UNIVERSIDADE DE LISBOA
Faculdade de Direito

Proteção de dados pessoais e autoridade de controle: perspectivas e desafios para o Brasil sob a ótica do direito comparado

Renata de Assis Calsing

Programa de pós-doutoramento em Direito

2019

UNIVERSIDADE DE LISBOA
Faculdade de Direito

Proteção de dados pessoais e autoridade de controle: perspectivas e desafios para o Brasil sob a ótica do direito comparado

Renata de Assis Calsing

Orientador: Prof. Doutor Pedro Romano Martinez

Relatório de pesquisa elaborado no âmbito do programa de pós-doutoramento em Direito, para discussão pública e obtenção de certificado.

2019

O progresso é impossível sem mudança; e aqueles que não conseguem mudar as suas mentes, não conseguem mudar nada.

George Bernard Shaw

Agradecimentos

À minha família e a todos os amigos que me apoiaram neste desafio de aprimoramento pessoal e intelectual.

À Controladoria-Geral da União e ao Centro Universitário do Distrito Federal, pela confiança, e por tornar possível o desenvolvimento deste trabalho.

Ao Prof. Dr. Pedro Romano Martinez, pela inspiração, sabedoria e gentileza, em nome de quem agradeço a todos os professores e servidores da Faculdade de Direito da Universidade de Lisboa.

A Portugal e aos portugueses, pela receptividade e pelas lições de história.

Resumo: O presente trabalho, usando o método do direito comparado, analisou a tutela dos dados pessoais no Brasil e na União Europeia. Partindo de seu conceito, mostrou-se os riscos que a recolha, uso, tratamento e compartilhamento de dados pessoais trazem para os direitos humanos fundamentais, e que impulsionaram a criação e aprimoramento de normas que visam salvaguardar a liberdade de escolha do titular, para que haja maior simetria na relação jurídica, o que é indispensável na sociedade da informação. Por fim, foram elencados os elementos institucionais basilares das autoridades de controle, que têm por missão incentivar os meios de *accountability* e segurança de dados, e aplicar penalidades para os casos de incumprimento, visando fomentar, proteger e permitir a autodeterminação informativa.

Palavras-Chaves: dados pessoais; RGPD; LGPD; autoridade de controle; direito comparado.

Abstract: Using the comparative law method, we have analyzed the protection of personal data in Brazil and in the European Union, and their legal regimes: RPGD and LGPD. We have shown the risks to fundamental human rights associated with personal data processing, which has led to the creation and improvement of norms that aim to safeguard the freedom of choice of the recipient, ensuring greater information symmetry in the legal relationship, vital in the information society. Finally, we have shown the basic institutional elements of the supervisory authorities, whose mission is to encourage accountability and data security, and to impose penalties for non-compliance in order to foster, protect and enable informative self-determination.

Key Words: personal data; GDPR; LGPD; data protection authorities; comparative law.

LISTA DE ABREVIATURAS E TERMOS PRÓPRIOS AO TEMA

AEPD - Autoridade Europeia para a Proteção de Dados

ANPD – Autoridade Nacional de Proteção de Dados (Brasil)

APD ou autoridades de controle - autoridades públicas independentes que controlam, através de poderes de investigação e de correção, a aplicação da legislação relativa à proteção de dados.

Carta - Carta dos Direitos Fundamentais da União Europeia

CEDH - Convenção Europeia dos Direitos do Homem

CEPD - Comitê Europeu de Proteção de Dados

CNPD - Comissão Nacional de Protecção de Dados (Portugal)

EEE - Espaço Econômico Europeu

EUA – Estados-Unidos da América

LGPD - Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14/08/2018 - Brasil).

Responsáveis (pelo tratamento) ou controladores - O primeiro termo é usado no RGPD, enquanto o segundo foi preferido pela LGPD. Usaremos os dois como sinônimos, pois ambos se referem à pessoa (singular ou coletiva), de direito público ou privado, a quem competem as decisões sobre as finalidades e os meios pelos quais os dados pessoais são tratados.

RGPD - Regulamento Geral sobre a Proteção de Dados

STF – Supremo Tribunal Federal (Brasil)

STJ – Superior Tribunal de Justiça (Brasil)

TEDH - Tribunal Europeu dos Direitos do Homem

Titulares - pessoa singular a que se referem os dados pessoais

TJUE - Tribunal de Justiça da União Europeia

TSE - Tribunal Superior Eleitoral (Brasil)

UE – União Europeia

CADE - Conselho Administrativo de Defesa Econômica (Brasil)

Sumário

Introdução

A proteção de dados pessoais foi recentemente regulamentada no Brasil pela Lei nº 13.709, de 14 de agosto de 2018, tendo recebido diversas alterações antes mesmo de sua entrada em vigor[1]. Como em diversos países, a regulamentação sobre o tema ainda gera uma série de dúvidas e divergências, por abranger diferentes áreas do conhecimento e por tratar de tecnologias que estão sendo constantemente descobertas e desenvolvidas.

Apesar dos questionamentos que são levantados, a proteção dos dados pessoais é importante, pois seu tratamento pode afetar direitos e liberdades fundamentais, entre os quais a lei brasileira destaca a liberdade, a privacidade e o livre desenvolvimento da personalidade[2].

O Regulamento Geral de Proteção de Dados (RGPD)[3] define a proteção de dados pessoais como um direito fundamental autônomo, reconhecendo sua influência para o fortalecimento de uma sociedade igualitária, onde há exercício da personalidade de forma digna[4]. É, assim, relevante para a manutenção do Estado democrático de Direito, e pré-requisito para a efetividade de diversas outras liberdades fundamentais[5] [6].

Por isso, as leis que serão analisadas nesta pesquisa promovem o consentimento como uma questão de democracia e cidadania, em que o titular volta a ser ouvido e considerado nas decisões que envolvem os seus dados, seja no uso indiscriminado por órgãos de governo, seja por empresas privadas para fins econômicos. Procura-se, portanto, incentivar uma forma de controle individual/social da gestão de dados, que é hoje um enorme patrimônio.

---

[1] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).
[2] *Idem,* art. 1º.
[3] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE - Regulamento Geral sobre a Proteção de Dados (RGPD), JO L119 de 4 de maio de 2016
[4] CALVÃO, Filipa Urbano. *Direito da Proteção de Dados Pessoais: relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*. Porto: Universidade Católica Editora, p. 41.
[5] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 92.
[6] Como, por exemplo, a criação de perfis sociais e de comportamento que podem impedir uma pessoa de viajar para um país estrangeiro (listas de pessoas perigosas, com associações criminosas ou religiosas indesejadas), o que acaba afetando não somente sua personalidade, mas o direito de ir e vir.

Deve-se equilibrar a assimetria informacional entre titulares e responsáveis, já que quanto mais aumentam os usos e oportunidades de tratamento de dados, menos o titular toma conhecimento do que acontece com eles e de como são compartilhados. Como lembra Alexandre Sousa Pinheiro, apesar do reconhecimento da proteção de dados ter por base princípios fortes como o da personalidade, da proteção da vida privada e do direito à autodeterminação[7], a verdade é que "o clima sociocultural em que vivemos não favorece nem a *privacy*, nem a protecção de dados. Estranha-as"[8].

Consequentemente, não adianta somente falar em princípios e regras, ou tampouco da jusfundamentalidade da proteção de dados. Como dizia Bobbio[9], os direitos humanos já não carecem mais de fundamentação, mas sim de aplicação, de efetividade. Em uma sociedade que estranha a privacidade e o resguardo de informações pessoais, as próprias características dos direitos humanos fundamentais devem passar por uma revisão de conteúdo, com abrangente crítica em relação à sua procedimentalização.

Neste aspecto, as leis brasileira e europeia se apoiam em dois pilares: no aumento de poder do titular, em um ambiente regulado em que lhe é garantido o controle sobre suas informações pessoais[10]; e no *enforcement* da lei por parte de uma autoridade de controle.

Diferentemente do modelo americano de *privacy*, em que a proteção de dados pessoais se dá por setores e de maneira descentralizada no corpo de outros normativos, uma lei geral fiscalizada por uma autoridade central pode ser um modelo mais adequado de revisão da procedimentalização de um direito considerado fundamental, para que verdadeiramente o seja.

A autoridade de controle também terá papel importante na ponderação de direitos e na harmonização legislativa, já que a proteção de dados pessoais se entremeia em outros

---

[7] PINHEIRO, Alexandre Sousa. *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*. Lisboa: AAFDL, 2015, p 105.

[8] *Idem*, p. 107.

[9] BOBBIO, Norberto. *A era dos direitos*. Rio de Janeiro: Elsevier, 2004, p. 37. Citamos *in verbis*: "O campo dos direitos do homem — ou, mais precisamente, das normas que declaram, reconhecem, definem, atribuem direitos ao homem — aparece, certamente, como aquele onde é maior a defasagem entre a posição da norma e sua efetiva aplicação".

[10] Desde logo, ressaltamos que o objetivo da LGPD e do RGPD não é de garantir sigilo absoluto aos dados pessoais, mas o controle dos dados por parte do titular, que deve ponderar quando e onde fornecer seus dados e em troca de quais benefícios.

campos, como acesso à informação, desenvolvimento tecnológico/econômico, liberdade de imprensa, entre outros. Ainda, será ponto central de interpretação de uma lei com caráter interdisciplinar, onde o Direito precisa de apoio de outras áreas para chegar a soluções mais razoáveis e efetivas. E, esta função não é restrita à esfera administrativa, já que sua *expertise* pode auxiliar o Poder Judiciário a aplicar o normativo de forma mais estável e adequada.

Ademais, o direito contemporâneo passa por um processo de transição, que acompanha a atual sociedade digital e globalizada, onde a informação tornou-se o principal ativo para concretização de acesso a bens, serviços, conveniências, política e até mesmo direitos fundamentais. Este processo é influenciado pela ampliação da complexidade e interação frequente entre os direitos nacionais, o direito de sistemas regionais de integração e o direito internacional, já que o mundo digital não tem fronteiras claras. Ou seja, os problemas enfrentados pelos diferentes países a respeito da proteção e melhor utilização dos dados pessoais estão interconectados, fazendo deste um campo fértil para a realização de pesquisas utilizando o método do Direito Comparado.

Isto posto, o tema escolhido: "Proteção de Dados Pessoais e autoridade de controle: perspectivas e desafios para o Brasil sob a ótica do direito comparado", mostra-se relevante diante da complexidade do regime e da constatação de que a criação de um órgão com poderes sancionatórios é um passo importante para que a LGPD possa ser efetivamente implementada no Brasil.

O objetivo geral é analisar os elementos indispensáveis a serem previstos no desenho institucional da autoridade de controle brasileira, a partir do exame comparado entre o RGPD e a LGPD, tendo em vista que o modelo europeu serviu de base/exemplo para a elaboração da lei brasileira. Desta maneira, uma pesquisa de direito comparado tem muito a contribuir para o momento de preparação do Estado brasileiro antes da entrada em vigor (*vacatio legis*) da LGPD.

Em relação ao recorte escolhido, como as autoridades europeia e portuguesa se encontram estabelecidas e com diversas decisões interessantes, seu estudo pode servir como embasamento para o modelo institucional que está sendo (ainda) discutido no Brasil.

Para desenvolver o tema e problema propostos, a pesquisa teve como objetivos específicos: investigar o que são dados pessoais e as razões de protegê-los; entender o caminho legislativo percorrido no âmbito europeu até a entrada em vigor do RGPD; analisar comparativamente o RGPD e a LGPD; relacionar as características e competências das autoridades de controle; e propor uma estrutura para a ANPD, a partir da experiência europeia.

Em relação à forma, escolheu-se uma escrita prática e objetiva, para alcançar um público-alvo amplo, abrangendo não somente os acadêmicos de Direito, mas também servidores públicos com diferentes formações, advogados, administradores, profissionais de tecnologia da informação e demais interessados no tema. Queremos, de tal modo, aproximar a academia da realidade do Poder Executivo brasileiro, construindo um caminho – que se não novo – é ainda pouco ou mal utilizado.

Muito se fala e se propaga a respeito da necessária inserção acadêmica no mercado de trabalho, e na função social da pesquisa como meio de contribuir para a melhoria da realidade cotidiana. Porém, essa faceta ainda é vista com desconfiança e retração pelo meio acadêmico mais tradicional, onde se inclui o Direito, o que pode gerar nos estudantes desinteresse em pesquisar, e a realização de pesquisas cuja divulgação ou conhecimento social são extremamente limitadas, porque realizadas para se manter dentro de um contexto universitário rígido, mais voltado para o cultismo do que para a sociedade.

Neste sentido, vemos a pesquisa de pós-doutoramento como um espaço privilegiado para a elaboração de análises mais práticas, diretas e voltadas para um foco específico, que esteja dentro da linha de trabalho e interesse do professor doutor, que já passou por diferentes estágios de prova acadêmica para atestar sua capacidade intelectual e metodológica dentro do ramo da ciência que escolheu.

Não queremos com isso dizer que o caminho escolhido é o único que se deva trilhar. Pelo contrário. Mas é importante que haja caminhos – no plural.

Definidos o problema e recorte metodológico, vamos demonstrar o caminho escolhido para alcançar os objetivos definidos. A tese se divide em 3 capítulos. O primeiro é voltado para o estudo da proteção de dados pessoais, onde se buscou definir e contextualizar o bem a ser protegido, apresentando a sociedade da informação, os

elementos que formam o conceito de dados pessoais, as razões pelas quais estes devem ser protegidos, e o caminho percorrido no âmbito legislativo europeu, passando pelos remédios civis de reparação de danos à personalidade, até o reconhecimento do *status* de direito fundamental.

Buscamos apresentar a questão ao leitor para que, entendendo os riscos que existem na coleta, uso, tratamento e armazenamento de dados, possa compreender porque foram criados e aprimorados os normativos que procuraram proteger a liberdade de escolha do titular, e como esse balanceamento de poder na relação jurídica pode ser um fator de empoderamento e autonomia, tão essenciais ao ser humano na sociedade da informação.

A ideia não é apresentar um histórico normativo completo e pormenorizado, porque tal estudo já foi realizado em outras obras, e sua extensão não permitiria que nos aprofundássemos no nosso tema de pesquisa. O que se buscou foi demonstrar que, no âmbito europeu, a proteção de dados passou por um processo de construção legislativo e jurisprudencial, enquanto no Brasil a inspiração veio das experiências internacionais, tendo sido um dos últimos países da América do Sul a ter uma lei sobre o tema[11].

Apresentadas a razão para se proteger os dados pessoais e o caminho percorrido no âmbito europeu, passamos para a comparação entre o RGPD e a LGPD (capítulo 2). Usando o método do direito comparado, iremos trazer um exame em dois eixos: direitos do titular e deveres e obrigações de empresas e órgãos públicos que tratam dados pessoais. A fim de contribuir de uma forma objetiva ao tema da pesquisa, foi dado enfoque nas inovações normativas e aspectos que carecem de ação da autoridade de controle.

Dentro do primeiro tópico, destacamos que o RGPD e a LGPD delimitam a base legal para que o tratamento seja considerado lícito. Como direitos do titular, enfatizamos o consentimento, que inova ao promover a noção de autodeterminação informativa; o tratamento de categorias especiais de dados, cuja intervenção do Estado é crucial diante

[11] Ronaldo Lemos fala que o RGPD teve um "efeito viral" para outros países, entre os quais está o Brasil. In: LEMOS, Ronaldo. *A GDPR terá um efeito viral*. Entrevista concedida à Luiz Gustavo Pacete. Disponível em: https://www.meioemensagem.com.br/home/midia/2018/05/21/a-gdpr-tera-um-efeito-viral.html, acesso em 30/09/2019.

dos riscos para as liberdades e direitos fundamentais; e o “direito ao esquecimento”, que não foi trazido de forma explícita pela lei brasileira.

Na parte das obrigações, realçamos a figura do encarregado de dados pessoais; os meios de *accountability* (como avaliação de impacto, elaboração de códigos de conduta e procedimentos certificados); e as multas e penalidades.

Passamos, então, para a terceira parte do nosso estudo, que analisa os mecanismos de *compliance* e *enforcement* usados para tornar a proteção de dados pessoais mais efetiva, o que requer a criação, estruturação e bom funcionamento das autoridades de controle (APD). Usando o método do direito comparado, investigamos a composição técnica, autonomia e as três principais competências destas autoridades: consultiva/regulamentar, decisão/controle e promoção/aperfeiçoamento.

Por fim, vamos apontar algumas discussões em torno do modelo escolhido pela legislação brasileira para a ANPD, e oferecer sugestões de ajuste que ainda podem ser realizadas, uma vez que a autoridade foi criada, mas ainda não foi estruturada, a partir dos desafios e perspectivas aprendidos com a experiência europeia.

Capítulo 1 - Dados Pessoais: o bem a ser protegido

Para que possamos compreender os normativos sobre a proteção de dados pessoais e as autoridades administrativas responsáveis pela sua aplicação, vamos, primeiro, estudar o que é a sociedade da informação (1.1.), o que nos dará um parâmetro de entendimento a respeito do conceito de dados pessoais (1.2) e da importância de sua proteção (1.3). Por fim, o capítulo mostrará a inserção dos dados pessoais dentro da esfera dos direitos da personalidade e o caminho percorrido para que fosse reconhecido como direito humano fundamental (1.4).

1.1. A sociedade da informação e o avanço tecnológico

Sociedade da informação é um dos termos utilizados para denominar a época contemporânea no que diz respeito ao imenso volume de informações e dados que estão à disposição das pessoas, demonstrando ainda o fato de que eles (informações e dados) são considerados um dos grandes valores econômicos atuais.

A escolha do termo sociedade da informação não exclui outros que possam, porventura, surgir ou serem utilizados para explicar o movimento da sociedade no que tange ao uso e expansão da comunicação, e de como ela afeta as relações sociais[12]. Isto porque, ao se tentar conceituar a expressão, estamos analisando um objeto com histórias, realidades e origens diferentes, o que a torna difícil de identificar, e permite que apareçam outros candidatos[13].

Não obstante, apesar de ainda estarmos na fase de definição dos elementos essenciais que a caracterizam, e de que não existe consenso sobre o que é a sociedade da informação, este conceito traz a ideia da "novidade civilizacional"[14] que estamos vivenciando com a constante inovação tecnológica[15].

---

[12] Há quem opine que não se pode falar em sociedade da informação, porque o que circula na internet não é essencialmente informação, mas comunicação. In: DRUMMOND, Victor. *Internet, Privacidade e Dados Pessoais*. Rio de Janeiro: Lumen Juris, 2003, pp. 1 e 2.

[13] NEVES, Artur Castro. *Como definir a sociedade da informação?* pp. 57 a 69. In: COELHO, José Dias. *Sociedade da Informação: o percurso português.* Portugal: Edições Sílabo, 2007, p. 58.

[14] *Idem*, p. 68.

[15] A título de exemplo, vemos, hoje, aplicações de celular onde se pode contratar produtos ou serviços sem haver qualquer interação direta entre o contratante e o contratado; órgãos do governo conversando com cidadãos por meio de *chatbots* em redes sociais; sistemas de monitoramento automatizados; e inúmeras informações passando pelo mundo de maneira quase instantânea.

De forma simplificada, podemos conceituar sociedade da informação como a representação de uma estrutura social baseada largamente na geração, processamento e disseminação de dados[16]. A centralidade não reside apenas nos conhecimentos, mas na geração de novos saberes e dispositivos de processamento/comunicação da informação, "em um ciclo de realimentação cumulativo entre a inovação e o seu uso"[17].

Nesta pesquisa, o conceito é importante para apontar a transição da sociedade pós-industrial, no que diz respeito à ampliação e amplificação da comunicação, cujos novos instrumentos "revolucionaram a mundividência comunicacional"[18].

Sob o ponto de visto sociológico,

> *a sociedade da informação leva ao paroxismo os fins da acumulação de capital e de exploração do trabalho da sociedade industrial capitalista mas, por outro lado, reconhece que aquela supera as antigas divisões de classe por via de uma nova determinação política em que o papel do Estado e os efeitos das políticas públicas são factores de produção social*[19].

A sociedade de informação tem dentre suas principais características a penetrabilidade das novas tecnologias nas atividades humanas (individuais e coletivas), o que nos leva a viver em uma lógica de redes, ou seja, em meio a relações complexas[20].

Duas mudanças fundamentais se mostram: de um lado, a ampliação da linguagem para incluir os códigos binários, próprio dos computadores; de outro, uma dependência crescente dos setores econômicos em relação à tecnologia, na produção e comercialização. A tecnologia é realidade em todas as áreas, ficando a ela exposta a sociedade com maior frequência, fazendo as antigas "regras do jogo" serem alteradas.

A sociedade de informação se vê formada, então, tanto pelas transformações sociais, econômicas e comerciais induzidas pelo aparecimento de uma rede mundial de computadores, como pela reorganização das relações capitalistas, industriais e laborais, nas novas indústrias de serviços[21].

---

[16] GUERRA, Sidney. *O direito à privacidade na internet: uma discussão da esfera privada no mundo globalizado*. Rio de Janeiro: América Jurídica, 2004, p. 1.
[17] CASTELLS, Manuel. *A Sociedade em rede*. São Paulo: Paz e Terra, 2000. v. 1, p. 69.
[18] PINHEIRO, Alexandre Sousa. *op. cit.,* p. 39.
[19] NEVES, Artur Castro. *op. cit.*, p. 57.
[20] CASTELLS, Manuel. *op. cit*., p. 108.
[21] NEVES, Artur Castro. *op. cit.*, p. 64.

Diante das relações complexas advindas desta nova dinâmica, os problemas também adquirem caráter multifacetário – podem ocorrer entre Estado e cidadão, cidadão e poder privado, e entre privados. Ou ainda entre Estados, entre empresas, entre grupos de pessoas... ao conectar tudo e todos, o alcance da informação (e os problemas que daí podem advir) é exponencialmente ampliado.

1.2. Dados pessoais - conceito

Os dados pessoais podem ser conceituados como quaisquer informações que identifiquem ou possam identificar uma pessoa. O conceito abrange os dados pelos quais é imediatamente possível identificar a pessoa, e as informações que em conjunto o permitam fazê-lo[22].

Alexandre Sousa Pinheiro afirma que o termo adveio do alemão *Datenschutz*, utilizado no início dos anos 1970, como meio de proteger os direitos individuais face aos avanços informáticos. Para ele, o termo é inadequado pela falta de clareza, tendo sido apenas a "palavra errada no momento certo"[23].

Apesar desta ressalva, é importante conhecer o conceito, especialmente pelas crescentes análises e publicações em torno do novo Regulamento Geral de Dados Pessoais, cujo artigo 4º define dados pessoais como:

> *informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*[24].

Do conceito se destacam quatro pontos, que são "pilares" para entender que tipo de informação deve ser considerada como dados pessoais: "qualquer informação", "relativa a", "identificada ou identificável", "pessoa singular".

---

[22] COMISSÃO EUROPÉIA. *O que são dados pessoais?* Acesso em 16/03/2019. In: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt.

[23] PINHEIRO, Alexandre Sousa. *op. cit.*, pp. 429 e 430.

[24] Artigo 4º/1 do RGPD, *op. cit.*

1.2.1. "Qualquer informação"

O primeiro pilar do conceito de dados pessoais denota sua amplitude, já que ele abrange dados independentemente de sua natureza ou do conteúdo da informação[25], podendo ser objetivos ou subjetivos, e se apresentar por diversos meios técnicos[26]. O RGPD determina, ainda, que a proteção de dados seja neutra em termos tecnológicos e independente das técnicas utilizadas[27] [28].

É, portanto, um conceito aberto e indeterminado, que permite maior flexibilidade na resposta jurídica a ser dada em diferentes circunstâncias[29], além de possibilitar à doutrina e jurisprudência "afinar" o conceito, de acordo com as inovações tecnológicas que venham a surgir. Entretanto, traz o risco de serem adotados entendimentos demasiadamente amplos ou, contrariamente, permitir "uma restrição indevida"[30] de seu alcance.

Diversos exemplos de dados pessoais podem ser citados: nome e sobrenome; documentos de identificação pessoal; endereço residencial; documentos e dados fiscais e patrimoniais, como conta bancária ou declaração de imposto de renda; imagens; dados familiares (filhos, agregado familiar); estado civil; voz do cliente que realiza operações pelo telefone; desenhos de pessoas, como caricaturas; dados geográficos como a localização de um telefone celular (telemóvel), endereços IP (protocolo internet) ou testemunhos de conexão (cookie), etiquetas de identificação por radiofrequência, entre outros[31].

---

[25] Não se requer que a informação seja verdadeira, até porque, por meio do RGPD, é possível pedir a retificação de dados.

[26] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. *Parecer 4/2007 do sobre o conceito de dados pessoais* (01248/07/PT, WP 136), pp. 26 e 27.
Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf, acesso em 30/11/2019.

[27] Considerando 15 do RGRP, *op. cit.*

[28] Ou seja, poderá ser considerado dado pessoal a informação em formato alfabético, numérico, gráfico, fotográfico ou acústico, em papel, armazenada na memória de um computador ou fita cassete. In: GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º, *op. cit.*, p. 8.

[29] *Idem*, p. 4.

[30] *Ibidem*, p. 5.

[31] Segundo o Considerando 30 do RGPD, *op. cit.*: "Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares".

1.2.2. "relativa a"

O segundo elemento esclarece, ainda no âmbito de um conceito ampliado, que há possibilidade de se incluir como dados pessoais informações que, à primeira vista, possam gerar dúvida se são referentes ou "relativas" à uma pessoa singular.

Um exemplo seria a informação sobre um objeto, como o valor de uma casa, que aparentemente não diz respeito a uma pessoa, mas que, em alguns casos, pode determinar a capacidade financeira ou a obrigação do titular de pagar determinados impostos[32].

Ou seja, o termo "relativa a" evoca a análise das circunstâncias do caso concreto, onde a finalidade e o resultado do uso dos dados determinam se ele é ou não pessoal, sendo "suficiente que a pessoa possa ser tratada de forma diferente de outras pessoas como resultado do tratamento desses dados"[33].

1.2.3. "identificada ou identificável"

O terceiro elemento levanta a discussão sobre a identificabilidade imediata ou necessidade de trabalhos adicionais para que se distinga o titular. Como exemplo, o nome completo é dado diretamente identificável, enquanto o número de identidade requer trabalho adicional – consulta de base de dados com nome e identidade - para se constatar quem é aquela pessoa específica.

Deve-se verificar se o responsável "tem ou terá os meios 'susceptíveis de serem razoavelmente utilizados' para identificar a pessoa em causa"[34].

Neste âmbito, falamos de métodos de anonimização, como a utilização de números, pseudônimos ou dados codificados com chave, em que a informação é trabalhada por meio de um código, enquanto a chave ou matriz estabelece a correspondência entre o código e os identificadores pessoais, sendo mantida em separado[35].

O crucial é distinguir se mediante a utilização de informações suplementares poder-se-á novamente voltar a identificar a pessoa singular. Se for possível, os dados ainda são considerados pessoais. Devem-se considerar os meios suscetíveis de serem razoavelmente

[32] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º, *op. cit.*, p. 10.
[33] *Idem*, p. 11.
[34] *Ibidem*, pp. 16 e 17.
[35] *Ibidem*, p. 19.

utilizados, levando em conta os custos e o tempo necessário para a identificação, a partir das tecnologias disponíveis[36]. Logo, "para que os dados sejam verdadeiramente anonimizados, a anonimização tem de ser irreversível"[37].

1.2.4. "pessoa singular"

O quarto e último elemento diz respeito ao titular. Como a proteção de dados pessoais é considerada um direito humano, o RGPD é aplicável independentemente da nacionalidade ou local de residência[38].

Se exclui a proteção a pessoas coletivas[39] [40], a não ser quando tiverem direta conexão com dados de pessoas singulares, como no caso de uma empresa ter seu nome derivado de um nome próprio[41], ou correios eletrônicos com dados personalizados, como (nome.sobrenome@empresa.com.br)[42].

A proteção dos dados pessoais das pessoas falecidas e dos nascituros[43] foi deixada a critério dos Estados-Membros, seguindo o entendimento de suas legislações internas[44].

Visto o que são dados pessoais, passaremos ao porquê da importância de se protegê-los.

---

[36] Considerando 26 do RGPD, *op. cit.*

[37] In: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt, acesso em 30/11/2019.

[38] Considerando 14 do RGPD, *op. cit.*

[39] "Incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva". In: Considerando 14 do RGPD, *op. cit*.

[40] Apesar de alguns direitos de personalidade já serem reconhecidos a pessoas coletivas, a interpretação do TJUE a respeito do artigo 8º/1 da Carta dos Direitos Fundamentais da União Europeia foi no sentido de restringir às pessoas singulares o direito à proteção de seus dados pessoais. Ressalta-se que alguns Estados-Membros, antes da entrada em vigor do RGPD, possuíam disposições em seus direitos nacionais em relação ao tratamento de dados pessoais de pessoas jurídicas, o que tem gerado discussões a respeito de sua manutenção. Ver mais sobre esta discussão em: CORDEIRO, Antônio Barreto Menezes. *O RGPD e a não proteção de pessoas coletivas.* In: *Vida Judiciária*, maio/junho de 2018, pp. 4 e 5. Também indicamos a leitura do Acórdão do Tribunal de Justiça (Grande Secção) de 9 de novembro de 2010, Volker und Markus Schecke GbR (C-92/09) e Hartmut Eifert (C-93/09) contra Land Hessen.

[41] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º, *op. cit.*, p. 25.

[42] Outros dados, como o número de registro da empresa ou e-mail genérico (informação@empresa.com), não se constituem como dados pessoais.

[43]Independentemente da legislação nacional, poderá haver proteção indireta, quando puderem personificar ou identificar pessoa viva, como no caso de doenças genéticas. Vale também lembrar que a confidencialidade médica não termina com a morte do paciente.

