os padrões e correlações e, a partir destas conclusões, se extrai modelos de resposta baseados na configuração pretendida. Permite-se que os

---

[147] COSTA, Inês da Silva – **A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas**, p. 38.
[148] *Idem* – ***Op. Cit.***, p. 39.
[149] EDWARDS, Lilian; VEALE, Michael – **Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for**, p. 25.
[150] COSTA, Diego Carneiro – **A Discriminação Algorítmica e as Novas Perspectivas Sobre o Tratamento de Dados Pessoais Sensíveis**, p. 166.

computadores sejam treinados e programados para aprender, raciocinar, reconhecer padrões, tomar decisões e resolver problemas de forma autônoma.[151]

Em relação ao tratamento de dados pessoais, a inteligência artificial pode desempenhar um papel importante, sendo utilizada para identificar padrões e correlações, promover classificações ou antecipar possíveis resultados com base nas informações disponíveis, trazer recomendações personalizadas, analisar riscos, detectar fraudes, dentre outros.

O Regulamento Geral de Proteção de Dados estabelece condições específicas para o tratamento automatizado de dados pessoais, como o direito dos indivíduos de não serem sujeitos a decisões exclusivamente automatizadas com efeitos jurídicos significativos, conforme disposto em seu artigo 22. Ademais, o art. 9, 52 da Convenção 108+, dispõe acerca da possibilidade de contestação a decisões automatizadas, permitindo ao titular que tenha sido objeto destas decisões a oportunidade de justificar a eventual inexatidão dos dados pessoais antes da sua utilização, a irrelevância do perfil a aplicar à sua situação específica ou outros fatores que tenham impacto no resultado da decisão automatizada. Todavia, esse direito de contestação é relativizado caso a decisão automatizada tenha previsão legal, que além de permitir este tratamento automatizado, deve tutelar meios adequados para salvaguardar os legítimos interesses do titular dos dados.

Portanto, os algoritmos, sejam utilizados em um contexto de *big data* ou de inteligência artificial, devem ser projetados para permitir a intervenção humana, a revisão das decisões e a possibilidade de contestação pelos indivíduos afetados, motivo pelo qual, avulta a necessidade de transparência, privacidade e segurança no processamento automatizado dos dados pessoais, exigindo que as organizações adotem medidas técnicas e organizacionais adequadas para proteger a confidencialidade, integridade e disponibilidade dos dados envolvidos.

Diante das referidas possibilidades de tratamento automatizado dos dados, em um cenário em que é possível a criação de perfis, podendo inclusive resultar na inferência de dados sensíveis, quais os mecanismos de proteção que são estabelecidos atualmente para garantia da privacidade? É o que pretendemos tratar no nosso último capítulo.

[151] COSTA, Inês da Silva – **A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas**, p. 40.

3. DEFINIÇÃO DE PERFIS E DADOS SENSÍVEIS

3.1. Da definição de perfis

O art. 4º, 4) do Regulamento Geral de Proteção de Dados traz o conceito da definição de perfis (*profiling*), dispondo ser qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações. Nas conclusões do Advogado Geral do processo C-634/21 do TJUE, conceituou-se a categorização em perfis como a avaliação de aspetos pessoais para analisar ou prever a situação económica, a fiabilidade ou o comportamento de uma pessoa singular.[152]

Cumpre destacar que, tratando acerca da definição de perfis e das decisões automatizadas, o artigo 29, Grupo de Trabalho, definiu que o *profiling* resulta de um conjunto de deduções estatísticas, sendo normalmente utilizado para fazer previsões sobre um grupo determinado, para tanto recorre-se de informações decorrentes de fontes diversas. O objetivo principal é inferir algo sobre um indivíduo, com base nas informações que detém de outros sujeitos assemelhados. Ademais, assevera também que a simples divisão de indivíduos em classes diferentes não necessariamente leva à definição de perfis, esta somente ocorrerá quando a categorização for levada a efeito com o objetivo de se estabelecer uma previsão ou tirar uma conclusão acerca do titular dos dados pessoais.[153]

Nessa toada, podemos conceituar o *profiling* como qualquer meio de processamento automático de dados pessoais, que utilize as informações coletadas de um banco de dados único ou de diversos bancos de dados, para avaliar aspectos singulares de um indivíduo e através do cruzamento dos elementos coletados proceder com uma representação preditiva do titular dos dados ou sua categorização em determinado grupo. Em outras palavras, os perfis são mosaicos constituídos pelo tratamento automatizado de dados fornecidos pelo usuário, em

[152] CONCLUSÕES do Advogado-geral Priit Pikamäe apresentadas em 16 de março de 2023: Processo C-634/21 OQ contra Land Hessen, sendo interveniente: Schufa Holding AG, [em linha].
[153] 29 DATA PROTECTION WORKING PARTY – **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**, [em linha].

uma formatação igualmente composta e circunstanciada das informações pessoais coletadas, das pegadas digitais rastreadas e do cruzamento de dados.[154]

Para o Grupo de Trabalho 29, o *profiling* envolve as atividades de coleta de informações pessoais de um indivíduo, incluindo suas características e padrões de comportamento, a inclusão desses dados em um grupo de indivíduo similares, para pós-processamento se proceder com predições ou avaliação de capacidade.[155] Conforme, Lisboa Melo Junior, ao encontrar padrões de comportamento entre os indivíduos de um determinado perfil, é possível se presumir qual será a próxima conduta que será levada a efeito, exemplifica da seguinte forma: "se o indivíduo A for semelhante ao indivíduo B nas características 1, 2 e 3, então é plausível que se o indivíduo B tiver a característica 4, o indivíduo A também apresentará esta característica 4.".[156]

Assim, a definição de perfis, uma subcategoria de tratamento de dados pessoais, é composta por três elementos que lhe caracterizam: (i) tratamento automatizado; (ii) de dados pessoais; (iii) com o propósito de aspectos dos titulares.[157]

O primeiro elemento – tratamento automatizado – aqui já conceituado e estudado, consiste no processamento de informações realizada de forma completa ou parcial através de meios de automatização. Destarte, os processamentos de dados feitos de maneira não automatizada, ou seja, manuais, estão excluídos do escopo do profiling. Todavia, esse banimento do tratamento manual não significa que os tratamentos parcialmente automatizados estejam também excluídos. Logo, eventual intervenção humana não altera a essência do profiling, desde que seja restrita ou limitada, pois o requisito fundamental da definição de perfis é a utilização de algum tipo de tratamento automatizado, seja total ou parcial.[158]

A segunda condição acima apontada é que o tratamento se dê sobre dados pessoais.[159] O RGPD também traz uma definição do que são os dados pessoais, consubstanciando como aqueles que contenham qualquer informação relacionada a uma pessoa singular identificada ou identificável (quando pode ser diretamente ou indiretamente identificada). O conceito

---

[154] SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden – **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD)**, p. 87.
[155] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, p. 7.
[156] JUNIOR, Glauto Lisboa Melo – **O consumidor de seguros na era do big data: desafios da atual regulamentação europeia frente às técnicas de definição de perfis, aprendizagem de máquina e decisões automatizadas**, p. 2140.
[157] CORREIA, Sergio Miguel – **Direito de Oposição à Definição de Perfis**, p. 192.
[158] OLIVEIRA, Madalena Perestrelo de – **Definição de Perfis e Decisões Individuais Automatizadas no Regulamento Geral sobre a Proteção de Dados**, p. 85.
[159] Há uma análise mais profunda a respeito do que são dados pessoais no tópico onde são tecidas considerações a respeito dos dados pessoais sensíveis.

engloba dados objetivos, factuais ou subjetivos, em qualquer formato ou suporte. Toda informação pessoal será relevante, merecedora de proteção jurídica, por mais fútil que possa se apresentar isoladamente, assumindo a definição uma flexibilidade e extensão em seu conceito.[160]

Nesse sentido, a mera coleta de dados não caracterizados como pessoais de indivíduos que se encontram no território da União Europeia, por meio de aplicativos ou portais, por exemplo, não resulta automaticamente na aplicação do RGPD, que tem como âmbito de regulamentação a tutela dos dados pessoais. No entanto, se os dados coletados forem utilizados para de forma automática ou semiautomatizada traçar o perfil dos usuários, então recairá sobre o resultado do processamento a tutela do Regulamento Geral de Proteção de Dados.[161]

Por último elemento, dispõe o RGPD que a definição de perfis contemplará a avaliação de fatores pessoais de um sujeito com o objetivo de predeterminar comportamentos e preferências. Neste ensejo, o *profiling* se utiliza de modelos de análise preditiva para estabelecer padrões de comportamento a partir de um conjunto de informações que são analisadas, utilizando-se também de estatística e probabilidade, para se chegar ao resultado mais fidedigno possível.

As informações analisadas, findam por encaixar a pessoa analisada em determinados grupos ou categorias ou, ainda, caso se trate de um perfil personalizado de determinado indivíduo, além de estabelecer quais os traços pessoais do analisado, tem os algoritmos mais recentes a capacidade de detalhar com grande probabilidade de acerto comportamentos que ainda vão ser levados a efeitos, por exemplo, mediante a preferência política do analisado, em qual candidato ele irá votar, dentre outros.[162]

A definição de perfis se apresenta normalmente como não distributiva, ou seja, os perfis são probabilísticos, utilizando os dados coletados para fazer uma previsão. Desta maneira, o controlador dos dados é capaz de tomar diversas decisões relativas a um titular. Em um cenário de comércio, por exemplo, pode definir taxas de juros de um empréstimo de acordo com o perfil do seu cliente. Trata-se de uma abordagem atuarial, que tomam como

[160] CORREIA, Sergio Miguel – **Direito de Oposição à Definição de Perfis**, p. 192.
[161] BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentário ao GDPR**, p. 408.
[162] SILVEIRA, Alessandra – **Automated individual decision-making and profiling [on case C-634/21 - SCHUFA (Scoring)**, [em linha].

base os dados de comportamento passado para fazer predições futuras, tudo com base no perfil que foi definido.[163]

O Grupo de Trabalho 29 dispõe que são três as possíveis formas de utilização do *profiling*: (i) definição geral de perfis; (ii) tomada de decisão manual tendo em vista um perfil disponível e; (iii) tomada de decisões exclusivamente automatizadas tendo em vista um perfil disponível. A primeira hipótese abordamos acima de forma pormenorizada. As duas outras hipóteses apesar de parecerem semelhantes, não se confundem, diferenciando-se na medida em que a decisão final é tomada por um ser humano ou se um algoritmo tomou a decisão final.[164]

Não há óbice ao proveito de decisões parcial ou totalmente automatizadas, desde que estejam respeitadas as condições e princípios previstos no RGPD ou na LGPD e tenham um fundamento lícito para tratamento.

Para Zanatta, a definição de um perfil social e as inferências decorrente desta atividade implicam em obrigações de natureza: "(i) informacional, relacionada à obrigação de dar ciência da existência do perfil e garantir sua máxima transparência, (ii) antidiscriminatória, relacionada à obrigação de não utilizar parâmetros de raça, gênero e orientação religiosa como determinantes na construção do perfil, e (iii) dialógica, relacionada à obrigação de se engajar em um "processo dialógico" com as pessoas afetadas, garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e de como decisões são tomadas.".[165]

Finalmente, no que pese a grande influência que a RGPD exerce sobre a Lei Geral de Proteção de Dados do Brasil, quanto ao *profiling* a normativa europeia não foi observada em sua integralidade, tendo a norma tupiniquim sido menos restritiva a definição de perfis, ao excluir um conceito jurídico expresso para a atividade e ao não positivar uma regra geral proibitiva.

3.1.1. Mecanismos de tutela em razão da definição de perfis

O Regulamento Geral de Proteção de Dados, como já destacado, consagra uma série de normas a serem observados quando do tratamento dos dados pessoais. Em relação ao

[163] JAQUET-CHIFFELLE, David-Olivier – **Reply: Direct and Indirect *Profiling* in the Light of Virtual Persons**, p. 35.
[164] 29 DATA PROTECTION WORKING PARTY – **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**, [em linha].
[165] ZANATTA, Rafael Augusto Ferreira – **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**, p. 3.

profiling, prevê normas específicas para autorização do processamento, consagrando um sistema mais restritivo que o geral. Assim, além de positivar uma definição do instituto[166], aqui já analisada, consubstancia uma regra geral de proibição a esse tipo de tratamento, além de diretrizes interpretativas diversas em seus considerandos.

Importante destacar que as limitações referidas no artigo 22 do RGPD têm como escopo tutelar a dignidade humana, obstando que o sujeito seja submetido a um processo decisório totalmente automático, ou seja, sem qualquer intervenção humana, esta serve como garantia que o titular dos dados poderá expor seu ponto de vista, buscar explicações sobre a decisão e o processo de tratamento e, ainda, lhe abre a possibilidade de impugnar a decisão.[167]

Antes de adentrar no regime de tratamento especial, cumpre destacar a importância que assume o princípio da transparência, este, como já dito anteriormente, é uma das pedras de toque do sistema de proteção dos dados pessoais, e na definição de perfis terá como escopo salvaguardar a clareza e exatidão das informações processadas, garantindo ao titular acesso aos instrumentos e modo que foram utilizados para o tratamento dos seus dados pessoais, bem como as consequências que poderão advir. Neste diapasão, caso haja definição de perfis e decisões automatizadas, com fulcro no art. 13, 2, 'f' do RGPD, devem os responsáveis pelo tratamento fornecer informações adicionais para garantir a transparência. Logo, diante do profiling, é necessário aplicar ao tratamento o princípio da transparência, de modo que o indivíduo seja informado sobre a realização do perfil e advertido acerca das possíveis consequências.[168]

Ademais, fundamental é a previsão legal, tanto no RGPD quanto na LGPD de um direito de oposição, o qual estabelece mecanismos para que os indivíduos possam refutar o tratamento de seus dados pessoais quando houver uma definição de perfis. Nessa esteira, prevê o RGPD que os indivíduos têm o direito de se opor a qualquer momento, por motivos relacionados à sua situação particular, ao tratamento de seus dados pessoais, incluindo a definição de perfis (Artigo 21 do RGPD). Outrossim, a LGPD assegura o direito de oposição ao titular dos dados (Artigo 18 da LGPD), dispondo que os titulares podem se opor ao tratamento com base em uma definição de perfis, ressalvada a hipótese em que exista uma base legal que justifique o tratamento, neste ponto, a lei brasileira é mais branda, excetuando e relativizando o direito de oposição.

---

[166] A Lei Geral de Proteção de Dados não possui conceito legal da definição de perfis, nesta hipótese estabelece proteção semelhante a aplicada as outras formas de tratamento.
[167] CONCLUSÕES do Advogado-geral Priit Pikamäe apresentadas em 16 de março de 2023: Processo C-634/21 OQ contra Land Hessen, sendo interveniente: Schufa Holding AG, [em linha].
[168] BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentários ao GDPR**, p. 140.

