DEPARTAMENTO DE DIREITO
MESTRADO EM DIREITO
ESPECIALIDADE EM CIÊNCIAS JURÍDICAS
UNIVERSIDADE AUTÓNOMA DE LISBOA
"LUÍS DE CAMÕES"

A proteção de dados como fator essencial para a admissibilidade da Resolução de Disputas Online (ODR) em Portugal e no Brasil

Dissertação para a obtenção do grau de Mestre em Direito

Autora: Denise Caldas Figueira
Orientadores: Professor Doutor Pedro Gonçalo Tavares Trovão do Rosário
Mestre Patrícia Cardoso Dias.
Número da candidata: 30005415

Dezembro de 2023
Lisboa

AGRADECIMENTOS

À minha mãe, Lucília, e ao meu pai, José Figueira Júnior (*in memoriam*), pelo carinho e esforço de uma vida inteira. À minha filha, Tarsila, pelo amor incondicional e parceria neste projeto. Aos queridos Maria Elizabeth Guimarães Teixeira Rocha e Romeu Ribeiro Bastos, pelo incentivo e apoio sempre presentes. Ao Professor Doutor Pedro Gonçalo Tavares Trovão do Rosário e à professora Mestre Patrícia Cardoso Dias, pelas observações perspicazes e pelo auxílio imprescindível.

RESUMO

A transmissão de dados e informações integra a organização socioeconómica de um mundo que se tornou global, em que as redes de comunicação não respeitam as fronteiras geopolíticas dos Estados. O uso intenso da tecnologia adentrou a sociedade e a vida diária daspessoas, e absorve de forma compulsiva e voraz seus dados pessoais. De outro lado, o Poder Judiciário possui um número extraordinário de processos, além de se revelar inacessível para parte da população. Com o intuito de facilitar o acesso à justiça de maneira mais rápida, equitativa e económica neste mundo globalizado, as resoluções alternativas de conflito vêm sendo amplamente utilizadas e, dentre elas, destaca-se a Resolução de Disputas Online ou Online Dispute Resolution (ODR). A ODR, que utiliza os meios informáticos, o ciberespaço e as informações pessoais para o seu desenvolvimento, deve também obedecer ao primado do direito fundamental à proteção de dados, resguardados pela Constituição de Portugal e do Brasil para a sua consecução. Além disso, o exame do Regulamento Geral de Proteção de Dados (RGPD) e da Lei Geral de Proteção de Dados Pessoais (LGPD), juntamente com os regulamentos pertinentes, asseguram a proteção adequada à segurança, à privacidade e à confidencialidade necessárias ao procedimento da ODR.

Palavras-chave: Proteção de dados – Online Dispute Resolution (ODR) Regulamento Geral sobre a Proteção de Dados (RGPD) – Lei Geral de Proteção de Dados Pessoais (LGPD)

ABSTRACT

The transmission of data and information is part of the socioeconomic organization of a world that has become global, where communication networks do not respect the geopolitical borders of States. The intense use of technology has entered society and people's daily lives, and compulsively and voraciously absorbs their personal data. On the other hand, the Judiciary has an extraordinary number of cases, in addition to being inaccessible to part ofthe population. In order to facilitate access to justice more quickly and economically in this globalized world, alternative conflict resolutions have been widely used and, among them, the Online Dispute Resolution (ODR) stands out. ODR, which uses computer means, cyberspace and personal information for its development, must also comply with the primacy of the fundamental right to data protection, protected by the Constitution of Portugal and Brazil, for its attainment. Furthermore, the examination of the General Data Protection Regulation (GDPR) and the General Data Protection Law (LGPD), together with relevant regulations, ensure adequate protection of thesecurity, privacy and confidentiality necessary for the ODR procedure.

Keywords: Data protection – Online Dispute Resolution (ODR) – General Data ProtectionRegulation (RGPD) – General Data Protection Law (LGPD)

SUMÁRIO

LISTA DE FIGURAS E TABELAS

LISTA DE SIGLAS E ABREVIATURAS

AB2L	Associação Brasileira de Lawtechs & Legaltechs
AEPD	Agência Espanhola de Proteção de Dados
AGNU	Assembleia Geral das Nações Unidas
ANPD	Autoridade Nacional de Proteção de Dados (Brasil)
CAP	Centro de Arbitragem Permanente
CDC	Código de Defesa do Consumidor (Brasil)
CEDH	Convenção Europeia dos Direitos Humanos
CF	Constituição da República Federativa do Brasil
CEJUSCS	Centro Judiciário de Solução de Conflitos e Cidadania
CEPD	Comité Europeu para a Proteção de Dados
CMC	Conselho do Mercado Comum (Mercosul)
CNH	Carteira Nacional de Habilitação
CNJ	Conselho Nacional de Justiça (Brasil)
CNPD	Comissão Nacional de Proteção de Dados (Portugal)
CNS	Centro Nacional de Cibersegurança
CP	Código Penal (Brasil)
CPA	Código do Procedimento Administrativo
CPC	Código de Processo Civil
CPF	Cadastro de Pessoas Físicas (Brasil)
CPTA	Código do Processo nos Tribunais Administrativos
CRP	Constituição da República de Portugal
CTN	Código Tributário Nacional (Brasil)
DUDH	Declaração Universal dos Direitos Humanos
ENAP	Escola de Nacional de Administração Pública (Brasil)
ETAF	Estatuto dos Tribunais Administrativos e Fiscais
IA	Inteligência Artificial
IBGE	Instituto Brasileiro de Geografia e Estatística (Brasil)
INE	Instituto Nacional de Estatística
LGPD	Lei Geral de Proteção de Dados (Brasil)
MERCOSUL	Mercado Comum do Sul
OCDE	Organização para a Cooperação e Desenvolvimento Econômico