[44] Considerando 27 do RGPD, *op. cit.*

1.3. Necessidade de proteção aos dados pessoais

A crescente preocupação na proteção de dados pessoais se deve à rápida difusão de tecnologias que envolvem riscos de intrusão na esfera íntima. Não que seja diferente a recolha de dados por meios digitais ou manuais, mas o tratamento informático amplia a facilidade, volume, velocidade e preocupação com a fidedignidade das informações recolhidas[45].

Analisaremos dois fatores importantes: a segurança informacional, que abrange riscos de coleta, uso, armazenamento e compartilhamento de dados (1.3.1); e o conceito de autodeterminação e jusfundamentalidade da proteção de dados pessoais (1.3.2).

1.3.1. Os riscos da coleta, uso e armazenamento de dados pessoais

Os dados pessoais são aqueles que compõem o núcleo íntimo e diferenciam os indivíduos, tornando seu uso um ativo notável para empresas e autoridades públicas, já que, ao conhecer o perfil de consumidores, contratantes, infratores ou usuários de serviços públicos, é possível desenvolver atividades de forma mais eficiente.

No que tange ao Estado, o tratamento de dados permite prestar serviços mais rápidos, de forma mais precisa e eficiente, como no uso da inteligência artificial para prever acidentes ou ampliar a produção agrícola[46]. Especialmente em relação à segurança, nota-se o crescente uso de tecnologias de reconhecimento facial e controle de movimentos financeiros e transfronteiriços, com base no princípio da prevenção e/ou da precaução[47].

Para as empresas privadas, os dados pessoais podem ser usados na oferta de produtos e serviços, e na determinação de perfis para decidir questões como empréstimos bancários, seguros ou contratação de funcionários.

Até o ano de 2020, estima-se que o valor econômico dos dados dobrará, alcançando a cifra de 739 mil milhões de euros, o que corresponde a 4% do PIB total da União

[45] PINHEIRO, Alexandre Sousa. *op. cit.*, p. 529.
[46] COMISSÃO EUROPEIA: *Um Mercado Único Digital conectado para todos.* Acesso em 8/6/2019. In: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017DC0228&from=PT.
[47] PINHEIRO, Alexandre Sousa. *op. cit.*, p. 126.

Europeia[48]. Estima-se também que o número de profissionais no setor passará de 6 milhões em 2016, para mais de 10 milhões até 2020[49].

Não é difícil coletar dados. A inovação digital e o crescimento das tecnologias de comunicação geram uma exposição crescente de informação pessoais, tanto de forma voluntária (redes sociais), como involuntária (leis e regulamentos).

Coletam-se dados diversos: interações em redes sociais; gostos, interesses, fotografias, opiniões; indicadores de capacidade econômica, como viagens e locais frequentados; dados de videovigilância[50]; consumo de energia e água; dados médicos transmitidos por aparelhos[51]; preferências e padrões de compra (uso de cookies[52]); entre tantos outros.

Podemos dizer que os dados pessoais têm um valor intrínseco (que estudaremos no tópico a seguir), e um valor econômico, que pode ser obtido tanto pelo uso do dado em si, como por sua combinação e tratamento. São usados programas que vão "conhecendo" a pessoa e criando seu perfil para antecipar gostos, como músicas, produtos, serviços e lugares a frequentar. Seria a "robotização associada à inteligência artificial para controlo do comportamento humano"[53].

Os algoritmos ampliam a capacidade de uso dos dados pessoais, fazendo com que as empresas tenham maior eficiência na conversão da compra de produtos e serviços que oferecem, o que acaba criando um círculo virtuoso/vicioso, em que "quem tiver mais clientes – acumula mais dados – obtém os melhores modelos algoritmos – e conquista o maior número de novos clientes"[54].

---

[48] COMISSÃO EUROPEIA: *Um Mercado Único Digital conectado para todos*, o*p. cit.*

[49] *Idem.*

[50]Por exemplo, câmeras de prédios públicos, pagamentos de pedágios/portagens, estacionamentos/parques, redes de Wi-Fi e etc.

[51] CALVÃO, Filipa Urbano, *op. cit.*, p. 15.

[52] A tecnologia de cookies envia dados das páginas navegadas na Internet diretamente para o navegador, registrando dados como carrinhos de compras, cliques e identificação pessoal, especialmente em redes sociais. A tecnologia é tão intrusiva que, além de coletar dados a partir do site que a pessoa está visitando, muitas vezes, ainda coleta dados para terceiros (*third party cookies*). Em: MEIRELES, Adriana Veloso. *Autonomia e privacidade no ambiente digital.* In: Revista Eletrônica de Ciência Política. nº 7, 2016, p. 15.

[53] CALVÃO, Filipa Urbano. o*p. cit.,* p. 14.

[54] DOMINGOS, Pedro. *O Algoritmo Mestre: Como a Busca Pelo Algoritmo de Machine Learning Definitivo Recriará Nosso Mundo*. São Paulo: Novatec, 2017, p. 36.

Explicando melhor, os dados coletados alimentam o mercado publicitário que, a partir do acesso aos dados pessoais, constrói perfis e segmentos que posteriormente são vendidos de acordo com o que a empresa busca. As preferências permitem que os anúncios sejam específicos, com base nos dados coletados[55].

Dois são os problemas em relação a este círculo virtuoso/vicioso: de um lado, o possível monopólio de grandes empresas digitais[56]; de outro, a chamada "discriminação algorítmica"[57] (em função do sexo, idade, religião, orientação sexual, etc.), que poderia restringir acesso a determinados setores, como o crédito bancário, por exemplo[58].

É certo que a recolha de dados pode ser uma troca entre empresas e seus clientes, como entre um *website* e seus utilizadores. Quem faz uma busca no Google sabe que alguns resultados serão anúncios pagos, e que as buscas serão gravadas. Ao usar o sistema, o usuário decide se vale a troca dos seus dados pela infraestrutura de pesquisa que utiliza[59].

A questão que se coloca é: quais dados as empresas coletam, a quem repassam e com qual finalidade? Não há empecilho em se comercializar alguns dados, mas isto deve ser feito "de forma livre e esclarecida"[60], e dentro dos padrões legais e éticos.

Um exemplo interessante sobre a finalidade da coleta de dados aconteceu no Brasil no ano de 2013. O Tribunal Superior Eleitoral (TSE) decidiu repassar informações cadastrais de 141 milhões de brasileiros para a Serasa, empresa privada que gerencia a situação de crédito dos consumidores. No Brasil, o cadastramento eleitoral é obrigatório, assim como o voto[61], cuja ausência acarreta multa e restrições de direitos[62].

---

[55] MEIRELES, Adriana Veloso. o*p. cit.,* p. 16.
[56] DOMINGOS, Pedro. o*p. cit*.
[57] Apesar de o RGPD prever a não sujeição a decisões tomadas exclusivamente com base no tratamento automatizado de dados (art. 22.º), o que inclui a definição de perfis, estamos diante de questões muito sutis e de difícil comprovação, ou até mesmo percepção por parte do titular.
[58] SILVEIRA, Alessandra e FROUFE, Pedro. *From the Internal Market to the citizenship of rights: the protection of personal data as the jus-fundamental identity question of our times.* In: UNIO - EU Law Journal, vol. 4, nº 2, julho de 2018, p. 10.
[59] *Idem*, p. 11.
[60] *Ibidem*.
[61] "São eleitores os brasileiros maiores de 18 anos que se alistarem na forma da lei". In: BRASIL. Código Eleitoral - Lei nº 4.737, de 15 de julho de 1965, artigo 4º.
[62] As sanções estão previstas no Código Eleitoral Brasileiro *op. cit.*, artigo 7º. Atentamos para o fato de que existem diferentes decisões judiciais e leis especiais que, de alguma forma, alteram o artigo.

O acordo de cooperação técnica[63], por meio do qual seriam compartilhados os nomes dos eleitores, número e situação da inscrição eleitoral, óbitos, nome da mãe e data de nascimento, ainda permitia à Serasa retransmiti-los a seus clientes – bancos, lojas, empresas financeiras, entre outros. Assim, poder-se-ia conhecer a situação do devedor, identificando-o corretamente (caso de duas ou mais pessoas que tenham o mesmo nome, por exemplo) e facilitando as ações de cobrança, além de evitar fraudes na realização de negócios ou na concessão de créditos em nome de pessoas já falecidas.

A contrapartida pela cessão dos dados era o fornecimento, aos servidores do tribunal, de uma "certificação digital" (assinatura eletrônica para documentos oficiais), o que facilitaria a tramitação de processos eletrônicos[64].

Mesmo diante da ausência de legislação específica, o acordo foi bastante criticado pela invasão de privacidade e não respeito aos direitos da personalidade, tendo a academia se posicionado pela necessidade de "consentimento expresso" dos eleitores para que o TSE pudesse repassar dados a uma entidade privada[65].

Ao final, o Supremo Tribunal Federal cancelou o acordo, com base no direito à privacidade[66]. Segundo a Ministra Carmem Lúcia, presidente do STF naquela altura:

> *não seria imaginável como possível que entidades particulares, com finalidades privadas, pudessem ou pretendessem ser autorizadas, legitimamente, pela Justiça Eleitoral a acessar os dados cadastrais, que os cidadãos brasileiros entregam aos órgãos do Judiciário com a certeza da confiança de manutenção do seu sigilo e de sua utilização restrita aos fins daqueles órgãos[67].*

Vemos, então, que a "finalidade" da coleta de dados é importante quando falamos de sua proteção na sociedade da informação.

---

[63] Acordo publicado em 23 de julho de 2013, no Diário Oficial da União.

[64] Apenas a título de curiosidade, a contrapartida oferecida pela Serasa ao TSE era de 1000 certificados digitais (segundo informação contida na notícia http://g1.globo.com/politica/noticia/2013/08/tse-firma-acordo-para-repassar-dados-de-eleitores-serasa.html), o que nos dias de hoje – 06/05/2019 – equivaleria a algo como 90 mil euros, por uma base cadastral de 140 milhões de pessoas.

[65] In:https://politica.estadao.com.br/noticias/geral,justica-eleitoral-repassa-dados-de-141-milhoes-de-brasileiros-para-a-serasa,1061255. Acesso em 30/09/2019.

[66] In: https://exame.abril.com.br/tecnologia/tse-anula-repasse-dos-dados-de-eleitores-a-serasa/. Acesso em 30/09/2019.

[67] In:www.valor.com.br/politica/3228492/tse-anula-acordo-com-serasa-para-fornecer-dados-de-eleitores. Acesso em 30/11/2019.

Outro exemplo é o da empresa *Cambridge Analytica*, que foi acusada de utilizar dados coletados por meio de um teste de personalidade no *Facebook* para auxiliar candidatos em processos eleitorais a se comunicar de forma estratégica[68], tanto nas eleições americanas de 2016, como no referendo sobre a saída da Grã-Bretanha da União Europeia[69]. Acontece que o usuário, ao consentir a participar do jogo, só foi informado sobre o uso de seus dados para estudos acadêmicos e científicos. Assim, se houve ou não dano, o fato é que a mera suspeita de influência já afeta a confiança e abala a democracia.

Outra questão é a do "vazamento", ou acesso não autorizado à base de dados, mesmo em grandes empresas do setor de informação, que possuem mecanismos de segurança modernos. A título de exemplo, em outubro de 2018, a Google encerrou o "Google+", sua mídia social e serviço de identidade criada em 2011, após uma falha de *software* que concedeu aos desenvolvedores acesso a nome, *e-mail*, profissão, gênero e idade o usuário de até 500.000 contas.

Os "vazamentos" e usos não consentidos de dados ocasiona uma situação de "falta de confiança" entre as partes contratantes[70], o que o RGPD tentou remediar ao proibir a recolha sem o consentimento do titular ou outra autorização legal, e seu tratamento para fins diversos do consentido/permitido, como fins políticos, militares ou ideológicos, o que pode comprometer a democracia e o livre exercício da cidadania[71].

1.3.2. Liberdade e autonomia

A autodeterminação e a liberdade são condições da democracia e do Estado Democrático de Direito. Por esta razão, deve-se encontrar resposta aos riscos e desafios

---

[68] Até a presente data, os fatos continuam sob investigação, mas o CEO do Facebook compareceu perante o Congresso americano assumindo a responsabilidade pelo "vazamento" dos dados. In:https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em 30/11/2019.

[69] Em 2018, importantes jornais de notícias, como o "The London Observer" e o "The New York Times" publicaram reportagens alegando que a empresa usou dados de 87 milhões de perfis para criar um programa a partir de preferências obtidas pela mineração de dados, sem consentimento. In:https://tek.sapo.pt/noticias/internet/artigos/as-perguntas-e-respostas-mais-importantes-sobre-o-caso-cambridge-analyticafacebook. Acesso em 30/11/2019.

[70] Por exemplo, se existe recolha de dados de um consumidor quando efetua uma compra *online*, para aprender seus gostos, é devido a ele o conhecimento deste processo, para que possa escolher utilizar outro serviço caso não concorde com seus termos.

[71] BAKSHY, Eytan; MESSING, Solomon; ADAMIC, Lada A. *Exposure to ideologically diverse news and opinion on Facebook*. In: Science, volume 348, nº 6239, 2015, pp. 1130-1132.

dos múltiplos tratamentos de dados[72], que podem afetar a capacidade dos indivíduos de guiar sua vida de acordo com suas escolhas, e de como quer ser conhecido pela sociedade.

Uma pessoa autônoma seria a que define seu comportamento e assume as responsabilidades de suas escolhas com base em seus próprios critérios, ou naqueles assumidos de forma consciente e voluntária, mesmo diante da complexidade das relações na sociedade da informação.

Essa complexidade, todavia, faz com que o exercício da autonomia deva ser analisado também a partir de como se formam suas preferências, por meio de quais influências e relações de poder/hierarquia, já que as escolhas são resultantes da relação entre preferências pessoais e o contexto em que ocorrem[73].

A autonomia privada é essencial para o desenvolvimento do Estado Democrático de Direito, já que dela depende a atuação pública dos cidadãos (cidadania). Dignidade, igualdade e liberdade são fatores essenciais para "a construção do indivíduo consciente e autônomo" [74], pré-requisito para o exercício da autonomia pública.

Preservar a autodeterminação permite viabilizar "as capacidades dos indivíduos para formar, manter e apresentar aos outros uma auto concepção coerente, autêntica e distinta"[75]. Para tanto, requer-se a proteção de "precondições constitutivas mínimas para que se tenha uma identidade própria"[76], o que passa tanto pela noção de "ser deixado em paz" como pela "inviolabilidade da personalidade e um sentimento de controle sobre as necessidades da própria identidade"[77].

Como parte do núcleo humano que diferencia os indivíduos, os dados pessoais são meios de se garantir a autonomia pessoal, o que se mostra extremamente relevante nos dias atuais, em que informações sobre a identidade das pessoas, sua residência, estado de saúde, orientações sexuais, religiosas e políticas estão passíveis de serem conhecidas e cruzadas com outras informações - próprias e de seus contatos – para a criação de

[72] CALVÃO, Filipa Urbano. o*p. cit.*, p. 21.
[73] MEIRELES, Adriana Veloso, *op. cit.*, pp. 9 e 10.
[74] HABERMAS, Jurgen. *Direito e Democracia: entre facticidade e validade*. Rio de Janeiro: Tempo Brasileiro, 1997, pp. 113-116.
[75] COHEN, Jean. *Repensando a privacidade: autonomia, identidade e a controvérsia sobre o aborto*. Revista Brasileira de Ciência Política, nº 7, 2012, p. 188.
[76] *Idem*.
[77] *Ibidem.*

"perfis"[78] ou "uma personalidade para os seus titulares"[79], com grande potencial discriminatório.

Vários são os riscos deste processo, como o a "numeralização" da personalidade e seu comércio[80]; a restrição de direitos fundamentais[81], a exemplo do direcionamento das pesquisas a partir do histórico de navegação (direito à informação); uso de dados de compras para estimativa de pagamento de imposto, etc.; a manipulação da identidade e da autonomia, com influência indevida em decisões pessoais[82]; e a "perpetuação da informação disponível na internet"[83], que faz com que a capacidade de refazer escolhas e recriar a personalidade seja muito limitada.

Consequentemente, seja por meio de danos diretamente causados ao titular pela exposição ou utilização não consentida de seus dados, ou por meio da coleta e cruzamento de dados que permitem criar tais perfis, a proteção dos dados pessoais visa assegurar um valor intrínseco da personalidade, que é a vida privada do indivíduo[84].

Pode-se falar de um *forum internum*[85] a ser protegido, cujo referencial é o princípio da dignidade, que impõe o tratamento da pessoa como uma "personalidade insubstituível", sendo o respeito de sua esfera privada um "pressuposto fundamental da existência"[86]. A transformação do indivíduo em objeto, pelo uso e transmissão indiscriminada de dados, viola a esfera digna de seu ser e, por consequência, a base do Estado Democrático de Direito (que é a dignidade).

Desta forma, Alexandre Sousa Pinheiro, sugere que o termo "proteção de dados pessoais" está superado, pois o que se quer promover é a "autodeterminação informacional"[87], examinando o tratamento quanto à "adequação" e "pertinência", e não

---

[78] CALVÃO, Filipa Urbano. *op. cit.*, p. 14. A professora cita exemplos de perfis como "provável ou potencial criminoso", "potencial evadido fiscal", "perfil de consumidor de bens do tipo x e Y", "potencial atleta de competição" e "condutor perigoso".
[79] DRUMMOND, Victor. *op. cit*., p. 36.
[80] *Idem*, p. 37.
[81] Explicando melhor, a atual dinâmica social está estruturada no uso de informações do cidadão para classificá-lo, categorizá-lo (*social sorting*), e decidir se ele terá acesso a vantagens, como um benefício de assistência social, bens de consumo e até acesso ao mercado de trabalho.
[82] CALVÃO, Filipa Urbano. *op. cit.*, p. 15.
[83] *Idem,* p. 17.
[84] DRUMMOND, Victor. *op. cit.*, p. 32.
[85] PINHEIRO, Alexandre Sousa. *op. cit.*, p. 797.
[86] *Idem,* p. 799.
[87] *Ibidem,* p. 805.

apenas pela fórmula casuística "dado-finalidade"[88]. Se garantiria a identidade, o livre exercício da personalidade, a proteção de dados, e a necessidade de intervenção pública para que haja um exercício seguro e isento das comunicações eletrônicas, em um ambiente que prima pela confiança e permite aos indivíduos explorar todos os recursos da sociedade da informação[89].

1.4. Da privacidade à proteção de dados pessoais

A proteção de dados pessoais, no âmbito europeu, percorreu um longo caminho até a entrada em vigor do RGPD. Uma lei não nasce do acaso. Ela nasce de um conjunto de fatores sociais, políticos, históricos e econômicos. Por isso, iremos, neste tópico, contextualizar e jogar luz em fatos, normas e decisões que a antecederam, começando pela autonomização da proteção de dados pessoais (1.4.1), e passando pelo seu enquadramento dentro da tutela geral da personalidade (1.4.2), e reconhecimento como direito fundamental autônomo (1.4.3)[90].

1.4.1. Autonomia da proteção de dados pessoais

Vários doutrinadores trazem como uma das possíveis origens da proteção de dados pessoais o conceito de *privacy*, introduzido nos EUA em 1890, pelo artigo "The right to privacy" de Samuel Warren e Louis Brandeis, onde se buscou solucionar o problema da intrusão de tecnologias, como a máquina fotográfica, na esfera privada dos indivíduos, sob o fundamento do *right to be left alone*[91].

A publicação do citado artigo daria origem a "moderna doutrina do direito à privacidade"[92], que evoluiu do "individualismo exacerbado"[93], cujo paradigma seria "a ausência de comunicação entre um sujeito e os demais", até chegar a versão mais temperada de "que a privacidade é um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade"[94].

---

[88] *Ibidem,* pp. 810 e 811.
[89] *Ibidem,* pp. 818 e 819.
[90] Como salientamos na introdução, não buscaremos ser exaustivos na reconstrução histórica, mas apenas demonstrar a diferença da origem da lei europeia e da brasileira.
[91] WARREN, Samuel e BRANDEIS, Louis. *The right to privacy*, pp. 193-220. In: Harvard Law Review, Vol. 4, Nº 5, dezembro de 1890, p. 196.
[92] DONEDA, Danilo, *op. cit.,* p. 91.
[93] *Idem.*
[94] *Ibidem.*

A semelhança dos conceitos de *privacy* e proteção de dados pessoais provoca discussão acadêmica considerável[95], tendo os que acreditam que há conexão ou equivalência[96], e outros que entendem que não se fundem dogmaticamente[97].

A primeira linha argumenta que, em razão da evolução tecnológica, o conceito de *privacy "*hoje compreende algo muito mais complexo do que o isolamento ou a tranquilidade"[98], podendo ser definido como uma reinvindicação (individual, de grupos ou instituições) para determinar, por si mesmo, quando, como e em qual extensão suas informações pessoais são comunicadas com os outros[99].

O conceito de *privacy* abrangeria, pois, quatro categorias: privacidade da pessoa; privacidade de comportamento; privacidade de dados; privacidade de comunicação. Ou seja, *privacy* não se equivaleria a proteção de dados, mas a abrangeria, pois diferentes tipos de "privacidade", requerem diferentes tipos de proteção. Logo, haveria pressupostos ontológicos idênticos ou semelhantes entre a proteção da privacidade e de dados pessoais, que seria sua "continuação por outros meios"[100].

A segunda linha vê o nascimento da proteção de dados pessoais a partir de precedentes jurisprudenciais e legais franceses, que reconheceram a pessoa como titular de um acervo de direitos, cujos danos sofridos se manifestariam na esfera imaterial da personalidade[101].

---

[95] A confusão é gerada por suas raízes em comum, pela dificuldade terminológica e de tradução, e pela "sobreposição" de conceitos e termos em textos acadêmicos, propostas legislativas e estudos governamentais.

[96] Ver, entre outros: GONZALES FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Suíça: Springer International Publishing, capítulo 5; GALLERT, Raphael e GUTWIRTH, Serge. *The Legal Construction of Privacy and Data Protection*. In: Computer Law and Security Review 522, 2013; KOKOTT, Juliane e SOBOTTA, Christoph. *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*. In: International Data Privacy Law, 2013, Vol. 3, Nº. 4.

[97]Destacamos, neste sentido, o professor Alexandre Sousa Pinheiro, que dedicou sua tese de doutoramento ao tema. In: PINHEIRO, Alexandre Sousa. o*p. cit.,* p. 39 e 267. Esclarece, contudo, que ambas têm origem nos direitos de personalidade.

[98] DONEDA, Danilo. *op. cit.*, p. 91.

[99] WESTIN, Alan F. *Privacy and Freedom*. New York: Athenum. 1967, p. 7. Do original: "…claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".

[100] DONEDA, Danilo. *op. cit.*, p. 91

[101] PINHEIRO, Alexandre Sousa. *op. cit.*, p. 432.

No direito francês, usa-se o conceito de "droit à la vie privée", previsto no artigo 9.1 do código civil: "todos tem o direito a ter sua vida privada respeitada"[102]. A partir da introdução do citado artigo pela reforma de 1970, o Conselho Constitucional francês definiu diferentes teses relacionadas com a privacidade e proteção de dados, como o sigilo de informações de saúde e a defesa da intimidade no tocante às relações e preferências sexuais[103].

Há quem argumente, neste sentido, que a proteção de dados é um dos ramos do caleidoscópio jurídico que é o "droit à la vie privée", sendo "desdobramentos" da privacidade: 1) o direito a ser deixado só (*privacy*); 2) o resguardo contra interferências alheias; 3) o segredo ou sigilo; e 4) o controle sobre informações e dados pessoais[104].

Um estudo realizado pela análise de decisões da Corte Europeia de Direitos Humanos e do Tribunal de Justiça da União Europeia entendeu que *privacy* e proteção de dados são termos interligados, mas não idênticos. Apesar das sobreposições entre os regimes, os autores sugerem que o que deveria ser questionado é se há maior salvaguarda de direitos fundamentais pela autonomização da proteção de dados[105].

Enquanto não se tem essa resposta, é válido destacar que a Carta de Direitos Fundamentais da UE dissociou a proteção de dados pessoais (artigo 8º) do respeito pela vida privada e familiar (artigo 7º)[106]. Uma recente publicação do Parlamento Europeu colocou entre os principais instrumentos legislativos em matéria de proteção de dados os supracitados artigos, dizendo que trazem direitos fundamentais estreitamente relacionados, mas distintos[107].

---

[102]Tradução livre. Do original : « Chacun a droit au respect de sa vie privée. » In: FRANÇA. *Code civil*, versão consolidada de 21 de julho de 2019.

[103] Não se trata de proteção absoluta, pois existem exceções, como no caso da imagem de pessoas públicas, ou da possibilidade de cumprir mandados judiciais em residências. Acesso em 30/06/2019. In:https://www.vie-publique.fr/decouverte-institutions/citoyen/citoyennete/definition/droits/chaque-citoyen-t-il-droit-au-respect-vie-privee.html.

[104] LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012. pp. 52-76.

[105] KOKOTT, Juliane e SOBOTTA, Christoph, *op. cit*. pp. 222 e 228.

[106] KULHARI, Shraddha. *Building-Blocks of a Data Protection Revolution: the uneasy case for blockchain technology to secure privacy and identity*. Alemanha: Nomos Verlagsgesellschaft mbH, 2018, p.24. In: https://www.jstor.org/stable/j.ctv941qz6.7. Acesso em 30/06/2019.

[107] MILT, Kristiina. *Proteção dos dados pessoais: Fichas técnicas sobre a União Europeia,* 2019, p.1. Acesso em 15/05/2019, in:http://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais.

A partir do reconhecimento da jusfundamentalidade da proteção de dados, Filipa Calvão defende sua "emancipação" científica, por apresentar características de direito público (consagração como direitos fundamentais e estrutura administrativa, como as autoridades de controle), de direito civil (v.g., a subcontratação), de direito internacional (transferência de dados) e de direito criminal (tipificação de certas violações de dados como ilícitos)[108].

Seguindo esta linha, neste trabalho, trataremos a proteção de dados como ramo emancipado para fins acadêmicos[109]. Entretanto, entendemos que a autonomização do conceito não põe fim às discussões, especialmente por acreditarmos que se deva desenvolver proteção mais ampla, como a proposta de "identidade informacional" exposta no tópico anterior[110].

1.4.2. Direitos de Personalidade e proteção de dados pessoais

Apesar da controvérsia terminológica, é certo que a proteção de dados pessoais tem em comum com a privacidade sua raiz nos direitos de personalidade[111]. A própria abrangência do conceito de privacidade (que inclui, dentre outros, a intimidade, a vida privada, a proteção da honra e das opções e preferências sexuais) advém da complexidade humana e sua personalidade multifacetária.

Já no texto de Warren e Brandeis, de 1890, se sugeriu que a apropriação de escritos/produções pessoais não se baseia unicamente na propriedade privada, mas no princípio da "personalidade inviolável"[112].

A categoria dos direitos da personalidade é construção recente, fruto de elaborações doutrinárias germânicas e francesas da segunda metade do século XIX[113], e de regulamentações do século XX, como o código civil italiano de 1942 e o português de 1966. Foram impulsionadas por mudanças sociais que passaram a trazer para o direito civil

[108] CALVÃO, Filipa. o*p. cit.,* pp. 32 e 33.
[109] O RGPD e a LGPD não mencionam ou fazem referência ao conceito de *privacy*. Contudo, a lei brasileira menciona a privacidade em vários artigos, mas nunca os utiliza como sinônimos. Pela leitura da lei, pode-se argumentar que a proteção de dados tem uma simbiose com a privacidade, mas não confusão terminológica.
[110] Proposta de PINHEIRO, Alexandre Sousa, *op. cit.*
[111] PINHEIRO, Alexandre Sousa, *op. cit*., p. 39.
[112] WARREN, Samuel e BRANDEIS, Louis, *op. cit.*, p. 196.
[113] TEPEDINO, Gustavo. *A tutela da personalidade no ordenamento civil-constitucional brasileiro*. In: TEPEDINO, Gustavo*. Temas de Direito Civil*. Rio de Janeiro: Renovar, 1999, p. 23.

questões anteriormente resolvidas em outras instâncias, como no âmbito familiar ou religioso[114].

A partir de então, os atributos do direito de propriedade e da personalidade começaram a se distanciar[115], já que as soluções antigas (baseadas na propriedade) não eram suficientes para lidar com a complexidade das relações humanas, e com a desigualdade cada vez mais latente. Uma renovação conceitual se fez necessária, e um de seus resultados é a tutela da personalidade[116].

Os direitos de personalidade são aqueles atrelados à pessoa em si mesma e suas projeções na sociedade[117], que constituem as "condições essenciais ao seu ser e devir"[118]. São "indispensáveis ao desenrolar saudável e pleno das virtudes psicofísicas que ornamentam a pessoa"[119], que resguardam a dignidade humana[120].

O desenvolvimento da personalidade parte de dois pressupostos: o primeiro, de que as pessoas são seres em formação; o segundo, da autodeterminação, no sentido de liberdade para buscar sua realização dentro do pluralismo cultural e de valores[121]. Não se trata, porém, de liberalismo exacerbado, já que estes direitos têm como limite e guia a própria dignidade humana[122].

Assevera-se que "perduraram, todavia, por muito tempo, hesitações da doutrina quanto à existência conceitual da categoria, expandindo-se dúvidas no que tange à sua natureza e conteúdo, bem como no que concerne à extensão da disciplina aplicável"[123].