Prosseguindo, o art. 22, item 1 do RGDP estabelece o direito pessoal do titular dos dados de não se sujeitar a decisões tomadas de forma exclusivamente automatizada com base na definição de perfis, estabelecendo uma regra geral de proibição do *profiling*. Apesar da terminologia utilizada, o dispositivo legal deve ser interpretado no sentido de que não há necessidade do titular dos dados invocar ativamente o direito, na verdade, aqui resta estabelecida uma proibição geral das decisões exclusivamente automatizadas que produzam efeitos na esfera jurídica ou que afetem significativamente o titular dos dados.[169] Desta feita, O doutrinador Bkran estabelece que para caracterizar a proibição em mote, três são os elementos que devem ter a decisão: (i) deve ser individual; (ii) baseada em processo automatizado de dados; (iii) com efeitos legais relevantes para o titular dos dados.[170]

Nessa esteira, exige-se uma decisão individualizada, pois com fulcro no art. 1º do RGPD, a arquitetura protetiva de dados pessoais é destinada à tutela das pessoas singulares, deduzindo-se a inaplicabilidade do sistema normativo quando as decisões são tomadas tendo em face um grupo ou coletividade, logo, há uma diferença no tratamento dos dados singulares e coletivos.

Em razão do exposto, é comum que os responsáveis pelo tratamento automatizado de dados trabalhem com o *profiling* em uma perspectiva grupal, isto é, categorizando perfis com características semelhantes em grupo e tomando a mesma decisão para o grupo todo. O objetivo deste método de tratamento é se afastar do âmbito de aplicação do regulamento. Contudo, defende Bkran que, neste mote, pode-se considerar que o que houve na verdade foi uma decisão única para diversos indivíduos, de modo que seria aplicável o regulamento, proibindo a definição de perfis.[171]

A segunda condição estabelecida para a proibição, é a de que a decisão seja tomada por meios de processamento exclusivamente automatizados. Por processamento automatizado, se entende aquele em que o responsável pelo processamento não possui poderes para influenciar na decisão final, seja para modificar ou rejeitar o que restou decidido pelo algoritmo.[172]

Como última condição, exige-se que a informação processada possa resultar em violação a legítimos interesses do titular dos dados ou o afete de maneira significativa. Neste

[169] CONCLUSÕES do Advogado-geral Priit Pikamäe apresentadas em 16 de março de 2023: Processo C-634/21 OQ contra Land Hessen, sendo interveniente: Schufa Holding AG, [em linha].
[170] BRKAN, Maja. – **Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond**, p. 9.
[171] *Ibidem*.
[172] TODOLÍ-SIGNES, Adrian – **Algorithms, artificial intelligence and automated decisions about workers and the risks of discrimination: The necessary collective governance of data protection**, p. 10.

ponto, uma decisão ou processamento utilizado, por exemplo, apenas para fins de pesquisa científica ou de estatística não teriam o condão de produzir qualquer efeito danoso ao titular dos dados, de modo que seria inaplicável a salvaguarda prevista no art. 22 da RGPD nesta hipótese. De outro lado, nos termos do considerando 71, a recusa automática de um pedido de crédito por via eletrônica é um exemplo claro de decisão que resulta em clara violação dos interesses legítimos do titular dos dados.

Por outro lado, a proibição de definição de perfis, nos termos do art. 22, 2 do RGPD, não será aplicada em três hipóteses: (i) para celebração ou execução de um contrato entre o controlador e o titular dos dados; (ii) quando houver consentimento explícito do titular; (iii) em razão de autorização legislativa da União Europeia ou Estado Membro autorize, desde que haja previsão de salvaguarda a outros direitos do titular.

Na primeira hipótese, é relevante a discussão acerca de quando será necessária uma definição de perfil para celebração ou execução de um contrato. Neste ponto, converge a doutrina que não se demanda que o tratamento seja absolutamente indispensável para realização do contrato, mas sim que deve ser observada uma razoabilidade entre o motivo para o tratamento dos dados e os direitos do seu titular, logo, configura-se a necessidade quando houver uma relação de causalidade entre o tratamento e a finalidade do contrato, não podendo o escopo do contrato ser atingido por outros meios.[173]

Em relação a segunda possibilidade, é permitida a definição de perfis quando houver o consentimento explícito do titular dos dados, isto é, o consentimento dado de forma livre, específica e informada, limitada ainda a finalidade para os estritos termos que foram autorizados. Trata-se de hipótese criticada, pois é comum o desequilíbrio entre as partes nas relações jurídicas em que há a definição de perfis. Como forma de validar essa disposição legal, formulou-se a ideia de que a permissão somente será tida como válida, nos casos em que o titular for informado sobre a possibilidade de a decisão ser tomada de forma automatizada, podendo ainda indicar o tipo de tratamento utilizado e inexista qualquer coerção para adoção do procedimento ou consequências negativas no caso de não ser dada a anuência.[174]

Enfim, para que se configure a terceira previsão para possibilitar a definição de perfis, exige-se que haja previsão legal de medidas adequadas para resguardar os direitos e legítimos

[173] RUCKER, Daniel; KUGLER, Tobias – **New European general data protection regulation, a practitioner´s guide: ensuring compliant corporate practice**, p. 150.
[174] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, p. 6.

interesses do titular dos dados, devendo haver esta autorização pela União ou Estado Membro a que o responsável do tratamento esteja sujeito.

Mais adiante, o art. 22, 3 do RGPD prevê a possibilidade de revisão das decisões tomadas em razão do profiling, com base no dispositivo, pode-se exigir que o controlador dos dados empreenda as medidas adequadas para resguardar direitos e legítimos interesses do titular dos dados, garantindo a possibilidade de intervenção humana para contestação da decisão tomada.[175]

Nessa esteira, resta positivado no regulamento o princípio do *human in the loop*, ou seja, a exigência da influência de humanos perante os sistemas automatizados, garantindo aos indivíduos o desempenho de papel relevante no treinamento, validação e supervisão dos algoritmos, para que assim possa haver melhor qualidade e precisão dos sistemas automatizados[176]. Em igual sentido, o considerando 71 do RGPD aduz que quando admitido o processamento automatizado, faz-se obrigatório o estabelecimento de instrumentos necessário a proteção dos dados, sendo a intervenção humana uma das medidas previstas.

Já o artigo 22, 4 c/c artigo 9º do RGPD, veda as definições de perfis com base em dados pessoais sensíveis, apenas possibilitando esse tratamento quando houver consentimento explícito do titular dos dados ou por motivos de interesse público, desde que respeitados direitos e liberdades e, ainda, os legítimos interesses do titular.

No que pese a arquitetura de proteção quando da definição de perfis acima exposta, ainda há uma preocupação crescente que novos meios de tratamentos automatizados de dados, muitas vezes sem qualquer intervenção humana em quaisquer dos processos, venha a resultar em ingerências indevidas sobre os direitos fundamentais da privacidade e da proteção dos dados pessoais.

Com efeito, tem se observado que os setores público e privado investem em novas formas de tratamento automatizado de um grande volume de dados e aperfeiçoamentos na definição de perfis, cada vez com menos participação humana no processo, por meio de algoritmos que muitas vezes tem seu processo decisório desconhecido pelo operador, resultando com isso em novas maneiras de explorar as informações, mas também em novos riscos a dignidade da pessoa humana.

Neste cenário, além das disposições acima elencadas, urge a aplicação da privacidade e da proteção de dados por design, no sentido de que a incorporação dos referidos direitos

[175] A princípio, a LGPD consagrava dispositivo semelhante, tendo a exigência de participação humana nas decisões automatizadas sido vetada.
[176] JONES, Meg Leta – **The right to a human in the loop: Political constructions of computer automation and personhood**, p. 4.

fundamentais no tratamento de dados automatizados deve ser um padrão da indústria de tratamento de dados, de modo que se tornem parte indissociável e a premissa fundadora de qualquer processamento de informações.[177] Neste cenário, uma engenharia da computação que tenha uma consciência direcionada a tutela da privacidade e da proteção de dados é primordial, para que a transparência e o controle do usuários sobre os seus dados se torne uma realidade.[178]

Ao tratar sobre a privacidade por design, Cavoukian estabelece sete princípios que devem ser incorporados ao tratamento de dados para que este promova a salvaguarda dos direitos fundamentais aqui tratados em todas suas etapas, são estes: (i) privacidade proativa e preventiva, o resguardo à proteção de dados deve se antecipar aos eventuais riscos que possam surgir do seu tratamento, corrigindo impactos negativos antes que eles aconteçam; (ii) privacidade por padrão, dados pessoais devem ser automaticamente protegidos no tratamento, não sendo necessário qualquer comportamento do titular dos dados neste sentido; (iii) privacidade codificada, no sentido de que deve ser parte essencial do algoritmo que proceda ao tratamento dos dados, e não um elemento a mais; (iv) funcionalidade total, de modo a imaginar soluções em que a privacidade e a proteção de dados sejam totalmente respeitadas mesmo em cenários onde haja aparente colisão com outros direitos fundamentais; (v) segurança de ponta a ponta, de modo a garantir que qualquer informação coletada seja mantida apenas pelo tempo necessário ao tratamento e logo depois de processada seja devidamente descartada; (vi) transparência, os algoritmos e métodos utilizados para o tratamento dos dados devem ser acessíveis e transparentes para o usuário e controladores; (vii) respeito pelo titular dos dados, que deve ser o centro das atenções quando da programação dos algoritmos para processamento dos dados.[179]

Neste sentido, o Regulamento Geral estabelece em seu artigo 25, (1), a previsão de uma proteção de dados desde a concepção, ou seja, antecipando um mundo cada vez mais revolucionário no que toca ao tratamento e exploração dos dados e os riscos decorrentes destas inovações, o RGPD estabelece que deve o responsável, no momento de definição dos meios de tratamento e no processamento, empregar as medidas técnicas e organizativas adequadas, com o fito de aplicar com eficácia os princípios da proteção de dados, trata-se da previsão legal de uma privacidade (ou proteção de dados) por design. Ademais, resta também

[177] CAVOUKIAN, Ann – **Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices**, [em linha].
[178] EUROPEAN DATA PROTECTION SUPERVISOR – **Opinion 7/2015: Meeting the challenges of big data**, p. 14.
[179] CAVOUKIAN, Ann – **Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices**, [em linha].

positivada a privacidade (ou proteção de dados) por padrão, ao se estabelecer no item (2) que o responsável deve por padrão estabelecer medidas técnicas e organizativas que assegurem o tratamento restrito dos dados pessoais, ou seja, que apenas se processe as informações que forem necessárias para cada finalidade específica do tratamento, estabelecendo, ainda a intervenção humana para que os dados pessoais sejam disponibilizados a um número indeterminado de pessoas. Assim, a proteção de dados por design e por padrão pode ser legalmente imposta aos responsáveis pelo tratamento de dados.[180]

A proteção de dados por design e por padrão desempenha um papel fundamental na garantia da privacidade, ao consagrar diretrizes e princípios inerentes a proteção de dados em todas as etapas do tratamento de dados, principalmente de maneira preventiva e proativa, buscando afastar eventual violação aos direitos fundamentais aqui tratados desde a programação dos sistemas de tratamento de dados automatizados.

De acordo com as linhas traçadas, percebe-se que o RGPD e a LGPD consagram uma arquitetura robusta de previsões normativas que devem ser observadas pelo setor privado e público nas hipóteses em que ocorram definição de perfis. O responsável pelo tratamento dos dados além de seguir de forma rígida os princípios que regem a atividade, deve aplicar em todas as etapas do processamento a proteção de dados como um padrão, desde a concepção do algoritmo até a tomada de decisão, para posteriormente observar também os limites referentes ao tratamento de quando da definição de perfis.

Contudo, mesmo diante deste regime jurídico robusto estabelecido, o atual poder de processamento de dados e de informações disponíveis é tão grande que por vezes, a definição de um perfil ou o cruzamento das informações que estão sendo tratadas resulta na publicização de um dado sensível.

Mas o que são dados sensíveis e como o *profiling* em um exercício de inferência pode vir a criar informações sensíveis resultando em riscos e possibilidade de discriminação ao titular dos dados pessoais? No mais, caso isso ocorra, quais são os mecanismos de tutela previstos no RGPD e no LGPD, bem como listados pela doutrina que podem salvaguardar o sujeito do processamento? As referidas perguntas serão respondidas nas próximas linhas.

[180] KURTZ, Christian; SEMMAN, Martin; BÖHMANN, Tilo – **Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors**, p. 2.

3.2. Dados pessoais sensíveis

3.2.1. Definição

De início, cumpre estabelecer um conceito do que são "dados pessoais" e qual a abrangência da sua definição, para posteriormente tecermos considerações acerca da definição dos dados pessoais sensíveis, bem como suas acepções materiais e formais.

Por dados, entende-se a informação que identifica ou quantifica elementos atinentes a pessoas ou coisas, logo, são representações de uma informação em determinada configuração que foi convencionada para facilitar o seu tratamento. Já pessoal é tudo aquilo que é inerente à pessoa ou exclusivo de certa pessoa.[181]

A definição do que seriam dados pessoais, não é uniforme globalmente e, dependendo da conotação dada pelo regime jurídico que lhe seja correspondente, irá resultar em uma concepção restritiva ou ampliativa, tendo como paradigma de extensão do conceito o fato de serem as pessoas identificáveis ou identificadas.

Neste ensejo, na abordagem restrita, dados pessoais se referem a informações que dizem respeito a pessoas identificadas, isto é, dados relacionados a alguém conhecido e individualizado em meio a certo grupo. Por outro lado, na concepção ampla, que é a prevalecente na doutrina, amplia-se o alcance para incluir também as representações sobre pessoas identificáveis, de modo que se considera um dado como pessoal independente da presença de identificadores diretos.[182] Conceitua-se como identificável, o sujeito que possa ser caracterizado, direta ou indiretamente, seja através de um número de identificação ou de outros elementos relacionados a sua identidade física, fisiológica, psíquica, económica, cultural ou social.[183]

Desta feita, para o nosso estudo, levando em conta o ordenamento jurídico europeu e brasileiro, importa definir os dados pessoais como um representações que dizem respeito a vida de um indivíduo identificado ou identificável, sejam essas informações relacionadas a alguns dos aspectos da personalidade (como nome, privacidade, imagem) ou eventos históricos relacionados ao titular dos dados. Os dados pessoais não se referem apenas a quem "sou", mas também ao que "fiz".

---

[181] DINIZ, Maria Helena – **Dicionário jurídico**, p. 3.
[182] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**, p. 58.
[183] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 19 de outubro de 2016, no caso Breyer (C-582/14, EU:C:2016:779)**, [em linha].