ODR	Online Dispute Resolution
ODS	Objetivos de Desenvolvimento Sustentável da ONU
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
PDL	Projeto de Decreto Legislativo (Brasil)
RAL	Resolução Alternativa de Conflitos (Portugal)/Resolução Adequada de Conflitos (Brasil)
RG	Registro Geral
RGPD	Regulamento Geral sobre a Proteção de Dados – Regulamento UE 2016/679
RJEOP	Regime Jurídico das Empreitadas de Obras Públicas
RLL	Resolução de Litígios em Linha
RSI	Resolution Systems Institute
STF	Supremo Tribunal Federal (Brasil)
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TJDFT	Tribunal de Justiça do Distrito Federal e Territórios (Brasil)
TJUE	Tribunal de Justiça da União Europeia
UDHR	Universal Declaration of Human Rights (Declaração Universal dos Direitos Humanos)
UNCINTRAL	Comissão das Nações Unidas para o Direito Comercial Internacional
UE	União Europeia
UnB	Universidade de Brasília
VM	Virtual Magistrate
WIPO	World Intellectual Property Organization (Organização Mundial de Propriedade Intelectual)

INTRODUÇÃO

> Dados. Nós amamos isso. Sabemos o quão importante é mantê-los seguros. Hoje em dia, estamos conectados em qualquer lugar e o tempo todo. Às vezes, podemos nem perceber o quão conectados realmente estamos enquanto nossos aplicativos, pesquisas na web e compras com cartão de crédito estão constantemente armazenando nossas ações em segundo plano.
>
> Katie Atkinson[1]

É certo que quase todas as pessoas já foram incomodadas com ligações telefónicas que visavam vender alguma coisa. O espantoso é que esses indivíduos possuem conhecimento profundo de dados pessoais. A pergunta a ser feita é: como conseguiram essas informações? É sabido que os governos em todo o mundo estão mudando radicalmente as suas políticas na esperança de incrementar novas oportunidades económicas e atrair investimentos internacionais, garantindo a segurança de suas sociedades e o fortalecimento de suas instituições.

Para tanto, desenvolvem constantemente novas estratégias que requerem a obtenção de mais e mais quantidade de dados dos indivíduos, o que implica mudança significativa nas relações estabelecidas entre o cidadão e o Estado devido ao acúmulo de informações pessoais. E isso não ocorre somente entre Estado e cidadãos. A indústria desempenha um papel fundamental ao fornecer ferramentas e serviços que podem afetar a privacidade das pessoas. A realidade descrita é nomeada como sistemas intensivos de dados, definidos como sistemas que processam referências pessoais, geram informações adicionais e as utilizam nas tomadas de decisões em relação aos sujeitos eventualmente examinados.

Atualmente, a informação pessoal é considerada uma verdadeira mercadoria, de grande valor monetário e disponibilizada pelas modernas tecnologias de informação, transformadas que foram em um bem de valor económico. Nesta perspectiva, a fim de exemplificar este argumento, pode-se destacar a violação de dados ocorrida no Brasil, em 28 de janeiro de 2021[22] e divulgada pela imprensa. Estima-se que, neste caso, a divulgação não autorizada de dados tenha superado o número de habitantes brasileiros, uma vez que as informações expostas incluíram o Cadastro de Pessoa Física (CPF),

---

[1] Katie Atkinson é Professora de Ciência da Computação e Reitora da Escola de Engenharia Elétrica, Eletrónica e Ciência da Computação da Universidade de Liverpool, Reino Unido. Sua pesquisa é voltada para a Inteligência Artificial e o Direito. Disponível em https://b-m.facebook.com/Technical0812/photos/a.332158000566047/1198322733949565/?type=3

[2] Disponível em https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. [Consult. 11 abr. 2021].

documento similar ao NIF português, além de nome, sexo e data de nascimento dos cidadãos, acrescido de dados de veículos e informações sobre empresas. Alguns dias depois, notícias de outras fontes divulgaram que foram fornecidas informações detalhadas a respeito de 140 milhões de veículos registrados nos órgãos estaduais de trânsito. Outra notícia informou terem sido expostos na *dark web* mais de 100 milhões de números de celular[3].