No Brasil, foram inseridos no Código Civil apenas na reforma de 2002, em capítulo específico da parte geral (artigos 11 - 21)[124], mas já estavam presentes no artigo 5º da

---

[114] DONEDA, Danilo. *Os direitos da personalidade no código civil*, pp. 71 – 79. In: Revista da Faculdade de Direito de Campos, Ano VI, nº 6, junho de 2005, p. 75.
[115] BEVERLEY-SMITH, Huw; OHLY, Ansgar e LUCAS-SCHLOETTER. *Privacy, property and personality: civil law perspectives on commercial appropriation.* Cambridge: Cambridge University Press, 2005, p. 52.
[116] DONEDA, Danilo. *Os direitos da personalidade no código civil*, *op. cit.,* p. 75.
[117] BITTAR, Carlos Alberto. *Os direitos da personalidade*. São Paulo: Saraiva, 2015, capítulo I.
[118] DRUMMOND, Victor. *op. cit.*, pp. 15 e 16.
[119] JABUR, Gilberto Haddad. *Liberdade de pensamento e direito à vida privada.* São Paulo: Revista dos Tribunais, 2000, p. 28.
[120] VENOSA, Silvio de Salvo. *Direito Civil: parte geral,* vol. 1, 4ª ed. São Paulo: Atlas, 2004, p. 151.
[121] GODINHO, Adriano Marteleto. *Pessoa, personalidade e direitos da personalidade*, pp. 9-40. In: *PHRONESIS*: Revista do Curso de Direito da FEAD, nº 5, 2009, p. 19.
[122] *Idem,* p. 11.
[123] TEPEDINO, Gustavo. *op. cit.*
[124] Artigos 11 a 21. In: BRASIL. *Código Civil*, Lei 10.406, de 10 de janeiro de 2002.

Constituição de 1988, que garante a inviolabilidade da intimidade, vida privada, honra e imagem[125]. São considerados como direitos intransmissíveis e irrenunciáveis, não podendo sofrer limitação voluntária[126].

Na Constituição portuguesa, foram reconhecidos os direitos "à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação"[127].

O Tribunal Constitucional português afirmou que assiste aos direitos da personalidade o maior grau de proteção do ordenamento jurídico, uma vez que a República Portuguesa se baseia na dignidade da pessoa humana, de modo a que os direitos a ela inerentes não podem ser postergados de nenhum modo. É, portanto, a pessoa, o valor central da sociedade[128].

O artigo 70 do Código português traz a tutela geral da personalidade:

> *1. A lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral.*
>
> *2. Independentemente da responsabilidade civil a que haja lugar, a pessoa ameaçada ou ofendida pode requerer as providências adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida[129].*

Se entende que este artigo clarifica a personalidade como objeto de direitos e deveres, cujo elemento qualificador é dado pela centralidade da pessoa e por sua capacidade jurídica de titularizar esses direitos e obrigações em concreto[130]. Assim, tais direitos são oponíveis à coletividade e ao Estado.

Vale lembrar que, apesar de se basearem na dignidade, os direitos de personalidade apresentam características de liberdade reconhecidas ao beneficiário, o que implica (ao

---

[125] BRASIL. *Constituição da República Federativa do Brasil*, de 5 de outubro de 1988.
[126] BRASIL. *Código Civil*, *op. cit*.
[127] PORTUGAL/ASSEMBLEIA CONSTITUINTE. *Constituição da República Portuguesa de 1976,* VII Revisão Constitucional, artigo 26.
[128] Tribunal Constitucional Português, Acórdão nº 6/84 de 18 de janeiro.
In: https://www.tribunalconstitucional.pt/tc/acordaos/19840006.html, acesso em 19/11/2019.
[129] PORTUGAL. *Código Civil*, DL n.º 47344/66, de 25 de novembro.
[130] SOUSA, Rabindranath Capelo. *O Direito Geral de Personalidade*. Coimbra: Coimbra Editora, 1995, p. 106.

menos parcialmente) em disponibilidade[131]. Deve-se partir da noção de autonomia, que confere poder de auto-regulamentação dos interesses privados. A regra é a impossibilidade de limitação voluntária, mas exceções são concedidas para preservar o livre desenvolvimento[132].

Assevera-se que não existem contornos exatos acerca da disponibilidade ou interferências legítimas sobre os direitos da personalidade, mas elas ocorrem todos os dias, quando se consente à um exame invasivo (integridade física, com possível risco à vida), nas propagandas comerciais (nome, imagem) e nas postagens em redes sociais (privacidade)[133].

Ademais, por serem direitos afetos às condições existenciais humanas, nem sempre sua violação terá repercussões econômicas ou patrimoniais. Logo, outras formas de reparação, como o direito de resposta ou a indenização pelo dano não-patrimonial (ou moral) se mostram compulsórias[134]. Ou seja, a amplitude dos direitos da personalidade projeta sua tutela para além da visão da responsabilidade civil.

Neste sentido, o artigo 12 do Código Civil brasileiro prevê a possibilidade de fazer cessar qualquer ameaça ou lesão, sem prejuízo do ressarcimento pelos danos causados[135]. A mesma abordagem é vista no RGPD, que repousa sobre duas premissas: a possibilidade de se obter medidas cautelares para impedir, conter ou fazer cessar o ato lesivo (*injunctions*); e a possiblidade de reparação do dano caso seja consumada a ofensa (*tort of damages*).

Sem embargo, estes remédios civis, que preveem tutela apenas em termos negativos, no sentido de repelir ingerências externas à livre determinação do sujeito, não são suficientes[136]. Não se pode conter em setores estanques os direitos humanos

---

[131] CORDEIRO, António Menezes. *Tratado de Direito Civil Português,* Parte Geral, Tomo III, 2ª ed. Lisboa: Almedina, 2007, p. 115.
[132] GODINHO, Adriano Marteleto. *op. cit.,* p. 22.
[133] *Idem.*
[134] BARROSO, Luís Roberto. *Colisão entre liberdade de expressão e direitos da personalidade: critérios de ponderação.* In: Revista de Direito Administrativo, Rio de Janeiro, janeiro/março de 2004, p. 12.
[135] BRASIL. *Código Civil*, *op. cit*.
[136] TEPEDINO, Gustavo, *op. cit.*

fundamentais[137] e as situações jurídicas de direito privado, pois a pessoa requer proteção integrada, que supere esta dicotomia e promova verdadeira dignidade[138].

Assim, o entendimento da proteção de dados como direito da personalidade, cuja importância é destacada para a promoção da autodeterminação do indivíduo, marca uma nova fase de tutela, que requer tratamento, também, dentro da jusfundamentalidade do Direito.

1.4.3. Proteção de dados pessoais como direito humano fundamental

Por mais que se fale de tutela geral da personalidade, diferentes projeções ou riscos específicos de lesões faz com que se procure autonomizar direitos que requerem defesa autônoma[139]. À título de exemplo, a fotografia motivou a formação da *privacy,* enquanto o computador, a *internet,* e os perigos de "objectualização" da pessoa levaram à criação do direito de proteção dos dados pessoais[140].

A autonomização da proteção de dados começou a se desenhar pela jurisprudência, notadamente em duas decisões do Tribunal Constitucional Federal alemão. A primeira faz menção a autodeterminação do indivíduo dentro da esfera de sua personalidade. No caso "Mikrozensus-Entscheidung"[141], foi garantido o direito de fiscalização da recolha de dados relativos à vida privada, onde se mencionou um "espaço interno" que a própria pessoa domina e controla[142].

O segundo, questionou a realização de um censo geral em 1983 em que se iriam confrontar os dados recolhidos com os constantes do registro civil. Seriam feitas perguntas

---

[137] Escolhemos usar o termo "Direitos Humanos fundamentais", tal como preconizado por Perez Luño (*Derechos Humanos, Estado de Derechos y Constitución*, 10. ed. Madrid: Tecnos, 2010) e Herrera Flores (*Reinvención Derechos Humanos*. Madrid: Atrapasuenos, 2008), por entendermos que o ser humano deve ser protegido e promovido onde quer que esteja, estabelecendo-se uma doutrina que aceita o uso das expressões – direitos humanos e direitos fundamentais - como similares, já que tem a mesma pretensão de proteção dos bens mais caros aos indivíduos e à sociedade.

[138] TEPEDINO, Gustavo, *op. cit.*

[139] GUIMARÃES, Maria Raquel. *A tutela da pessoa e da sua personalidade: algumas questões relativas aos direitos à imagem, à reserva da vida privada e à reserva da pessoa íntima ou direito ao carácter*. In: CENTRO DE ESTUDOS JUDICIÁRIOS. *A tutela geral e especial da personalidade humana*, Lisboa: Centro de Estudos Judiciários, 2017, p. 26

[140] PINHEIRO, Alexandre Sousa. *op. cit*., p. 823.

[141] LINDEN RUARO, Regina e RODRIGUES, Daniel Piñeiro. *O direito à proteção de dados pessoais e a privacidade*. In: Revista da Faculdade de Direito – UFPR, Curitiba, nº 53, 2011, p. 55.

[142] Em decisões posteriores, se utilizou o argumento de que o indivíduo poderia escolher como se representar na sociedade, abrangendo o direito à imagem. In: RUARO, Regina L. e RODRIGUES, Daniel P., o*p. cit.*

de cunho pessoal, incluindo práticas religiosas e políticas. A Corte decidiu pela inconstitucionalidade da medida, tendo como um dos seus argumentos a divergência de finalidade. Foi, então, reconhecido o direito à autodeterminação como a faculdade dos indivíduos de decidir, por eles mesmos, quando e dentro de quais limites seus dados pessoais poderiam ser utilizados[143].

Esta decisão fundamentou o "novo direito" – autodeterminação - em princípios constitucionais: dignidade, direito geral de personalidade e seu livre desenvolvimento. Daí porque, o compartilhamento de informações passaria a ser limitado à finalidade instituída para cada órgão público[144], já que um poder geral de uso de dados às entidades estatais não atenderia aos direitos e liberdades fundamentais em jogo.

A nível normativo, temos no artigo 8.º da Convenção Europeia de Direitos do Homem (CEDH), de 1950, que "todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência"[145].

Este artigo foi usado pelo Tribunal Europeu dos Direitos do Homem (TEDH) para defender a proteção de dados pessoais[146], se diferenciando da solução germânica que partiu do princípio da dignidade[147]. A Jurisprudência do TEDH foi importante para ampliar a visão do que é vida privada, nela enquadrando, ou a partir dela evoluindo, para as informações pessoais. Além disso, previu não somente a obrigação dos Estados de se absterem de praticar violações aos direitos previstos no artigo 8.º, mas também impôs, em certos casos, a obrigação de assegurá-los[148].

Em Portugal, o legislador constitucional previu, em 1976, no artigo 35, o direito de todos os cidadãos a terem acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam. Proibiu o tratamento sem consentimento expresso, e à dados referentes a

---

[143] *Idem.*
[144] PINHEIRO, Alexandre Sousa, *op. cit.*, p. 827.
[145] In: https://www.echr.coe.int/Documents/Convention_POR.pdf, acesso em 30/09/2019.
[146] CONSELHO DA EUROPA. *Manual da Legislação Europeia sobre Proteção de Dados*. In: https://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf. Acesso em 30/6/2019, p. 15.
[147] PINHEIRO, Alexandre Sousa. o*p. cit.*, p. 546.
[148] Ver, por exemplo, TEDH, acórdão I. c. Finlândia, de 17 de julho de 2008, petição n.º 20511/03; TEDH, acórdão K.U. c. Finlândia, de 2 de dezembro de 2008, petição n.º 2872/02.

"convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica"[149].

Ou seja, já se previa "uma vertente ativa de titularidade do poder de controlo sobre os (...) próprios dados pessoais"[150], cuja escolha vai além da vertente passiva do direito à privacidade, que meramente habilita o titular a excluir terceiros de sua esfera de intimidade[151].

Contudo, apesar de ter sido um grande avanço a previsão constitucional ainda nos anos de 1970, a proteção de dados pessoais ficou condicionada à legislação ordinária, que só foi completada em 1991 (Lei nº 10/91, revogada pela Lei n.º 67/98), quando foram definidos dados pessoais e as condições em que eles poderiam ser tratados[152].

Em meados da década de 70, o Comitê de Ministros do Conselho da Europa adotou várias resoluções sobre a proteção de dados pessoais que faziam referência ao artigo 8.º da CEDH[153]. Mas, foi somente em 1981, que foi criado o primeiro instrumento internacional juridicamente vinculativo neste domínio - Convenção 108 do Conselho da Europa[154], ratificada por todos os Estados-Membros da UE[155]. Nela, se procurou garantir o respeito à vida privada, notadamente face ao tratamento automatizado[156].

A partir de então, passou-se a se exigir recolha e tratamento dentro das previsões legais e com finalidade determinada, sendo conservados apenas pelo tempo necessário.

---

[149] Artigo 35 da Constituição portuguesa, *op. cit*. Estes dados, que hoje chamamos de sensíveis, afora o consentimento, poderiam receber tratamento com autorização dada por lei, desde que houvesse garantias de não discriminação, ou anonimização dos dados.

[150] TEIXEIRA, Guilherme da Fonseca. *Identidade e autodeterminação informacional no novo Regulamento Geral de Proteção de Dados: a inevitável privatização dos deveres estaduais de proteção,* pp. 11-38. In: Católica Law Review, VOLUME II, nº 1, janeiro 2018, p. 20.

[151] *Idem*, p. 21.

[152] Segundo o ortigo 35.2 da Constituição portuguesa, *op. cit*.: "A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente".

[153] Ver referências em: CONSELHO DA EUROPA. *Manual da Legislação Europeia sobre Proteção de Dados. op. cit.*, p.16.

[154] CONSELHO DA EUROPA. *Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal*, STCE n.º 108, 1981. Vale lembrar que a Convenção se aplica ao tratamento realizado pelo setor público e privado, além do fluxo transfronteiriço de dados pessoais.

[155] Em 15 de junho de 1999, a Convenção foi alterada para permitir a adesão da UE – CdE (STCE n.º 108): artigo 23.º, n.º 2, na redação em vigor. Em 2001, foi adotado um protocolo adicional à Convenção que estabelece disposições sobre fluxos transfronteiriços de dados para Estados não signatários, os chamados países terceiros, e sobre a criação obrigatória de autoridades nacionais de controle de proteção de dados.

[156] PARLAMENTO EUROPEU. *Fichas técnicas sobre a União Europeia*, 2019, acesso em 30/09/2019. In:http://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais.

Fala-se também em adequação, pertinência, proporcionalidade e exatidão de dados, além do direito do titular a informações e retificação.

De maior relevância ao nosso estudo, a Carta dos Direitos Fundamentais da União Europeia, proclamada no ano 2000[157], e tornada vinculativa como direito primário da UE com a entrada em vigor do Tratado de Lisboa em 2009[158], emancipou a proteção dos dados pessoais da vida privada, reconhecendo-lhe como direito fundamental (artigo 8º)[159]. Como inovação, prevê a fiscalização da proteção de dados por uma autoridade independente[160], uma vez que, por ser um direito humano fundamental, requer tratamento diferenciado em relação às normas jurídicas ordinárias[161].

Todavia, vale lembrar que nem mesmo os direitos humanos são absolutos, já que vivemos em um mundo plural e diverso, de relações complexas, em que a conciliação se torna necessária[162]. No caso dos dados pessoais, temos um claro jogo de interesses entre os titulares e as empresas privadas e órgãos públicos, em diferentes atividades, como comércio, controle policial e fiscal e monitoramento de serviços públicos.

Na balança estão direitos fundamentais: de um lado, a autodeterminação, privacidade e proteção de dados; do outro, a livre iniciativa, liberdade de imprensa e segurança pública, entre outros. Como não há um direito fundamental que deva prevalecer sobre o outro, devem eles coexistir, sendo necessário a análise no caso concreto que permita a manutenção dos elementos essenciais de cada um destes direitos.

Neste sentido, o TJUE já decidiu que a proteção assegurada pelo artigo 8.º da Carta "não é uma prerrogativa absoluta, mas deve ser tomada em consideração relativamente à sua função na sociedade"[163]. O artigo 52.1 do mesmo texto legal permite restrições ao

---

[157] *Carta dos Direitos Fundamentais da União Europeia*, JO de 18 de dezembro de 2000, C 326, 2012.
[158] Ver artigo 6.º/1, do *Tratado da União Europeia*, JO de 7 de junho de 2016, C 202/13.
[159] CONSELHO DA EUROPA. *Manual da Legislação Europeia sobre Proteção de Dados. op. cit*, p. 21.
[160] Artigo 8.3 da Carta dos Direitos Fundamentais da União Europeia, *op. cit., in verbis: "(...)* O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente".
[161] Um direito humano fundamental tem características próprias que os distinguem de outros direitos: universalidade; fundamentalidade; abstração; moralidade; e prioridade. In: ALEXY, Robert. *Teoria Discursiva do Direito***.** Rio de Janeiro: Forense Universitária, 2014, p. 111.
[162] *Idem.*
[163] Ver, por exemplo: TJUE, Acórdão de 9/11/2010 nos processos apensos C-92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen, n. 48. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:62009CJ0092. Acesso em 29/09/2019.

exercício de direitos, desde que sejam proporcionais e previstas em lei, e não subtraiam ou desvirtuem seu conteúdo essencial[164].

[164] CONSELHO DA EUROPA. *Manual da Legislação Europeia sobre Proteção de Dados, op. cit.,* p. 23.

Capítulo 2 – Proteção de dados em perspectiva comparada – RGPD e LGPD

Tanto o RGPD como a LGPD são bastante complexos, e, por esta razão, este estudo não terá como objetivo esgotar a discussão a respeito deles, mas se disporá a oferecer subsídios para a compreensão de seus principais pontos, com ênfase nos temas relacionados à atuação da autoridade de controle. Para que a análise comparada possa ser mais precisa e útil, serão apreciados os mesmos tópicos em relação aos dois normativos: considerações introdutórias (2.1); direitos assegurados ao titular (2.2); e deveres e obrigações dos responsáveis pelo tratamento (2.3).

2.1. Notas introdutórias, apresentação e entrada em vigor

O processo de entrada em vigor do RGPD e da LGPD é diferente. No âmbito europeu, a proteção de dados pessoais percorreu um caminho, ao longo de décadas, em que o tema foi tratado em convenções e diretivas, além de importantes decisões judiciais, até que culminasse na aprovação do Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril (2.1.1). Já no Brasil, seu reconhecimento é recente, tendo a LGPD trazido diversas inovações ao sistema jurídico pátrio (2.1.2).

2.1.1. Regulamento Geral sobre a Proteção de Dados (RGPD)

Como vimos anteriormente, todos os países da União Europeia assinaram a Convenção 108, cujo objetivo é garantir o respeito pela vida privada face ao tratamento automatizado de dados pessoais[165]. Sendo um tratado, instrumento do Direito Internacional, que busca coordenar a atuação de diversos Estados em busca de objetivos comuns, a citada Convenção não logrou alcançar tratamento uniforme de seus membros sobre a proteção almejada.

A efetividade de um tratado realmente depende de um somatório de fatores, como a incorporação nas legislações nacionais, sua adaptabilidade a outros normativos internos, pressão/aceitação popular e/ou política, viabilidade econômica etc. Por isso, mesmo quando governos implementam os acordos internacionais, por meio de leis e decretos, sua execução nem sempre é suficiente para alcançar os objetivos do regime.

[165] Convenção 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, *op. cit*.

Ou ainda, diante de uma linguagem mais fluida e abrangente, que é comum em um tratado, cujos signatários têm diferentes sistemas jurídicos, pode haver diferenças pronunciadas de execução[166]. E, foi isso que aconteceu com a Convenção 108, já que nem todos os membros tinham legislação específica sobre proteção de dados pessoais, ou, tendo, ofereciam graus de tutela deficiente em comparação aos objetivos do acordo.

Para resolver a questão, foi adotada a Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados – "Diretiva de Proteção de Dados" (JO L 281, 1995), cujo objetivo era harmonizar e promover igualdade no tratamento de dados pessoais no âmbito europeu.

A Diretiva - aplicável aos 28 Estados-Membros da UE e aos que fazem parte do Espaço Econômico Europeu (EEE): Islândia, Listenstaine e Noruega – apresentou princípios de tutela na recolha e tratamento; definiu critérios e padrões de transferência internacional e determinou o estabelecimento de autoridades centrais responsáveis pela proteção de dados pessoais (autoridades de controle)[167].

Acontece que, mesmo após sua adoção, a proteção de dados pessoais e a aplicação da Convenção 108 mantiveram-se irregular entre os Estados-membros, o que penalizava o mercado interno e gerava insegurança jurídica[168]. Um instrumento jurídico mais cogente

[166] WEISS, Edith Brown e JACOBSON, Harold K. *Engaging Countries: strengthening Compliance with international environmental accords*. Cambridge: MIT Press, 2000, pp. 1 e 2.

[167] Outros normativos foram aprovados ao longo dos danos, sobre questões específicas, como a Decisão 2000/520/CE, de 26 de Julho, relativa ao nível de proteção assegurado pelos princípios de «porto seguro», para compatibilizar a legislação setorial e a auto regulação norte-americanas com a legislação europeia; o Regulamento (CE) n.º 45/2001 relativo ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados; a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais no setor das comunicações electrónicas (alterada pela Diretiva 2006/24/CE e Diretiva 2009/136/CE); e a Decisão-Quadro 2008/977/JAI do Conselho, relativa à proteção dos dados pessoais no âmbito da cooperação policial e judiciária em matéria penal.

[168] EUROPEAN DATA PROTECTION SUPERVISOR. *The History of the General Data Protection Regulation*. In: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation-en, acesso em 21/10/2019.

era necessário, e, em 2016, foi aprovado o Regulamento Geral sobre a Proteção de Dados[169], que entrou em vigor em maio de 2018[170].

Cumpre destacar que a espécie normativa "regulamento", diversamente da espécie "diretiva", não tem transposição para o direito nacional. Ou seja, o "regulamento", no direito europeu, não requerer incorporação, podendo ser aplicado diretamente. Nada obstante, o RGPD não pode ser considerado como um texto totalmente unificador da proteção de dados na UE[171], já que os artigos 23, e 85 a 91 permitem adaptações.

Pode-se dizer que p RGPD é uma evolução da Diretiva 95/46/CE, fruto de um longo processo democrático, o que faz com que parte de suas disposições já estive prevista na Diretiva revogada. Traz, sem embargo, inovações, como conceitos e garantias fundamentais (artigos 1 - 11); e definições[172], especialmente com o uso dos considerandos como guias de interpretação[173].

Essa estrutura de níveis e princípios permite maior dinamização da legislação, fazendo com que seja menos suscetível a desatualizações, já que se idealizou que os princípios e garantias fossem tecnologicamente neutros – ou seja, adaptáveis, ainda que ocorram mudanças (razoáveis) no campo tecnológico[174].

---

[169] Neste tópico vamos focar a atenção ao RGPD. Contudo, cumpre assinalar que também existem duas diretivas europeias sobre aspectos específicos da proteção de dados, que são: Diretiva (UE) 2016/680, que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais; e a Diretiva (UE) 2016/681 que delimita a utilização dos dados dos registos de identificação dos passageiros [PNR] para repressão das infrações terroristas e da criminalidade grave.

[170] É possível visualizar os normativos que antecederam o RGPD em forma de gráfico, associados a *milestones* do desenvolvimento tecnológico, o que facilita a visão e entendimento do leitor, acesso em 21/10/2019, in: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation.

[171] PINHEIRO, Alexandre Sousa (coord.). *Comentário ao Regulamento Geral de Protecção de Dados*. Coimbra: Edições Almedina, 2018, p. 21.

[172] Os conceitos-chave são definidos principalmente no artigo 4º. Alguns já estavam na Diretiva 95/46/CE, e outros foram aprimorados pelo novo regulamento. A Diretiva tinha 8 definições em seu artigo 2º, e o RGPD tem 26, entre elas, a de autoridade de controle.

[173] Os considerandos são muito úteis para a interpretação e compreensão do RGPD, ajudando a explicar e contextualizar seus elementos. Mais sobre em: FAZENDEIRO, Ana. *Regulamento Geral sobre a proteção de dados*. Portugal: Almedina, 2 ed., 2018, p. 10.

[174] POLIDO, Fabrício B. Pasquot et al. *GDPR e suas repercussões no direito brasileiro: Primeiras impressões de análise comparativa*. Brasil: IRIS, 2018, p. 8.

2.1.2. Lei Geral de Proteção de Dados Pessoais (LGPD)

No Brasil, a proteção de dados pessoais foi recentemente regulamentada pela Lei nº 13.709, de 14 de agosto de 2018. A Lei Geral de Proteção de Dados Pessoais[175] já foi alterada duas vezes, antes de sua entrada em vigor, em razão das discussões que gerou e ainda gera, especialmente no tocante à criação da autoridade de controle.

Diferentemente do regime europeu que, como vimos, foi sendo moldado ao longo do tempo, por convenções e pela Diretiva 95/46/CE, a LGPD representa inovação no direito brasileiro, que apenas mencionava a tutela de informações pessoais na lei de *habeas data*[176] e em alguns aspectos da legislação consumerista[177].

O termo "dados pessoais" foi utilizado pela Lei 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet[178], tendo como um dos seus princípios a proteção dos dados pessoais, "na forma da lei". Logo, a eficácia desta proteção ficou condicionada à positivação de um novo instrumento jurídico.

A supracitada lei exige – em relação aos usuários da internet – o consentimento; direitos de informação[179]; finalidade restrita; e a possibilidade de exclusão definitiva de

---

[175] A LGPD foi discutida durante 8 anos no Brasil, mas não de forma ininterrupta. Foram realizadas 2 consultas e 13 audiências públicas para aprofundar as discussões de dois projetos de lei (PLs 4060/12 e 5276/16) que tramitavam na Câmara Legislativa Federal. Durante o mesmo período tramitava outro Projeto no Senado, o PLS 330/13, que contou com 2 audiências públicas e acabou sendo arquivado. Ver mais sobre o histórico legislativo em: MONTEIRO, Renato Leite *et al*. *Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos*, acesso em 04/11/2019.
In:https://www.academia.edu/38940887/Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_e_GDPR_hist%C3%B3rico_an%C3%A1lise_e_impactos.

[176] A garantia do *habeas data* está presente na Constituição brasileira de 1988, *op. cit.,* artigo 5º, LXXII. Esta ação constitucional tem o propósito de garantir ao cidadão o acesso e retificação de seus dados que estejam armazenados em registros governamentais e bancos de dados de caráter público. Tem, contudo, âmbito de aplicação bastante restrito. Foi regulamentado pela Lei nº 9.507/1997.

[177] BRASIL. *Lei nº 8.078*, de 11 de setembro de 1990 - Código de Defesa do Consumidor. Em seu artigo 43, disciplina os bancos de dados e cadastro de consumidores, especialmente no que tange à coleta de informações sobre inadimplemento para fins de concessão de crédito. Garante acesso a informações existentes em cadastros, fichas, registros e dados de consumo, bem como sobre as suas fontes. Os dados devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, podendo haver retificação.

[178] BRASIL. *Lei 12.965*, de 23 de abril de 2014 – Marco Civil da Internet.

[179] Em relação à coleta, guarda, armazenamento e tratamento de dados pessoais, foi determinado que os provedores e aplicações de internet deverão prestar informações acerca do cumprimento legal, e que na provisão de aplicações de internet, é vedada a guarda dos registros de acesso a outras aplicações sem que consentimento do titular, bem como a guarda de dados pessoais que sejam excessivos em relação à finalidade.

dados, a requerimento, ou mediante término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória previstas na Lei[180].

Vemos, portanto, que alguns importantes conceitos já estavam presentes no ordenamento jurídico brasileiro desde 2014, mas tendo seu escopo limitado aos provedores e aplicações de internet. Somente após a entrada em vigor da LPGD, em agosto de 2020, a proteção de dados pessoais passará a ser assegurada em qualquer meio de recolha e tratamento[181].

Salientamos que no Brasil a proteção de dados pessoais não é considerada um direito fundamental autônomo. Entre os objetivos da LGPD está a proteção dos direitos fundamentais de liberdade[182], privacidade e livre desenvolvimento da personalidade[183]. Não se sabe se não houve interesse do legislador em conferir jusfundamentalidade à proteção de dados pessoais, por entender que ela está abrangida no direito à privacidade, ou se a escolha se deu em razão do difícil processo político necessário à sua incorporação via emenda constitucional, procedimento indispensável para o reconhecimento de direitos fundamentais no Brasil[184].

Finalmente, temos uma diferença de estrutura e detalhamento entre os dois normativos comparados. A LGPD é mais compacta, com 58 artigos distribuídos em 9 capítulos[185]. Já o RGPD foi composto por 11 capítulos e 99 artigos, além de 173 considerandos.

2.2. Direitos do titular de dados pessoais

O RGPD e a LGPD criaram, em seus respectivos âmbitos de aplicação, uma estrutura de responsabilidade dupla: a primeira, individual, de cada pessoa singular sobre os seus dados (direitos do titular); a segunda, de responsabilização de empresas/órgãos públicos

[180] A Seção II da lei estabeleceu que os dados pessoais e as comunicações privadas devem atender à preservação da intimidade, da vida privada, da honra e da imagem, sendo necessária ordem judicial para a quebra de seu sigilo. Contudo, dados como qualificação pessoal, filiação e endereço podem ser requisitados por autoridades administrativas com competência legal.
[181] Lei nº 13.709, *op. cit.*, artigo 3°.
[182] O Direito à privacidade está previsto na Constituição brasileira, *op. cit.,* artigo 5º, incisos X e XI.
[183] Lei nº 13.709, *op. cit.*, artigo 1°.
[184] O procedimento de emenda constitucional está previsto no artigo 60 da Constituição brasileira, *op. cit.,* e requer que a proposta seja discutida e votada em cada Casa do Congresso Nacional, em dois turnos, sendo aprovada por três quintos dos votos dos respectivos membros.
[185] Existe um capítulo adicional dedicado à alteração pontuais da Lei nº 12.965, *op. cit.*

que os recolhem e tratam. São dois pilares em sintonia: um de componente econômico, outro de proteção de direitos e liberdades fundamentais[186].

Particularmente em relação aos titulares, entende-se que houve um "recorte dogmático" que procurou garantir a tutela dos dados pessoais consoante a maior ou menor proximidade das informações com o núcleo íntimo da pessoa, que passa a ter o poder de gestão sobre elas[187]. Dentre estes direitos, vamos destacar o consentimento (2.2.1), o tratamento de categorias especiais de dados (2.2.2) e o direito a ser esquecido (2.2.3).