Corroborando com o exposto o, TJUE no processo C-487/21, consagrou uma definição ampla do conceito de «dados pessoais», de modo que o entendimento foi que este não abarca somente as informações recolhidas e conservadas, mas inclui também os dados resultantes de um processamento dos dados que digam respeito a uma pessoa identificada ou identificável, tais como a apreciação da sua solvência ("quem sou") ou da sua intenção de pagar ("o que fiz ou pretendo fazer").[184]

O RGPD, em seu artigo 4º estabelece uma definição sucinta acerca dos dados pessoais, consagrando estes como a informação relativa a uma pessoa singular identificada ou identificável. Em complemento, cumpre registrar que o Grupo de Trabalho 29, agora conhecido como Comitê Europeu de Proteção de Dados, estabeleceu que para um dado ser considerado pessoal, o conteúdo, o motivo ou o resultado da informação processada deve dispor a respeito de um sujeito identificado ou identificável.[185]

Os tipos dados pessoais são diversos, podem dispor acerca de múltiplos elementos que permeiam o indivíduo, por exemplo, são consideradas informações pessoais: o nome, endereço, número de telefone, histórico acadêmico, dados bancários, estado civil, ligações familiares, dentre outros. Igualmente, diversificado são os meios em que se pode exteriorizar essas informações: ficheiros, jornais, revistas, escritura públicas, fotografias, pen drives, discos rígidos, armazenamento em nuvem, etc.. O dado pessoal não será definido em razão do seu suporte, seja este físico ou digital, mas sim pela separação da informação que é parcela da intimidade de um indivíduo, de sua pessoa, vindo a ser exteriorizada pela fixação em determinado suporte.[186]

Até mesmo dados que não são ligados diretamente ao indivíduo ou que não lhe identifiquem *prima facie* podem ser considerados dados pessoais. Quanto ao tema em cotejo, o Acórdão de 19 de outubro de 2016, no caso Breyer (C-582/14, EU:C:2016:779) do Tribunal de Justiça da União Europeia (TJUE), definiu que os endereços IP dinâmicos (*internet protocol*), em certas circunstâncias podem ser considerados dados pessoais, haja vista a possibilidade do responsável pelo processamento de dados identificar o indivíduo associado a um endereço dinâmico, através do cruzamento de informações que detém. [187]

---

[184] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 4 de maio de 2023 (Primeira Secção) Processo 487/21**, [em linha].
[185] WACHTER, Sandra; MITTELSTADT, Brent – **A right to reasonable inferences: re-thinking data protection law in the age of big data and AI**, p. 25.
[186] GUIDI, Guilherme Berti de Campos – **Proteção de Dados Pessoais: a composição de sistemas pelo Direito Internacional**, p. 19.
[187] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 19 de outubro de 2016, no caso Breyer (C-582/14, EU:C:2016:779)**, [em linha].

Logo, os dados pessoais não são apenas aqueles produzidos pelo seu titular. As inferências feitas por algoritmos ou através de um processamento manual também podem ser consideradas dados pessoais. Esse tema assume grande relevância, haja vista que só estão protegidos pelo escopo do RGPD e da LGPD os dados pessoais (abrangência material de aplicação do diploma normativo) e não todo e qualquer dado. Por inferências se compreende os dados obtidos do processamento automatizado ou manual, os quais utilizam métodos indutivos para processar informações relacionadas a uma pessoa identificada ou identificável. Esse processamento é capaz de extrair conclusões e informações adicionais com base nos dados brutos que tenham sido disponibilizados, resultando assim na criação de novos dados relevantes sobre o indivíduo em questão. Se o dado criado puder identificar ou tornar identificável certo indivíduo, estamos diante de um dado pessoal.

Se dados pessoais são qualquer informação relacionada a pessoa identificada ou identificável, quando os resultados do processamento dispuserem acerca de pessoa identificada ou identificável, essas inferências são consideradas como fazendo parte dos dados pessoais, pois relacionadas à identidade ou características da pessoa em questão. Embora os dados inferidos não tenham sido diretamente fornecidos pela própria pessoa, eles são obtidos por meio de análise e processamento de outros dados pessoais relacionados a ela.

Como o RGPD adota uma abordagem ampla e abrangente no conceito de dados pessoais, reconhecendo que os dados podem ser combinados e analisados para revelar informações adicionais sobre uma pessoa (como na definição de perfis), as inferências feitas são consideradas também como dados pessoais. Isso implica que esses dados estão sujeitos às disposições do RGPD, incluindo os princípios de proteção de dados, direitos dos titulares dos dados e obrigações para os controladores e processadores de dados.[188]

Destas primeiras linhas podemos concluir que a definição de dados pessoais é elástica abrangendo, tanto os dados produzidos diretamente, quanto os produzidos indiretamente por pessoa física identificada ou identificável. Assim, uma vez caracterizado como pessoal, o dado estará resguardado de maneira geral pela RGPD, no cenário europeu, e pela LGPD, no Brasil.

Prosseguindo, alguns dados por conterem em seu conteúdo informações delicadas, ligadas a vida privada, liberdade e dignidade da pessoa humana, foram objetos de tratamento especial pela legislação, estabelecendo uma maior limitação no seu processamento.

---

[188] WACHTER, Sandra; MITTELSTADT, Brent – **A right to reasonable inferences: re-thinking data protection law in the age of big data and AI**, p. 20.

Trata-se dos dados pessoais sensíveis, categoria especial de dados pessoais, que tem na sua acepção material o reconhecimento de que o armazenamento, processamento e circulação de certos tipos de informações resultam em um maior risco maior à pessoa singular, especialmente quando consideradas práticas discriminatórias. Corroborando com exposto, Doneda aduz que o conceito de dados sensíveis serve para definir uma área na qual a probabilidade de uso discriminatório das informações é potencialmente mais alta.[189]

De fato, considerando a diversidade de dados pessoais possíveis de serem coletados, há aqueles que possuem uma maior propensão a contribuir para processos sociais de exclusão e segregação, o que justifica materialmente sua qualificação como dados sensíveis. A atribuição dessa adjetivação é fundamental para uma abordagem mais cuidadosa e protetiva em relação a esses dados, visando salvaguardar a privacidade, liberdade, igualdade e dignidade da pessoa humana.[190]

Com efeito, com fulcro no art. 6, 55 da Convenção 108+, o tratamento de dados que contenham informações sensíveis pode resultar em violações dos interesses, direitos e liberdades das pessoas, principalmente quando observado que esse processamento possa resultar em um potencial risco de discriminação ou dano à dignidade ou integridade física de alguém, por exemplo, quando a esfera mais íntima da vida da pessoa, como sua vida sexual ou orientação sexual, está em jogo, ou quando o processamento de dados pode afetar a presunção de inocência.

Assim, partindo desse entendimento que os riscos ligados à circulação e ao tratamento dos dados pessoais sensíveis tem o condão de resultar em situações discriminatórias e de desigualdade, é que se justifica a consagração de um regime jurídico diferenciado com disposições próprias, direcionada a essa categoria.[191]

Ademais, no que pese qualquer informação possa ser processada com um escopo discriminatório, o potencial lesivo é maior que a média quando estamos diante do tratamento de dados sensíveis. Aliás, a própria classificação de uma informação como sensível é resultado da necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória é potencialmente maior que nas outras.[192]

---

[189] DONEDA, Danilo – **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**, p. 27.
[190] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**, p. 42.
[191] NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana**, p. 73.
[192] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 163.

Nesse sentido, o considerando (51) do RGPD aduz que merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Em igual sentido, dispõe o art. 6, 56 da Convenção 108+, ao dispor que o tratamento dos dados sensíveis deve dispor de mecanismos de tutela próprios, que levem em consideração os riscos em causa e os interesses e direitos que visa proteger.

Além deste caráter material do conceito, orientado ao potencial lesivo à igualdade material e, consequentemente, ao potencial discriminatório, também há uma acepção abstrata/formal, dispondo serem os dados sensíveis àqueles consagrados normativamente, ou seja, tem-se uma enumeração de dados pessoais especiais com base em seu conteúdo informativo, por conseguinte, são especificados abstratamente quais dados pessoais são considerados sensíveis.[193]

Logo, dentro do caráter formal, o dado pessoal sensível é definido aprioristicamente, por meio de uma lista exaustiva e limitada de situações jurídicas objetivas. Ao atribuir a qualificação de sensível a um determinado dado, consequentemente, é aplicado um conjunto de normas legais próprias, especialmente mais protetivas, devido aos riscos envolvidos no seu tratamento.[194]

Nesse diapasão, o Regulamento Geral de Proteção dos Dados Pessoais consubstancia em seu artigo 9º, um tratamento diferenciado para os dados com os seguintes conteúdos: origem racial/étnica, opiniões políticas, convicções religiosas/filosóficas, filiação sindical, dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde/vida sexual/orientação sexual.

No que pese o rol estabelecido pelo artigo 9º, acima reproduzido, não se pode considerar exaustivo o rol legal de dados sensíveis. Como já exposto, a possibilidade de cruzamento de informações, a utilização de inteligência artificial e algoritmos, conduz a cenários de discriminação do indivíduo através de dados que em um primeiro momento não teriam esse condão. Nesta senda, tem-se observado nos Estados Unidos a negativa de concessão de crédito para pessoas cujos nomes são mais recorrentes na comunidade afrodescendente, por exemplo. Assim, evidencia-se que o prenome, que aprioristicamente não

[193] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**, p. 45.
[194] NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana**, p. 74.

foi considerado um dado sensível pela norma em tela, a depender das circunstâncias em que foi tratado, pode ser considerado um dado sensível para fins de tutela da igualdade e dignidade do titular do dado.[195]

A partir da construção delineada, verifica-se que os dados pessoais sensíveis comportam uma definição que abrange tanto aspecto material, no sentido de tutelar dados pessoais que por sua natureza o processamento possa acarretar riscos discriminatórios; quanto o aspecto formal, onde a definição decorre do enquadramento do dado dentro das hipóteses normativas previstas pela legislação de proteção dos dados pessoais. Desta forma, os dados sensíveis representam pedras angulares da privacidade. São dados que devido à sua natureza e ao tipo de informações que contêm, podem levar à discriminação ilegal ou abusiva do seu titular, e, portanto, devem receber uma proteção mais rigorosa e precisa.[196]

Para além, caracterizado como um dado pessoal sensível, há mecanismos de tutela especial estabelecidos no Regulamento Geral de Proteção de Dados e na Lei Geral de Proteção de Dados, o tópico abordará as salvaguardas previstas nos referidos diplomas normativos.

3.2.2. Mecanismos de tutela dos dados pessoais sensíveis

Diante das considerações feitas acima, acerca da definição e característica dos dados sensíveis, como um tipo especial de dado pessoal, importa no presente momento identificar os meios de tutela previstos no RGPD e na LGPD para a proteção desta categoria especial de informação, onde será possível atestar que em comparação ao regime comum de proteção aos dados pessoais, estamos diante hipóteses mais restritas para o tratamento.

Com efeito, o considerando (51) do RGPD consagra expressamente que os dados pessoais sensíveis, em razão de sua natureza que os vincula aos direitos e liberdades fundamentais, deve ser objeto de um tratamento diferenciado, devendo ser estabelecida uma proteção específica. Ademais, consubstancia também que além dos requisitos específicos para o tratamento de dados neste caso, devem também ser aplicadas os princípios gerais e outras disposições do regulamento, em especial no que se refere às condições para o tratamento lícito.

---

[195] TEPEDINO, Gustavo; TEFFÉ, Chiata Spadaccini de – **O Consentimento na circulação de Dados Pessoais**, p. 104.
[196] RODOTÀ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje**, p. 96.

Neste sentido, além das disposições principiológicas e regras de tratamento aqui já apontadas, o RGPD e a LGPD estabelecem outras amarras ao processamento de dados sensíveis, as quais serão abordadas a seguir.

3.2.2.1. Do Consentimento qualificado

Como exposto, o consentimento se apresenta como um dos fundamentos legais positivados que autorizam o tratamento dos dados pessoais. Trata-se de uma faculdade conferida pela lei ao titular dos dados que outorga a possibilidade de modificação da própria esfera jurídica, no sentido de permitir que terceiros coletem e processem as informações pessoais do sujeito.

No regime geral de proteção de dados pessoais, o RGPD conceitua o consentimento como uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Já em relação aos dados sensíveis consagra o art. 9º, 2) 'a' que a anuência deve ser explícita e a finalidade específica para o processamento dos dados pessoais. Em igual sentido, o art. 11, I da LGPD, estabelece que na ocorrência de tratamento de dados pessoais sensíveis o consentimento deve ser dado de forma específica e destacada e para finalidades específicas.

A qualificação do consentimento através da atribuição de requisitos próprios (explícito e com finalidade específica), considerando a essência dos dados pessoais que serão tratados, é o que distingue a priori o regime especial do tratamento de dados sensíveis. Justifica-se tal medida, pois o titular dos dados pessoais está em posição vulnerável na relação jurídica com o controlador dos dados, pois na maioria dos casos está comprometendo uma parcela dos seus direitos para a contratação de um serviço ou aquisição de um produto.[197]

Entrementes, ressalta-se que com o fundamento no direito fundamental a liberdade e na autodeterminação informativa, conforme também estabelecido no regime comum de proteção dos dados pessoais, o consentimento deve ser livre. Trata-se de adjetivação que salvaguarda o direito do usuário permitir ou não a utilização dos seus dados pessoais, não admitindo quaisquer situações ou condições que viciem a autonomia da vontade, devendo

[197] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**, p. 68.

ainda ser ponderada a liberdade face a assimetria que existe entre as partes na relação jurídica (pública ou privada) em que foi dada a autorização de processamento.[198]

Ocorre que nas relações jurídicas atuais, o titular que opta por não dar acesso aos seus dados pessoais, em exercício da autodeterminação informativa, resta afastado também do acesso a determinados bens ou serviços, cuja utilização demanda, muitas vezes de maneira adesiva, o fornecimento dos dados pessoais. Abre-se então uma lógica disparidade de poder, entre os sujeitos de quem são demandadas as informações pessoais e aquele que as solicita, fazendo que na maioria dos casos exista uma situação de tudo ou nada.[199]

Assim, tendo como escopo a garantia de um consentimento verdadeiramente livre, urge a doutrina pela adoção de técnicas de consentimento granular, ou seja, o titular dos dados detém a escolha acerca dos dados pessoais que serão cedidos, as finalidades que serão utilizados e os termos da utilização. Noutros termos, a obtenção da anuência do titular é realizada de maneira mais detalhada e específica, permitindo que o indivíduo conceda ou negue permissões para diferentes finalidades de processamento de seus dados pessoais.[200] Para o considerando 43 do GDPR, a anuência não será considerada livre se não for possível este consentimento granular para as diferentes operações de tratamento de dados que forem realizadas.