2.2.1. Tratamento lícito e consentimento

a. Tratamento Lícito e consentimento no RGPD

Uma das grandes premissas em que se baseia o RGPD é a necessidade de o tratamento se dar dentro de uma das seis hipóteses legais, que são: consentimento; execução de contratos ou de diligências, a pedido do titular; cumprimento de obrigação jurídica a que o responsável esteja sujeito; defesa de interesses vitais do titular ou de outra pessoa natural; interesse público ou exercício da autoridade pública; necessidade para efeito de interesses legítimos do responsável ou de terceiros, exceto se prevalecerem interesses, direitos ou liberdades fundamentais, em especial se o titular for uma criança[188].

Dentre eles, o consentimento se destaca por trazer o titular de volta para o centro da relação jurídica, ampliando o respeito pela vontade da pessoa natural, lhe delegando a ponderação de valores entre a necessidade, adequação e proporcionalidade do tratamento,[189] e os benefícios que ele recebe em troca.

O consentimento deve ser claro, inteligível e proporcional ao objetivo em causa. Ou seja, deverá haver uma explicação do propósito da coleta de dados e seus fins, para que o usuário saiba exatamente ao que está consentindo.

O artigo 4.11 do RGPD define «consentimento» como:

> *uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo*

[186] PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, p. 11.
[187] TEIXEIRA, Guilherme da Fonseca, *op. cit.,* p. 21.
[188] Artigo 6.1 do RGPD, *op. cit.*
[189] PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, pp. 244 e 245.

> *inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.*

Não existe consentimento por omissão, cabendo a prova ao responsável[190]. Além disso, o pedido de tratamento deve ser destacado dos demais, caso esteja em documento que regule outros assuntos, como um contrato, e com redação clara e simples, de fácil acesso e compreensão. A não observância de quaisquer destes pontos torna o consentimento não vinculativo.

De mais a mais, como o consentimento é condição de legitimidade do tratamento, ele deve ser opcional, não se concebendo o "consentimento obrigatório"[191]. Desafios à questão podem ser previstos em casos trabalhistas, em contratos de consumo e diante de autoridades públicas, ou seja, sempre que não houver equilíbrio entre as partes.

A finalidade da recolha deve ser informada previamente ao fornecimento dos dados, e é vinculante para tratamentos futuros. Logo, se uma empresa, no momento da compra, recolhe dados visando uma campanha publicitária, deverá informar o fato inequivocamente ao consumidor, não podendo atrelar a venda ao fornecimento de dados, já que não são necessários para a plena execução do contrato[192].

Por conseguinte, há que se diferenciar, nos contratos, qual é o fator de licitude do tratamento – se ele é indispensável à execução do serviço ou, caso contrário, se houve consentimento. Como é a empresa que determina quais dados são indispensáveis para a execução contratual, múltiplas controvérsias poderão surgir[193], sendo a atuação da autoridade de controle imperativa para prevenir e remediar casos de abuso.

Finalmente, cumpre salientar que, por ser uma manifestação de vontade livre, o consentimento pode ser retirado a qualquer momento pelo titular, o que não compromete a licitude do uso anterior[194]. O importante é que "o consentimento deve ser tão fácil de retirar quanto de dar"[195], para que não se criem situações onde a burocracia e dificuldade de acesso acabem legitimando tratamento com o qual o titular deixou de concordar.

---

[190] Artigo 7.1 do RGPD, *op. cit.*
[191] PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, p. 167.
[192] Vide artigo 7.4 do RGPD, *op. cit.*
[193] MARTINEZ, Pedro Romano. Apresentação proferida em palestra.
[194] Artigo 7.3 do RGPD, *op. cit.*
[195] *Idem.*

b. Tratamento Lícito e consentimento na LGPD

A LGPD traz quatro hipóteses de tratamento lícito a mais do que RGPD, sendo as demais bastante semelhantes. Em comum, tem-se: consentimento; execução de contrato ou de procedimentos preliminares, a pedido do titular; cumprimento de obrigação legal ou regulatória; proteção da vida ou da incolumidade física do titular ou de terceiros; para atender interesses legítimos[196], exceto quando prevalecerem direitos e liberdades fundamentais do titular[197].

Em relação ao tratamento por autoridades públicas, a LGPD vincula o tratamento à execução de políticas públicas previstas em leis ou em contratos/convênios. O termo é mais restritivo do que o usado no RGPD (interesse público ou autoridade a que está investida o responsável), o que poderia inferir maior controle. Contudo, a expressão "políticas públicas" também é bastante ampla, sendo questionável que haja diferenças práticas na aplicação dos dois dispositivos neste ponto.

Entre os casos adicionais de tratamento lícito, temos a realização de estudos por órgão de pesquisa, que não está condicionado a outro tipo de autorização, como no RGPD. A Lei não deixa claro como os dados serão recolhidos para este fim, nem se isto seria possível sem o conhecimento dos titulares. Todavia, prevê que serão anonimizados sempre que possível, o que nos parece indispensável para a proteção do titular, em especial pela ausência de regulamentação a respeito da finalidade destas pesquisas e o possível compartilhamento de dados ou resultados.

De mais a mais, permitiu-se o tratamento de dados de saúde por profissionais da área, serviços de saúde ou autoridade sanitária. No RGPD, tais dados são elencados como sensíveis, sendo proibido seu tratamento, com exceções[198]. Neste ponto, foi mais permissivo o legislador brasileiro. Em especial, cabe discussão do que seriam os "serviços

[196] A LGPD adicionou a hipótese legal de tratamento para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Não destacaremos a análise desta questão porque, apesar de ser hipótese não prevista nominalmente no artigo 6º do RGPD, ela aparece em seu texto, especialmente como exceção à proibição de tratamento dos dados sensíveis e em derrogações, como o direito a ser esquecido e a limitação de tratamento. Ainda, a autorização para o uso de dados em processos no RGPD pode ser entendida dentro da permissiva de uso para fins de interesses legítimos.
[197] Lei nº 13.709, *op. cit.*, artigo 7º.
[198] Artigo 9 do RGPD, *op. cit.*

de saúde", e se entre eles poder-se-ia incluir as seguradoras ou entidades que controlam os planos de saúde privados, o que poderia ter imenso impacto em direitos fundamentais.

Outro ponto que chama atenção é a inclusão da "proteção do crédito" dentro dos tipos lícitos de tratamento de dados pessoais, em razão do lobby efetuado pelas entidades privadas que atuam na área[199].

Em relação ao consentimento, o conceito introduzido pela lei brasileira: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[200], é bastante similar ao do RGPD. Em ambos, «consentimento» é uma manifestação livre, informada e inequívoca[201], que requer adesão em cláusula destacada e voluntária, e cuja prova cabe ao responsável.

Autorizações genéricas serão nulas, de acordo com os princípios da adequação do tratamento[202] e da necessidade[203], também sendo desconsideradas quando "as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca"[204]. O consentimento pode ser revogado a qualquer momento, mediante manifestação do titular, por procedimento gratuito e facilitado[205].

---

[199] São exemplos de entidades de proteção ao crédito: Boa Vista Serviços, administradora do SCPC, que fornece informações de restrição cadastral através do seu banco de dados e calcula a pontuação do tipo "score de crédito". Estes dados são utilizados largamente em processos de análise e de concessão de crédito aos consumidores e como restrição ao uso de cheques; CCF– Cadastro de Emitentes de Cheques sem Fundos do Banco Central, cujo banco de dados contém nomes das pessoas que emitem cheques sem ter saldo em sua conta para o pagamento; SERASA Experian, empresa privada que possui um dos maiores bancos de dados do mundo e que presta serviços de interesse geral informações de dívidas vencidas e não pagas, registros de protesto de título, ações judiciais, etc.; SPC Brasil, que é um banco de dados privado de informações de crédito, alimentado por associações comerciais e câmaras de dirigentes lojistas do país que são filiadas à Confederação Nacional de Dirigentes Lojistas.

[200] Lei nº 13.709, *op. cit.,* artigo 5º/XII.

[201] Apesar de não se mencionar no conceito que o consentimento é uma manifestação "de vontade", o que entendemos fortalecer a ideia de aceitação voluntária, tal atributo foi definido no princípio da finalidade, aplicável ao consentimento, segundo o qual o tratamento deve ter propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de uso posterior de forma incompatível com essas finalidades. In: Lei nº 13.709, *op. cit., a*rtigo 6º/I.

[202] Lei nº 13.709, *op. cit., a*rtigo 6º/II: "Artigo 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) II: adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento".

[203] Lei nº 13.709, *op. cit., a*rtigo 6º/III: "Artigo 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) III: necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

[204] Lei nº 13.709, *op. cit., a*rtigo 9º, §1º.

[205] Lei nº 13.709, *op. cit.,* artigo 8º, §5º.

2.2.2. Tratamento de categorias especiais de dados pessoais

a. Tratamento de categorias especiais de dados pessoais no RGPD

O RGPD destaca uma categoria especial de dados pessoais, que são mais conhecidos como "dados sensíveis"[206]. Vejamos:

> *Artigo 9.1: É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.*

O tratamento destes dados apresenta maior potencial discriminatório e de restrição a direitos fundamentais[207] e, por isso, a opção do legislador europeu foi de proibi-lo, sendo as exceções à essa proibição causas de exclusão da ilicitude[208], em razão de interesses preponderantes que justifiquem o uso[209]. São elas: consentimento explícito[210]; obrigação em razão de legislação laboral[211], de segurança social e de proteção social; quando necessário para declaração, exercício ou defesa de um direito em processo judicial; interesse público relevante; diagnóstico médico ou gestão de sistemas e serviços de saúde[212].

Apesar da proteção diferenciada se fazer mister[213], nem sempre é claro o limite do que são ou não dados sensíveis. O tratamento de fotografias, por exemplo, não é considerado sistematicamente dentro das categorias especiais de dados, mas elas podem facilmente revelar a origem racial ou étnica da pessoa, além de suas opiniões políticas ou convicções religiosas/filosóficas[214], a depender do contexto onde foram tiradas.

A derrogação cuja categoria é a mais ampla e que pode gerar dúvidas no caso concreto é a do interesse público relevante, que pode abranger questões sociais como

---

[206] Ver também artigo 4.º, nº 13, 14 e 15 e considerandos 51 a 56 do RGPD, *op. cit*.
[207] Em relação aos dados genéticos, por exemplo, nem mesmo dizem respeito somente ao titular, abrangendo também a família consanguínea. In: PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, p. 237.
[208] Artigo 9.º do RGPD, *op. cit*.
[209] PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, p. 238.
[210] Esta possibilidade pode ser excluída por direito da União ou de um Estado-Membro. In: artigo 9.2, a, do RGPD, *op. cit*.
[211] Dentre elas, medidas de medicina preventiva ou avaliação da capacidade de trabalho do empregado.
[212] Inclui contrato com profissional de saúde.
[213] Considerando 51 do RGPD, *op. cit*.
[214] MARTINEZ, Pedro Martinez, *op. cit.*

pensões, segurança pública, e saúde (prevenção ou controle de doenças transmissíveis e outras ameaças graves à saúde[215])[216].

Especificamente neste último caso, o Regulamento prevê que não deverão ser utilizados dados de saúde para outros fins por terceiros, como empregadores, companhias de seguros e entidades bancárias[217]. Se aplica aqui o princípio da finalidade em acepção estrita, limitando o tratamento à objetivos adequados, pertinentes e estritamente vinculados aos fins da recolha («minimização dos dados»)[218].

Sobre este aspecto, a Comissão Nacional de Protecção de Dados de Portugal (CNPD) decidiu, em análise de pedido de tratamento para fins de investigação clínica, que a concretização do princípio da proporcionalidade se dá nas vertentes de adequação, necessidade e proibição do excesso. O responsável deve ponderar a restrição de direitos fundamentais, tratando somente os dados "indispensáveis à realização da concreta finalidade do estudo e apenas na medida em que do seu tratamento não resulte lesão insuportável e excessiva daqueles direitos"[219].

Em outro parecer[220], o mesmo órgão afirmou que os dados médicos obtidos pela realização de exames de trabalhadores ou candidatos a emprego mantém a relação de confidencialidade entre médico e paciente[221], devendo ser franqueada ao empregador somente a aptidão ou não para exercício da atividade[222].

Ainda assim, o tratamento deve ser limitado ao estritamente necessário para os fins perseguidos, não podendo ser exigido exames e testes sem vínculo com a função exercida.

---

[215] Segundo o considerando 54 do RGPD, *op. cit*., a noção de «saúde pública» deverá ser interpretada de acordo com a definição constante do Regulamento (CE) n° 1338/2008 do Parlamento Europeu e do Conselho.
[216] Considerando 52 do RGPD, *op. cit*.
[217] Considerando 56 do RGPD, *op. cit*.
[218] Artigo 5.º/1/c do RGPD, *op. cit*.
[219] Deliberação n.º 1704/2015, aplicável aos tratamentos de dados pessoais efetuados no âmbito de Investigação Clínica, acesso em 21/10/2019.
In: https://www.cnpd.pt/bin/orientacoes/DEL_2015_InvestClinica.pdf.
[220] Deliberação n.º 890 /2010, aplicável aos tratamentos de dados pessoais com a finalidade de medicina preventiva e curativa no âmbito dos controlos de substâncias psicoactivas efectuados a trabalhadores. In: https://www.cnpd.pt/bin/orientacoes/20_890_2010.pdf. Acesso em 21/10/2019.
[221] Segundo o artigo 17/1/b do Código do Trabalho de Portugal (Lei n.º 7/2009, publicada no Diário da República n.º 30/2009, Série I de 2009-02-12), é proibido exigir informações relativas à vida privada, saúde ou estado de gravidez, com exceção da realização ou apresentação de testes ou exames médicos para proteger a segurança do trabalhador ou de terceiros, em atividades que os justifiquem.
[222] podendo ainda o titular controlar os dados que forneceu (conhecê-los e saber os fins da recolha).

Como exemplo, a CNPD já decidiu que o tratamento de dados como raça e/ou origem étnica é excessivo, inadequado e não pertinente no âmbito da medicina do trabalho[223].

Isto posto, a proteção dos dados sensíveis abrange também as situações em que houve negativa de consentimento por parte do titular, não podendo haver discriminação em razão dela (negativa), a não ser que situação excepcional justifique o tratamento[224].

b. Tratamento de categorias especiais de dados pessoais no RGPD

O conceito de dados sensíveis na LGPD é muitíssimo similar ao de "categorias especiais de dados pessoais"[225] do RGPD. Vejamos:

> *Artigo 5º. II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.*

Contudo, o legislador brasileiro não proibiu seu tratamento. Ao contrário, trouxe um rol de hipóteses legais, similar ao dos demais dados pessoais, que diferem apenas pela possibilidade de uso para prevenção à fraude e à segurança do titular, e nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Se excluem as permissões de uso para atender aos interesses legítimos do controlador ou terceiros e a proteção ao crédito. É, portanto, um rol extenso, que traz riscos, especialmente em relação à recolha de dados biométricos.

Caso especial é o relacionado aos dados de saúde. No Brasil, a saúde pública não é capaz de atender a contento toda a população, o que faz com que um número expressivo de cidadãos recorra à contratação de serviços de saúde complementar. Por isso, a possibilidade de tratamento de dados de saúde pelas empresas que prestam este serviço causou grande discussão, pelo potencial dano discriminatório (análises de risco e exclusão de beneficiários).

---

[223] Deliberação n.º 840/2010, aplicável aos tratamentos de dados no âmbito da gestão da informação dos serviços de segurança e saúde no trabalho, acesso em 21/10/2019.
In: https://www.cnpd.pt/bin/orientacoes/DEL_840_2010_MED_trabalho_actualizada.pdf.
[224] PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, p. 240.
[225] Artigo 9º do RGPD, *op. cit.*

Como já mencionamos, a LGPD passou por duas alterações antes de chegar na versão atual. Inicialmente, permitia a comunicação de dados de saúde com objetivo de obter vantagem econômica caso houvesse aquiescência do titular no pedido de portabilidade. Na primeira revisão da norma, ocorrida em 2018, adicionou-se à essa possibilidade o tratamento diante da "necessidade de comunicação para a adequada prestação de serviços de saúde suplementar"[226].

Na revisão efetuada em 2019, condicionou-se a comunicação e uso compartilhado de dados de saúde, com objetivo de obter vantagem econômica aos interesses do titular[227], sendo "vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários"[228].

Apesar da pertinência e importância da mudança legislativa, acreditamos que deveria ter sido seguida a inteligência do RGPD de proibir o tratamento destes dados, salvo nos casos onde o interesse público prepondere. Os contratos de saúde complementar não permitem alterações ou paridade de posição ao titular, e o consentimento pode ser questionado. Ainda, à título de exemplo, se proibiu o tratamento para a seleção de risco na contratação e exclusão de beneficiários, mas não para o reajuste de valores, o que, na prática, pode equivaler a uma exclusão, a depender do impacto financeiro da medida.

2.2.3. Direito de acesso, informação e apagamento de dados

a. Direito de acesso, informação e apagamento de dados no RGPD

Independentemente da hipótese de licitude do tratamento, o titular pode obter do responsável a confirmação da posse e uso de seus dados, lhe sendo informada a origem; finalidade; categoria; destinatários (transferência/divulgação); prazo de conservação; decisões automatizadas e definição de perfis. Este conhecimento possibilita ao titular

[226] Redação dada pela Medida Provisória nº 869, de 2018.
[227] Tanto no caso de portabilidade solicitada pelo titular, como para permitir compartilhamento de transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde e assistência farmacêutica, incluídos os serviços auxiliares de diagnose e terapia.
[228] Lei nº 13.709, *op. cit.,* artigo 11, § 5º.

solicitar a retificação, apagamento ou limitação do tratamento, cabendo reclamação à autoridade de controle se houver descumprimento[229].

Esse dever de comunicação entre as partes é forçoso para o exercício dos demais direitos do titular, já que estamos diante de uma relação onde não há paridade de forças[230]. Por isso, as informações devem ser oferecidas de forma concisa e inteligível[231], "sem demora injustificada"[232], no prazo de um mês, prorrogável em razão da complexidade e/ou volume de pedidos.

Poderá o responsável deixar de dar seguimento ao pedido do titular se eles forem manifestamente infundados ou excessivos, caso em que caberá taxa para os custos administrativos[233], ou quando houver dúvidas razoáveis quanto à identidade do solicitante, que deverá comprová-la[234]. O importante é que comunique as razões da negativa e sua fundamentação, permitindo que o titular adote as providências cabíveis, seja reformulando seu pedido, reclamando à autoridade de controle ou via ação judicial.

Além disso, o titular deve ser informado dos seus direitos de retificação e apagamento de dados, além da limitação e/ou oposição ao tratamento.

A retificação serve para corrigir ou complementar dados de acordo com as finalidades do tratamento, por meio de declaração do titular, o que corrobora seu papel de parte ativa na relação jurídica, deixando de ser somente a pessoa a quem os dados se referem. Já a limitação ou oposição servem para contestar a guarda/uso de dados quando o motivo do tratamento deixar de existir, mas sua manutenção for prevista em lei, como para exercício ou defesa de direito em processo judicial, por exemplo.

O mais relevante é que o titular se pronuncia sobre os dados já armazenados, podendo limitar seu tratamento quando deixar de consentir para determinada finalidade;

[229] Artigo 15.1 do RGPD, *op. cit*.
[230] PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, p. 359.
[231] Artigo 12.1 do RGPD, *op. cit*.
[232] Artigo 12.3 do RGPD, *op. cit*.
[233] Artigo 12.5 do RGPD, *op. cit*.
[234] Artigo 12.6 do RGPD, *op. cit*.

ou, no caso da oposição, ser ouvido quando o tratamento se basear no interesse público, ou visar a comercialização direta, incluindo a definição de perfis[235] [236].

Ademais, conforme previsão do Artigo17 do RGPD, o titular pode solicitar a quem os possua que eles sejam apagados, interrompendo o compartilhamento e uso, quando não mais existir o fundamento jurídico que possibilitou o tratamento[237], desde que não seja necessário para preservar a liberdade de expressão e de informação; o cumprimento de uma obrigação legal ou necessidade em processo judicial; interesse público superior[238]; e investigação científica, histórica ou para fins estatísticos[239].

O apagamento de dados, também conhecido como «direito a ser esquecido», tem acepção peculiar quando falamos de *internet.* Diferentemente do direito à memória ou do direito de não ser lembrado, no âmbito digital, a proposição revela-se mais como um direito do usuário de ter suas informações pessoais desindexadas, notadamente quando não forem corretas, relevantes ou atualizadas[240].

Neste viés, o direito a ser esquecido foi mencionado em diferentes decisões judiciais na União Europeia, como no caso *Google SL* e *Google Inc* versus Agencia Española de Protección de Datos e Mario Costeja González, de 2014. Nele, se discutiu a possibilidade de o titular exigir a não associação de seu nome, nos motores de busca, com matérias jornalísticas prejudiciais à sua imagem.

---

[235] Artigos 18 e 21 do RGPD, *op. cit*.

[236] Segundo o artigo 4.4 do RGPD, pode ser considerado como definição de perfil: "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". Lembramos que existem restrições a decisões automatizadas, que usam "perfis" para decidir, o acesso do titular a bens, produtos ou serviços sem que se tenha uma ponderação ética. São exceções à sua proibição: necessidade para celebração ou execução de um contrato; presença de interesses legítimos e salvaguarda de direitos e liberdades; consentimento. Nestes casos, por exemplo, poderia haver a não contratação de uma pessoa pelo software/algoritmo ter previsto desempenho profissional abaixo da média, ou negativa de acesso à um seguro pela análise de risco de saúde totalmente automatizada.

[237] Inclui os casos onde o tratamento deixou de ser necessário para a finalidade de recolha e no caso de não mais se justificarem os interesses legítimos prevalecentes do responsável, ou ainda nos casos de oferta de serviços da sociedade da informação a crianças. In: Artigo 17.1 do RGPD, *op. cit*.

[238] Por exemplo, exercício da autoridade pública, saúde pública e arquivo de interesse público.

[239] Artigo 17.3 do RGPD, *op. cit*.

[240] Seriam dois conflitos de direitos com características próprias: no âmbito analógico, a ponderação entre direitos individuais e a liberdade de imprensa; no direito ao esquecimento digital, pondera-se os direitos do titular face aos direitos dos buscadores.

A agência espanhola de proteção de dados entendeu que o jornal estava em seu direito de publicar a matéria, mas que o *Google* era abrangido pela Diretiva 95/46, e deveria deixar de indexar a notícia. Questionada no judiciário (espanhol, inicialmente, mas remetido ao TJUE), foi sentenciado que os motores de busca tratam dados pessoais, mesmo que de forma automática, quando indexam conteúdos disponíveis na internet.

Especificamente em relação ao caso, estipulou-se que não existiam razões de interesse público predominante, devendo o *Google* suprimir os referidos *links* quando se buscasse o nome do requerente[241].

Em setembro de 2019, outro caso foi apreciado pelo tribunal de Justiça Europeu, novamente tendo como parte o *Google*. Desta vez, participou da contenda a agência francesa de proteção de dados - Commission nationale de l'informatique et des libertés, que em 2015 ingressou contra o mecanismo de busca para deixar de veicular resultados de determinadas pessoas. O *Google* havia suprimido o *link* para as páginas/pessoas solicitadas, mas somente quando a busca se iniciava nas versões/extensões europeias, o que levou à agência francesa a multar a empresa.

O TJUE afirmou que a legislação europeia de proteção de dados não tem alcance sobre todas as versões do buscador, mesmo que sede e filiais estejam indissociavelmente ligadas. Contudo, afirmou que o *Google* deve prevenir ou desencorajar, seriamente, os internautas a efetuarem buscas prejudiciais aos direitos fundamentais[242].

b. Direito de acesso, retificação e apagamento de dados na LGPD

Assim como no RGPD, a LGPD, por meio do princípio da transparência, garante ao titular a obtenção de "informações claras, precisas e facilmente acessíveis" a respeito do tratamento de seus dados (finalidade; forma e duração; identificação e contato do controlador; compartilhamento). É um rol mais restrito em comparação com o RGPD, que

[241] Destacamos parte da decisão, *in verbis* "(...) tendo em conta o caráter sensível, para a vida privada dessa pessoa, das informações contidas nesses anúncios e o facto de a sua publicação inicial remontar há 16 anos, a pessoa em causa tem comprovadamente direito a que essas informações já não sejam associadas ao seu nome através dessa lista. Por conseguinte, na medida em que, no caso em apreço, não parece haver razões especiais que justifiquem um interesse preponderante do público em ter acesso a essas informações". In: Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014, processo C-131/12, Google Spain SL, Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.

[242] Acórdão do Tribunal de Justiça (Grande Secção) de 29 de setembro de 2019, Processo C-507/17, Google Inc. contra Commission nationale de l'informatique et des libertés (CNIL - França).

deveria ser complementado para incluir o período de guarda, origem, categoria, tratamentos automatizados e definição de perfis.

Um aspecto singular da lei brasileira é a constante repetição da observação dos segredos comercial e industrial em diversos dos seus incisos e artigos, em razão da preocupação dos legisladores com o impacto econômico que as novas regras podem ocasionar às empresas.

Em relação ao direito de acesso do titular, a questão foi colocada como condicionante para a entrega da forma e duração do tratamento. Melhor teria sido não condicionar a duração, mas somente a forma, quando necessário, já que não vemos como tais informações podem afetar a concorrência leal. Ademais, saber por quanto tempo seus dados serão tratados é um direito basilar do titular, sem o qual não há controle sobre o destino de suas informações.

Entre os aspectos que diferenciam os dois regimes, no Brasil, não foi prevista qualquer cobrança, mesmo que a título administrativo. Os dados devem ser entregues de "maneira imediata" (e não sem demora injustificada) e no prazo de até 15 dias[243].

Da negativa caberá reclamação não somente à autoridade de proteção de dados, mas também aos organismos de defesa do consumidor. A medida, que procurou facilitar o acesso do titular ao exercício de seus direitos, pode gerar interpretação errônea sobre a necessidade de vínculo de consumo para o acesso ou retificação de dados.

A retificação[244] e oposição são possíveis apenas quando houver descumprimento, não havendo previsão de limitação do tratamento ou apagamento de dados. Sobre este último aspecto, cumpre ressaltar que no Brasil não existe um caso paradigmático como o do *google* no âmbito europeu, mas o direito ao esquecimento já foi abordado em diferentes decisões judiciais.

[243] Segundo o artigo 18, § 4º Lei nº 13.709, *op. cit.,* "Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência".
[244] Artigo 6º, incisos IV e V da Lei nº 13.709, *op. cit.*

Mais especificamente em relação à indexação de dados pessoais, temos decisão recente (2018) do Superior Tribunal de Justiça (STJ) [245] que alterou o posicionamento da Corte de afastar a responsabilidade dos buscadores, pela impossibilidade de lhes atribuir função de "censor", demandando ao prejudicado que direcionasse sua pretensão aos provedores de conteúdo.

Todavia, neste caso, em que o nome do autor era associado a suspeitas de fraude em concurso público que foi julgada inexiste, haviam circunstâncias "excepcionalíssimas" que demandavam intervenção judicial, já que o vínculo criado nos bancos de dados não guardam relevância para o interesse público, "seja pelo conteúdo eminentemente privado, seja pelo decurso do tempo"[246].

Concluíram que o rompimento do vínculo sem a exclusão da notícia compatibiliza os interesses individual do titular, e coletivo de acesso à informação, "na medida em que viabiliza a localização das notícias àqueles que direcionem sua pesquisa fornecendo argumentos relacionados ao fato noticiado, mas não àqueles que buscam exclusivamente pelo nome do autor"[247].

Não foi feliz, pois, o legislador brasileiro, ao só permitir o direito ao apagamento quando a base do tratamento for o consentimento, permitindo, assim mesmo, exceções (cumprimento de obrigação legal; estudo por órgão de pesquisa; transferência a terceiro; e uso exclusivo do controlador, desde que anonimizados).

Se a base da Lei é a vontade do titular – assente no seu consentimento expresso, explícito e vinculado a fins determinados – não teria ele o direito de ter seus dados apagados, com exceção das situações de cumprimento legal ou medidas de interesse regulatório (casos em que o consentimento não é requerido de início)?

A medida também nos parece contraditória diante de outra previsão contida no mesmo artigo, que prevê que "o responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a

---

[245] STJ. REsp nº 1.660.168-RJ, acórdão publicado em 05.06.2018. Acesso em 26/11/2019. In: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1628798&num_registro=201402917771&data=20180605&formato=PDF

[246] *Idem.*

[247] *Ibidem.*

correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento"[248].

2.3. Deveres e obrigações dos responsáveis pelo tratamento

A responsabilização dos controladores por violações é o segundo ponto de alteração da lógica do regime de proteção de dados pessoais, complementando a maior autonomia dada ao titular. No âmbito europeu, se exigia autorização prévia por parte da autoridade de controle, o que foi dispensado no RGPD, que aumentou substancialmente as penalidades por incumprimento[249] (2.3.2) e passou a exigir determinadas medidas técnicas de segurança para prevenir danos (2.3.1).

2.3.1. Responsabilidade e medidas de "accountability"

a. Responsabilidade e medidas de "accountability" no RGPD

O RGPD conceitua violação como a destruição, perda, alteração, divulgação ou acesso não autorizado de dados pessoais, que podem ocorrer de modo acidental ou volitivo. A responsabilização independe de dolo, não sendo necessário demonstrar objetivo específico de quem causou os danos para que este seja reconhecido[250].

Para prevenir danos, é exigido dos responsáveis a adoção de medidas técnicas e organizativas adequadas para assegurar e comprovar que o tratamento de dados é feito de acordo com as regras do RGPD[251]. Deve-se observar a natureza, âmbito e finalidade do tratamento, onde serão avaliados os riscos e a gravidade dos possíveis danos[252].

Dentre as diferentes soluções encontradas para preservar "a relação entre a tecnologia e o Direito"[253], estão a proteção de dados desde a conceção e por defeito (artigo 25º do RGPD); as medidas de segurança do tratamento (artigo 32º do RGPD) e a avaliação de impacto sobre a proteção de dados (artigo 35º do RGPD).

[248] Artigo 18, §6º da Lei nº 13.709, *op. cit*.
[249] MARTINEZ, Pedro Romano, *op. cit.*
[250] Artigo 4.12 do RGPD, *op. cit.*
[251] Artigo 24 do RGPD, *op. cit*.
[252] Considerando 74 do RGPD, *op. cit.*
[253] Resolução do Conselho de Ministros n.º 41/2018, publicada no Diário da República n.º 62/2018, Série I de 2018-03-28, pp. 1424 – 1430. In: https://data.dre.pt/eli/resolconsmin/41/2018/03/28/p/dre/pt/html

A proteção de dados desde a concepção (*by design*) visa assegurar que o projeto seja pensado com base na segurança da informação, ou seja, que ela exista desde a criação de um novo produto ou serviço, mediante análise das técnicas disponíveis e seu custo, em relação à natureza, âmbito, contexto e finalidades do tratamento[254]. As medidas de segurança passam a ser, portanto, parte do processo criativo, e não somente formas de solucionar problemas.

Já a "privacy by default" impõe que medidas técnicas e organizativas de proteção de dados sejam padrão, para assegurar de forma automática/preferencial que apenas será recolhida, utilizada e conservada a quantidade necessária de dados, não os disponibilizando, sem intervenção humana, a um número indeterminado de pessoas[255].

A ideia é "abarcar não apenas a arquitetura das plataformas físicas (...), mas também todos os procedimentos"[256], devendo o responsável ponderar o custo-benefício durante todo o ciclo de vida do tratamento[257], demonstrando que agiu com lealdade, licitude, transparência, integridade e confidencialidade.

Para as empresas com mais de 250 trabalhadores, ou aquelas que tratam dados sensíveis, e as que permanentemente realizem operações de tratamento (nomeadamente em razão do tipo de atividade empresarial), é exigido registo escrito e atualizado de operações. Ele deve ser mantido em segurança, evitando-se riscos de utilização indevida ou vazamento, e registrar: finalidades; categorias; destinatários; prazo de guarda e, quando possível, medidas técnicas e de segurança[258].

É, assim, um meio de "accountability"[259] e de prova que, juntamente à "avaliação de Impacto", se mostra relevante diante da ausência de autorização prévia e das penalidades possíveis.

---

[254] Artigo 25 do RGPD, *op. cit.*
[255] *Idem*.
[256] PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, p. 400.
[257] *Idem*, p. 401.
[258] Artigo 30 do RGPD, *op. cit.*
[259] No âmbito do RGPD, 'accountability' poderia ser vista como a exigência de implementação de "um programa capaz de monitorizar a conformidade em toda a organização, e demonstrar às autoridades e aos titulares que as informações pessoais que tratam estão seguras. In:http://www.openlimits.pt/pt/thinking-ahead-blog/glossario-rgpd-regulamento-europeu-protecao-dados/?all=1.

Enquanto o registro facilita a fiscalização e comprovação de cumprimento da Lei, a avaliação prévia busca identificar e minimizar riscos, sendo realizada antes do início da atividade. Será útil, em especial, quando o tratamento utilizar novas tecnologias ou apresentar potencial restrição de direitos e liberdades fundamentais[260], como no uso de dados sensíveis.

Vemos, aqui, a alteração na lógica de responsabilização. Antes, a autoridade nacional dava seu parecer sobre a possiblidade de realização do tratamento, avaliando, de antemão, seu *design*/conceito e possíveis impactos. Agora, temos um leque de medidas que o responsável realiza, à sua discrição, assumindo as consequências do resultado.

Como meio auxiliar de verificação da conformidade, em especial no que diz respeito à identificação de riscos, probabilidade e gravidade de danos, bem como à identificação de melhores práticas, foi incentivado no RGPD a criação de códigos de conduta e certificações, que dependem de aprovação da APD [261].

As associações e organismos representes de categorias, além dos certificadores, trabalharão em conjunto com as autoridades de controle para construir patamares de proteção e promover técnicas seguras de tratamento, incentivando os responsáveis a mudar seu comportamento[262]. E, dentro desta composição heterogênea de conformidade legal, temos o encarregado de dados pessoais, que abordaremos no próximo tópico (2.3.2).

b. Medidas de "accountability" na LGPD

Na LGPD, a responsabilização e prestação de contas é um princípio, que exige a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"[263].

---

[260] Artigo 35.1 do RGPD, *op. cit*.
[261] Considerando 77 do RGPD, *op. cit*.
[262] Esse tema foi abordado na Seção 5 do RGPD "Códigos de conduta e certificação", entre os artigos 40 e 43. O tópico não será extensamente trabalhado porque, como veremos, não está presente da mesma forma na LGPD e não fará, portanto, parte importante da atuação da autoridade brasileira, objetivo deste trabalho.
[263] Artigo 6º, inciso X da Lei nº 13.709, *op. cit*. Outros princípios visando a segurança das atividades foram normatizados nos incisos VII e VIII do mesmo artigo, como o da necessidade de "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais", e o princípio da segurança, que requer "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".

O conceito de *privacy by design* está no artigo 46 da Lei, que requer que a adoção das medidas de segurança seja observada "desde a fase de concepção do produto ou do serviço até a sua execução"[264]. O conceito de *privacy by default* está entremeado em dois princípios: adequação e necessidade, que exigem tratamento compatível com, e limitado às finalidades informadas ao titular, além do uso de dados pertinentes, proporcionais e não excessivos.

O registro de operações é requerido especialmente quando o tratamento se basear no legítimo interesse[265], se estendendo a todas as empresas. Acreditamos que a autoridade de controle deve regulamentar a questão para restringir esta obrigação a apenas um grupo de empresas, como foi feito no âmbito europeu, já que seu impacto em pequenas e médias empresas que tratam dados ocasionalmente é desproporcional ao benefício auferido[266]. O normativo poderia, ainda, detalhar o que deverá haver neste registro, noção que foi omitida na LGPD[267].

Outra diferença entre os normativos analisados reside sobre a "avaliação de Impacto". Enquanto o RGPD a requer antes do início da atividade de alto risco, por iniciativa do responsável, a LGPD determina que a ANPD poderá requisitá-la do controlador[268]. A redação do artigo 38 não informa se seria um estudo prévio, visando mitigar riscos, algo semelhante à autorização prévia, ou se será decorrente de reclamação contra a empresa.

As duas normas também se afastam em relação aos códigos de conduta e certificações. Estas últimas não estão previstas na LGPD, enquanto os códigos foram tratados à título de "regras de boas práticas e de governança", que apenas "poderão" ser

---

[264] Artigo 46, § 2º da Lei nº 13.709, *op. cit.*

[265] Artigo 37 da Lei nº 13.709, *op. cit*.

[266] No Brasil existe a figura de micro e pequenas empresas, além de microempreendedores individuais. Eles somam 6,4 milhões de estabelecimentos e respondem por 52% dos empregos formais no setor privado. In: http://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD.

[267] Como dissemos anteriormente, o RGPD requer um registro com o nome e os contatos do responsável pelo tratamento e do encarregado da proteção de dados, além das finalidades do tratamento e a descrição das categorias de titulares e de dados pessoais, dos destinatários a quem foram ou serão divulgados e as transferências. Adicionalmente, se possível, os prazos previstos para o apagamento das diferentes categorias de dados e das medidas técnicas e organizativas no domínio da segurança para prevenir violações.

[268] Este "relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados". In: Artigo 38, § único, da Lei nº 13.709, *op. cit*.

reconhecidas e divulgadas pela autoridade de controle[269]. Ou seja, poderá haver códigos estruturados pelos controladores, individualmente ou por meio de associações, sem que haja aval ou mesmo conhecimento da ANPD[270].

Nos parece que, no caso brasileiro, diferentemente do RGPD, o que se previu foram códigos internos, à exemplo dos programas de *compliance*, que foram introduzidos pela Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira[271].

Estes programas de *compliance* são avaliados e sopesados na aplicação de sanções[272], sendo sua efetividade indispensável para a realização do "acordo de leniência", capaz de reduzir as multas em até dois terços do seu valor original.

Também na LGPD, a adoção de boas práticas e medidas de governança serão levadas em conta quando da aplicação da multa, mas não há indicação de percentuais de redução. O grande incentivo seria a expectativa de reduzir a "culpabilidade" do controlador e, consequentemente, o valor da sanção.

Apesar do RGPD também considerar o cumprimento de códigos de conduta e processos de certificação na imposição de coimas[273], nos parece que sua estrutura é mais apropriada para promover maior conformidade legal e incentivar a efetividade do normativo, enquanto que no Brasil a tendência é que sejam adotados códigos *pro forma*, visando apenas reduzir a penalização pecuniária, caso haja violação.

---

[269] Outro peso tem esta prática no âmbito europeu, uma vez que os códigos de conduta são elaborados pelos Estados-Membros, autoridades de controle, Comité e Comissão, ou ainda por associações e outros organismos representantes de setores específicos.

[270] O programa de governança em privacidade deve, no mínimo: demonstrar o comprometimento do controlador em adotar processos de proteção, sendo aplicável a todo o conjunto de dados pessoais que estejam sob seu controle; estar de acordo com sua estrutura, escala, tipo e volume de operações; estabelecer políticas de avaliação sistemática de impactos e riscos à privacidade; estar integrado a sua estrutura geral de governança e estabelecer relação de confiança com o titular dos dados; dispor de planos de resposta a incidentes e remediação e estar sempre atualizado. In: Artigo 50, I, da Lei nº 13.709, *op. cit*.

[271] BRASIL. *Lei nº 12.846*, de 1º de agosto de 2013.

[272] O artigo 7º, inciso VIII da Lei nº 12.846, *op. cit*., fala da "existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica".

[273] Artigo 83, 2, j, do RGPD, *op. cit*.

2.3.2. Encarregado da proteção de dados

a. encarregado da proteção de dados no RGPD

A figura de encarregado de proteção de dados[274] não existia na Diretiva 95/46/CE, mas já era prevista em diferentes países, como a Alemanha[275]. A partir da entrada em vigor do RGPD, deverão designar um encarregado da proteção de dados: autoridades públicas[276]; empresas cuja operação implique em tratamento de dados que, devido à sua natureza, âmbito e/ou finalidade, exijam controle regular e sistemático em grande escala; e empresas que tratem dados sensíveis ou relacionados com condenações penais e infrações[277].

O encarregado pode ser um empregado ou uma empresa especializada[278], para uma única entidade ou para todo o grupo empresarial, desde que nele tenha fácil acesso a todos os estabelecimentos. O mesmo acontece para organismos públicos, respeitando-se sua estrutura organizacional e dimensão[279].

Ele deve ter conhecimentos de Direito e de práticas de proteção de dados[280], desempenhando seu papel com isenção, sem receber instruções relativamente ao exercício das suas funções[281]. Além disso, precisa ser "envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais"[282].

Isso não quer dizer, contudo, que tenha poderes de direção ou comando. À título de exemplo, ele deve dar, obrigatoriamente, parecer nas avaliações de impacto realizadas pela entidade, mas suas fundamentações e conclusões não são vinculantes[283].

Para garantir sua independência, não poderá ser destituído ou penalizado por exercer suas atribuições, se reportando diretamente a direção de mais alto nível da

[274] Previsto no artigo 37 do RGPD, *op. cit*.
[275] POLIDO, Fabrício B. Pasquot et al. *op. cit.,* p. 19.
[276] Com exceção dos tribunais no exercício da sua função jurisdicional. Porém, estes mesmos tribunais precisam nomear um encarregado para o exercício de outras funções. In: artigo 32.1 do RGPD, *op. cit*.
[277] Considerando 97 do RGPD, *op. cit*.
[278] com base num contrato de prestação de serviços.
[279] Artigo 37 do RGPD, *op. cit*.
[280] Artigo 37.5 do RGPD, *op. cit*.
[281] Artigo 38.3 do RGPD, *op. cit*.
[282] Artigo 38.1 do RGPD, *op. cit*.
[283] Artigo 35.2 do RGPD, *op. cit*.

entidade. Deve guardar sigilo e confidencialidade, se preservando de conflitos de interesses[284].

Cabe ao encarregado: supervisionar e monitorar a atuação da empresa em relação às obrigações do RGDP; elaborar relatórios de conformidade; realizar treinamentos; ser consultado, quando cabível, sobre a avaliação de impacto; cooperar e servir de ponto de contato diante da autoridade de controle[285].

Terá, portanto, três funções básicas: fomentador da conformidade legal; auditor das atividades de tratamento; e interlocutor (perante autoridades administrativas). Assim, não se deve confundir o encarregado com uma consultoria especializada[286], nem com o advogado que irá patrocinar causas da empresa ou órgão público[287].

b. encarregado da proteção de dados na LGPD

Papel similar ao do encarregado de dados no RGPD pode ser encontrado no Brasil entre os *compliance officers*, responsáveis pela prevenção da corrupção em empresas, que se difundiu com a entrada em vigor da Lei nº 12.846 de 2013.

Contudo, a LGPD traz apenas como funções do encarregado[288] a comunicação com os titulares e com a autoridade nacional; e a orientação de funcionários e terceirizados do controlador a respeito de práticas de proteção de dados[289]. Se possibilita que ele execute outras atribuições, determinadas pelo controlador ou por normas complementares.

O papel reduzido dado ao encarregado pela lei brasileira pode representar mais custos para a empresa do que benefícios a direitos dos titulares. Ademais, a LGPD deixou para a ANPD estabelecer as "hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento"[290].

---

[284] Artigo 38 do RGPD, *op. cit*.
[285] Artigo 39 do RGPD, *op. cit*.
[286] PINHEIRO, Alexandre Sousa (coord.), *op. cit.*, p. 472.
[287] *Idem,* p. 477.
[288] O texto original da LGPD requeria que o encarregado fosse uma pessoa natural, sendo esta exigência excluída pela redação dada pela Medida Provisória nº 869, de 2018. Tal alteração facilita o processo de contratação, mas também retira o caráter personalíssimo deste encarregado, o que pode ter reflexos tanto no contato com a autoridade nacional, como em processos de responsabilização.
[289] Artigo 41, § 2º da Lei nº 12.846, *op. cit*.
[290] Artigo 41, § 3º da Lei nº 12.846, *op. cit*.

Deveria tal regulamento ser um dos primeiros atos da ANPD, a fim de se evitar que pequenas empresas que tratam dados com pouca frequência tenham que incorrer nos custos de contratação de um encarregado, que deveria ser um profissional altamente especializado[291]. Neste ponto, acreditamos que essa mesma normativa também poderia, a exemplo do RGPD, elencar requisitos ou conhecimentos que deve ter o encarregado para exercer suas funções.

2.3.3. Multas e penalidades

a. Multas e penalidades no RGPD

Como já mencionamos, o RGPD traz como um de seus paradigmas a responsabilização, fazendo com que a proteção de dados pessoais passe a ser um "corporate risk"[292], uma vez que o custo da violação pode ser elevado.

São duas vertentes de responsabilidade: a primeira reside na possibilidade de o titular acionar judicialmente o responsável, demonstrando os pressupostos da responsabilidade civil: ato ilícito, culpa/dolo, dano e nexo causal (artigo 82.1 do RGPD)[293]. A segunda repousa na possibilidade de aplicação de penalidades administrativas para os casos de violação[294], devendo elas serem efetivas, proporcionais e dissuasivas[295].

Consoante as circunstâncias de cada caso, as APD poderão: emitir advertências sobre a suscetibilidade de um tratamento violar o RGPD; retirar ou ordenar ao organismo de certificação que retire ou deixe de emitir uma certificação; impor coima ou limitação temporária ou definitiva ao tratamento; ou proibir e suspender o envio de dados para países terceiros ou organizações internacionais[296].

---

[291] Pela extensão continental do Brasil e pela pouca especialização no tema, acredita-se ainda que a medida seria salutar no caso de pequenas empresas localizadas em estados de menor porte, onde um profissional com os requisitos necessários deverá ser escasso, ao menos nos primeiros anos da entrada em vigor da Lei.
[292] POLIDO, Fabrício B. Pasquot et al. *op. cit.,* p. 11.
[293] Diz o citado artigo que: "Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos".
[294] O artigo 84 do RGPD prevê que os Estados-Membros podem estabelecer outras sanções aplicáveis aos casos de violação do regulamento, nomeadamente às violações que não são sujeitas a coimas.
[295] Artigo 83.1 do RGPD, *op. cit*.
[296] Artigo 58 do RGPD, *op. cit*.

Em relação às multas, na apreciação do caso individual, deve-se considerar: a natureza, a gravidade e a duração da infração; a natureza, objetivo e número de titulares afetados pelo tratamento; o dolo ou culpa; as medidas de atenuação ou suspensão de danos e as medidas de segurança adotadas; além da reincidência e grau de cooperação com a autoridade de controle[297].

Outros fatores, como o implemento de códigos de conduta aprovados ou de procedimentos de certificação poderão ser sopeados, assim como outros fatores agravantes e atenuantes verificados na análise do caso concreto[298].

Em relação ao valor das sanções, serão quantificadas cada violação realizada, mas o montante é limitado ao especificado para a violação mais grave dentro do âmbito das mesmas operações de tratamento ou de operações ligadas entre si[299].

O teto valorativo foi dividido em dois blocos: o primeiro prevê coimas de até €10 milhões ou 2% do total do faturamento anual global no exercício financeiro anterior, o que se aplica para os atos de descumprimento considerados menos gravosos, como a violação de medidas técnicas e a não designação de um encarregado[300]. O segundo impõe a penalização em até €20 milhões ou 4% do total do faturamento anual mundial no exercício anterior, por violações aos princípios básicos do tratamento, incluindo o consentimento, e direitos do titular (estabelecidos nos artigos 5º, 6º, 7º, 9º, 12 a 22, 44 a 49 do RGPD)[301].

Este procedimento deve se sujeitar às garantias processuais adequadas, e permitir revisão judicial em processo equitativo[302].

---

[297] Artigo 83.2 do RGPD, *op. cit*.
[298] *Idem.*
[299] As multas menos gravosas poderão ser aplicadas aos organismos de certificação e supervisão, no caso de descumprimento das regras pertinentes a si, e as multas mais gravosas poderão incidir quando há violação das obrigações do capítulo IX, relativo a situações específicas, como o tratamento de dados laborais, que poderão ser reguladas pelos Estados-Membros. Estas também poderão abranger o incumprimento de uma ordem de limitação ou suspensão emitida pela autoridade de controle.
[300] O patamar é aplicável para a efetiva ou potencial violação dos direitos estabelecidos nos artigos 8º, 11, 25, 39, 42 e 43 do RGPD. Ver: Artigo 83.4 do RGPD, *op. cit*.
[301] Artigo 83.5 do RGPD, *op. cit*.
[302] Artigo 83.8 do RGPD, *op. cit*.

b. Multas e penalidades na LGPD

A LGPD não define "violação de dados pessoais", mas traz conceito parecido ao do RGPD no princípio da segurança, que decreta a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"[303].

Temos, aqui também, a possibilidade de responsabilização por danos causados "de modo acidental ou ilícito", ou seja, não há necessidade de comprovar dolo ou intenção. A LGPD considera irregular o tratamento quando não observada a legislação, e quando não fornecer segurança ao titular dos dados, seja pelo modo ou técnicas usados no tratamento, seja pelos resultados e riscos que dele se esperam[304]. Só não haverá responsabilidade em caso de "culpa exclusiva do titular dos dados ou de terceiros"[305].

Para as entidades privadas, haverá responsabilização civil e aplicação de sanções administrativas pela autoridade de controle[306], dentre as quais estão: advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% do faturamento da empresa, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos e limitada a R$ 50.000.000,00 por infração; multa diária, observado o limite da multa simples; publicização da infração após confirmação de sua ocorrência; e bloqueio e eliminação dos dados pessoais a que se refere a infração[307].

Alguns apontamentos são válidos: primeiro, nos parece possível o uso de advertência no lugar de outras penalidades, já que se usou o termo "medidas corretivas"[308]. Ainda, existe a possibilidade de aplicação de multas diárias, a fim de fazer

[303] Artigo 6º, caput e inciso VII, da Lei nº 12.846, *op. cit*.
[304] Artigo 44 da Lei nº 12.846, *op. cit*.
[305] Artigo 43 da Lei nº 12.846, *op. cit*.
[306] Qualquer sanção deve ser precedida de procedimento administrativo que possibilite a oportunidade da ampla defesa. Os procedimentos se basearão em critérios de: I - gravidade e a natureza das infrações e dos direitos pessoais afetados; II - boa-fé do infrator; III - vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - reincidência; VI - grau do dano; VII - cooperação; VIII - adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano; IX - adoção de política de boas práticas e governança; X - pronta adoção de medidas corretivas; e XI - proporcionalidade entre a gravidade da falta e a intensidade da sanção.
[307] Artigo 52 da Lei nº 12.846, *op. cit*. O mesmo artigo, em seu § 2º, dispõe que estas penalidades não substituem a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.
[308] Diferente é o caso do RGPD que fala especificamente em "advertências sobre a suscetibilidade de um tratamento violar o RGPD".

cessar a atividade de violação, devendo descrever a "obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa"[309].

Ademais, na sua última revisão, ocorrida em 2019, foi acrescido o §7º ao artigo 52 da LGPD, que passou a admitir conciliação direta entre controlador e titular em casos de vazamento individual ou acessos não autorizados, excluindo outras penalidades caso haja acordo.

Em outro, no Brasil, existe apenas um teto de valor para as multas, que corresponde à menor faixa do RGPD em termos percentuais. Também se determinou que a ANPD crie um regulamento, que deverá ser objeto de consulta pública, explicando as metodologias que orientarão o cálculo do valor-base das multas[310], de forma objetiva e com dosimetria de cálculo[311].

Por fim, a previsão de responsabilização para o setor público é consideravelmente diferente do antevisto no RGPD. O controle consistirá na possibilidade de a ANPD solicitar dados sobre as operações de tratamento realizadas, especificamente sobre o âmbito e a natureza dos dados, podendo emitir parecer técnico para promover o cumprimento da Lei. Em caso de violação, poderá enviar informe com medidas cabíveis para cessá-la, e solicitar a publicação de relatórios de impacto, sugerindo a adoção de boas práticas.

Ou seja, não haverá qualquer penalização. Aliás, a depender de como será estruturada a autoridade de controle, poderá lhe faltar hierarquia para que seus pedidos sejam atendidos e suas sugestões acatadas.

[309] Artigo 54, § único, da Lei nº 12.846, *op. cit*.
[310] Artigo 53 da Lei nº 12.846, *op. cit*.
[311] Artigo 53, § 1º da Lei nº 12.846, *op. cit*.

Capítulo 3 - Autoridades de proteção de dados e a efetividade do regime jurídico

Neste capítulo, vamos, primeiro, traçar uma discussão conceitual sobre a estrutura da norma jurídica e os mecanismos de *enforcement* e *compliance* que tratam do problema da efetividade (3.1), para depois analisar o papel das autoridades de controle europeias, com foco em sua constituição, autonomia e funções (3.2). A partir dos exemplos examinados, vamos traçar um perfil da autoridade brasileira, já criada, mas ainda não constituída, sugerindo alterações legislativas que permitam melhor desempenho, e a conformidade com os parâmetros postos pelo Comité Europeu de Proteção de Dados (CEPD) para autorizar o intercâmbio internacional de dados (3.3).

3.1. *Enforcement, compliance* e efetividade das normas jurídicas

A efetividade das normas deveria ser a regra, já que o Direito é um instrumento determinador da conduta social. Contudo, nem sempre as normas são eficazes (3.1.1), e por isso se fazem necessários instrumentos e órgãos de controle que buscam monitorar sua aplicação e sancionar os incumprimentos (3.1.2)[312].

3.1.1. Entre o ser e o dever ser: o problema da efetividade das normas jurídicas

O mundo jurídico não importa em um campo de causalidade fática, mas em uma ordem de validade, que é o plano do *dever ser*[313]. Contudo, mesmo sendo abstrata enquanto ditadora de hipóteses, a norma incide no plano físico, quando o seu suporte

[312] Apesar deste tópico trazer uma visão mais positivista do Direito, de base kelseniana, entendemos que existem outras concepções jurídicas importantes, que questionam fundamentos do Direito procurando aproximá-lo de soluções mais justas. Esperamos ter mostrado, ao longo desta tese, que nos apoiamos largamente nestas discussões, sobretudo, na linha do exposto por José de Oliveira Ascensão, de que os princípios são orientações das quais se depreendem, não apenas o complexo legal, mas toda a ordem jurídica. Ou seja, eles estruturam o ordenamento, gerando consequências concretas, tendo marcada função para a sociedade, de promover o Direito com base na dignidade da pessoa, que é o seu fim último. (In: ASCENSÃO, José de Oliveira. *Introdução à ciência do Direito*. Rio de Janeiro: Renovar, 3ª Edição, 2005, p. 404). Esperamos também ter demonstrado, que os princípios constitucionais e os direitos humanos fundamentais são sempre os parâmetros primeiros a serem utilizados na análise de qualquer caso concreto, uma vez que eles sustentam a integridade da ordem jurídica, e por isso um trabalho sistemático de interpretação é fundamental, para "reencontramos a realidade do sistema" e enquadrar situações buscando um resultado mais justo. (ver mais sobre esta análise e sobre críticas e proposições a respeito do direito alternativo em: ASCENSÃO, José de Oliveira. *Direito alternativo*. Acesso em 27/11/2019.
In:http://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Ascensao-Jose-Oliveira-DIREITO-ALTERNATIVO.pdf

[313] MELLO, Marcos Bernardes. *Teoria do Fato Jurídico: plano da existência*. São Paulo: Saraiva, 2003, p. 13.

fático se concretiza. Assim, ela, normalmente, dita regras que devem ser ou acontecer[314], e é sobre esse tipo normativo que vamos discorrer nas próximas páginas.

O verbo "dever" traz ato programado para ser executado, sendo o *dever ser* uma norma válida e vigente, que vincula os destinatários[315]. O ato de vontade que a satisfaz *é,* representando o *ser*. Vale, entretanto, ressaltar que as normas são hipotéticas, porque só se aplicam quando se produz um facto que corresponda à previsão. Explica-se: se for instituído que determinado ato constitui um crime, a regra não se aplica automaticamente, tendo que haver a ação humana ali descrita para que a incidência da norma ocorra. Isso significa que a aplicação de uma regra está sempre dependente da verificação de certos pressupostos[316].

O Direito é, neste viés, um sistema de normas ideais, de princípios-guia para a ação social[317], não limitado à descrição da realidade. "Se assim não fosse, seria desnecessária a regra, pois não haveria sentido algum em impor-se, por via legal, algo que ordinária e invariavelmente já ocorre"[318].

Mas, a intenção do legislador é sempre ver a norma aplicada, concretizando os objetivos pretendidos quando de sua criação. Consequentemente, a efetividade ou eficácia social pode ser conceituada como a coincidência do comportamento social com os modelos e padrões traçados pelas normas jurídicas[319], sendo um mínimo de efetividade requisito forçoso para que o conjunto seja válido[320].

Acontece que, nem sempre, há consenso entre a norma e os valores sociais, o que é agravado em temas novos ou polêmicos, uma vez que a comunidade é formada de indivíduos e grupos com enormes diferenças culturais, físicas, políticas, sociais e jurídicas.

---

[314] José de Oliveira Ascensão pondera que a maior parte das regras tem função orientadora de condutas humanas, mas há casos em que esse escopo está completamente ausente, como quando as regras produzem efeitos jurídicos automáticos, são retroativas ou tratam de outras normas, revogando-as ou suspendendo-as. In: ASCENSÃO, José de oliveira. *O Direito. Introdução e Teoria Geral. Uma perspectiva Luso-Brasileira*. Lisboa: Fundação Calouste Gulbenkian, 1984, pp. 181 e 182.

[315]KELSEN, Hans. *Teoria pura do Direito*. São Paulo: Martins Fontes, 1999, pp. 5 a 9.

[316] ASCENSÃO, José de oliveira. *O Direito. Introdução e Teoria Geral. Uma perspectiva Luso-Brasileira*, *op. cit.,* p. 185.

[317]A elaboração de normas do dever-ser, mesmo que não cheguem a se concretizar, tem a sua função de orientação, de coordenação dos valores que são esperados da sociedade. In: BARROSO, Luís Roberto. *O direito constitucional e a efetividade de suas normas: limites e possibilidades da Constituição Brasileira*. Rio de Janeiro: Renovar, 2003, p. 75.

[318] KELSEN, Hans, *op. cit.*, p. 174.

[319]MELLO, Marcos Bernardes. *op. cit.,* pp. 13 e 14; e KELSEN, Hans. *op. cit.*, pp. 11, 29 e 30.

[320]KELSEN, Hans. *op. cit.*, p. 174.

Não faltam exemplos de leis ou tratados que, embora em vigor, não se concretizam, permanecendo, por assim dizer, "no limbo da normatividade abstrata"[321].

Em razão deste antagonismo, são previstas as sanções[322], que buscam reforçar a exigência do comando legal. Junto a elas, deve o Direito buscar outros meios ou mecanismos de efetividade, como a criação de normas com limites razoáveis de alcance e execução; que se coadunem com as regras e valores de ao menos parte da sociedade; com proposições claras e objetivos bem definidos[323].

A força não é o fim do Direito, apesar de poder aumentar sua eficácia social em determinados casos[324], desde que seja acompanhada de instituições, políticas públicas, ações e procedimentos capazes de fazer atuar concretamente os comandos normativos[325]. Ou seja, é necessário que o jogo real de poder permita que suas disposições sejam cumpridas, não dependendo de situações ótimas para se concretizarem[326]. É importante, pois, que se combinem mecanismos de *compliance*[327] e *enforcement* para dar maior efetividade ao regime.