O RGPD estabelece, ainda, que o consentimento para o tratamento de dados sensíveis deve ser explícito, o que significa que o titular dos dados precisa fornecer uma manifestação de vontade clara, inequívoca e informada, através de uma ação afirmativa ou declaração escrita, oral ou eletrônica. Na verdade, essa autorização especial deve ser compreendida como um meio de permitir ao titular um controle mais preciso sobre como suas informações serão usadas.[201]

Por informado entende-se que o anuente deve estar ciente de todas as informações concernentes ao tratamento dos seus dados pessoais, sendo exigida a leitura do acesso aos termos de consentimento, os quais devem ser fiéis as técnicas de processamento, trazendo informações transparentes, claras e adequadas e satisfatórias acerca dos riscos do tratamento dos dados pessoais.[202] Já o consentimento inequívoco é aquele que não pode ser dúbio, mas

---

[198] TEPEDINO, Gustavo; TEFFÉ, Chiata Spadaccini de – **Consentimento e proteção de dados pessoais na LGPD**, p. 290.
[199] DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**, p. 373.
[200] BIONI, Bruno – **Proteção de dados pessoais: a função e os limites do consentimento**, p. 198.
[201] *Ibidem*.
[202] TEPEDINO, Gustavo; TEFFÉ, Chiata Spadaccini de – **Consentimento e proteção de dados pessoais na LGPD**, p. 301.

sim evidente e se dar uma forma clara, consubstanciando uma conduta concludente do titular dos dados pessoais.[203]

De acordo com o art. 11, I da LGPD deve o consentimento ainda ser destacado, isto é, além de previsões de cláusulas contratuais isoladas dos termos gerais, é imprescindível que o titular dos dados pessoais esteja ciente do que está anuindo, mais especificamente acerca da cessão de tratamento dos dados pessoais sensíveis, de modo que esse isolamento da cláusula de consentimento resulta em uma maior participação do indivíduo na manifestação de vontade.[204]

Em relação a exigência de uma finalidade específica para tratamento dos dados pessoais sensíveis, cumpre relembrar o já exposto quando tratamentos acerca do princípio da finalidade. Neste sentido, a exigência de um tratamento específico dos dados pessoais já existe no regime comum, sendo reiterado pelo legislador e destacado também para a hipótese de tratamento dos dados pessoais sensíveis.

Finalmente, a RGPD, em seu art. 9º, item 2, 'a', consagra a possibilidade de direito da União ou do Estado-Membro afastar a possibilidade de consentimento como uma das bases legais para o processamento do dado sensível.[205] Com efeito, Rodotà advoga a ilegitimidade do consentimento se utilizado para legitimar qualquer tratamento de dados pessoais sensíveis, isto porque em face dos desníveis de poder, a autorização dada pelo titular dos dados, nos termos já delineados, será sempre limitada. Desta feita, a restrição em cotejo consagra uma diminuição do poder de decisão do titular, por entender que determinados tratamentos de dados demandam uma proteção mais elevada, que não pode ser afastada por uma decisão individual.[206]

3.2.2.2. Demais hipóteses autorizativas

Para além da manifestação de vontade do titular dos dados, o RGPD estabelece outras hipóteses legais em que será possível o tratamento dos dados pessoais. De fato, em uma sociedade que baseia parte de suas políticas públicas através de censos e onde a importância da informação no tecido social é de alta relevância, o processamento dos dados sensíveis,

[203] BIONI, Bruno – **Proteção de dados pessoais: a função e os limites do consentimento**, p. 199.
[204] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**, p. 74-75.
[205] Dispositivo sem correspondente positivado na LGPD.
[206] RODOTÀ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje**, p. 150.

desde que com base nos limites legalmente previstos e sobretudo baseando-se no princípio da não discriminação, pode ser útil aos indivíduos e à própria coletividade.

Nestes casos, de maneira abstrata, foi realizada uma ponderação entre o interesse do titular dos dados pessoais sensíveis e o interesse público no processamento destes dados, restando o permissivo legal independente do consentimento. Para Korkmaz, não é incoerente a defesa dos dados sensíveis e, ao mesmo tempo, a promoção de sua utilização em situações legítimas, em razão do valor social que detém a informação. Até mesmo a privacidade evoluiu de uma acepção negativa *(the right to be alone*), para uma acepção positiva.[207]

Entretanto, o tratamento de dados, especialmente quando relacionado à dados sensíveis, deve apresentar razões objetivas e limitadas. Assim, os parâmetros devem ser definidos por finalidade específica (em algumas hipóteses, a única finalidade admissível será o interesse da própria pessoa), exigindo-se também uma comunicação prévia ao interessado sobre o uso de seus dados pessoais. Cumpre ressaltar que as hipóteses legais para o tratamento dos dados sensíveis não são uma licença irrestrita, e sua utilização requer uma análise específica e contextual dos termos do tratamento dos dados, especialmente à luz dos princípios estabelecidos no RGPD.[208]

O Regulamento Geral de Proteção de Dados estabelece nove hipóteses legais que permitem o tratamento de dados sensíveis, nos casos em que for indispensável este tratamento para a finalidade pretendida, nas próximas linhas vamos tratar de maneira sucinta a respeito de cada uma delas.

De início, há permissão legal especial para o tratamento de dados pessoais sensíveis, em matéria de legislação laboral, de segurança social e de proteção social, quando houver necessidade, do responsável ou titular dos dados, de dar cumprimento às obrigações ou no exercício de direitos específicos. Esta primeira hipótese apenas é admitida, caso haja permissão de direito da União ou dos Estados-Membros ou caso haja uma convenção coletiva que estabeleça garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados.

Por conseguinte, resta positivado a possibilidade dos entes associativos (fundação, associação ou outros sem fins lucrativos), no âmbito das suas atividades legítimas e mediante garantias adequadas, promova o tratamento dos dados sensíveis dos seus membros, antigos

[207] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**, p. 75.
[208] RODOTÀ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje**, p. 157.

membros e terceiros que tenham um contato regular com o ente, desde que não sejam divulgados os dados processados a terceiros sem a permissão dos seus titulares.

Quanto as duas hipóteses acima elencadas, a Lei Geral de Proteção de Dados, em seu art. 11, 'a', abarcando os fundamentos acima elencados, estabelece de forma genérica a possibilidade de tratamento, independente do consentimento do titular dos dados sensíveis, para cumprimento de obrigação legal ou regulatória pelo controlador.

Outras duas possibilidades listadas no RGPD, são a possibilidade de tratamento se os dados já tiverem se tornado públicos pelo seu titular e, em outra alínea, a permissão quando for necessário a exercício, defesa ou declaração de um direito num processo judicial, bem como, no exercício das funções jurisdicionais. Quanto a última hipótese, também houve uma extensão da base legal pela LGPD, além dos procedimentos judiciais, os administrativos e arbitrais também admitem o tratamento dos dados sensíveis (art. 11, 'd').

Mais adiante, se reconhece como base legal o interesse público, desde que o tratamento do dado sensível seja proporcional ao escopo buscado e se estabeleçam medidas adequadas e específicas para resguardarem os direitos fundamentais e interesses do titular dos dados pessoais.[209]

Em relação aos dados pessoais relacionados à saúde[210], o Regulamento Geral de Proteção de Dados consagra em três alíneas a possibilidade do tratamento dos dados sensíveis. Estas informações estão sujeitas a um regime de proteção especial por corresponder a uma categoria de dados que podem resultar na estigmatização e discriminação dos seus titulares através revelação de aspectos da sua fisiologia orgânica que enformam o reduto máximo da privacidade.[211]

Assim, temos a possibilidade de tratamento dos dados pessoais para proteção de interesses vitais do titular dos dados ou de terceiros, especialmente na hipótese em que o titular esteja impedido, física ou legalmente, de autorizar o processamento. Nesta hipótese, mesmo sem o consentimento explícito do titular dos dados, é possível realizar o tratamento das informações sensíveis quando se trata de uma questão de proteção da integridade física. Contudo, é importante ressaltar que o tratamento dos dados deve ser proporcional e necessário

[209] Previsão semelhante a contida no art. 11, 'b' da LGPD.
[210] A LGPD também ressalva a possibilidade de tratamento das informações de saúde, nas hipóteses de tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 11, 'f').
[211] DIAS, Patrícia Cardoso – **Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública**, p. 15.

para alcançar o objetivo de proteger os interesses vitais, evitando-se qualquer uso abusivo ou desnecessário dos dados sensíveis.

Outrossim, há previsão de processamento de dados sensíveis caso seja necessário para medicina preventiva ou do trabalho, diagnóstico médico, tratamentos de saúde, gestão de sistemas sociais ou de saúde e, ainda, por força de um contrato médico. Permite-se também para os casos de interesse público no domínio da saúde pública, em razão, por exemplo de pandemias, com o objetivo de elevar o nível de qualidade e dos cuidados da saúde, de medicamento e dispositivos médicos.

A última previsão legal contida no RGPD diz respeito ao tratamento de dados pessoais sensíveis para os seguintes fins: (i) arquivo de interesse público; (i) investigação científica; (iii) investigação histórica; (iv) estatísticos. Neste caso, o processamento dos dados deve ser proporcional ao escopo pretendido e deve observar os direitos fundamentos e interesses do titular dos dados. Na LGPD também há possibilidade para tratamento nestas hipóteses, desde que, sempre que possível, se proceda a anonimização dos dados (art. 11, ‘c’).

Finalmente, uma das previsões contidas na Lei Geral de Proteção de Dados que não encontra semelhante no RGPD é a possibilidade de processamento para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Após a análise de como se procede a regulamentação acerca da proteção de dados em âmbito europeu e brasileiro, no que toca a definição de perfis e os dados sensíveis, bem como esclarecido como aquele estes pode resultar na exposição destes, faz-se necessário tratar dos benefícios e riscos associados aos perfis, bem como da possibilidade de violação da privacidade e da utilização de praticas discriminatórias caso não observado o arcabouço legal ora estabelecido.

3.3. Dos benefícios e riscos associados a definição de perfis

O presente tópico tem como escopo analisar os benefícios e riscos associados ao profiling (definição de perfis) no contexto da privacidade e da proteção dos dados pessoais.

O *profiling* tem se mostrado um instrumento fundamental na sociedade contemporânea, proporcionando diversos benefícios para empresas, governos e indivíduos, fazendo surgir até mesmo novas formas de negócio. Com efeito, como já exposto, o

investimento no processamento de dados para geração de perfis tem o condão de potencializar o progresso e resultar em inovações que concorrerão para o bem-estar social.[212]

Listando alguns benefícios de maneira geral, a análise de dados automatizada abre portas, por exemplo, para uma personalização de serviços e experiências, haja vista que uma vez traçado o perfil do usuário, faz-se possível identificar preferências, comportamentos e necessidades individuais, possibilitando a elaboração de produtos e serviços adaptados às demandas específicas de cada indivíduo.

Neste panorama, as empresas após coletarem e processarem os dados pessoais, catalogando as diferentes informações analisadas em grupos, irão obter a capacidade de identificar padrões, comportamentos e prioridades, possibilitando o ingresso dos usuários em perfis pré-determinados, que serão mais compatíveis com seus gostos pessoais.[213]

Por exemplo, sites de comércio passam a lhe oferecer produtos semelhantes aos já adquiridos, e com base nas escolhas de outros usuários que compraram o mesmo produto, passa também a oferecer outros produtos que o indivíduo possa gostar.

Este banco de dados de clientes, ao personalizar a experiência de compra, resulta em uma maior taxa de sucesso de vendas, sendo estes resultados uma direta ocorrência do tratamento de dados. Estes perfis traçados, ajudam a empresa também no ajuste de sua estratégia de marketing, além de estabelecer uma revisão dos produtos que serão oferecidos ao seu público-alvo.

No estágio atual do comércio eletrônico, a personalização automatizada através de perfis e utilização de *big data* já se tornou imprescindível. A sociedade contemporânea apresenta uma dependência tecnológica colossal, sendo comum que a quantidade e qualidade dos algoritmos de aprendizagem sejam pedras angulares para definir o sucesso ou fracasso de um empreendimento.[214]

No setor da saúde, a categorização e classificação dos dados também é imprescindível, pois resulta na melhoria da tomada de decisões, ao fornecer elementos valiosos que contribuem para identificação de um padrão ou tendência de contágio. Com isto, se permite uma atuação efetiva para o controle sobre doenças, orientando políticas públicas e determinando o rigor do isolamento que deve ser observado.[215]

---

[212] COSTA, Inês da Silva – **A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas**, p. 40.
[213] CHELES, Tamára – **Os Desafios dos Consumidores na Era de Big Data**, p. 158.
[214] *Idem* – ***Op. Cit.***, p. 159.
[215] COSTA, Inês da Silva – ***Op. Cit.***, p. 40.

Ademais, os benefícios do *profiling* podem ser observados em diversos ramos de atividade e ter múltiplas aplicações práticas, já sendo comumente utilizados para cibersegurança, na previsão de conflitos, na prevenção e deteção de fraudes financeiras, criação de novos postos de trabalho e identificação dos candidatos mais apropriados para as vagas, enfim, diversas são as implicações que a definição de perfis tem produzido nas nossas vidas.

Nessa esteira a Resolução do Parlamento Europeu de 14 março de 2017, dentro seus considerandos, reconhece o impacto do tratamento automatizado de um grande volume de dados, dispondo quanto aos seus benefícios que, grandes volumes de dados proporcionam vantagens competitivas para os processos de tomada de decisão das empresas europeias, enquanto o setor público pode beneficiar de uma maior eficiência graças a informações mais exatas sobre os diferentes níveis de desenvolvimento socioeconómico.[216]

Não obstante seja clara a mais-valia para os indivíduos, empresas e setor público, conforme apresentado nas linhas acima, não se pode negligenciar os riscos associados a essa atividade, que pode acarretar significativa fragilização da dignidade da pessoa humana, em razão de riscos significativos no que diz respeito à proteção dos direitos fundamentais, resultando na possibilidade de discriminação do titular dos dados e violação do direito à privacidade, à proteção dos dados pessoais, bem como ingerências não justificadas na liberdade de expressão, tal como garantidos pela Carta dos Direitos Fundamentais da União Europeia.[217]

A evolução tecnológica, que permite o tratamento automatizado através de algoritmos, até mesmo sem qualquer intervenção humana, como aqui já exposto, não foi acompanhada da necessária regulamentação jurídica das ferramentas. Em razão disto, tem-se observado no cenário atual que as decisões automatizadas por vezes se mostram tendenciosas e discriminatórias, principalmente para pessoas e grupos sociais periféricos.[218]

De fato, os algoritmos apesar de serem uma fórmula matemática de se tomar a melhor decisão lógica, não são naturalmente imparciais, neutros e equânimes, isto porque, os dados passados e os resultados apresentados como *input*, por replicarem o que acontece na nossa sociedade, também não o são.