3.1.2. *Compliance* e *enforcement* na proteção de dados

Como vimos acima, a efetividade das normas "tem um caráter experimental, porquanto se refere ao cumprimento efetivo do direito por parte de uma sociedade, ao 'reconhecimento' do Direito pela comunidade, ou mais particularmente, aos efeitos de

[321]REALE, Miguel. *Lições Preliminares do Direito*. São Paulo: Bushatsky, 1974, p. 125.

[322]Pensar em um regime sendo válido somente na condição de ele ser totalmente efetivo é incorrer no erro de confundir a validade de uma norma com a sua eficácia social, ou, como diz Kelsen, descrever o Direito como um enunciado do ser e não do dever ser.

[323] Não sendo necessário, contudo, a sanção em sua acepção tradicional. O fato de a norma prever uma sanção ou consequência para o seu descumprimento não dá a ela um caráter de alternativa, ou seja, de opção entre a adimplência ou inadimplência. Muito pelo contrário, "a hipoteticidade da norma expressa a objetividade de um valor a ser atingido, e, ao mesmo tempo, se salvaguarda o valor da liberdade do destinatário, ainda que para a prática de um ato de violação". In: BARROSO, Luís Roberto. *op. cit.*, p. 89.

[324]BOBBIO, Norberto. *Teoria do Ordenamento jurídico*. Brasília: UNB, 1997, pp. 65 e 66.

[325]BARROSO, Luís Roberto. *op. cit.*, p. 280.

[326]SILVA NETO, Manoel Jorge E. *O princípio da máxima efetividade e a interpretação constitucional*. São Paulo: LTR, 1999, p. 18.

[327] Sobre a "*compliance*", cumpre ressaltar, desde logo, conforme ponderação de Pedro Romano Martinez, que alude mais a diretrizes de conduta, a "boas práticas", do que a condutas jurídicas devidas. Para que essas medidas sejam devidas, se faz necessária sua juridificação. Contudo, a razão de tratamos do tema, repousa em nosso entendimento de que as APDs não devem somente impor sanções, mas também, e principalmente, promover meios de cumprimento das regras de proteção de dados. Por ser um direito humano fundamental, o mais importante é que as liberdades do titular sejam conquistadas, e seus dados preservados, e não que haja sanções ou penalizações ao controlador.

uma regra suscitada através do cumprimento"[328]. Dessa maneira, a efetividade não será somente o meio pela qual são executadas as leis, mas também a sua correspondência com a finalidade para a qual foram cunhadas.

O conceito de c*ompliance* vem ganhando espaço no mundo jurídico para indicar as medidas necessárias para o cumprimento de uma lei por uma empresa ou Estado (no caso de um tratado)[329]. Ele define a conformidade para com o regime normativo, ou seja, a aplicabilidade das condutas impostas pela norma, o que geralmente requer medidas econômicas e administrativas[330].

Por vezes, as medidas de *compliance* são definidas em lei, quando se detalham ações que promovem melhor cumprimento da regra, ou seja, quando se delimita um conjunto de práticas que pode levar à execução a contento dos objetivos legais. Esta é a razão pela qual a ideia tem ganhando espaço no âmbito de grandes empresas e em regimes normativos que envolvem *corporate risks*.

As principais causas de não-*compliance* são a falta de comprometimento ou concordância com as regras, a falta de diligência na aplicação e a falta de recursos. O comprometimento pode ser reforçado pela pressão da sociedade civil e dos Estados. A diligência, normalmente relacionada à complexidade da lei e a novidade das medidas que impõe, pode ser direcionada por códigos de conduta e boas práticas. Já o impacto financeiro, sopesado pelo agente na análise custo-benefício de cumprir a lei, tem como remédio a imposição de sanções.

Assim, os mecanismos de *compliance* laboram como um modelo de gerenciamento de atividades para cumprir as regras e evitar ou reduzir as penalizações. Já os mecanismos de *enforcement,* podem ser vistos como a capacidade do Estado de monitorar os casos de desconformidade e punir os responsáveis. Ou seja, são medidas com poder de "compelir" a execução normativa[331], ou ao menos, tentar aprimorar sua efetividade. As sanções nem sempre são necessárias, ou bem-vindas, mas entendemos que, quando existirem, devem

[328] Para Reale, em uma comparação com a sua teoria tridimensional do direito, a vigência representa a norma, a eficácia social representa o fato e o fundamento da norma representa o seu valor. In: REALE, Miguel. *op. cit.*, p. 126.
[329] WEISS, Edith Brown e JACOBSON, Harold K. op. cit., p. 4 e 5.
[330] WOLFRUM, Rudiger. *Recueil des Cours : Collected Courses.* Volume 272, Hague Academy of International Law, 1998, p. 29.
[331] SHELTON, Dinah. *Techniques and Procedures in International Environment Law*. Geneva: UNITAR – United Nations Institute for Training and Research, Course 3, 2. ed., 2004, p. 105.

estar acompanhadas de medidas de incentivo, para fomentar que o cumprimento da lei seja mais interessante do que o risco de seu incumprimento. Um bom sistema de controle administrativo pode também reduzir as disputas judiciais e promover maior segurança jurídica aos atores.

No campo da proteção de dados, as autoridades de controle têm essa dupla função: incentivar os mecanismos de c*ompliance* e aplicar medidas de *enforcement*. Destarte, os membros das APDs devem ser capazes e independentes. E a autoridade ser concebida para se adaptar às mudanças econômicas, tecnológicas e científicas, mantendo agenda flexível e compreensiva de ações, servindo como *fórum* especializado na interpretação das regras, para torná-las mais objetivas e realizáveis, mas sempre com foco na promoção de direitos e liberdades fundamentais, pois a dignidade é a base que sustenta o regime.

3.2. Autoridades europeias de proteção de dados

As autoridades de controle são órgãos com poderes de investigação, correção, promoção e aperfeiçoamento das normas de proteção de dados pessoais[332], que servem como consultores dos Estados e seus órgãos, visando a coerência da aplicação do RGPD.

Nesta tese, iremos analisar duas APDs com o objetivo de conhecer suas características essenciais, e poder sugerir adequações à autoridade de controle brasileira. Escolhemos analisar a Autoridade Europeia para a Proteção de Dados (3.2.1) e a autoridade portuguesa (3.2.2). A primeira, em razão de sua atuação não depender de estruturas e políticas internas de um Estado; a segunda, pela proximidade do direito brasileiro e português, e por ser o país de realização deste pós-doutoramento.

3.2.1. Autoridade Europeia para a Proteção de Dados (AEPD)

Dentro do sistema europeu de proteção de dados, temos três tipos de autoridades de controle. O primeiro é a Autoridade Europeia para a Proteção de Dados (AEPD), que monitora a tutela de dados nas instituições e órgãos da UE. O segundo, são as autoridades dos diferentes países que compõe a União Europeia e que tem competência dentro de seus respectivos territórios. Por último, temos o Comité Europeu de Proteção de Dados

[332] FAZENDEIRO, Ana, *op. cit.*, p. 10.

(CEPD)[333], constituído pelas autoridades de controle dos Estados e pela AEPD, e que tem por missão contribuir para a aplicação coerente do RGPD entre eles[334].

a) composição e autonomia

A Autoridade Europeia para a Proteção de Dados, criada em 2004, é uma entidade supervisora independente[335], que fiscaliza o cumprimento do Regulamento UE 2018/1725, de 23 de outubro de 2018[336], pelas instituições e órgãos da UE[337].

A AEPD visa ser um centro de excelência para a execução e fortalecimento das normas de proteção de dados e da vida privada, e por isso propõe recomendações, soluções práticas e orientações estratégicas para responder aos desafios que impactem seu tema de atuação[338].

É uma instituição independente[339], situada em Bruxelas/Bélgica, e presidida por um supervisor e um adjunto, com apoio de secretariado composto de advogados, especialistas em tecnologia da informação e administradores, somando, em média, 60 funcionários. O mandato dos dirigentes é de cinco anos, renováveis[340].

---

[333] O CEPD era anteriormente conhecido como Grupo de Trabalho do artigo 29. Tem estatuto de organismo da UE dotado de personalidade jurídica e possui secretariado independente. Dispõe de poderes para decidir litígios entre as autoridades de controle nacionais e prestar aconselhamento e orientação sobre o RGPD.

[334] Mais especificamente, são atribuições do CEPD: emitir *guidelines*, recomendações e boas práticas para clarear o escopo do RGPD; servir de conselheiro para a Comissão Europeia no que tange à proteção de dados pessoais, podendo propor legislações; adotar *consistency findings* para casos transnacionais; promover cooperação e compartilhamento de informações e boas práticas entre as APDs; criar relatar suas atividades para o público e para o Parlamento, Conselho e Comissão Europeia.

[335] In:https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor-pt. Acesso em 11/11/2019.

[336] Regulamento UE 2018/1725, do Parlamento Europeu e do Conselho de 23 de outubro de 2018 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n. 45/2001 e a Decisão n. 1247/2002/CE.

[337] São Instituições da UE: Parlamento; Conselho Europeu; Conselho da União Europeia; Comissão Europeia; Tribunal de Justiça da União Europeia; Banco Central Europeu; Tribunal de Contas; Serviço Europeu para a Ação Externa; Comité Económico e Social; Comité das Regiões; Banco Europeu de Investimento; Provedor de Justiça; AEPD, in: https://europa.eu/european-union/about-eu/institutions-bodies-pt.

[338] In: https://edps.europa.eu/about-edps-en. Acesso em 11/11/2019.

[339] Um aspecto importante a se destacar é a necessidade de independência das autoridades de controle, prevista nos artigos 16.2 do Tratado de funcionamento da UE (TFEU), no artigo 8.3 da Carta de Direitos Fundamentais e capítulo VI do RGPD. Para ser independente, deve preservar sua capacidade decisória sem que haja influência externa direta ou indireta.

[340] In:https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor-pt. Acesso em 11/11/2019.

As instituições europeias devem apontar um encarregado da proteção de dados[341] que assegure, de maneira independente, que o órgão cumpra as disposições legais[342]. Os desafios para sua independência são apontados pela AEPD: estrutura hierárquica e clima organizacional da instituição; expectativas de colegas de trabalho, especialmente os mais sensíveis ao tema; e capacidade de propor soluções que sirvam como *benchmark* para outras instituições, já que deve haver uma aplicação coesa do regulamento[343].

Conta com dois institutos principais: «supervisão e aplicação», que avalia a *compliance* dos órgãos europeus; e «política e consulta»[344], órgão de assessoria. O setor de tecnologia da informação subsidia sua função de monitorar novas tecnologias suscetíveis de ter impacto em matéria de proteção de dados[345].

b) Função consultiva

Dentro de sua missão consultiva, a AEPD aconselha as instituições e os organismos da UE sobre o tratamento, políticas e legislação de dados pessoais, trabalhando com as autoridades nacionais para garantir coerência na aplicação do RGPD entre os Estados-Membros.

Ela pode aconselhar, sob demanda ou por iniciativa própria, as instituições e órgãos da UE, que devem-na informar sobre a elaboração de medidas administrativas e regras internas relativas ao tratamento de dados pessoais que queiram adotar[346]. Também responde a consultas da Comissão Europeia sobre propostas legislativas[347] e execução de

[341] A AEPD tem o seu encarregado, que colabora com as demais intuições sob a égide do Regulamento UE 2018/1725.In:https://edps.europa.eu/about/data-protection-within-edps/data-protection-officer-edps_en

[342] As instituições são responsáveis por manter registro das atividades de tratamento, devendo os encarregados serem consultados sobre ele. Um estudo interessante traz *guidelines* sobre o perfil do encarregado em órgãos públicos, acesso em 11/11/2019.
In: https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf.

[343]As funções dos encarregados serão tratadas por normativo da AEPD, que está sendo construído com base em estudos sobre o tema.
Destaca-se: https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf.

[344]In:https://edps.europa.eu/about/data-protection-within-edps/data-protection-officer-edps_en, acesso em 11/11/2019.

[345] Outros setores que compõe o órgão são: setor de comunicação e informação; recursos humanos e administração; setor de arquivo e suporte técnico.

[346] Artigo 41 do Regulamento UE 2018/1725, *op. cit.*

[347] As opiniões formais são publicadas em seu website e nos jornais oficiais europeus, além de enviadas aos órgãos legislativos competentes. In: https://edps.europa.eu/data-protection/our-role-advisor-en

outros normativos[348]. Pode atuar perante a Corte de Justiça como interveniente[349] e dar indicações sobre a interpretação dos normativos de proteção de dados[350].

c) Função de supervisão

A função de supervisão permite que a AEPD processe queixas e conduza inquéritos, além de supervisionar as atividades de tratamento dentro das instituições da UE, que abrangem diversos assuntos, como segurança alimentar, prevenção de doenças e estabilidade financeira[351]. Também supervisiona a Europol, responsável por cooperar com autoridades policiais e judiciárias no combate internacional ao crime e ao terrorismo.

A supervisão inclui a investigação de reclamações, resposta a consultas e auditorias. As consultas são dirigidas ao encarregado de proteção de dados da AEDP, e serão respondidas por escrito em forma de opiniões, comentários, decisões, cartas ou *papers*, e de maneira verbal por meio de uma *hotline*[352].

As reclamações podem ser realizadas por indivíduos, que as devem primeiro remeter aos responsáveis pelo tratamento na instância onde pensam que foi cometida a violação, seguido do encarregado da instituição ou do organismo da UE responsável. Se a diligência não tiver resultado satisfatório, pode apresentar queixa à AEPD, que investigará o caso, informado o titular de sua decisão quanto ao fundamento da queixa e da forma de corrigir a situação[353]. Já os inquéritos, podem ser abertos por meio de denúncias ou informações recebidas de terceiros, do órgão que cometeu a infração[354], ou por iniciativa da AEPD.

As penalidades são: advertência, com imposição de medidas a serem cumpridas para sanar a violação; ou imposição de restrições temporárias ou definitivas a uma

[348] Caso a normativa em análise possa ter grande impacto sobre direitos pessoais, a Autoridade Europeia e o Comité Europeu para a Proteção de Dados devem se coordenar e emitir parecer comum em até oito semanas. In: Art. 42.2do Regulamento UE 2018/1725, *op. cit.*

[349] Em 17 de março de 2005, na decisão conhecida como "PNR-cases", a CJUE reconheceu o direito da AEDP de intervir em todos os casos relativos ao processamento de dados pessoais, não sendo ela limitada aos casos em que o uso de dados se deu por órgãos europeus. Acesso em 11/11/2019, In: https://edps.europa.eu/data-protection/data-protection/case-law-and-guidance_en.

[350] In: https://edps.europa.eu/data-protection_en. Acesso em 11/11/2019.

[351] In: https://edps.europa.eu/data-protection/our-role-supervisor_en. Acesso em 11/11/2019.

[352] *Idem.*

[353] A decisão poderá ser contestada judicialmente no Tribunal de Justiça da UE.

[354] Desde 12/12/2018, quando houver riscos elevados, as violações devem ser notificadas dentro de 72 horas para a AEDP e para os titulares.

atividade de tratamento de dados específica. Em casos mais graves, poderá impor multa, ou referir o caso para o TJUE.

d) Função de promoção/aperfeiçoamento

A AEPD deve promover ações educativas, como a publicação de artigos, *guidelines*, opiniões, consultas e decisões, além de oferecer opinião técnica a respeito das tecnologias que acompanha e que trazem riscos aos dados pessoais[355]. Dentre suas metas está o desenvolvimento de um repositório eletrônico com informações sobre proteção de dados, e a promoção de treinamentos de melhores práticas para os órgãos da UE[356].

Na divulgação das estratégias da AEPD para o quadriênio 2015-2020, foi ressaltado que sua missão não se atém a fomentar o *compliance* normativo, pois o verdadeiro objetivo do regime é promover uma alteração de paradigma e consolidar a cultura de *accountability* para com os direitos fundamentais[357].

Adicionalmente, a AEPD divide com as autoridades nacionais a supervisão de sistemas de tecnologia da informação que detém grandes quantidades de dados pessoais[358], como é o caso do Eurodac, que possui mais de duas milhões de impressões digitais; ou o sistema VIS, que monitora milhões de pedidos de vistos por ano[359]. A coordenação é realizada em reuniões bianuais, e podem incluir a partilha de informações, assistência mútua na realização de auditorias e inspeções, exame das dificuldades de interpretação ou de aplicação do RPGD e proposição de soluções harmonizadas sobre problemas comuns[360].

3.2.2. Comissão Nacional de Protecção de Dados (CNPD) - Portugal

A proteção dos dados pessoais foi inserida na Constituição da República Portuguesa (artigo 35º) em 1976, tendo sido regulamentada 15 anos depois, pela Lei 10/91 de 29 de

---

[355] In: https://edps.europa.eu/data-protection_en, acesso em 11/11/2019.
[356] A agenda de treinamentos da AEPD é bem extensa e pode ser conferida aqui: https://edps.europa.eu/about-edps/members-mission/agenda_en. Acesso em 11/11/2019.
[357]"EDPS Strategy 2015-2019", discurso de Giovanni Buttarelli, proferido em Bruxelas em 2/32015, in: https://edps.europa.eu/node/334, acesso em 11/11/2019.
[358] As atividades de cooperação estão previstas nos artigos 61 e 62 do Regulamento UE 2018/1725, que traz a necessidade de partilhar informações relevantes e de cooperar ativamente para "assegurar uma supervisão eficaz dos sistemas informáticos de grande escala e dos órgãos e organismos da União".
[359] In: https://edps.europa.eu/data-protection/supervision-coordination_en, acesso em 11/11/2019.
[360] Artigo 62 do Regulamento UE 2018/1725, *op. cit*.

abril, que sofreu alterações com a publicação da Lei 28/94 de 29 de agosto[361]. Foi somente então, em 7 de janeiro de 1994, que teve início o mandato da Comissão Nacional de Proteção de Dados Pessoais Informatizados – CNPDPI, cuja independência administrativa foi consagrada pela revisão constitucional de 1997[362].

Com a promulgação da Lei 67/98 de 26 de outubro[363], que transpôs a Diretiva 95/46/CE, o leque de atribuições e competências da Comissão foi alargado, e seu nome alterado para *Comissão Nacional de Protecção de Dados* - CNPD[364]. A Lei nº 58/2019, que entrou em vigor em 9 de agosto de 2019[365], adaptou a legislação portuguesa ao RGPD, destacando em seu capítulo segundo a composição, independência e atribuições da Comissão, como veremos a seguir.

a) Composição e autonomia

A CNPD é uma entidade administrativa independente, com poderes de autoridade, que funciona junto à Assembleia da República[366]. Ela é composta de sete membros, todos com mandatos de cinco anos, renováveis uma vez[367].

A independência no exercício das funções e poderes da APD é considerado "elemento essencial" para uma efetiva proteção de dados pelo RGPD[368], que também ressalta a importância de que seus membros só sejam exonerados em razão de falta grave, ou se tiverem deixado de cumprir as obrigações exigidas para o exercício de seus cargos[369].

---

[361] In: https://www.cnpd.pt/bin/cnpd/historia.htm. Acesso em 11/11/2019.
[362] *Idem.*
[363] A Lei 67/98 de 26 de outubro (PORTUGAL. *Lei 67/98, de 26 de outubro*. Publicada no Diário da República n.º 247/1998, Série I-A de 1998-10-26) revogou as leis 10/91 e 28/94.
[364] Novas atribuições foram dadas à CNPD com a publicação de leis específicas, como a Lei 69/98 (Posteriormente revogada pela Lei 41/2004, de 18 de Agosto) que transpôs a Diretiva de telecomunicações (Diretiva 97/66/CE) e Lei 2/94 de 19 de Fevereiro (dados pessoais relativas ao espaço Schengen) e Lei 68/98, de 26 de Outubro (Europol). In: https://www.cnpd.pt/bin/cnpd/historia.htm. Acesso em 11/11/2019.
[365] PORTUGAL. Lei n.º 58/2019, de 8 de agosto, publicada no Diário da República n.º 151/2019, Série I de 2019-08-08.
[366] Artigo 4.1 da Lei n.º 58/2019, *op. cit*.
[367] O artigo 5.º da Lei 58/2019 deixa em aberto a composição e funcionamento da CNDP: "A composição, o modo de designação e o estatuto remuneratório dos membros da CNPD, bem como a respetiva orgânica e quadro de pessoal, são aprovados por lei da Assembleia da República".
[368] Considerando 117 do RGPD, *op. cit.*
[369] 53.4 do RGPD, *op. cit.*

Os membros da CNPD são inamovíveis, exercendo mandatos a termo fixo, que serão perdidos apenas em razão de incapacidade[370] ou incompatibilidade[371]. São faltas graves a ausência, no mesmo ano civil, a três reuniões consecutivas ou seis interpoladas sem motivo justificado, ou a não observância do sigilo profissional[372]. Deles se requer que não pratiquem atividades, remuneradas ou não, incompatíveis com o mandato assumido, com exceção da atividade de docência no ensino superior e de investigação[373].

A independência também é resguardada pela dotação administrativa e financeira autônomas[374], tendo a lei garantido à CNPD "independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos"[375].

Conforme dita o RGPD, os membros da autoridade de controle devem ser escolhidos por processo definido em lei[376], e em razão de suas habilitações, experiência e conhecimentos técnicos, nomeadamente no domínio da proteção de dados pessoais[377].

A legislação portuguesa definiu um método de escolha plural, pelo qual o presidente e dois vogais são eleitos pela Assembleia da República; um magistrado judicial, com mais de 10 anos de carreira, designado pelo Conselho Superior da Magistratura; um magistrado do Ministério Público, com mais de 10 anos de carreira, designado pelo Conselho Superior do Ministério Público e dois vogais designados pelo Governo[378].

De acordo com o RGPD, parte da independência das autoridades de controle nacionais está em ser isenta de influências externas ou instruções de *outrem*, inclusive em

---

[370] Além das hipóteses de perda, é previsto o término precoce do mandato em caso de morte ou impossibilidade física permanente ou que ultrapasse o termo do mandato, e a renúncia. In: Artigo 5º da Lei 43/2004, *op. cit*.

[371] Artigo 5.4 da Lei n.º 58/2019, *op. cit.,* assim dispõe: "Os membros da CNPD ficam sujeitos ao regime de incompatibilidades estabelecido para os titulares de altos cargos públicos, não podendo, durante o seu mandato, desempenhar outra atividade, remunerada ou não, com exceção da atividade de docência no ensino superior e de investigação".

[372] Artigo 7 e 8º da Lei 43/2004, *op. cit*.

[373] Artigo 4.4 da Lei n.º 58/2019, *op. cit*. Alexandre de Sousa Pinheiro acredita que a disposição também deve se aplicar a atividades desenvolvidas em associações ou outro tipo de pessoas coletivas. In: PINHEIRO, Alexandre Sousa (coord.). *op. cit.*, p.538.

[374] artigo 5.º da Lei n.º 58/2019, *op. cit*.

[375] *Idem.*

[376] Considerando 121 do RGPD, *op. cit.*

[377] Artigo 53 do RGPD, *op. cit.*

[378] Para ser membros da CNPD, deve o cidadão se encontrar em pleno gozo dos seus direitos civis e políticos. Dados sobre e a atual composição da CNPD pode ser encontra no link: https://www.cnpd.pt/bin/cnpd/composicao.htm

relação ao seu próprio pessoal, que deve ficar sob sua "direção exclusiva"[379]. O quadro de pessoal da CNPD conta com 32 funções previstas em lei[380], sendo divididas em serviços de apoio administrativo, Informação e Relações Internacionais, Informática e Inspeção, e setor de processos[381], além de um gabinete de Atendimento ao Público[382].

A Comissão funciona em carácter permanente, em Lisboa, e realizada reuniões ordinárias e extraordinárias. As reuniões não são públicas, mas o presidente pode, com o acordo da Comissão, convidar qualquer pessoa cuja presença seja considerada útil a participar, salvo na fase decisória[383].

Suas deliberações são tomadas pela maioria dos membros presentes, tendo o presidente voto de qualidade[384]. Individualmente, poderá o membro da Comissão arquivar as reclamações, queixas e petições manifestamente infundadas que lhe tenham sido distribuídas[385].

b) Função consultiva

Dentre suas atribuições, compete à CNPD aconselhar os órgãos e instituições portuguesas a respeito das medidas legislativas e administrativas relacionadas com o tratamento de dados pessoais[386].

Segundo o RGPD, a autoridade de controle pode emitir, por iniciativa própria ou se solicitado, pareceres dirigidos aos poderes legislativo ou executivo do Estado-Membro, bem como a outras instituições e organismos, ou ao público, sobre assuntos relacionados com a proteção de dados pessoais[387]. Também deve prestar informações aos titulares[388].

---

[379] Artigo 52 do RGPD, *op. cit*.
[380] In: https://www.cnpd.pt/bin/cnpd/QuadroCNPD.pdf. Acesso em 10/07/2019.
[381] O considerando 120 do RGPD afirma que "Deverão ser dados às autoridades de controlo os recursos financeiros e humanos, as instalações e as infraestruturas necessárias ao desempenho eficaz das suas atribuições, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo da União".
[382] Segundo o artigo 22 da Lei 43/2004: "1- A CNPD dispõe de serviços de apoio próprios. 2 — Os serviços de apoio compreendem: Serviço Jurídico (SJ); b) Serviço de Informação e Relações Internacionais (SIRI); c) Serviço de Informática e Inspecção (SII); d) Serviço de Apoio Administrativo e Financeiro (SAAF)".
[383] Artigo 13º da Lei 43/2004, *op. cit*.
[384] Artigo 15º da Lei 43/2004, *op. cit*.
[385] Artigo 17.4 da Lei 43/2004, *op. cit*.
[386] Art. 57.1 – c, do RGPD, *op. cit.*, e artigo 6.1 da Lei n.º 58/2019, *op. cit*.
[387] Art. 58: 3, d, do RGPD, *op. cit.*
[388] Art. 57.1, e, do RGPD, *op. cit.*

A Lei 58/2019 conferiu à CNPD a atribuição de se pronunciar, a título não vinculativo, sobre as medidas legais e demais instrumentos jurídicos relativos à proteção de dados pessoais[389]. Uma análise numérica aponta a importância desta função, já que foram 59 pareceres emitidos em 2018[390] e 56 até o dia 13 de novembro de 2019[391]. Como a proteção de dados é um tema relativamente novo e de contornos, por vezes, não tão bem definidos, esta função de orientação sobre a compatibilidade de lei, projeto de lei ou política pública é indispensável para o sucesso do regime.

Outra função consultiva prevista no RGPD solicita da APD a elaboração de cláusulas contratuais-tipo[392], uma lista de exigências para as avaliações de impacto[393] e orientações sobre operações onde os responsáveis não identificaram ou atenuaram suficientemente potenciais riscos[394]. A CNPD, complementarmente, publica em seu *website*, além da lista de tratamentos sujeitos ou não a avaliação de impacto[395], critérios do que entende como "elevado risco"[396].

Durante o interstício da entrada em vigor do RGPD e a publicação da Lei 58/2019, em que a Lei 67/98 continuou a vigorar, a CNPD emitiu diversos posicionamentos sobre a compatibilidade dos normativos, como a substituição de autorizações prévias[397] pelas avaliações de impacto; e a necessidade de as empresas revisarem se o consentimento obtido foi expresso e necessário para o objeto do contrato, já que, diante da negativa, nova autorização seria indispensável[398].

Nota-se que a função consultiva pode e deve ser exercida de forma simples e direta. A CNPD utiliza recurso já conhecido, mas bastante eficaz: "perguntas frequentes". É uma

---

[389] Tanto no nível interno, como no europeu e internacional. Artigo 6.º, 1, a da Lei 58/2019, *op.* cit.
[390] In:https://www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2018&segunda_escolha=40. Acesso em 10/07/2019.
[391] In:https://www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2019&segunda_escolha=40. Acesso em 13/11/2019.
[392] Estas cláusulas são utilizadas nos casos de subcontratação e transferência de dados para um país terceiro ou organização internacional. In: Art. 57.1, j, do RGPD, *op. cit.*
[393] Art. 57.1, k, do RGPD, *op. cit.*
[394] Art. 57.1 – I do RGPD, *op. cit*. Prevê o artigo 36 do mesmo Regulamento que deve o responsável pelo tratamento consultar a autoridade de controle antes de proceder ao tratamento quando a avaliação de impacto indicar elevado risco. Quando a autoridade considerar que o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, deverá dar orientações, por escrito, ao responsável.
[395] O que não impede sua realização por iniciativa dos responsáveis. In: art. 7 da Lei 58/2019, *op. cit.*
[396] Artigo 6.1, c, da Lei 58/2019, *op. cit.*
[397] Lei 67/98*, op. cit.*, artigo 22.
[398] artigo 13º do RGPD, *op. cit.*

ferramenta que permite consulta rápida dos interessados, ajudando a prevenir casos de descumprimento da Lei por desconhecimento ou dúvidas. Uma das respostas da CNPD deixa claro que é dispensado o consentimento dos trabalhadores no âmbito da gestão administrativa ou de processamento de remunerações, já que se trata de execução do contrato de trabalho[399].

Em uma esfera mais formal, a CNPD emite diretrizes/deliberações para orientar os responsáveis sobre diferentes questões[400]. Um exemplo interessante é a disponibilização de dados de alunos em *websites* de estabelecimentos de ensino. A prática vem se tornando usual, pois permite contato mais direto, célere e econômico entre escola e sociedade. No entanto, pode afetar direitos, liberdades e garantias dos titulares, especialmente de crianças[401].

Nesta feita, a CNPD emitiu orientação, em 2016, para que estes dados fossem armazenados em áreas reservadas, e as informações separadas de acordo com a finalidade[402]. Asseverou que o consentimento era necessário para recolha de imagens, e mesmo assim, deveria ser avaliado os riscos/impactos de sua disponibilização[403].

Em 2018, o tema voltou a ser debatido na Comissão[404], mas sob a perspectiva da disponibilização de informação pessoal de estudantes, professores e servidores de estabelecimentos de ensino[405].