---

[216] UNIÃO EUROPEIA – **Resolução do Parlamento Europeu 14/2017 – Implicação dos Grandes Volumes de Dados nos Direitos Fundamentais**, [em linha].
[217] *Ibidem*.
[218] FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro – **Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos**, p. 3.

Com o emprego de dados e resultados viciados e representativos de uma sociedade discriminatória, igualmente o algoritmo irá repetir essas tendências, pois entenderá como sucesso as mesmas práticas sociais que observa.[219] Os algoritmos têm sua aprendizagem condicionada aos dados e resultados que lhe são apresentados, ou seja, aos exemplos demonstrados pelo programados. Se os exemplos utilizados como *input* refletirem o mesmo preconceito característico da sociedade, as decisões tomadas pela máquina vão apenas reforçar esse paradigma.[220]

Nessa toada, parcela da doutrina[221], destaca alguns riscos como os principais decorrentes das práticas de definição de perfis, vejamos.

3.3.1. Dos riscos decorrentes da opacidade na tomada de decisões

No que toca a opacidade da tomada de decisões e dos algoritmos utilizados, diversos são os riscos colocados por estas novas tecnologias disruptivas. Ora, o processamento dos dados está sujeito a imprecisões e incertezas, se baseia em correlações e não em causalidades, logo o resultado pode ser uma mera aproximação da verdade, uma tomada de decisão aleatória.

Aliás, impende registrar que esta opacidade se manifesta de várias maneiras, a iniciar pelo fato de que na maioria dos processamentos de dados o funcionamento do algoritmo é desconhecido para o titular (*blackboxes),* sendo que em algumas hipóteses, como aqui já mencionado, até mesmo os programadores desconhecem a lógica utilizada para a tomada da decisão automatizada.[222]

De fato, em algumas situações, como na utilização de inteligências artificiais baseadas em *machine learning,* o funcionamento do algoritmo pode ser opaco até mesmo para os seus criadores. Nessas circunstâncias, os algoritmos inteligentes se tornam inescrutáveis, devido à complexidade das suas regras, desafiando a compreensão humana, mesmo daqueles mais especializados. Essa névoa que envolve os algoritmos dificulta a sua fiscalização e controle, bem como a elaboração de um regime jurídico adequado.[223]

---

[219] O'NEIL, Cathy – **The era of blind faith in big data must end. TEDIdeas**, [em linha].
[220] FERRARI, Isabela; BECKER, Daniel – **Algoritmo e preconceito**, [em linha].
[221] HERT, Paul de; LAMMERANT, Hans – **Predictive profiling and its legal limits: Effectiveness gone forever**, p. 148.
[222] PASQUALE, Frank – **The black box society: the secret algorithms that control money and information**, p. 6.
[223] COSTA, Inês da Silva – **A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas**, p. 38.

Afora esta opacidade, ainda há o problema acerca da natureza dos dados coletados, haja vista que os algoritmos se alimentam de informações brutas, ou seja, não contém o contexto ou histórico no qual se produziu o dado que será objeto de tratamento, logo, a informação processada pode apontar resultados falhos, que não captam as pessoas em sua essência, não entendem a razão que motivou o dado que agora se encontra eternizado em camadas e mais camadas de processamento.

Ora, simplesmente, é lançada uma informação que será utilizada para construir um perfil, que por vezes não vai corresponder a realidade. O processamento automatizado não captura o usuário em sua verdadeira essência e por vezes se baseando em dados brutos irá distorcer características inerentes ao titular dos dados. Ocorre que, mesmo diante dessa incoerência, ainda assim o resultado algorítmico será utilizado para decidir aspectos relevantes da vida.[224]

Nessa toada, Pasquale defende a necessidade de se regular direitos procedimentais que outorguem ao titular dos dados pessoais meios de se contrapor as decisões automatizadas que lhe recaem, como são o direito de requerer uma explicação sobre uma decisão automatizada, mas também o direito de obter uma auditoria externa de aspectos discriminatórios de algoritmos[225].

3.3.2. Do impacto negativo na privacidade

A definição de perfis se apresenta comumente como um tratamento automatizado intrusivo, ainda mais quando utilizado rotineiramente no mercado, em todos os contextos possíveis.

Como dito quando tratamos de *big data,* os pequenos custos para o processamento de dados, atrelados ao grande potencial dos resultados advindos do *profiling*, acabam por reforçar a crescente coleta de dados comportamentais, com o intuito de desvendar e antecipar comportamentos e hábitos. Ainda que haja uma cessão voluntária das informações, sempre deve haver uma expectativa legítima de privacidade, que na prática é constantemente violada na caracterização de perfis[226].

---

[224] SOLOVE, Daniel – **The digital person: technology and privacy in the information age**, p. 49.
[225] CITRON, Danielle Keats; PASQUALE, Frank – **The scored society: due process for automated predictions**, p. 1.
[226] HERT, Paul De; LAMMERANT, Hans – **Predictive profiling and its legal limits: Effectiveness gone forever**, p. 152.

Ademais, para perfis mais precisos, são necessários cada vez mais dados e menos amarras sobre o tratamento, o que pode levar o já fragilizado usuário a abrir mão mais ainda sobre o controle que detém sobre sua privacidade, ou seja, na redução de controle sobre os dados pessoais, passando os tratadores a ter cada vez mais controle sobre nossas vidas privadas.

Com efeito, a relativização da nossa privacidade e do controle dos nossos dados passou a ser moeda de troca para utilização de "serviços gratuitos", como são as redes sociais, aplicativos de mapas e fitness. Assim, em troca de um monitoramento constante dos hábitos de consumo, transporte, saúde, interações sociais, ou seja, através da retirada do véu sobre nossa vida privada é disponibilizado ao usuário serviços sem os quais a falta de acesso resultaria em uma "alienação" da sociedade da informação e evidente prejuízos sociais para a pessoa humana[227]

Por vezes, os dados coletados através destes consentimentos quase que compulsórios são utilizados sem observância dos princípios da necessidade, adequação e finalidade do tratamento. Desta forma, essa coleta e tratamento fora dos propósitos, com a criação de perfis não autorizados ou não previstos quando do consentimento para coleta dos dados, também se apresenta como um risco a privacidade.

Finalmente, outro risco relevante decorrente da definição de perfis é a possibilidade de criação de novos dados em razão da categorização do titular das informações pessoais. Nesta senda, a identificação da pessoa dentro de um grupo determinado, potencializada através das técnicas de correlação e inferência aplicadas pelo algoritmo, resultam em descoberta de atributos específicos do indivíduo, que este não transmitiu, nem sequer deduziu que poderia ser descoberto a partir dos dados apresentados.[228]

Trata-se aqui de inferências algoritmas, ou seja, induções são feitas através do tratamento automatizado, que utiliza os dados que foram inicialmente coletados para chegar a uma conclusão, por vezes esse resultado apresenta características e natureza totalmente diversa quando comparado com os dados brutos que foram coletados. Em outras palavras, as inferências são dados criados através de indução ou racionamento, sobre pessoa identificada ou identificável, sem necessidade de observação ou coleta direta da referida informação do titular dos dados[229].

---

[227] BIONI, Bruno Ricardo – **Proteção de dados pessoais: a função e os limites do consentimento**, p. 88.
[228] CORREIA, Sergio Miguel – **Direito de Oposição à Definição de Perfis**, p. 200.
[229] WACHTER, Sandra; MITTELSTADT, Brent – **A right to reasonable inferences: re-thinking data protection law in the age of big data and AI**, p. 40.

Por exemplo, os dados de geolocalização de um indivíduo que indiquem a visita constante a um determinado hospital oncológico, somado aos seus hábitos de consumo de medicamentos, podem apontar um perfil que indique que o indivíduo esteja em tratamento de um certo tipo de câncer. Da mesma forma, os dados de geolocalização de uma pessoa podem também ser utilizados, neste caso, isoladamente, para indicar qual a religião que ela pratica, apenas com base na frequência que se dirige para determinado tempo. Ainda nesse esteira, as chamadas "curtidas" nas redes sociais, mesmo que não diretamente relacionada a qualquer dado sensível do usuário, em seu conjunto podem indicar indiretamente dados sensíveis, sobre os quais o interessado não gostaria que terceiros, muito menos empresas, tivessem conhecimento, como a sexualidade do titular dos dados.

Aliás, a criação de perfis e a identificação do titular dos dados é possível mesmo em casos em que não haja inferências realizadas por algoritmos, como reportado no Acórdão de 13 de maio de 2014, Google Spain e Google, C-131/12, EU:C:2014:317, n.os 35 a 37, onde se verificou que os motores de busca ao organizarem e agregarem informações online para facilitar o acesso dos usuários, possibilitam a pesquisa pelo nome de uma pessoa determinada, fornecendo uma visão estruturada das informações disponíveis na Internet sobre esta pessoa, permitindo aos usuários do serviço criar um perfil detalhado do pesquisado em questão, sem que haja qualquer hipótese autorizativa para o referido tratamento, resultando em indubitável violação a privacidade e a proteção de dados.[230]

Dentro dessa ótica, essas inferências, mesmo que inicialmente apenas baseadas em dados brutos, são plenamente identificáveis, razão pela qual demandam também a tutela especial prevista para proteção dos dados pessoais quando há definição dos perfis, principalmente quando dessas inferências resultam a exposição de dados pessoais sensíveis, como acima exposto.

Verifica-se, portanto, que a definição de perfis, além de comprometer a privacidade individual, abre caminho para riscos substanciais relacionados à exposição de dados pessoais sensíveis, podendo resultar em discriminação do titular dos dados. O próximo subtópico abordará casos de discriminação em decorrência da definição de perfis, ampliará essa discussão, explorando como as inferências automatizadas podem contribuir para a criação de categorias discriminatórias e aprofundando as preocupações éticas associadas ao uso indiscriminado de dados pessoais na era digital.

[230] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, ECLI:EU:C:2014:317)**, [em linha].

3.3.3. Dos potenciais efeitos discriminatórios

A criação de perfis se baseia em uma forma de operação indutiva, ou seja, em um processo lógico que parte de observações de um conjunto de dados específicos para chegar a uma conclusão geral ou uma generalização provável. Então, se identificam padrões e é feita uma previsão de futuros comportamentos.

Por óbvio que, mesmo com o poder computacional atual, é impossível uma análise de todos os dados existentes, desta feita, o programador aprioristicamente define quais as informações serão selecionadas para se chegar na conclusão pretendida, logo, há grande risco de os resultados obtidos serem direcionados e parciais, não podendo se atestar a neutralidade do algoritmo, o que poderá resultar em discriminação do titular dos dados.[231] Nesta hipótese, a discriminação digital decorre da concepção da arquitetura da máquina, ou seja, em razão da forma como foi programado o algoritmo, este já apresentará um viés inclinado a tomar decisões discriminatórias.[232]

Por outro lado, a discriminação por meio dos dados que alimentam os algoritmos ocorrerá, por obvio, após a criação da ferramenta, através da seleção das informações que são inseridas no programa. Neste caso, as informações são colacionadas de modo enviesado, sem que o programador sequer perceba que realiza seu trabalho sob influência de suas convicções políticas, religiosas, filosóficas.[233]

Ademais, os algoritmos estabelecem grande parte de suas decisões com base em estatística, a definição de perfis procede com divisão de indivíduos fundamentada nas características de um grupo e na expectativa das pessoas integrantes daquele perfil agir de determinada forma. Logo, a definição de perfis, apenas superficialmente aparenta objetividade no processo decisório, haja vista a possibilidade de a estatística utilizada reproduzir vieses discriminatórios já existentes, levando também a resultados discriminatórios.[234]

Sobre o tema, O'Neil destaca como os sistema de profiling, viciado por vieses estruturais e alimentado com estatística falhas, pode levar a discriminação de milhares de pessoas, exemplificando, traz o caso de um birô de crédito que estabelece um sistema de "scoring de pessoas", sendo estas informações utilizadas por recrutadores de empregos para

[231] LEAL, Ana Alves – **Big data e proteção de dados pessoais – desafios à luz do Regulamento Geral de Proteção de Dados**, p. 19.
[232] MARTINAZZO, Waleska Malvina Piovan – **O trabalhador e a proteção de dados para o combate à discriminação digital nas relações de trabalho: um estudo de caso a partir de julgado do TRT da 18ª região**, p. 42.
[233] *Ibidem.*
[234] MENDES, Laura; MATIUZZO, Marcela – **Discriminação algorítmica: conceito, fundamento legal e tipologia**, p. 09.

discriminar determinados "grupos de risco", normalmente excluindo pessoas de cor, imigrantes, grupos religiosos, minoras sexuais, pois são pessoas que carregam muito mais o peso do monitoramento, já que mais expostas ao sistema públicos e privados de coletas de informações.[235]

Nessa esteira, Clarke expõe que alguns perfis seriam considerados inapropriados ou até mesmo opressivos, caso fossem conhecidos e debatidos pela Sociedade, principalmente levando em conta a maneira como são formados e os resultados que deles decorrem. Por exemplo, cita que a seletividade de anúncios ou notícias direcionadas para apenas uma parcela da população finda por se tornar uma ferramenta de manipulação e de limitação de informações, ocasionando discriminação de pessoas.

Aliás, diversas são as formas de discriminação que se pode decorrer em razão da definição de perfis, como é exemplo claro a discriminação de preços e ou de pessoas com quem se irá contratar. A doutrina tem indicado duas formas de interferência no comércio.

A um, procede-se com a discriminação do preço com base no que o cliente está disposto a pagar, ou seja, ao conhecer o consumidor com base em seu perfil, a fornecedora é capaz de cobrar exatamente o que o cliente está disposto a pagar, eliminando a pressão para redução do preço que é estabelecida organicamente em uma situação de normalidade, haja vista a existência de consumidores conscientes do valor do produto, disto resulta no estabelecimento individualizado de valores no patamar máximo que o algoritmo indica que estaria o escrutinado disposto a pagar.

A dois, a discriminação é realizada com base em características relativas ao cliente, por exemplo, já se observa na Europa empresas de seguro que ao identificar o estilo de vida e hábitos de consumo do cliente, precificam o valor do prêmio com base nessa correlação, resultando em casos mais extremos a recusa de contratação.[236]

Neste ponto, o conhecimento prévio do perfil de uma pessoa ou grupo de pessoas permite ao fornecedor do produto ou serviço melhor direcionar a propaganda a um público específico, mas também pode resultar no estabelecimento um preço diferenciado para quem procura com afinco àquele bem ou serviço ou mesmo na discriminação de certas pessoas em razão de determinadas características.[237]

---

[235] O'NEIL, Cathy – **Weapons of math destruction: How big data increases inequality and threatens democracy**, p. 110.
[236] JUNIOR, Glauto Lisboa Melo – **O consumidor de seguros na era do big data: desafios da atual regulamentação europeia frente às técnicas de definição de perfis, aprendizagem de máquina e decisões automatizadas**, p. 2155.
[237] BORGESIUS, Frederik Zuiderveen, POORT, Joost – **Online Price Discrimination and EU Data Privacy Law**, p. 350.

Com efeito, a Organização para a Cooperação e Desenvolvimento Econômico já expressou que o aumento no uso de algoritmos que estabelecem decisões automatizadas, com base apenas em correlações e sem interferência humana, pode resultar em insegurança cibernética, inacessibilidade de fundos ou impossibilidade de finalizar negócios.[238] Outrossim, porém direcionado especificamente para a área de seguros, há também uma preocupação da Autoridade Europeia de Supervisão, que expressou que as definições de perfil realizadas pelas seguradoras resultam em prêmios tão altos que impedem a contratação do seguro, concluindo que esta individualização estabelecida pelo perfil traçado pode, inclusive, resultar na quebra do princípio da solidariedade que rege o setor e na exclusão de uma parcela da população a contratação do seguro.[239]

Por exemplo, em um cenário fictício, a companhia de seguros de vida analisa dados brutos de determinada pessoa, erroneamente inferindo que esta é fumante devido à sua presença constante em eventos sociais onde o tabaco é utilizado. A empresa cria um perfil que classifica erroneamente esta pessoa como pertencente a um grupo de risco, já que associado a um estilo de vida não saudável. Com base nessas inferências incorretas, a seguradora poderá discriminar, recusando a oferta de seguro de saúde ou estabelecendo um valor tão alto que inviabiliza a contratação, evidenciando os riscos de decisões automatizadas e discriminação associada à definição de perfis.

Resta, pois, evidenciado como a definição de perfis pode contribuir para a perpetuação de práticas discriminatórias, ressaltando a importância de políticas e regulamentações que protejam a privacidade e as pessoas humanas contra decisões exclusivamente automatizadas, principalmente, quando inferências levam a revelação de dados sensíveis.

---

[238] JUNIOR, Glauto Lisboa Melo – **O consumidor de seguros na era do big data: desafios da atual regulamentação europeia frente às técnicas de definição de perfis, aprendizagem de máquina e decisões automatizadas**, p. 2152.

[239] MELO JUNIOR, Glauto Lisboa – **O consumidor de seguros na era do big data: desafios da atual regulamentação europeia frente às técnicas de definição de perfis, aprendizagem de máquina e decisões automatizadas**, p. 2152.

CONCLUSÃO

Os contínuos avanços tecnológicos na coleta, processamento e circulação de dados pessoais, atividades comuns na sociedade da informação, resultam em mudanças significativas nas relações sociais e governamentais.

Os dados pessoais são tratados como verdadeira *commodity*, servindo como moeda de troca para prestação de serviços "gratuitos", como pressupostos indispensáveis para celebração de contratos ou, ainda, como baliza definidora das políticas públicas a serem implementadas. Dentro desse contexto, a discussão acerca das formas de garantir a preservação do direito fundamental à vida privada e intimidade do titular dos dados nunca esteve tão em evidência.

Como exposto, a privacidade decorre de uma necessidade orgânica, é reconhecida socialmente desde a antiguidade (mesmo quando ainda não era um direito) e é um dos pressupostos a dignidade da pessoa humana, pois indispensável é ao exercício das liberdades não vigiadas para formação do caráter e para a autonomia privada do indivíduo. A sua definição, como direito, não comporta um conceito fechado, deve ser tida como uma cláusula geral aberta, que terá seu conteúdo preenchido de acordo com o contexto histórico, social e geográfico. Neste ensejo, desenvolveu-se duas acepções da privacidade: negativo, como o direito de se opor a interferências indevidas na vida privada; e positivo, como o controle das informações pessoais, ou seja, a escolha de quem pode compartilhar os dados pessoais do indivíduo.

No que pese esta mutação do direito fundamental à privacidade, o estágio atual da nossa sociedade revelou que ainda assim persistia uma falta de controle e regulamentação sobre a coleta, circulação e tratamento de dados pessoais, resultando na necessidade de uma nova arquitetura de proteção das informações pessoais que não fossem sensíveis. Desta feita, surge o direito fundamental a proteção dos dados pessoais, o qual após passar por uma ampliação conceitual e normativa, atualmente, pode ser conceituado como o direito fundamental dos indivíduos de controlar suas informações pessoais e decidir como terceiros as coletam, usam, armazenam e compartilham. Igualmente a privacidade, a proteção dos dados pessoais é extremamente necessária, haja vista ser inevitável o tratamento de dados, o que precisa ser regulado para evitar abusos e garantir a autonomia da vontade, a liberdade e a privacidade do titular das informações.

Os referidos direitos fundamentais, por óbvio, não são absolutos e podem sofrer limitações em prol de outros direitos fundamentais, da segurança pública e do interesse

público. As ingerências ou limitações devem ser previstas em lei, respeitar o conteúdo essencial do direito, ser necessárias e proporcionais aos fins buscados, e observar o interesse público ou os direitos fundamentais de terceiros. A ponderação de valores é fundamental para resolver os conflitos aparentes entre a proteção dos dados pessoais e outros direitos fundamentais.

Ademais, a privacidade e proteção dos dados pessoais, apesar de apresentarem pontos de contato, não se confundem. A proteção dos dados pessoais, diferente da privacidade, não busca a opacidade das informações, mas sim a transparência, tem como escopo dar ao titular o controle sobre todas as etapas do tratamento de seus dados: a partir da coleta até a decisão final. Nessa esteira, embora evidente a relação complementar entre esses dois direitos, a proteção dos dados pessoais é vista como um direito autônomo, com múltiplas funções, que vão além da tutela da privacidade.

De fato, tratam-se de direitos fundamentais distintos e autônomos, a privacidade denota um poder de controle sobre as informações pessoais que revelem aspectos íntimos do sujeito, aspectos da vida privada que o indivíduo não tem intenção de compartilhar. Já a proteção de dados pessoais não se limita às informações privadas, haja vista as diversas formas de tratamento dos dados pessoais, seu campo de proteção se estende ao processamento automatizado, semiautomatizado ou manual de dados pessoais de pessoas singulares identificadas ou identificáveis.[240]

Assim, reconhecida a autonomia do direito a proteção de dados pessoais, importante destacar que o Regulamento Geral de Proteção de Dados, no cenário europeu, e a Lei Geral de Proteção de Dados, no Brasil, consagraram uma arquitetura jurídica ampla, que estabelece as bases legais e princípios a serem seguindo quando houver o tratamento das informações pessoais. A compreensão e aplicação adequadas dos fundamentos legais e das máximas são essenciais para garantir um tratamento adequado e legal dos dados pessoais, de modo a não resultar em ingerências injustificadas.

Para além das previsões gerais acerca do tratamento dos dados pessoais, tanto o diploma europeu, quanto o brasileiro, estabelecem normas específicas a serem observadas nas hipóteses em que ocorra a definição de perfis e no tratamento de dados sensíveis, tendo as referidas disposições sido objeto de análise neste trabalho.

Quanto ao tratamento de perfis, restou estabelecido sua definição como o tratamento automatizado de dados pessoais que consiste em, através das informações que são coletadas,

[240] BIONI, Bruno Ricardo – **Proteção de Dados Pessoais: A função e os limites do consentimento**, p. 92-101.

avaliar aspectos pessoais de uma pessoa singular, como desempenho profissional, hábitos de consumo, comportamento, dentre outros. Diante deste *profiling,* ocorrerá a categorização dos indivíduos, sendo as informações processadas utilizadas para fazer previsões ou conclusões sobre o titular dos dados pessoais.

Em razão das novas tecnologias da informação, há uma colheita massificada de dados, que são processados com o intuito de classificar os indivíduos em diferentes grupos, estudar seus hábitos e prever padrões de comportamentos futuros. Todo computador, aparelho de celular, *smartwatch* é um agregador de dados, que utiliza as informações coletadas para formar verdadeiros dossiês dos seus titulares.

Sem dúvidas que o *profiling* pode oferecer benefícios significativos para empresas e governos que processam e capitalizam através das informações, mas também há ganhos para os indivíduos, como na personalização de serviços, melhoria da tomada de decisões, desenvolvimento de políticas públicas mais apropriadas, dentre outras benfeitorias. Entretanto, grave são os riscos decorrentes da definição de perfis, sendo os mais mencionados pela doutrina: a violação da privacidade, a opacidade no tratamento e na tomada de decisões automatizadas, que podem resultar em efeitos discriminatórios.

Ademais, este processamento, mesmo que tenha como base de acesso apenas dados brutos, podem resultar na revelação de dados sensíveis, como a identificação da origem racial ou étnica do indivíduo, suas convicções políticas e filosóficas, religião, dados de saúde, filiação sindical; sendo todas estas informações dados especiais, conforme previsto no art. 9, 1 do RGPD, que têm o potencial de serem utilizadas indevidamente, resultando em discriminação ou violação dos direitos fundamentais do titular dos dados, especialmente da privacidade.

Assim, quando dados brutos[241] são processados e analisados por meio de uma definição de perfis, ou seja, através de um tratamento automatizado de dados, que utiliza as informações coletadas de um banco de dados único ou de diversos banco de dados, para avaliar características singulares de um indivíduo e através do cruzamento dos elementos coletados procede com uma representação preditiva e/ou sua categorização em determinado grupo do titular dos dados, é possível obter informações detalhadas e sensíveis sobre um indivíduo, resultando até mesmo na criação de dados pessoais sensíveis.

[241] Os dados brutos de maneira isolada não podem ser considerados dados pessoais sensíveis, pois a natureza e conteúdo destas informações não revelam aspectos específicos de uma pessoa, por exemplo, os dados de localização quando tratados de maneira restrita, não tem o condão de gerar situações de risco que justifiquem sua categorização como dado sensível.

Diversos são os exemplos práticos de como o *profiling* com base em dados brutos pode resultar na criação de dados sensíveis e, através da informação minerada, proceder o controlador dos dados com a discriminação do indivíduo: (i) nos perfis de saúde, empresas de seguro poderão utilizar as informações de deslocamento do indivíduo e os seus hábitos de consumo para utilizando algoritmos avaliar o risco de um indivíduo desenvolver certas condições médicas; (ii) nos perfis laborais, os empregadores podem usar a definição de perfis para avaliar a solvência de um indivíduo, seu histórico de pagamentos e de litigância trabalhista. Se o perfil revelar informações sobre pagamentos realizados a sindicatos, um alto número de processos trabalhistas, isso poderia levar a decisões discriminatórias em oportunidades de emprego; (iii) nos perfis sociais: algoritmos podem se utilizar de dados como localização geográfica, associações sociais, hábito de consumo para inferir a orientação sexual de um indivíduo. Isso pode levar a tratamento diferenciado, segregação ou exclusão.

Com efeito, as situações acima ilustram de maneira clara como a definição de perfis, mesmo a que se baseia em dados brutos, pode revelar informações sensíveis que podem ser usados para discriminar, prejudicar ou violar a privacidade do titular dos dados. Com efeito, as inferências exemplificadas, como já tratado, são dados obtidos por meio de algoritmos, utilizando métodos indutivos para processar informações relacionadas a uma pessoa identificada ou identificável. Esse processamento é capaz de extrair conclusões e informações adicionais com base nos dados coletados, resultando na criação de novos dados, inclusive, sensíveis.

Diante disto, o RGPD e a Lei Geral de Proteção de Dados consagram dispositivos específicos e maiores restrições tanto para a definição de perfis, quanto para o tratamento de dados pessoais sensíveis, visando garantir a privacidade e a não discriminação do titular dos dados.

Quanto a definição de perfis, as normas de proteção limitam o tratamento dos dados, estabelecendo, uma regra geral de proibição (excetuada a hipótese em que haja consentimento explícito, celebração ou execução de um contrato, ou autorização legislativa com salvaguardas adequadas), determinando ainda a observância ao princípio da transparência, além de consagrar os direitos de oposição e revisão das decisões automatizadas. Além disso, o RGPD proíbe a definição de perfis com base em dados pessoais sensíveis, a menos que haja consentimento explícito do titular ou motivos de interesse público com respeito aos direitos e liberdades do titular, prevendo também que deve ser adotada uma proteção de dados por padrão e desde a concepção do tratamento.

Já em relação aos mecanismos de tutela para tratamento dos dados sensíveis, os diplomas normativos supracitados estabelecem uma abordagem especial garantindo uma proteção mais rigorosa desses dados devido à sua natureza sensível e ao risco potencial à privacidade dos seus titulares. O processamento destes dados especiais deve ser proporcional e necessário para alcançar a finalidade pretendida. A proteção dos direitos fundamentais e interesses dos titulares dos dados deve ser garantida em todas as etapas do processo.

Assim, o consentimento deve ser livre, sem coerção ou consequências negativas no caso de recusa, e os titulares devem ter controle granular sobre quais dados são compartilhados e para quais finalidades. Além do consentimento, outras bases legais para o tratamento de dados sensíveis são: o cumprimento de obrigações legais ou regulatórias, interesses legítimos do controlador dos dados, exercício de direitos em processos judiciais ou administrativos, interesse público com medidas adequadas de proteção, proteção dos interesses vitais do titular ou de terceiros, finalidades de saúde, pesquisa científica, estatísticas, entre outros.

Em suma, os mecanismos de tutela acima delineados regulam a proteção dos dados quando da definição de perfis resulta a criação de dados sensíveis, garantindo a privacidade e a não discriminação dos indivíduos que foram perfilados. Logo, no intuito de mitigar os efeitos da definição de perfis, se estabeleceu mecanismos adequados de controle sobre processamento das informações.

Com efeito, essas medidas de proteção de dados sensíveis previstas no RGPD e na LGPD visam garantir a privacidade e os direitos dos titulares dos dados. É importante observar que o tratamento de dados sensíveis requer uma base legal mais sólida que deve ser acrescida também dos mecanismos de tutela e controle previstos para a definição de perfis quando os dados sensíveis foram extraídos em razão do *profiling* do titular dos dados.

Finalmente, evidenciado o amplo espectro de previsões constantes no RGPD e na LGPD acerca das matérias em mote, pode-se montar um mosaico de proteção do qual fazem parte os princípios apontados, as regras acerca do tratamento automatizado dos dados e o regime mais restrito para o processamento dos dados pessoais sensíveis.