---

[399] Sobre este ponto, lembra a Comissão que "o consentimento dos trabalhadores não é de uma maneira geral considerado válido, pois raramente poderá ser dado em condições de liberdade, atendendo ao desequilíbrio entre as partes". https://www.cnpd.pt/bin/faqs/faqs.htm. Acesso em 10/07/2019.

[400] A CNPD tem importante papel no que tange a orientar ao púbico sobre o tratamento de dados pessoais, sejam os titulares deste direito ou as entidades que tratam estes dados. Até 2017, ou seja, anteriormente à entrada em vigor do RPGD, emitiu orientações sobre: Saúde; Trabalho; Acesso a dados pessoais; Educação; Informação de crédito; Fluxos internacionais; Videovigilância; Marketing político e eleitores; Novas tecnologias; Dados Manuais e Telecomunicações.

[401] In: www.cnpd.pt/bin/orientacoes/DEL_1495_2016_dados_alunos_Internet.pdf, acesso em 10/07/2019.

[402] Políticas como: mecanismos de autenticação; gestão de utilizadores e de atribuição de perfis que garantam a confidencialidade das transmissões de dados e o registo dos acessos (logs).

[403] Lembrando que se deve aplicar sempre o princípio do interesse superior das crianças.
In: https://www.cnpd.pt/bin/orientacoes/DEL_1495_2016_dados_alunos_Internet.pdf

[404] In:https://www.cnpd.pt/bin/decisoes/Diretrizes/Diretriz_1_2018_disponibilizacao_dados_on-line_instituicoes_ensino_superior.pdf. Acesso em 10/07/2019.

[405] Diante da Lei de Acesso à Informação brasileira, e da política adotada desde então de ampla disponibilização dos dados pessoais de servidores e daqueles que, de alguma forma, recebem recursos públicos, o tema se apresenta de especial interesse para o nosso objeto de pesquisa.

Inicialmente, aponta a CNPD que se trata de um equilíbrio de interesses entre o princípio da transparência e da minimização de dados pessoais[406], cuja conciliação impõe a opção "pela divulgação agregada ou anonimizada"[407]. Ou seja, não se deve deixar de promover ampla transparência, especialmente quando há recursos públicos envolvidos, pois a gestão financeira do Estado deve passar pelo controle social, mas ela deve ser executada de forma a minimizar riscos e restrições de direitos dos titulares.

Como exemplo, somente devem ser disponibilizadas *on-line* as informações (como nome e contatos) dos principais órgãos dirigentes da organização, e dos serviços de atendimento ao público (v.g., secretaria, biblioteca). Os dados dos demais docentes e servidores deve ser reservado aos estudantes e funcionários da instituição[408].

Pelo mesmo argumento, expõe que as decisões sancionatórias não devem ser tornadas públicas, já que nem a função punitiva, nem a função pedagógica/preventiva da medida disciplinar parecem exigir mais do que a aplicação da sanção e a sua notificação ao destinatário, sendo certo que a divulgação implicaria em restrição desnecessária e excessiva do direito à proteção de dados pessoais[409].

As duas deliberações acima foram aprovadas em sessão plenária da Comissão que, como vimos anteriormente, deve ser realizada por consenso.

Outras deliberações, como a n.º 923/2016, foi adotada pela Presidente da Comissão, de forma singular[410], indicando que os empregadores não devem facultar aos solicitadores e agentes de execução dados pessoais constantes do recibo de vencimento de seus trabalhadores, mesmo que sejam partes em processo judicial de natureza civil. Nestes casos, o acesso é restrito a informações relativas ao vencimento líquido, ilíquido e penhoras[411]. Desta forma, aplica-se concretamente o princípio da minimização dos dados pessoais, que não importa na negação de compartilhamento diante de uma justificativa

---

[406] Foi promovida ampla consulta pública para entender os diferentes pontos de vista sob as questões expostas no parecer.

[407] In:https://www.cnpd.pt/bin/decisoes/Diretrizes/Diretriz_1_2018_disponibilizacao_dados_on-line_instituicoes_ensino_superior.pdf

[408] *Idem.*

[409] *Ibidem.*

[410] In: https://www.cnpd.pt/bin/orientacoes/DEL_923_2016.pdf. Acesso em 10/07/2019.

[411] *Idem.*

legal, mas na ponderação de direitos, somente sendo informados os dados relevantes para o objetivo perseguido.

Duas decisões recentes da CNPD no âmbito interpretativo podem ter grande impacto no regime de proteção de dados em Portugal.

A primeira, determina que a dispensa de aplicação de coimas pelo prazo de três anos para as entidades públicas, previstas na Lei 58/2019[412], não pode ser dada em abstrato. Diante de várias solicitações, disse a Comissão que o pedido fundamentado deve ser requerido somente após a acusação de uma contraordenação, quando se sopesariam os interesses e direitos conflitantes na situação concreta[413].

A segunda, bastante polêmica, mas determinante para que o RGPD cumpra sua função de salvaguardar os direitos do titular e assegurar o primado do direito da União Europeia, trata-se da decisão de não aplicar algumas disposições da Lei 58/2019, que, segundo entende a CNPD, manifestamente restringem, contrariam ou comprometem o efeito útil e a plena efetividade do RGPD[414].

c) Função de supervisão

Cumpre também à CNPD o controle e fiscalização do cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais no Estado português[415]. Para isso, deve receber e tratar reclamações apresentadas pelos titulares, e realizar investigações[416], sancionando casos de incumprimento, sendo que as decisões de natureza contraordenacional podem ser arguidas perante os tribunais administrativos[417].

[412] Artigo 44.2 da Lei 58/2019, *op. cit.*
[413] In: https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_495.pdf. Acesso em 13/11/2019.
[414] São elas: Artigo 2.º, nº 1 e 2; Artigo 20.º, nº 1; Artigo 23.º; Artigo 28.º, nº 3, alínea a; Artigo 37.º, nº 1, alíneas a), h) e k), e n.º 2; Artigo 38.º, nº 1, alínea b), e nº 2; Artigo 39.º, nº 1 e 3; Artigo 61.º, nº 2 e Artigo 62.º, nº 2. In: https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_494.pdf. Acesso em 13/11/2019.
[415] Artigo 5.4 e 6.1 b. da Lei 58/2019, *op. cit.*
[416] Considerando 122 do RGPD, *op. cit.*
[417] Artigo 34.º da Lei 58/2019, *op. cit.*

Em Portugal, o titular pode fazer cumprir os seus direitos na esfera administrativa[418], sem prejuízo de apresentação de queixa à CNPD[419], por meio de tutela petitória ou impugnatória, ou por meio da responsabilidade civil que decorre do tratamento ilícito de dados ou outras violações ao RGPD e à lei 58/2019[420].

A CNPD já concluiu um caso de contraordenação em que foi o próprio titular que realizou queixa[421], sob a alegação de que o responsável deixou de fornecer cópia de duas ligações entre as partes, tendo apagado a primeira delas diante da intercorrência do prazo de 90 dias desde sua gravação.

A empresa alegou que não havia conseguido identificar o solicitante como titular no tempo oportuno, mas, durante a instrução processual, a CNPD teve acesso a cópia de um e-mail do encarregado em que o responsável instruía a que cópias de ligação telefônica somente fossem oferecidas mediante ordem judicial ou pedido de um organismo oficial. Uma multa de 20.000 euros foi aplicada pela violação do artigo 15º, nº 1[422].

Em regra, as deliberações da CNPD nos casos de contraordenação são publicadas sem citar o nome das partes. Nada obstante, a Lei portuguesa faculta, nos casos de crime ou coima superior a € 100.000, que se dê publicidade à condenação no Portal do Cidadão, com a identificação do agente, os elementos da infração e as sanções, por período não inferior a 90 dias[423].

---

[418] Diz o artigo 32 da Lei 58/2019: "Sem prejuízo do direito de apresentação de queixa à CNPD, qualquer pessoa pode recorrer a meios de tutela administrativa, designadamente de cariz petitório ou impugnatório, para garantir o cumprimento das disposições legais em matéria de proteção de dados pessoais, nos termos previstos no Código do Procedimento Administrativo".

[419] Artigo 35 da Lei 58/2019: "Sem prejuízo da observância das regras relativas ao patrocínio judiciário, o titular dos dados tem o direito de mandatar um organismo, uma organização ou uma associação sem fins lucrativos constituída em conformidade com o direito nacional, cujos fins estatutários sejam de interesse público e cuja atividade abranja a defesa dos direitos, liberdades e garantias do titular dos dados quanto à proteção de dados pessoais para, em seu nome, exercer os direitos previstos nos artigos 77.º, 78.º, 79.º e 82.º do RGPD".

[420] Artigo 33.º da Lei 58/2019, *op. cit*.

[421] Processo 2018/10778, cuja decisão está disponível em: https://www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2019&segunda_escolha=20.

[422] Artigo 15º do RGPD, *op. cit.*: "Direito de acesso do titular dos dados: 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais (...)".

[423] Artigo 56 da Lei 58/2019, *op. cit*.

Assim como no RGPD[424], a lei portuguesa dividiu as violações em duas categorias. O artigo 37º trata das contraordenações muito graves[425], como a não observância dolosa dos princípios do RGDP e tratamentos sem consentimento ou outra base legal. O artigo 38º trata das contraordenações graves, que são aplicadas para violações de medidas técnicas e organizativas[426].

Dentre as disposições da Lei 58/2019 questionadas pela CNPD, conforme vimos no tópico acima, três tratam de contraordenações. A primeira vincula a não observância dos princípios do RGPD a uma atividade dolosa, o que contraria o disposto no próprio RGPD, artigo 83, que não diferencia dolo e culpa para que haja uma violação, sendo a intenção do responsável levada em conta apenas para fins de quantificação da penalidade.

A segunda se refere ao enquadramento do incumprimento das decisões da CNPD na moldura mais gravosa, sendo que no RGPD seria ele sancionado na moldura menos gravosa. A terceira traz relativização do valor das sanções de acordo com a dimensão e natureza da pessoa coletiva, ou pelo fato de se tratar de uma pessoa singular[427].

Em todos os três casos, entende a CNPD que não poderia o legislador nacional modificar o RGPD, que pretende uniformizar as regras de proteção de dados no âmbito europeu, não podendo a lei nacional reduzir ou mudar sua aplicabilidade[428].

---

[424] O artigo 83 do RGPD estabelece duas categorias de violação, sujeitas a multas de até 10 milhões de euros ou 2% do volume de negócios anual a nível mundial para os casos considerados menos graves e até 20 milhões de euros ou 4% do volume de negócios na categoria considerada mais gravosa.

[425] São elas: inobservância dolosa dos princípios do artigo 5.º do RGDP ; tratamentos sem base em consentimento ou outra condição de legitimidade (artigo 6.º do RGPD); incumprimento das regras de consentimento (artigo 7.º do RGPD) , de dados sensíveis (artigo 9.º do RGPD) ou relacionados com condenações penais e infrações (artigo 10.º do RGPD); que exijam pagamento (à exceção dos infundados ou excessivos, nomeadamente de caráter repetitivo, em que o responsável pode cobrar taxa razoável para cobrir custos administrativos); não prestação de informação sobre as finalidades, destinatários ou direito de retirar o consentimento (artigos 13.º e 14.º do RGPD); não permitir, não assegurar ou dificultar o exercício de direitos (artigos 15.º a 18.º e 19.º a 22.º do RGPD); violação dos requisitos de transferência internacional (artigos 44.º a 49.º do RGPD); incumprimento das decisões da autoridade de controlo ou recusa da colaboração e violação das regras de pessoal da CNPD.

[426] Como a proteção de dados desde a conceção e por defeito; violações nos casos de subcontratação; designação e garantias do encarregado de proteção de dados e questões relativas a códigos de conduta e utilização de selos ou marcas. In: Artigo 38 da Lei 58/2019, *op. cit*.

[427] Para as contraordenações mais graves, o artigo 37.2 cria o seguinte parâmetro para as sanções: grandes empresas - entre € 5.000 a € 20 milhões ou 4% do volume de negócios anual; PME - de € 2.000 a € 2 milhões ou 4% do volume de negócios anual; e entre € 1.000 a € 500.000 no caso de pessoas singulares. Para as contraordenações graves, o artigo 38.2 prevê: de €2500 a € 10 000 000 ou 2% do volume de negócios anual para grandes empresas; de € 1000 a € 1 000 000 ou 2% do volume de negócios para PME e entre € 500 a € 250 000, no caso de pessoas singulares. In: Lei 58/2019, *op. cit*.

[428] A não ser em casos em que o próprio RGPD disponha que poderá o Estado-Membro editais tais regras.

Como regra geral, deve a CNPD utilizar os critérios do artigo 83º, 1, a-k do RGPD para avaliar a gravidade da infração e determinar o valor das sanções de forma individualizada[429]. Vejamos um caso concreto apreciado em 9 de outubro de 2018, que tratou de falha na concepção de sistemas de informação em estabelecimentos médico-hospitalares.

A Comissão, inicialmente, invalidou o argumento da dificuldade de se determinar *a priori* o tipo de informação necessária para cada perfil de acesso, estabelecendo que houve dolo eventual na conduta, já que a entidade sabia das limitações de seu sistema. Como fator agravante, foi constatado descumprimento de medidas de segurança (auditoria fiável), e o alto risco do tratamento (dados de saúde), cujo dano potencial alcançou várias dezenas de milhares de titulares. Como fator atenuante, reconheceu-se que o monitoramento dos *logs* de acesso não dependia da arguida, que mitigou os danos desde a inspeção realizada pela CNPD.

Valorados os critérios, aplicou duas penalidades de 150.000 euros pela prática das contraordenações do artigo 5º, 1, al. c e f; e uma de 100.000 euros pela violação dos artigos 32º, 1, b e d, e artigo 83º, 4, a.3, totalizando uma coima de 400.000 euros. Cada violação foi avaliada em relação aos critérios do artigo 83 (atenuantes e agravantes), mas recebeu sanção individualizada, que ficou aquém do limite máximo estabelecido pelo RGPD.

A Lei 58/2019 estabeleceu um critério adicional, para que se considere a situação econômica da entidade na definição do montante da coima. Não foram detalhados como estes aspectos devem ser avaliados, mas é um ponto que deve ser destacado, já que um balanço deficitário não deveria justificar pena menor.

A CNPD analisou dois casos relativos a sistemas de videovigilância sem notificação visível, encaminhados pela Polícia de Segurança Pública[430]. Em um deles, a empresa alegou dificuldades financeiras. Contudo, a Comissão elencou como fatores para determinar o valor da sanção: a ilicitude média; não se tratar de dados sensíveis; ter sido praticado por negligência; e não haver benefício econômico resultante da prática.

[429] In: https://www.cnpd.pt/bin/decisoes/Delib/20_984_2018.pdf. Acesso em 5/10/2019.
[430] Deliberação 2019/207: www.cnpd.pt/bin/decisoes/Delib/DEL_2019_207.pdf.
Deliberação 2019/222: www.cnpd.pt/bin/decisoes/Delib/DEL_2019_222.pdf.

Assim, apesar de ser infração punível com a moldura mais grave prevista no RGPD, e não ter havido notificação da própria arguida, as multas em ambos os casos foram fixadas em 2.000 euros. Como a empresa que alegou estar em situação econômica precária não ofereceu qualquer prova a este respeito, não houve atenuação do valor da coima.

Em relação ao destino das multas, a Lei 58/2019 fixou que 40% seja revertida para CNPD e os outros 60% para o Estado[431]. No Brasil, se discute se isto poderia representar um incentivo à aplicação de penalidades, já que o órgão poderia, caso necessitasse de maior financiamento, comprometer, em alguma medida, sua imparcialidade.

É uma discussão pertinente, porquanto ambas correntes apresentam argumentos válidos. De um lado, poder-se-ia considerar a economia para o Estado, já que a entidade passa a ser mantida, ao menos parcialmente, pelos valores que arrecada, crescendo em estrutura e projetos à medida que sua atuação for se ampliando. De outro, a dependência de recursos casuísticos pode afetar a estrutura básica do órgão, na ausência de violações ou penalidades, além do já citado incentivo, mesmo que de forma implícita, à aplicação de sanções (maiores).

Por fim, um dos pontos mais críticos em relação à nova Lei portuguesa foi a opção de que o processamento de fato que for, ao mesmo tempo, crime e contraordenação, seja realizado pela autoridade criminal - Ministério Público. Se trata de um possível esvaziamento das competências da CNPD, uma vez que constitui crime diferentes atos de violação previstos no RGPD, como o uso incompatível com a finalidade da recolha; o acesso indevido e o desvio, a viciação, inserção falsa e a destruição de dados; além do dever de sigilo[432].

Entendemos que a disposição contraria o RGPD, já que ele afirma que nos casos de violação caberá reclamação à autoridade de controle, cuja atuação será independente. Ainda, parece-nos que uma entidade especializada na proteção de dados pode estar mais apta a responder aos desafios tecnológicos que perpassam a questão, e fornecer resposta mais rápida do que um procedimento criminal.

[431] Artigo 42.º da Lei 58/2019, *op. cit*.
[432] Os crimes estão elencados na Seção III da Lei 58/2019, *op. cit*.

O melhor seria manter os dois órgãos atuando de forma harmônica, segundo o princípio da independência das instâncias. Caberia à CNPD investigar as violações e atuar dentro de suas competências administrativas, enviando sua análise, conclusões e provas obtidas ao Ministério Público, quando haja suspeita de atividade criminosa[433].

d) Função de promoção/aperfeiçoamento

Chamamos de função de cooperação, promoção ou aperfeiçoamento todas as ações da autoridade de controle que visam sensibilizar o público para riscos, regras, garantias e direitos associados ao tratamento de dados pessoais[434], bem como as atividades de orientação e aprovação de códigos de conduta[435] e demais medidas para efeitos de comprovação da conformidade das operações de tratamento com o regime de proteção de dados[436].

Como estudamos no capítulo dois, as atividades de certificação e de aprovação de códigos de conduta não estão previstas na Lei brasileira (LGPD), e por isso não iremos nos aprofundar neste estudo. O mesmo vale para os deveres de colaboração da CNPD para com os órgãos e entidades europeus e demais APDs.

Contudo, gostaríamos de ressaltar que a Lei 58/2019 previu, em seu artigo 8º, um dever de colaboração das entidades públicas e privadas para com a CNPD, facultando-lhe as informações solicitadas no exercício das suas atribuições e competências, especialmente em relação ao exame de sistemas informáticos e ficheiros de dados pessoais, bem como toda a documentação relativa ao tratamento e transmissão de dados[437].

As campanhas educativas e de cooperação com outros órgãos são informadas pela CNPD nos seus planos de atividades anuais. Sem embargo, os documentos não trazem detalhes que permitam exame mais aprofundado. Mas, ressalta-se que a Comissão

[433] A Lei 58/2019, manteve como atribuições da CNPD intervir em processos judiciais no caso de violações à proteção de dados e denunciar ao Ministério Público as infrações penais de que tiver conhecimento no exercício de suas funções, bem como praticar atos cautelares para assegurar os meios de prova.
[434] Considerando 122 do RGPD, *op. cit*.
[435] Nos termos do artigo 40.5 do RGPD, *op. cit.*
[436] A lei 58/2019, *op. cit.,* definiu como autoridade competente para a acreditação dos organismos de certificação em matéria de proteção de dados é o Instituto Português de Acreditação - IPAC, I.P. (art. 14,1).
[437] Artigo 8.2 da Lei 58/2019, *op. cit.*

organiza, desde 2015, a Revista Fórum, que busca ampliar conhecimentos sobre privacidade e proteção de dados.

3.3. Autoridade brasileira de proteção de dados

Antes mesmo de sua entrada em vigor, a LGPD já passou por duas revisões, majoritariamente baseadas no arranjo institucional da Autoridade Nacional de Proteção de Dados (ANPD). A versão aprovada inicialmente no Congresso Nacional, criava uma entidade com natureza de autarquia especial, vinculada ao Ministério da Justiça, que gozaria de independência administrativa e técnica, com mandato a termo fixo para os dirigentes e autonomia financeira.

No entanto, a Lei possuía vício de iniciativa, já que a Constituição Federal, em seu artigo 61, §1°, II, afirma que são de iniciativa privativa do Presidente da República as leis que disponham sobre a criação, estruturação e atribuições dos órgãos da administração pública e seus cargos e funções. Ainda, não poderia o projeto de lei ter criado gastos não previstos no orçamento.

O Presidente poderia ter mantido a estrutura da ANPD por Medida Provisória (sanando o vício de iniciativa), mas preferiu modificá-la[438]. Em 27 de dezembro de 2018, foi editada a Medida Provisória n° 869, que trouxe novo formato para a ANPD[439], tendo alguns de seus pontos sido revisados na alteração de 8 de julho de 2019[440].

3.3.1. Composição e autonomia

a) Estrutura atual da ANPD

A versão atual da LGPD dispõe que a ANPD será criada sem aumento de despesas[441], e integrará a Presidência da República. Sua natureza jurídica é transitória, pois poderá ser submetida ao regime autárquico especial em até dois anos da entrada em vigor de sua estrutura regimental. Por enquanto, o órgão máximo da Autoridade é o Conselho Diretor,

[438] Em 14 de agosto de 2018, foram vetados os artigos 55 a 59 da LGPD, que organizavam a ANPD e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.
[439] A título de informação, uma medida provisória tem aplicação imediata, mas depende de aprovação do Congresso Nacional para se transformar definitivamente em lei.
[440] Redação dada pela Lei nº 13.853, de 2019, *op. cit.*
[441] Segundo o artigo 55, § 3º da Lei 13.709/2018, *op. cit.,* o provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias.

com 5 integrantes, sendo um diretor-presidente[442]. Os membros serão escolhidos pelo Presidente da República e nomeados após aprovação do Senado Federal.

Os diretores serão selecionados dentre brasileiros que tenham reputação ilibada, nível superior de educação e "elevado conceito no campo de especialidade dos cargos para os quais serão nomeados"[443]. O mandato é de quatro anos, salvo para as primeiras nomeações (duração variável de dois a seis anos)[444].

A perda do cargo só poderá ocorrer por renúncia, condenação judicial transitada em julgado, ou pena de demissão decorrente de processo administrativo disciplinar. Aos membros do Conselho Diretor se aplica a lei de conflito de interesses, que exige sigilo profissional e impede a prestação de serviço para pessoas ou entidades com quem tenha estabelecido relacionamento relevante em razão de suas atividades públicas, mesmo após o término do mandato[445], sob pena de caracterização de improbidade administrativa[446].

Além do Conselho Diretor, a ANDP será formada pelo Conselho Nacional de Proteção de Dados Pessoais e Privacidade e por unidades especializadas[447]. A estrutura regimental será disposta por ato do Presidente da República, por meio de remanejamento de cargos e funções de outros órgãos do Poder Executivo Federal[448].

b) Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP)

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP), cuja intenção é promover debates multisetoriais, inspirados no Comitê Gestor da Internet, foi previsto em todas as versões da LGPD.

Ele será composto de vinte e três representantes, escolhidos da seguinte forma: cinco do Poder Executivo federal; um do Senado Federal; um da Câmara dos Deputados;

---

[442] Os diretores ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5, nomeando eles mesmos os demais cargos.
[443] Artigo 55 D, §2º, da Lei 13.709/2018, *op. cit.*
[444] Artigo 55 D, § 3º e 4º, da Lei 13.709/2018, *op. cit.*
[445] Excepcionalmente, a prestação do serviço pode ser autorizada pela Comissão de Ética Pública ou pela Controladoria-Geral da União.
[446] BRASIL. *Lei nº 12.813*, de 16 de maio de 2013.
Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm.
[447] As unidades especializadas são: assessoramento jurídico próprio, corregedoria, ouvidoria, unidade administrativa e unidades especializadas a serem definidas.
[448] Até que o remanejamento de cargos seja efetivado, a APD receberá apoio técnico e administrativo da Casa Civil. In: Artigo 55 G, §1º, da Lei 13.709/2018, *op. cit.*

um do Conselho Nacional de Justiça e outro do Conselho Nacional do Ministério Público; um do Comitê Gestor da Internet; três de entidades da sociedade civil; três de instituições científicas, tecnológicas e de inovação; três de confederações sindicais representativas das categorias econômicas do setor produtivo; dois de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e dois de entidades representativas do setor laboral.

Todos serão designados por ato do Presidente da República, permitida a delegação, sendo os representantes de entidades privadas indicados na forma de regulamento, que ainda será elaborado.

O CNPDP poderá propor diretrizes estratégicas para a elaboração da Política Nacional de Proteção de Dados Pessoais e Privacidade, publicando anualmente relatórios de avaliação sobre sua execução, e fornecer subsídios para a atuação da ANPD, sugerindo à e ela ações e estratégias. Poderá também elaborar estudos e realizar debates e audiências públicas, além de disseminar conhecimentos, o que também são funções da ANPD.

Sob nosso ponto de vista, a criação do Conselho foi uma escolha infeliz do legislador, já que a interação entre poder público e sociedade pode ser pensada de forma mais democrática e aberta, como por meio de consultas e audiências públicas, pesquisas de opinião, atividades de ouvidoria e demais mecanismos de controle social.

Além disso, os representantes do Conselho que não são servidores públicos, representam categorias que não refletem a proteção dos direitos e liberdades fundamentais do titular, só estando representadas as categorias econômicas, sujeitas à fiscalização e controle pela ANPD.

Neste aspecto, nota técnica elaborada no âmbito do Ministério da Justiça, afirma que haveria disparidade de representação[449], o que aliado ao fato de que a participação do Conselho não é remunerada, poderia gerar risco de captura do órgão por interesses privados. E, se assim fosse, a ANPD poderia passar a servir a duas finalidades básicas: "instituir barreiras de mercado a novos entrantes e legitimar formalmente retornos

[449] Seriam 10 representantes do governo contra 12 da sociedade civil, além do integrante do Comitê Gestor da Internet no Brasil, que poderá ou não ser um membro do governo. Ainda, nada impede que o governo indique pessoas que atuam na iniciativa privada, o que já ocorreu em uma nomeação do Poder Legislativo (que se antecipou à entrada em vigor do Conselho).

econômicos acima do que seria viável no mercado privado"[450]. Sugerem, pois, que a composição seja alterada para equilibrar interesses[451].

Percebemos, contudo, que existe ainda o risco de institucionalização de um fórum político, que poderia exercer *lobby* ou influência indevida no Poder Público, e afetar o trabalho técnico e independente da ANPD. A comparação com o Comitê Gestor da Internet não é apropriada, já que a internet é um espaço aberto e interdisciplinar, e não um órgão de controle, que lida com casos concretos e tem poder de polícia (autoridade).

O Conselho também aumenta os custos de manutenção da ANPD, o que não se justifica em um cenário político e econômico que está envidando esforços para reduzir o tamanho do Estado. Mesmo que os cargos de conselheiro não sejam remunerados, eles precisarão de espaço físico e corpo técnico/administrativo auxiliar para realizar suas funções e atividades.

Ademais, a burocracia necessária para reunir um grupo tão eclético deve ser considerada. Por fim, não se previu sujeição dos conselheiros à lei de conflito de interesses, o que reforça que a plataforma seja usada para negociação de contratos e serviços (barreira de mercado), além do perigo de vazamento de informações sensíveis[452]. Melhor seria, portanto, a extinção do CNPDP, a fim de garantir isenção e independência da ANPD.

[450] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Nota técnica n.º 4/2019/gab-senacon/senacon/mj, Processo nº 08012.001058/2019-61.

[451] Eis a sugestão da nota: O CNPDP será composto por 23 representantes, titulares suplentes, dos seguintes órgãos: I - seis do Poder Executivo federal, sendo dois representantes obrigatoriamente do Ministério da Justiça e Segurança Pública; II - um do Senado Federal; III - um da Câmara dos Deputados; IV - um do Conselho Nacional de Justiça; V - um do Conselho Nacional do Ministério Público; VI - um do Comitê Gestor da Internet no Brasil; VII – quatro três de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais; VIII - quatro de instituições científicas, tecnológicas e de inovação; e IX - quatro três de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; X - dois de entidades de defesa do consumidor."

[452] Sem citar fontes ou nomes, sob pena de incorrer em exposição indevida de dados pessoais, há advogados utilizando o apontamento de um sócio/parceiro para compor o Conselho como validação de seus serviços advocatícios e *expertise* da sociedade empresarial. Confirma-se, portanto, o receio de que o CNPDP seja usado para fins indevidos, onde os riscos ultrapassam os possíveis benefícios.

3.3.2. Funções e competências

a) Função consultiva

As funções e competências da ANPD estão previstas em um único artigo, 55-J, que tem vinte e quatro incisos e seis parágrafos. Entre elas está zelar pela proteção dos dados pessoais e pela observância dos segredos comercial e industrial[453].

Ao contrário do que vimos no RGPD e na legislação portuguesa, o papel consultivo da ANPD é reduzido, sendo a ela reservado apenas funções propositivas/regulamentares, como: a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; formas de publicidade sobre operações de tratamento; edição de regulamentos e procedimentos, bem como relatórios de impacto para tratamentos de alto risco; e edição de normas, orientações e procedimentos simplificados e diferenciados para pequenas empresas, *startups* ou empresas de inovação.

Nada é mencionado a respeito de uma verdadeira função consultiva onde a ANPD pudesse auxiliar na análise de leis ou projetos de leis que versem ou impactem na proteção de dados ou responder questionamentos de outros órgãos públicos para auxiliá-los a se adequar ao novo regramento jurídico. Ela tem, entretanto, poder para deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD[454].

Logo, a escolha dos membros da Comissão se mostra de especial importância, pois pior do que possíveis dúvidas sobre a aplicação da lei, é ter orientação dada vinculativamente por órgão com reduzida capacidade técnica, ou que receba interferências externas. O objetivo da ANPD é, antes de tudo, promover direitos e liberdades fundamentais, e esta missão deve balizar a escolha e nomeação de seus membros.