Assim, em um cenário onde a a definição de um perfil possa resultar na divulgação de dados sensíveis e possível discriminação do titular dos dados pessoais, há um robusto arcabouço jurídico para salvaguardar os dados pessoais, sendo possível atestar a existência de uma arquitetura de controle sobre práticas invasivas de tratamento de dados automatizados, de modo que a observância das regras ora estabelecidas, mesmo com o avanço das técnicas de tratamento dos dados e a opacidade dos algoritmos ora utilizados, atualmente, tem o condão

de resguardar o direito à privacidade do titular dos contra ingerências indevidas do responsável.

REFERÊNCIAS BIBLIOGRÁFICAS

29 DATA PROTECTION WORKING PARTY – Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. [Em linha]. **European Commission**, [*s. d.*]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/index_en.htm. [Consult. em 14-05-2023].

29 DATA PROTECTION WORKING PARTY – Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector. [Em linha]. **European Commission**, [*s. d.*]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf. [Consult. em 27-06-2023].

ALEXY, Robert – **Teoria dos Direitos Fundamentais. 2.ª ed.** São Paulo: Malheiros, 2011. ISBN: 978-8539200733.

ÁLVAREZ, José Luis Rodríguez – Transparencia y protección de datos personales: criterios legales de conciliación. *In* AMETLER, Dolors Canals (ed.) – **Datos: Protección, transparencia y buena regulación**. Girona: Documenta Universitaria, 2016.

ARCHANJO, Daniela Resende – O princípio da proporcionalidade na solução de colisões de direitos fundamentais. [Em linha]. **Espaço Jurídico Journal of Law**. Vol. 9, n.º 2 (2008), p. 151-168. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1914. [Consult. em 16-11-2021].

ARISTÓTELES – **Politique, I, II.** Paris: Les Belles Lettres, 2003. ISBN 978-22-51-0005-72.

BARCELLOS, Ana Paula de – **Ponderação racionalidade e atividade jurisdicional.** Rio de Janeiro: Renovar, 2005. ISBN: 9788571475113.

BIONI, Bruno Ricardo – **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo – Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**. N.º1 (2022), p. 8-19. Disponível em: https://ciencia.ucp.pt/pt/publications/intersec%C3%A7%C3%B5es-e-rela%C3%A7%C3%B5es-entre-a-lei-geral-de-prote%C3%A7%C3%A3o-de-dados-lg. [Consult. em 16-11-2024].

BLUM, Renato Opice; MALDONADO, Viviane Nobrega – **Comentário ao GDPR.** São Paulo: RT, 2018. ISBN 978-8553212309.

BOBBIO, Norberto – **A Era dos Direitos.** Rio de Janeiro: Elsevier, 2004. ISBN 88-06-12174-X.

BORGESIUS, Frederik Zuiderveen, POORT, Joost – Online Price Discrimination and EU Data Privacy Law. **Journal Consume Policy**. Vol. 40 (2017), p. 347-366.

BRKAN, Maja – **Do algorithms rule the world? Algorithmic decision-making in the framework of the gdpr and beyond.** Maastricht: Maastricht University - Faculty of Law, 2017. Disponível em: https://ssrn.com/abstract=3124901. [Consult. em 05-10-2020].

CABRAL, Rita Amaral **– O Direito à intimidade da vida privada. Breve reflexão acerca do artigo 80º do Código Civil. Separata dos Estudos em memória do prof. Doutor Paulo Cunha**. Lisboa: [*s. n.*], 1988.

CAMPOS, Diogo Leite de – O Direito e os Direitos da Personalidade. [Em linha]. *In* CAMPOS, Diogo Leite de – **Nós: Estudos sobre os direitos das pessoas**. Coimbra: Almedina, 2004, p. 201-224. Disponível em: http://www.oa.pt/upl/%7B7f3725e2-d544-4142-8f45-d3b6ff311355%7D.pdf. [Consult. em 30-09-2023].

CAMPOS, Diogo Leite – Lições de Direitos da Personalidade. **Boletim da Faculdade de Direito da Universidade de Coimbra**. N.º 67 (1991), p. 129-223.

CAMURÇA, Lia Carolina Vasconcelos – **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário.** [Em linha]. Fortaleza, 2020. Dissertação de Mestrado em Direito, apresentada à Faculdade de Direito, Universidade Federal do Ceará (polic.ª). Disponível em: http://www.repositorio.ufc.br/handle/riufc/51045. [Consult. em 27-02-2021].

CANCELIER, Mikhail Vieira de Lorenzi – O Direito a Privacidade hoje: perspectiva histórica e o cenário brasileiro. [Em linha]. **Seqüência**. N.º 76 (08-2017), p. 213-240. Disponível em: www.scielo.br/pdf/seq/n76/2177-7055-seq-76-00213.pdf. [Consult. em 20-03-2018].

CANOTILHO, José; MOREIRA, Vital – **Constituição da República Portuguesa Anotada. Vol. I**. 4.ª ed. Coimba: Coimbra Editora, 2007. ISBN 978-97-23-22286-9.

CANOTILHO, José Joaquim Gomes – **Direito Constitucional e Teoria da Constituição.** Almedina: Lisboa, 2003. ISBN 978-9724021065.

CAVOUKIAN, Ann – Privacy by design: The 7 foundational principles: Implementation and mapping of fair information practices. [Em linha]. **Privacy by design**, [*s. d.*]. Disponível em: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. [Consult. em 06-10-2023].

CHELES, Tamára – Os Desafios dos Consumidores na Era de Big Data**.** [Em linha]. **Anuário da Proteção de Dados**. (2021), p. 155-176. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/6.-Tamara-Cheles.pdf. [Consult. em 07-03-2022].

CITRON, Danielle Keats; PASQUALE, Frank **–** The scored society: due process for automated predictions. [Em linha]. **Washington Law Review**. Vol. 89, n.º 1 (2014), p. 1-33.

CLARKE, Roger – Profiling: A hidden challenge to the regulation of data surveillance. [Em linha]. **Journal of Law & Information Science**. Vol. 4 (1993), p. 403-419.

Disponível em: http://www5.austlii.edu.au/au/journals/JlLawInfoSci/1993/26.html. [Consult. em 07-03-2022].

CÓDIGO Civil brasileiro e normas correlatas. 9.ª ed. Brasília: Senado Federal, Coordenação de Edições Técnicas, 2017. ISBN 978-85-7018-838-0.

CÓDIGO Civil e legislação complementar. 19.ª ed. Lisboa: Quid Juris Sociedade Editora, 2014. ISBN 978-972-724-672-4.

CONCLUSÕES da Advogada-geral Eleanor Sharpston apresentadas em 17 de Junho de 2010: Processos apensos C-92/09 e C-93/09 Volker und Markus Schecke GbR (Processo C-92/09) contra Land Hessen. [Em linha]. [*s. n.*], (17-06-2010). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62009CC0092&from=EN. [Consult. em 18-11-2024].

CONCLUSÕES do Advogado-geral Giovanni Pitruzzella apresentadas em 15 de dezembro de 2022: Processo C-487/21 F.F. sendo intervenientes: Österreichische Datenschutzbehörde, CRIF GmbH. [Em linha]. **InfoCuria: Jurisprudência**, (15-12-2022). Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=268626&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=203370. [Consult. em 01-10-2023].

CONCLUSÕES do Advogado-geral Henrik Saugmandsgaard Øe, apresentadas em 19 de julho de 2016: Processos apensos C-203/15 e C-698/15 Tele2 Sverige AB contra Post- och telestyrelsen (C-203/15). [Em linha]. **InfoCuria: Jurisprudência**, (19-07-2016). Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=194669. [Consult. em 27-09-2023].

CONCLUSÕES do Advogado-geral Manuel Campos Sánchez-Bordona apresentadas em 27 de abril de 2023: Processo C-807/21 Deutsche Wohnen SE contra Staatsanwaltschaft Berlin. [Em linha]. **InfoCuria: Jurisprudência**, (27-04-2023). Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=272981&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=200935. [Consult. em 01-10-2023].

CONCLUSÕES do Advogado-geral Paolo Mengozzi apresentadas em 1 de fevereiro de 2018: Processo C-25/17 Tietosuojavaltuutettu contra Jehovan todistajat — uskonnollinen yhdyskunta. [Em linha]. **InfoCuria: Jurisprudência**, (01-02-2018). Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=testemunha%2Bjeov%25C3%25A1&docid=198949&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=11717530#ctx1. [Consult. em 05-01-2024].

CONCLUSÕES do Advogado-geral Priit Pikamäe apresentadas em 16 de março de 2023: Processo C-634/21 OQ contra Land Hessen, sendo interveniente: Schufa Holding AG. [Em linha]. **InfoCuria: Jurisprudência**, (16-03-2023). Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=271343&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=205363. [Consult. em 01-10-2023].

CONCLUSÕES do Advogado-geral Yves Bot, apresentadas em 23 de setembro de 2015: Processo C-362/14 Maximillian Schrems contra Data Protection Commissioner. [Em linha]. **InfoCuria: Jurisprudência**, (23-09-2015). Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=197008. [Consult. em 27-09-2023].

CONSEIL DEL'EUROPE – **S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04**, **4 December 2008**. [Em linha]. Disponível em: https://rm.coe.int/168067d216. [Consult. em 05-03-2022].

CONSTITUIÇÃO da República Federativa do Brasil, de 05 de outubro de 1988. 12.ª ed. São Paulo: Saraiva, 2016. ISBN 978-85-02-63516-6.

CONSTITUIÇÃO da República Portuguesa: Lei Constitucional n.º 01/2005, de 12 de agosto. 2.ª ed. Lisboa: Quid Juris Sociedade Editora, 2012. ISBN 978-972-724-586-4.

CONVENÇÃO Europeia dos Direitos do Homem. São Paulo: Revista dos Tribunais, 2015. ISBN 9788553216642.

CORDEIRO, António Barreto Menezes – **Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019.** Lisboa: Almedina, 2020. ISBN 9789724083049.

CORREIA, Sérgio Miguel José – Direito de oposição à definição de perfis. **Anuário de Proteção de Dados**. (2022), p. 189-215.

COSTA, Diego Carneiro – A Discriminação Algorítmica e as Novas Perspectivas Sobre u Tratamento de Dados Pessoais Sensíveis. *In* REQUIÃO, Maurício – **Proteção de Dados Pessoais: Novas Perspectivas**. Salvador: EDUFBA, 2022.

COSTA, Inês da Silva – A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. [Em linha]. **Revista Eletrónica de Direito.** Vol. 24, n.º 1 (02-2021), p. 33-82. Disponível em: https://cij.up.pt//client/files/0000000001/4-ines-costa_1677.pdf. [Consult. em 13-04-2022].

COUNCIL OF EUROPE. COMMITTEE OF MINISTERS – **Convenção para proteção das pessoas relativamente ao tratamento de dados de carácter pessoal**. [Em linha]. [*s. n.*], (18-05-2018). Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. [Consult. em 01-10-2023].

DIAS, Patrícia Cardoso **– Proteção de dados pessoais no contexto da pandemia provocada pelo corona vírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública.** [Em linha]. [sl]: [sn], [sd]. [consulta 18 fev 2021] Disponível em: http://julgar.pt/protecao-de-dados-pessoais-no-contexto-da-pandemia-provocada-pelo-novo-coronavirus-sars-cov-2-aspetos-etico-juridicos-relevantes-da-protecao-de-dados-de-saude-no-ambito-da-emergencia-de-saude-publica/.

DINIZ, Maria Helena – **Dicionário jurídico.** 3.ª ed. São Paulo: Saraiva, 2008. ISBN 978-8502071841.

DOMINGOS, Pedro – **The master algorithm: how the quest for the ultimate machine learning will remake our world.** Nova York: Basic Books, 2015. ASIN: B012271YB2.

DONEDA, Danilo Cesar Maganhoto – **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Brasília: Escola Nacional de Defesa do Consumidor/SDE/DPDC, 2010.

DONEDA, Danilo Cesar Maganhoto – **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006. ISBN: 978-857-14-75-625.

EDWARDS, Lilian; VEALE, Michael – Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. [Em linha]. **Duke Law & Technology Review**. Vol. 16, n.º 1 (2017), p. 18-84. Disponível em: https://ssrn.com/abstract=2972855. [Consult. em 10-04-2022]

EUROPEAN COURT OF HUMAN RIGHTS. COUR EUROPÉENNE DES DROITS DE L'HOMME – **Case of Barbulescu v. Romania No. 61496/08, 05 September 2017**. [Em linha]. Disponível em: https://hudoc.echr.coe.int/spa?i=001-177082. [Consult. em 05-03-2022].

EUROPEAN DATA PROTECTION BOARD – **Guidelines on Consent under Regulation 2016/679**. [Em linha]. [*s. n.*], (04-05-2020). Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. [Consult. em 13-09-2023].

EUROPEAN DATA PROTECTION SUPERVISOR – **Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.** [Em linha]. Strasbourg: European Data Protection Supervisor, 2017. Disponível em: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf. [Consult. 14-09-2023].

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS – **Big data: discrimination in data-supported decision making**. [Em linha]. Vienna: European Union Agency for Fundamental Rights, 2018. Disponível em: https://fra.europa.eu/en/publication/2018/big-data-discrimination. [Consult. em 13-04-2022].

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. COUNCIL OF EUROPE – **Handbook on European data Protection Law**. [Em linha]. Luxembourg: Publications Office of the European Union, 2018. Disponível em: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf. [Consult. em 15-04-2022].

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro – *Arbitrium ex machina*: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais**. Vol. 107, n.º 995 (09-2018), p. 635-655.

FERRARI, Isabela; BECKER, Daniel – Algoritmo e preconceito. [Em linha]. **Jota.** (12-12-2017). Disponível em: https://www.jota.info/opiniao-e-analise/artigos/algoritmo-e-preconceito-12122017. [Consult. em 27-09-2023].

FORTES, Vinicius – **O direito fundamental à privacidade: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil.** Rio de Janeiro, 2015. Tese de Doutorado apresentada à Universidade Estácio de Sá (polic.ª).

GIANNOTTI, Edoardo – **A tutela constitucional da intimidade.** Rio de Janeiro: Forense, 1987.

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE**. [Em linha]. (09-04-2014). Disponível em: https://www.uc.pt/site/assets/files/475840/20140409_wp_217_parecer_6_2014_conceito_interesses_legitimos_resp_trat_diretiva_95.pdf. [Consult. em 10-06-2023].

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**. [Em linha]. (06-02-2018). Disponível em: https://ec.europa.eu/newsroom/article29/items/612053/em. [Consult. em 18-11-2024].

GUIDI, Guilherme Berti de Campos – **Proteção de Dados Pessoais: a composição de sistemas pelo Direito Internacional.** [Em linha]. São Paulo, 2022. Tese de doutorado apresentada à Universidade de São Paulo (polic.ª). Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2135/tde-05092022-080749/. [Consult. em 27-06-2023].