Vale mencionar que quaisquer normas editadas pela ANPD devem ser precedidas de consulta e/ou audiência públicas, bem como de análises de impacto regulatório. Duas questões podem ser levantadas: a primeira diz respeito a função do CNPDP, que nos parece dispensável diante da obrigatoriedade de a Autoridade realizar consultas e audiências públicas, já que esta seria uma das principais competências do Conselho[455]. Segundo, não

[453] Como já mencionado, a LGPD tem preocupação especial com os segredos comercial e industrial, que são mencionados 11 vezes em seu texto, sendo 3 delas no artigo que trata das funções da ANPD.
[454] Artigo 55 J, XX, da Lei 13.709/2018, *op. cit.*
[455] A duplicidade da realização destes eventos aumentaria custos e tempo para a publicação de normas.

acreditamos que todas as normativas a serem criadas pela ANPD carecem destas atividades de consulta, como no caso de simples regulamentos para o funcionamento interno da entidade.

b) Função de supervisão

As funções de fiscalização e aplicação de sanções da ANPD são similares ao estudado no âmbito português. A Autoridade poderá, diante de caso de descumprimento, aplicar as penalidades previstas em lei, em processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso[456].

Caberá à ANPD apreciar petições de titulares quando o controlador não houver solucionado as reclamações no prazo estabelecido, por meio de mecanismos simplificados, inclusive por meio eletrônico[457]. Reclamações semelhantes poderão ser analisadas de forma agregada, para que eventuais providências sejam adotadas de forma padronizada[458].

Terá poderes para realizar auditorias e celebrar compromissos com controladores para eliminar irregularidades, incertezas jurídicas ou situações contenciosas, devendo comunicar às autoridades competentes as infrações penais das quais tiver conhecimento, e aos órgãos de controle interno o incumprimento por entidades da administração pública federal[459].

A LGPD assevera que a aplicação de penalidades às entidades privadas deve observar o conceito de intervenção mínima previsto no artigo 170 da Constituição Federal, que trata dos princípios gerais da atividade econômica, como a valorização do trabalho e a livre iniciativa[460].

Lembramos que não há sanções financeiras aos órgãos públicos, o que poderia ser contraproducente no Brasil, já que eles são mantidos pelo Estado. Na prática, o dinheiro sairia de uma conta da União para possivelmente retornar a essa mesma conta. Por isso, o

[456] Artigo 55 J, IV, da Lei 13.709/2018, *op. cit.*
[457] Artigo 55 J, V, da Lei 13.709/2018, *op. cit.*
[458] Artigo 55 J, §6º, da Lei 13.709/2018, *op. cit.*
[459] Artigo 55 J, da Lei 13.709/2018, *op. cit.*
[460] Mais especificamente, fala dos seguintes princípios: soberania nacional; propriedade privada; função social da propriedade; livre concorrência; defesa do consumidor e do meio ambiente; redução das desigualdades regionais e sociais; busca do pleno emprego; e tratamento favorecido para as empresas brasileiras de capital nacional de pequeno porte.

ideal seria a responsabilização dos servidores, especialmente no caso de dolo, por meio de processo administrativo disciplinar, devendo alcançar o dirigente máximo da Instituição, a fim de abranger toda a cadeia de comando.

Caso a ANPD se constitua como um órgão técnico e imparcial, suas decisões poderiam ter oportuna função uniformizadora, orientando o implemento da LGPD para controladores públicos e privados, além de servir como parâmetro para a revisão judicial, cujos membros podem carecer do conhecimento especializado que a matéria exige, e emitir interpretações irregulares sobre o tema, causando insegurança jurídica.

c) Função de promoção/aperfeiçoamento

A LGPD deu bastante destaque às atividades de cooperação da ANPD. O legislador elaborou, dentre os poderes da Autoridade, uma série de funções para garantir a disseminação de informações, demonstrando maior viés para o lado incentivador de c*ompliance* do que para os poderes consultivos ou mesmo punitivos.

A propósito, a entrada em vigor da estrutura regimental da ANPD deveria ser prioridade para o governo brasileiro, a fim de que pudesse começar a disseminar conhecimentos desde logo. Como o tema ainda é novidade, a transmissão de materiais educativos sobre medidas de segurança e boas práticas, poderia favorecer a implementação da lei, desde o início, com mais qualidade e segurança jurídica.

Entendemos que o período de *vacatio legis* de dois anos foi antevisto exatamente para que se promovam estudos sobre práticas nacionais e internacionais sobre padrões de segurança e técnicas de anonimização, visando orientar os controladores a planejar suas atividades; e para disseminar informações aos titulares, para que exerçam melhor controle sobre seus próprios dados.

Interessante notar que o RGPD obriga que o tratamento de dados de crianças seja realizado de forma especial, enquanto na LGPD caberá à ANPD garantir o acesso claro, simples, acessível e adequado ao tratamento de dados de idosos, demonstrando preocupação com a pouca habilidade desta parcela da população brasileira com inovações tecnológicas e instrumentos informáticos.

Ainda dentro das atividades da ANPD, está a de se articular com autoridades reguladoras para exercer suas competências em setores específicos da atividade econômica e governamental de forma coordenada com as autoridades setoriais. Essa cooperação entre órgãos e agências deve promover maior eficiência e adequação da LGPD com os setores que observam legislação específica.

Para tanto, sugere a Lei que a ANPD mantenha "fórum permanente de comunicação, inclusive por meio de cooperação técnica"[461], com os demais órgãos e entidades da administração pública, a fim de facilitar suas competências regulatória, fiscalizatória e punitiva. Não há previsão legal, infelizmente, para que a ANPD promova o monitoramento de inovações e tecnologias, propondo boas práticas e diretrizes de proteção de dados.

3.3.3. Análise comparada e propostas de adequação

Analisadas as três APDs escolhidas para compor este trabalho, vemos, primeiro, uma diferença no âmbito de atuação, uma vez que a Autoridade Europeia para a Proteção de Dados tem mandato sobre as instituições e órgãos da UE, enquanto a CNPD e ANPD tem competência estatal. A influência deste fato na composição e atribuições é incerta, mas observa-se que a AEPD apresenta características diferentes das autoridades nacionais.

Em relação à composição, a AEPD adota modelo baseado em um comando central - supervisor e adjunto – contando com suporte técnico especializado (advogados, especialistas em tecnologia da informação e administradores), que atua em institutos com funções determinadas: "supervisão e aplicação", "política e consulta" e "tecnologia da informação". É, pois, uma estrutura que favorece a equipe, e centraliza a tomada de decisões a partir do suporte recebido dos peritos.

Por outro lado, a CNPD e a ANPD centralizam sua estrutura nos membros que compõe a entidade – 7 em Portugal e 5 no Brasil - onde prevalecem atributos de independência para os titulares, cujo método de escolha lusitano é plural, enquanto no caso brasileiro a decisão cabe ao Presidente da República, carecendo de aval do senado.

[461] Artigo 55 J, §4º, da Lei 13.709/2018, *op. cit.*

Poder-se-ia, contudo, ser fortalecida a equipe técnica, em ambos os casos. Na CNPD, nos parece que falta assessoria especializada, a exemplo dos institutos da AEPD. No Brasil, o modelo também seria bem-vindo, mas acreditamos que o método de escolha dos membros poderia ser mais próximo ao de Portugal, favorecendo a pluralidade e mantendo na composição magistrados e membros do Ministério Público. Esta também seria uma opção para garantir mais diversidade na formação da Autoridade, já que sugerimos que a criação do CNPDP seja revisada.

Falta, ainda, à autoridade brasileira, a autonomia financeira e de pessoal que possui a CNPD, requisito essencial para salvaguardar a perenidade de suas atividades e dar maior independência técnica ao órgão.

Em relação às atribuições e competências das APDs examinadas, vê-se na AEPD maior preocupação, ou foco, nos encargos consultivos e de promoção de conhecimentos. Na esfera opinativa, a AEPD divulga sua posição sobre diferentes temas, como acordos internacionais, uso de evidências eletrônicas em processos, e na prevenção de fraudes tributárias[462]. Do mesmo modo, tem vasta atuação na publicação de *guidelines* para orientar titulares, controladores, APDs e Estados, como no caso de denunciantes de boa-fé e governança de tecnologias da informação.

Adicionalmente, publica manuais, estudos jurisprudenciais e guias de orientação sobre proteção de dados, além de fomentar cursos e conferências, realmente cumprindo com os mandamentos de disseminar informações e boas práticas. Por fim, é a única das APDs analisadas que faz controle de novas tecnologias e se manifesta em como elas podem impactar os direitos dos titulares, dando sugestões de como mitigar estes riscos.

É, portanto, um centro de referência, o que deveria ser almejado por toda as APDs nacionais, visando, conforme estratégia da AEPD, alterar o paradigma de controle para consolidar a cultura de *accountability* para com os direitos fundamentais.

Ainda em relação a competências, a CNPD tem atuação consultiva importante, seja em relação a questionamentos de outros órgãos públicos, seja em relação a propostas

[462] In: https://edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_en, acesso em 27/11/2019.

legislativas. As posições adotadas são sempre muito técnicas, comedidas, e baseadas nos direitos dos titulares.

Comparativamente, falta à ANPD atribuições consultivas, sendo suas missões mais focadas no domínio regulamentar e decisório (função punitiva). E, ainda assim, com sérios questionamentos a respeito do foco nos direitos de personalidade, já que as menções a questões econômicas são pronunciadas na LGPD; e não há sanção para órgãos públicos, apenas previsão de cooperação entre autoridades no desempenho de suas funções, não necessariamente na proteção de dados pessoais. Logo, busca-se mais coordenação do que efetividade na salvaguarda de direitos e liberdades dos titulares.

Posto que a estrutura atual da ANPD poderá ser revisada em até dois anos de sua entrada em vigor, acreditamos que seja salutar que estas falhas sejam repensadas no momento presente. O modelo de autarquia especial, com personalidade jurídica de direito público, proposta pelo Congresso Nacional, é mais favorável à independência técnica, financeira e de pessoal do que a proposta do Poder Executivo, que a subordinada diretamente ao governo, reforçando o poder de vigilância do Estado.

O distanciamento das maiorias parlamentares e do Poder Executivo pode ajudar as autoridades administrativas independentes a servirem como "bolsas de neutralidade"[463], o que é especialmente importante "em matérias em que, por natureza, a decisão técnica supera, em ganho para o bem comum, a opção política"[464], como é o caso da proteção de dados. Não que o formato de autarquia especial garanta, por si só, autonomia. Mesmo os órgãos da administração indireta passam por processos políticos de escolha de seu dirigente. Porém, em se tratando de entidade com competência técnica, cujo orçamento para desenvolver políticas públicas é limitado, essa influência é reduzida.

Assim, o ideal é que fosse criada uma autarquia a exemplo do Conselho Administrativo de Defesa Econômica – CADE, que, apesar de vinculado ao Ministério da Justiça, atua de forma técnica, investigando e decidindo, em última instância, sobre matéria concorrencial, além de fomentar e disseminar a cultura da livre concorrência[465].

---

[463] PINHEIRO, Alexandre Sousa. *op. cit.,* p. 732.
[464] *Idem.*
[465] Em 2019 (até 10/11), o CADE julgou 508 processos, com total de multas aplicadas de R$ 781.669.920.In: http://cadenumeros.cade.gov.br/QvAJAXZfc/opendoc.htm?document=Painel%2FCADE%20em%20N%C3%BAmeros.qvw&host=QVS%40srv004q6774&anonymous=true. Acesso em 10/11/2019.

Conclusão

A expressão “sociedade da informação” representa uma tentativa de conceituar a importância e o papel da informação na sociedade contemporânea, que tem passado por inúmeras transformações, como a rápida evolução tecnológica, a globalização econômica e a mudança da estrutura capital/trabalho para uma sociedade em rede.

Informação e conhecimento - impulsionados e massivamente disponibilizados pelos novos recursos tecnológicos disponíveis - são pilares fundamentais nas dinâmicas governamentais, laborais e empresariais. O uso da *internet, smartphones*, sistemas computadorizados e de inteligência artificial faz com que um número de dados cada vez maior seja recolhido, tratado, conservado e utilizado de diferentes maneiras e pelos mais diversos atores.

Este aspecto tecnológico da sociedade da informação amplia sem precedentes à liberdade humana, mas também gera limitações a direitos fundamentais. Entre eles estão os dados pessoais, assim consideradas quaisquer informações que identifiquem ou possam identificar um ser humano. São ainda considerados dados pessoais aqueles obtidos por meio da junção de diferentes informações que em si não personalizam o indivíduo, mas que, combinadas, permitem sua identificação.

Assim, para que a proteção de dados pessoais possa ser eficiente, é importante valorar cada dado isolado, porque o tratamento permite organizar diferentes informações para obter um perfil pessoal. Ainda, como são danos de difícil reparação, se fazem necessários mecanismos preventivos e dissuasivos.

Ademais, tem-se um problema de assimetria informacional, onde falta ao titular conhecimentos – de fatos e de direitos – para participar das escolhas e decisões sobre o destino de seus dados. Muitas vezes, ele nem sabe quem os possui, para que são usados, como são tratados ou se são compartilhados.

Este é um dos aspectos principiais trazidos pelo RGPD e pela LGPD, que visam criar contornos concretos de proteção aos dados pessoais, tanto na esfera privada como pública, para que haja reequilíbrio na relação jurídica e se evitem potenciais danos pelo tratamento não autorizado ou realizado fora dos patamares de segurança. Tem-se, por conseguinte, uma estrutura dupla de responsabilidade, onde o titular participa e tem acesso a

informações sobre o uso de seus dados, e onde os responsáveis pelo tratamento são investidos em mecanismos de controle para evitar o pagamento de altas multas.

Esta "dupla responsabilidade" representa uma nova fase da tutela de dados, em que não se proíbe o tratamento, mas se requer que ele seja realizado de acordo com princípios de segurança, lealdade e finalidade. Seria a aplicação do modelo proposto por Stefano Rodotà a respeito do direito à privacidade, segundo o qual deixamos de ter uma estrutura baseada no eixo "pessoa-informação-segredo", e passamos a adotar um modelo de "pessoa-informação-circulação-controle"[466].

E, na esfera da sociedade da informação, onde se fala de *big data* e *internet* das coisas, é salutar que se pense em como tutelar a circulação de dados e a quem cabe este controle, ao invés de se pretender proibir o avanço tecnológico. Contudo, para que isto seja possível, são necessárias regras claras e mecanismos de responsabilidade.

E é neste contexto que foram criadas as autoridades de controle, que devem instrumentalizar a proteção de direitos e liberdades fundamentais, não deixando que preocupações econômicas ou de segurança pública se sobreponham (sempre, sem critérios) à necessária autodeterminação informativa, causando danos à personalidade e ao núcleo mais íntimo do titular.

É um balanço delicado, que exige ponderação de direitos e análise técnica, mas de interesse vital para a efetividade do regime. Caberá, assim, às APDs, regular a "integridade" do fluxo de informações[467], fomentando uma estrutura de "governança da privacidade"[468] assente na conciliação do desenvolvimento tecnológico, econômico e de segurança estatal com a proteção da esfera pessoal e do poder de escolha dos indivíduos. Se faz mister que a tecnologia não se sobreponha aos direitos individuais, transformando a pessoa em um *perfil*, objetivando a personalidade e desvinculando-a de sua capacidade, necessidade e prerrogativa de autodeterminação.

---

[466] RODATÀ, Stefano. *A vida na sociedade da vigilância*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 17.

[467] NISSENBAUM, Helen. *Privacy in context*. Stanford: Stanford Law Books, 2009, p. 119.

[468] BENNET, Colin e RAAB, Charles. *The Governance of Privacy*. Michigan: The MIT Press, 2006. Ideia contida no capítulo 8, que discorre sobre os regimes de privacidade.

Referências bibliográficas

ALEXY, Robert. *Teoria Discursiva do Direito*. Rio de Janeiro: Forense Universitária, 2014.

____. *Teoria dos Direitos Fundamentais*. São Paulo: Malheiros, 2008.

ASCENSÃO, José de Oliveira. *Direito alternativo*. Disponível em: www.fd.ulisboa.pt/wp-content/uploads/2014/12/Ascensao-Jose-Oliveira-DIREITO-ALTERNATIVO.pdf, acesso em 27/11/2019.

____. *Introdução à ciência do Direito*. Rio de Janeiro: Renovar, 3ª ed., 2005.

BAKSHY, Eytan; MESSING, Solomon; ADAMIC, Lada A. *Exposure to ideologically diverse news and opinion on Facebook*, pp. 1130-1132. In: Science, volume 348, nº 6239, 2015.

BARBOSA, Mafalda Miranda. *Proteção de dados e direitos da personalidade: uma relação de interioridade constitutiva*, pp. 13-47. In: AB Instantia, Ano V, nº 7, 2017.

____. *Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva: os beneficiários da proteção e a responsabilidade civil*, pp.75-184. In: Estudos de Direito do Consumidor, Coimbra, n.12, 2017.

BARROSO, Luís Roberto. *Colisão entre liberdade de expressão e direitos da personalidade: critérios de ponderação.* In: Revista de Direito Administrativo, Rio de Janeiro, janeiro/março, 2004.

____. *O direito constitucional e a efetividade de suas normas: limites e possibilidades da Constituição Brasileira*. Rio de Janeiro: Renovar, 2003.

BENNET, Colin e RAAB, Charles. *The Governance of Privacy*. Michigan: The MIT Press, 2006.

BEVERLEY-SMITH, Huw; OHLY, Ansgar e LUCAS-SCHLOETTER, A. *Privacy, property and personality: civil law perspectives on commercial appropriation*. Cambridge: Cambridge University Press, 2005.

BITTAR, Carlos Alberto. *Os direitos da personalidade*. São Paulo: Saraiva, 2015.

BOBBIO, Norberto. *A era dos direitos*. Rio de Janeiro: Elsevier, 2004, 7ª reimpressão.

____. *Teoria do Ordenamento jurídico*. Brasília: UNB, 1997.

BOTHE, Michael. *The evaluation of enforcement mechanisms in international environmental law: an overview*. In: WOLFRUM, Rudiger (ed). *Enforcing environmental standards: economic mechanisms as viable means?* Alemanha: Springer, 1996.

CALSING, Renata de Assis e SANTOS, Júlio Edstron S. *Fundamentos históricos, sociais e políticos dos direitos humanos fundamentais sociais no contexto internacional e interno*

brasileiro: uma análise crítica. In: CALSING, Renata de Assis e ALVARENGA, Rúbia Zanotelli de (coord.). *Direitos Humanos e Relações Sociais e Trabalhistas*. São Paulo: LTR, 2017.

CALVÃO, Filipa Urbano. *Direito da Proteção de Dados Pessoais: relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*. Porto: Universidade Católica Editora, 2018.

CASTELLS, Manuel. *A Sociedade em rede*, volume 1. São Paulo: Paz e Terra, 2000.

CASTRO, Catarina Sarmento e. *Novas tecnologias e relação laboral - alguns problemas: tratamentos de dados pessoais, novo regulamento geral de protecção de dados e direito à desconexão*, pp. 271-299. In: Revista do CEJ, Lisboa, nº 1, 1º Semestre 2018.

COHEN, Jean L. *Repensando a privacidade: autonomia, identidade e a controvérsia sobre o aborto*, pp. 165-203. In: Revista Brasileira de Ciência Política, nº 7, 2012.

COMISSÃO EUROPÉIA. *O que são dados pessoais?* Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt, acesso em 16/03/2019.

____. *Um Mercado Único Digital conectado para todos*. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017DC0228&from=PT, acesso em 8/6/2019.

CONSELHO DA EUROPA. *Manual da Legislação Europeia sobre Proteção de Dados*. Disponível em: www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf, acesso em 30/6/2019.

CORDEIRO, Antônio Barreto Menezes. *O RGPD e a não proteção de pessoas coletivas*, pp. 4 e 5. In: Vida Judiciária, maio/junho, 2018.

CORDEIRO, António Menezes. *Tratado de Direito Civil Português,* Parte Geral, Tomo III, 2ª ed. Lisboa: Almedina, 2007.

COSTA, Rita de Sousa. *O direito à portabilidade dos dados pela lente do direito da concorrência: breve relance em contagem decrescente para a aplicação do regulamento geral sobre a protecção de dados*, pp.291-298. In: Revista de Concorrência e Regulação, Coimbra, ano 9, nº 33-34, Jan.-Jun, 2018.

DOMINGOS, Pedro. *O Algoritmo Mestre: Como a Busca Pelo Algoritmo de Machine Learning Definitivo Recriará Nosso Mundo*. São Paulo: Novatec, 2017.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

DRUMMOND, Victor. *Internet, Privacidade e Dados Pessoais*. Rio de Janeiro: Lumen Juris, 2003.

DUARTE, Diogo Pereira. *Registo de tempos de trabalho e proteção de dados pessoais*, pp. 173-183. In: RAMALHO, Maria do Rosário Palma e MOREIRA, Teresa Coelho (coord.). *Tempo de trabalho e tempos de não trabalho: o regime nacional do tempo de trabalho à luz do direito europeu e internacional*. Lisboa: AAFDL Editora, 2018.

EUROPEAN DATA PROTECTION SUPERVISOR. *The History of the General Data Protection Regulation*. Disponível em https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en, acesso em 21/10/2019.

FAZENDEIRO, Ana. *Regulamento Geral sobre a proteção de dados*. Portugal: Almedina, 2 ed., 2018.

GALLERT, Raphael e GUTWIRTH, Serge. *The Legal Construction of Privacy and Data Protection*. In: Computer Law and Security Review, nº 522, 2013.

GARCÍA MURCIA, Joaquín e RODRÍGUEZ CARDO, Iván Antonio. *Implicaciones laborales del Reglamento 2016/679 de la Unión Europea sobre protección de datos personales*, pp.35-67. In: Questões Laborais, Coimbra, ano 24, nº 51, Jul.-Dez de 2017.

GODINHO, Adriano Marteleto. *Pessoa, personalidade e direitos da personalidade*, pp. 9-40. In: *PHRONESIS*: Revista do Curso de Direito da FEAD, nº 5, 2009.

GONZALES FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Suíça: Springer International Publishing, 2014.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. *Parecer 4/2007 do sobre o conceito de dados pessoais*, 01248/07/PT, WP 136. Disponível em: www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf, acesso em 30/11/2019.

GUERRA, Sidney. *O direito à privacidade na internet: uma discussão da esfera privada no mundo globalizado*. Rio de Janeiro: América Jurídica, 2004.

GUIMARÃES, Maria Raquel. *A tutela da pessoa e da sua personalidade: algumas questões relativas aos direitos à imagem, à reserva da vida privada e à reserva da pessoa íntima ou direito ao carácter*. In: CENTRO DE ESTUDOS JUDICIÁRIOS. *A tutela geral e especial da personalidade humana*, Lisboa: Centro de Estudos Judiciários, 2017.

HABERMAS, Jurgen. *Direito e Democracia entre facticidade e validade*. Rio de Janeiro: Tempo Brasileiro, 1997.

HERRERA FLORES, Joaquín. *Reinvención Derechos Humanos*. Madrid: Atrapasuenos, 2008.

JABUR, Gilberto Haddad. *Liberdade de pensamento e direito à vida privada*. São Paulo: Revista dos Tribunais, 2000.

KELSEN, Hans. *Teoria pura do Direito*. São Paulo: Martins Fontes, 1999.

KOKOTT, Juliane e SOBOTTA, Christoph. *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*. In: International Data Privacy Law, Vol. 3, Nº. 4, 2013.

KULHARI, Shraddha. *Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*. Alemanha: Nomos Verlagsgesellschaft mbH, 2018.

LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012.

LINDEN RUARO, Regina e RODRIGUES, Daniel Piñeiro. *O direito à proteção de dados pessoais e a privacidade*. In: Revista da Faculdade de Direito – UFPR, Curitiba, nº 53, 2011.

LYON, David. *The Electronic Eye: the rise of surveillance society*. Minneapolis: University of Minnesota Press, 1994.

MAGALHÃES, Filipa Matias e PEREIRA, Maria Leitão. *Regulamento geral de proteção de dados: manual prático*. Porto: Vida Económica, 2017.

MEIRELES, Adriana Veloso. *Autonomia e privacidade no ambiente digital*. In: Revista Eletrônica de Ciência Política. Nº 7, 2016.

MELLO, Marcos Bernardes de. *Teoria do Fato Jurídico: plano da existência*. São Paulo: Saraiva, 2003.

MENDES, Jorge Barros. *O novo regulamento de proteção de dados: as principais alterações*, pp.11-34. In: Revista Portuguesa de Direito do Consumo, Coimbra, nº 89, Mar. 2017.

MILT, Kristiina. *Proteção dos dados pessoais*: Fichas técnicas sobre a União Europeia, 2019. Disponível em: http://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais, acesso em 15/05/2019.

MONTEIRO, Renato Leite et al. *Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos*. Disponível em: www.academia.edu/38940887/Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_e_GDPR_hist%C3%B3rico_an%C3%A1lise_e_impactos, acesso em 04/11/2019.

MOREIRA, Teresa Coelho. *Algumas implicações laborais do Regulamento geral de proteção de dados pessoais no trabalho 4.0*, pp.9-34. In: Questões Laborais, Coimbra, ano 24, nº 51, Jul-Dez. 2017.

NETO, Afonso Araújo. *RGPD: uma revolução invisível*, pp.35-42. In: Revista Portuguesa de Direito do Consumo, Coimbra, nº 89, Mar. 2017.

NEVES, Artur Castro. *Como definir a sociedade da informação?*, pp. 57 a 69. In: COELHO, José Dias (coord.). *Sociedade da Informação: o percurso português*. Portugal: Edições Sílabo, 2007.

NISSENBAUM, Helen. *Privacy in context*. Stanford: Stanford Law Books, 2009.

PÉREZ LUÑO, Antonio-Enrique. *Derechos Humanos, Estado de Derechos y Constitución*. Madrid: Tecnos, 10. ed., 2010.

PINHEIRO, Alexandre Sousa (coord.). *Comentário ao Regulamento Geral de Protecção de Dados*. Coimbra: Edições Almedina, 2018.

PINHEIRO, Alexandre Sousa e MOURA, Carolina. *Utilização de tecnologia de geolocalização e o tratamento de dados pessoais no regime jurídico português: a propósito da deliberação nº 7680/2014 da Comissão Nacional de Protecção de Dados e jurisprudência posterior*, pp.14-31. In: Fórum de Proteção de Dados, Lisboa, nº 3, Jul. 2016.

PINHEIRO, Alexandre Sousa. *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*. Lisboa: AAFDL, 2015.

POLIDO, Fabrício B. Pasquot et al. *GDPR e suas repercussões no direito brasileiro: Primeiras impressões de análise comparativa*. Brasil: IRIS, 2018.

REALE, Miguel. *Lições Preliminares do Direito*. São Paulo: Bushatsky, 2ª ed, 1974.

RODATÀ, Stefano. *A vida na sociedade da vigilância*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SAIAS, Marco Alexandre. *Reforço da responsabilização dos responsáveis pelo tratamento de dados*, pp.67-85. In: Revista Portuguesa de Direito do Consumo, Coimbra, n.89, Mar. 2017.

SHELTON, Dinah. *Techniques and Procedures in International Environment Law*. Geneva: UNITAR – United Nations Institute for Training and Research, Course 3, 2. ed., 2004.

SILVA NETO, Manoel Jorge E. *O princípio da máxima efetividade e a interpretação constitucional*. São Paulo: LTR, 1999.

SILVA, Fernando. *Sistemas de geolocalização e monitorização de veículos: do início do GPS às novas tendências*, pp.33-45. In: Fórum de Proteção de Dados, Lisboa, n.3, Jul. 2016.

SILVEIRA, Alessandra e FROUFE, Pedro. *From the Internal Market to the citizenship of rights: the protection of personal data as the jus-fundamental identity question of our times*. In: UNIO - EU LAW JOURNAL Vol. 4, Nº. 2, Julho de 2018.

SILVEIRA, Hélio Freitas de Carvalho da e ANDRADE, Marcelo Santiago de Pádua. *Tratamento de dados pessoais e a propaganda eleitoral na internet: os desafios do direito eleitoral no atual momento de desenvolvimento tecnológico*, pp.96-105. In: Revista do Advogado, São Paulo, ano 38, nº 138, Jun. 2018.

SOLOVE, Daniel. *Understanding Privacy*. Cambridge: Harvard University Press, 2010.

SOUSA, Rabindranath Capelo. *O Direito Geral de Personalidade*. Coimbra: Coimbra Editora, 1995.

SOUZA, Duarte Abrunhosa. *Registo dos tempos de trabalho e proteção de dados pessoais*, pp. 117-156. In: PALMA, Maria do Rosário e MOREIRA, Teresa Coelho (coord.). *Tempo de trabalho e tempos de não trabalho: o regime nacional do tempo de trabalho à luz do direito europeu e internacional*. Lisboa: AAFDL Editora, 2018.

TEIXEIRA, Guilherme da Fonseca. *Identidade e autodeterminação informacional no novo Regulamento Geral de Proteção de Dados: a inevitável privatização dos deveres estaduais de proteção*, pp. 11-38. In: Católica Law Review, VOLUME II, n.º 1, janeiro 2018.

TEPEDINO, Gustavo. *A tutela da personalidade no ordenamento civil-constitucional brasileiro*. In: TEPEDINO, Gustavo. *Temas de Direito Civil*. Rio de Janeiro: Renovar, 1999.

TZANOU, Maria. *The fundamental right to data protection: normative value in the context of counter-terrorism surveillance*. Oxford: Hart Publishing, 2017.

VENOSA, Silvio de Salvo. *Direito Civil*: parte geral. Vol. 1. São Paulo: Editora Atlas, 4ª ed., 2004.

WARREN, Samuel e BRANDEIS, Louis. *The right to privacy*, pp. 193-220. In: Harvard Law Review, Vol. 4, No. 5, dezembro de 1890.

WEISS, Edith Brown e JACOBSON, Harold K. Engaging Countries: strengthening Compliance with international environmental accords. Cambridge: MIT Press, 2000.

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

WOLFRUM, Rudiger. *Recueil des Cours: collected courses*. Volume 272, Hague Academy of International Law, 1998.