GUTWIRTH, Serge; HERT, Paul de – Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. **Revista Direito Público**. Vol. 18, n. 100 (10/12-2021), p. 500-549. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6200/pdf. [Consult. em 17-11-2024].

HERT, Paul De; LAMMERANT, Hans – Predictive profiling and its legal limits: Effectiveness gone forever. *In* SLOOT, Bart van der; BROEDERS, Dennis; SCHRIJVERS, Erik (eds.). – **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016.

JAQUET-CHIFFELLE, David-Olivier – Reply: Direct and Indirect *Profiling* in the Light of Virtual Persons. *In* HILDEBRANDT, Mireille; GUTWIRTH, Serge (edts) – **Profiling the European Citizen: Cross-Disciplinary Perspectives**. Berlin: Springer, 2008.

JONES, Meg Leta – The right to a human in the loop: Political constructions of computer automation and personhood. [Em linha]. **Social Studies of Science**. Vol. 47, n.º 2 (2017), p. 216-239. Disponível em: https://dx.doi.org/10.2139/ssrn.2758160. [Consult. em 11-11-2022].

JUNIOR, Glauto Lisboa Melo – O consumidor de seguros na era do big data: desafios da atual regulamentação europeia frente às técnicas de definição de perfis, aprendizagem de máquina e decisões automatizadas. **Actualidad Jurídica Iberoamericana**. N.º 18 (02-2023), p. 2134-2163.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade.** [Em linha]. Juiz de Fora, 2019. Dissertação de pós-

graduação em Direito da Faculdade de Direito, apresentada à Universidade Federal de Juiz de Fora (polic.ª). Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/11438. [Consult. em 11-11-2022].

KURTZ, Christian; SEMMAN, Martin; BÖHMANN, Tilo – Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. [Em linha]. **Researchgate**, (08-2018). Disponível em: https://www.researchgate.net/publication/325415927_Privacy_by_Design_to_Comply_with_GDPR_A_Review_on_Third-Party_Data_Processors. [Consult. em 23-09-2023].

LEAL, Ana Alves – Big data e proteção de dados pessoais – desafios à luz do Regulamento Geral de Proteção de Dados. [Em linha]. **Opinião.** N.º 207 (05/06-2018), p. 18-19. Disponível em: https://www.cidp.pt/noticia/big-data-e-protecao-de-dados-pessoais-artigo-de-opiniao-da-investigadora-ana-alves-leal-na-revista-vida-judiciaria/32. [Consult. em 27-08-2022].

LEITE, Beatriz da Costa Gomes – **Proteção de dados e privacidade em linha.** [Em linha]. Coimbra, 2021. Dissertação de mestrado em Ciências Jurídico-Forenses, apresentada à Universidade de Coimbra (polic.ª). Disponível em: https://estudogeral.uc.pt/bitstream/10316/98822/1/Disserta%C3%A7%C3%A3o.pdf. [Consult. em 10-10-2022].

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de – Da Evolução das Legislações sobre a Proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. Revista de Direito**. Vol. 12, n.º 02 (2020), p. 1-33.

MARCACINI, Augusto Tavares Rosa – Regras aplicadas ao tratamento de dados pessoais. *In* LIMA, Cíntia Rosa Pereira de (coord.) – **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

MARTINAZZO, Waleska Malvina Piovan – **O trabalhador e a proteção de dados para o combate à discriminação digital nas relações de trabalho: um estudo de caso a partir de julgado do TRT da 18ª região**. Brasília-DF, 2023. Tese de doutorado em Direito

Constitucional, apresentada ao Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa (polic.ª).

MELLO, Celso Antonio Bandeira – **Curso de Direito Administrativo.** 26.ª ed. São Paulo: Malheiros, 2009.

MENDES, Laura Schertel – **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. ISBN 978-8502218963.

MENDES, Laura; MATIUZZO, Marcela – Discriminação algorítmica: conceito, fundamento legal e tipologia. [Em linha]. **Direito Público**. Vol. 16, n.º 90 (2019). Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. [Consult. em 10-01-2024].

MENDES, Paulo de Sousa – A privacidade digital posta à prova no processo penal. [Em linha]. **Quaestio facti. Revista Internacional sobre Razonamiento Probatorio**. N.º 2 (2021), p. 225-250. Disponível em: https://www.raco.cat/index.php/quaestio-facti/article/view/399271. [Consult. em 27-09-2023].

MENKE, Fabiano – A possibilidade de cumulação de bases legais nas operações de tratamento de dados pessoais. [Em linha]. **Migalhas**, (26-02-2021). Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/340890/cumulacao-de-bases-legais-nas-operacoesde-tratamento-de-dados. [Consult. 23-01-2023].

MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada.** Lisboa: Universidade Católica, 2017. ISBN 978-9725405413.

MOEREL, Lokke; PRINS Corien – On the Death of Purpose Limitation. [Em linha]. **Iapp**, (02-06-2015). Disponível em: https://iapp.org/news/a/on-the-death-of-purpose-limitation/. [Consult. em 10-04-2022].

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon – A normatividade dos dados sensíveis na lei geral de proteção de dados:

ampliação conceitual e proteção da pessoa humana. [Em linha]. **Revista de Direito, Governança e Novas Tecnologias**. Vol. 5, n.º 1 (2019), p. 63–85. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479. [Consult. em 11-11-2022].

NOVAIS, Jorge Reis – **As restrições aos direitos fundamentais não expressamente autorizadas pela constituição.** Imprenta: Coimbra, Wolters Kluwer, 2010. ISBN 9789723218336.

OLIVEIRA, Madalena Perestrelo de – Definição de Perfis e Decisões Individuais Automatizadas no Regulamento Geral sobre a Proteção de Dados. *In* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Coord.) – **FinTech II – Novos Estudos sobre Tecnologia Financeira**. Lisboa: Almedina, 2019.

O'NEIL, Cathy – The era of blind faith in big data must end. [Em linha]. **TED: Ideas change everything**, (04-2017). Disponível em: https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end/transcript. [Consult. em 10-09-2023].

O'NEIL, Cathy – **Weapons of math destruction: How big data increases inequality and threatens democracy.** Portland: Broadway Books, 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – **Declaração Universal dos Direitos do Homem.** [Em linha]. [*s. n.*], [*s. d.*]. Disponível em: http://www.onu.org.br/img/2014/09/DUDH.pfg. [Consult. em 20-01-2021].

PASQUALE, Frank – **The black box society: the secret algorithms that control money and information.** Cambridge: Harvard University Press, 2015.

PEREIRA DE SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius – Considerações iniciais sobre os interesses legítimos do controlador na lei geral de proteção de dados pessoais. [Em linha]. **Direito Público.** Vol. 16, n.º 90 (12-2019). Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744. [Consult. em 10-06-2019].

PILATI, Jose; OLIVO, Mikhail – Um Novo Olhar sobre o Direito à Privacidade: caso Snowden e pós-modernidade jurídica**.** [Em linha]. **Seqüência**. N.º 69 (12-2014), p. 281-300. Disponível em: www.scielo.br/pdf/seq/n69/12.pdf. [Consult. em 29-03-2020].

PINTO, Paulo Mota – O direito à reserva sobre a intimidade da vida privada. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. 69 (1993), p. 479-586.

PIRES, Lucas – **Direito à Privacidade no Âmbito da Sociedade da Informação: reflexões em torno da questão nos inícios do século XXI.** Coimbra, 2014. Dissertação de mestrado em Ciências Jurídico-Políticas, apresentada à Universidade de Coimbra (polic.ª). Disponível em: https://bit.ly/3ldxL1E. [Consult. em 10-11-2021].

RODOTÀ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008. ISBN: 978-85-71-47688-2

RUCKER, Daniel; KUGLER, Tobias – **New European general data protection regulation, a practitioner´s guide: ensuring compliant corporate practice**. Munique: Beck Hart Nomos, 2017. ISBN 978-1509920600.

RUCKER, Daniel; KUGLER, Tobias – **New European general data protection regulation, a practituioner´s guide: ensuring compliant corporate practice.** Baden-Baden: Nomos Verlagssgesellschaft, 2018. ISBN 978-3-8487-3262-3.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden – **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) – L. 13.709/2018.** [Em linha]. Revista Direitos Fundamentais & Democracia. Vol. 26, n.º 2 (05/08-2021), p. 81-106. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/download/2172/694/5371. [Consult. em 20-05-2023].

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel – **Curso de direito constitucional.** São Paulo: Revista dos Tribunais, 2012. ISBN: 9788520343166.

SCHWARTZ, Paul – The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. [Em linha]. **The American Journal of Comparative Law**. [Em linha]. Vol. 37, n.º 04 (1989), p. 675-701. Disponível em: https://lawcat.berkeley.edu/record/1113532. [Consult. em 30-01-2021].

SILVEIRA, Alessandra – Automated individual decision-making and profiling [on case C-634/21 - SCHUFA (Scoring)]. [Em linha]. **UNIO – EU Law Journal**. Vol. 8, n.º 2 (03-2023), p. 74-85. Disponível em: https://revistas.uminho.pt/index.php/unio/article/view/4842/5331. [Consult. em 20-05-2023].

SOLOVE, Daniel J. – Privacy Self-Management and the Consent Dilemma. [Em linha]. **Harvard Law Review**. Vol. 126 (2013), p. 1880-1903. Disponível em: https://ssrn.com/abstract=2171018. [Consult. em 10-03-2022].

SOMBRA, Thiago – **Fundamentos da regulação da privacidade e proteção de dados pessoais.** São Paulo: Thomson Reuters Brasil, 2019. ISBN: 9788553219919.

STUMM, Raquel Denize – **Princípio da proporcionalidade no direito constitucional brasileiro.** Porto Alegre: Livraria do Advogado, 1995. ISBN 8585616814.

SUPREMO TRIBUNAL FEDERAL – **Acórdão do Supremo Tribunal Federal com número MS 23.452, 28 de maio de 1999.** [Em linha]. Relator: Celso de Mello. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=1763585. [Consult. em 28-04-2018].

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario – Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. [Em linha]. **Civilistica.com: Revista Eletrônica de Direito Civil.** Vol. 9, n.º 1 (2020), p. 1-38. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd. [Consult. em 30-06-2023].

TEPEDINO, Gustavo; TEFFÉ, Chiata Spadaccini de – Consentimento e proteção de dados pessoais na LGPD. *In* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coords.) – **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. ISBN 978-8553216635.

TEPEDINO, Gustavo; TEFFÉ, Chiata Spadaccini de – O Consentimento na circulação De Dados Pessoais. **Revista Brasileira De Direito Civil.** Vol. 25, n.º 03 (11-2020), p. 83.

TODOLÍ-SIGNES, Adrian – Algorithms, artificial intelligence and automated decisions about workers and the risks of discrimination: The necessary collective governance of data protection. [Em linha]. **Sage Journals**. Vol. 25, n.º 4 (23-09-2019). Disponível em: https://journals.sagepub.com/doi/abs/10.1177/1024258919876416. [Consult. em 12-11-2022].

TODOLÍ-SIGNES, Adrian – Algorithms, artificial intelligence and automated decisions about workers and the risks of discrimination: The necessary collective governance of data protection. [Em linha]. **Transfer: European Review of Labour and Research**. Vol. 25, n.º 4 (2019), p. 1-17. Disponível em: http://dx.doi.org/10.2139/ssrn.3316666. [Consult. em 05-10-2020].

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 6 de outubro de 2015 (Grande Secção), Schrems (C-362/14, EU:C:2015:650).** [Em linha]. Relator: T. von Danwitz. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=197008. [Consult. em 05-10-2023].

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 8 de abril de 2014 (Grande Secção), Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238).** [Em linha]. Relator: T. von Danwitz. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=197811. [Consult. em 05-10-2023].

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 24 de novembro de 2011 (Terceira Secção), C-468/10, C-469/10).** [Em linha]. Relator: K. Lenaerts. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=115205&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=200079. [Consult. em 05-10-2023].

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 4 de maio de 2023 (Primeira Secção) Processo 487/21**. [Em linha]. Relator: I. Ziemele. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=273286&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=203370. [Consult. em 05-10-2023].

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 6 de novembro de 2003 (Grande Secção), Lindqvist (C-101/01, EU:C:2003:596)**. [Em linha]. Relator: D. A. O. Edward. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=204415. [Consult. em 05-10-2023].

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 19 de outubro de 2016, no caso Breyer (C-582/14, EU:C:2016:779)**. [Em linha]. Relator: A. Rosas. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=207265. [Consult. em 03-10-2023].

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA – **Acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, ECLI:EU:C:2014:317)**. [Em linha]. Relator: M. Ilešič. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1050249. [Consult. em 03-12-2023].

UNIÃO EUROPEIA – Carta dos Direitos Fundamentais da União Européia. [Em linha]. **Jornal Oficial da União Europeia**, (26-10-2012). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12012P/TXT&from=PT. [Consult. em 12-12-2020].

UNIÃO EUROPEIA – Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. [Em linha]. **Jornal Oficial.** Nº L 281 (23/11/1995), p. 31-50. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. [Consult. em 12-12-2020].

UNIÃO EUROPEIA – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. [Em linha]. **Jornal Oficial da União Europeia**, (04-05-2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. [Consult. em 15-03-2020].

UNIÃO EUROPEIA – Resolução do Parlamento Europeu 14/2017 – Implicação dos Grandes Volumes de Dados nos Direitos Fundamentais. [Em linha]. **Jornal Oficial da União Europeia**, (14-03-2017). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017IP0076&from=LV. [Consult. em 25-09-2023].

VASCONCELOS, Pedro Pais de – **Direito de Personalidade**. Coimbra: Almedina, 2006. ISBN: 9789724029948.

VIEIRA, Tatiana Malta – **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Brasília-DF, 2007. Dissertação de mestrado científico em Direito, apresentada à Universidade de Brasília (polic.ª).

VOIGT, Paul; BUSSCHE, Axel von dem – **The EU General Data Protection Regulation (GDPR): A Practical Guide.** Berlin: Springer, 2017. ISBN 978-3319862910.

WACHTER, Sandra; MITTELSTADT, Brent – A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. [Em linha]. **Columbia Business Law Review**. Vol. 2019, n.º 2 (05-10-2018), p. 1-130. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. [Consult. em 27-08-2022].

WARREN, Samuel; BRANDEIS, Louis – The right to privacy. [Em linha]. **Civilistica.com: Revista Eletrônica de Direito Civil**. Vol. 2, n.º 3 (2013), p. 1-22. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/127. [Consult. em 15-03-2021].

WESTIN, Alan F. **– Privacy and Freedom**. New York: Atheneum, 1967.

ZANATTA, Rafael A. F. – Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. [Em linha]. **ResearchGate**, (02-2019). Disponível em: https://www.researchgate.net/publication/331287708. [Consult. em 02-01-2024].