O mais preocupante, contudo, é que até o momento a procedência dessas ações e os responsáveis pela perpetração de tais crimes são desconhecidos. Conquanto o fato pareça ser uma particularidade da modernidade líquida, está longe de ser banal e vem sendo replicado em outros países, tornando-se uma imensa preocupação mundial. Em Portugal, onde as leis que punem esse tipo de crime são mais severas e mais antigas, houve um episódio de violaçãode dados clínicos de pacientes que estavam internados em um hospital, e o resultado foi a aplicação de multa em milhares de euros[44], além de outras coimas.

Não obstante a competente fiscalização, em 9 de abril de 2021, a Comissão Nacional de Proteção de Dados (CNPD) divulgou comunicado e informou que a exposição de dados pessoais nas redes sociais afeta milhões de utilizadores em Portugal. A exposição de dados oriundos do Facebook sem autorização, por exemplo, atingiu apenas em Portugal mais de dois milhões de utilizadores[5]. O resultado da apuração do ocorrido ainda não foi divulgado, porémo CNPD fez recomendações aos utilizadores das redes sociais, aos prestadores de serviços online, e, inclusive, já se manifestou como autoridade de controlo interessada, nos termos do artigo 60 do Regulamento Geral sobre a Proteção de Dados (RGPD).

O que se quer destacar, portanto, é que a proteção de dados se apresenta como um bem económico e um direito fundamental do titular de dados e, por isso, deve ser adequadamente protegido. Pode-se inferir, portanto, o valor atribuído às informações pessoais quando se discute direitos dos cidadãos, ao utilizar as ferramentas das soluções

---

[3] Disponível em https://www.jacobsconsultoria.com.br/post/o-que-se-sabe-sobre-o-grande-vazamento-de-dados-de-janeiro-de-2021. [Consult. 06 ago. 2021].

[4] Disponível em https://www.iabnacional.org.br/noticias/advogado-portugues-diz-que-vazamento-de-dados- pessoais-gera-altas-multas-em-seu-pais. [Consult. 30 mar. 2021]. https://www.lgpdbrasil.com.br/em-portugal-centro-hospital-e-multado-em-400-mil-euros-por-violar-gdpr/. [Consult. 30 mar. 202]1. https://visao.sapo.pt/atualidade/2020-03-20-hospital-do-barreiro-multado-em-380-mil-euros-pela-comissao-de-

[5] CNPD – Exposição de dados pessoais de redes sociais afeta milhões de utilizadores em Portugal. Disponível em https://www.cnpd.pt/media/wq2pjyyc/informa%C3%A7%C3%A3o-da-cnpd-e-recomenda%C3%A7%C3%B5es_fb-e-linkedin_abril-2021.pdf. [Consult. 11 abr. 2021].

adequadas de resolução de conflitos no ambiente virtual. Tem-se, portanto, que a proteção de dados é fator essencial para a admissibilidade de resolução de disputas online.

1. A PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL

1.1 A SOCIEDADE DIGITAL

O século XXI consolida a presença digital na vida de pessoas e organizações. Se em meados do século passado os registros se restringiam às combinações de zeros e uns como forma de inserção nas plataformas rudimentares de dados, no presente a interação pela internet e a massificação dos dispositivos eletrônicos, bem com a expansão exponencial dos recursos de *software* e *hardware* nos mais variados planos da existência humana, mergulhou a pessoa comum, as empresas de diversos portes e os organismos estatais num oceano de dados digitais. Num ambiente tão vasto como este, a falta de uma cultura organizacional – com mecanismos de proteção adequados – pode tornar cidadãos e empresas vulneráveis diante de ameaças de violações de direitos fundamentais no que concerne à sua privacidade e segurança. Por isso tornou-se indispensável disciplinar estas relações respeitando os direitos fundamentais e de privacidade, notadamente mediante o Regulamento Geral sobre a Proteção de Dados, em Portugal, e a Lei Geral de Proteção de Dados, no Brasil, além de normativos complementares.

Não obstante, a fim de contextualizar o tema, importa pontuar alguns conceitos que irão permear esta dissertação.

1.1.1 Ciberespaço

Poucas inovações modificaram tanto as sociedades provocando transformações impactantes sobre as atividades económicas, sociais, políticas, culturais e científicas como o ciberespaço. Este termo foi proposto pela primeira vez por William Gibson,[6] em 1984, em seuromance de ficção científica *Neuromancer*.

Desde meados dos anos 1990, diversos autores se debruçaram sobre a definição do conceito de ciberespaço. Para Daniel T. Kuehl,[7] por exemplo, o ciberespaço é um ambiente de redes fundamentada nas tecnologias de informação para criar, modificar,

[6] GIBSON, William – Neuromancer. New York: Ace Books, 2003. p. 51.

[7] Para Kuehl, ciberespaço pode ser definido nos seguintes termos: "O conjunto de um domínio global dentro do ambiente de informação cujo caráter único e distinto é dado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando as tecnologias de informação e comunicação." KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. In KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **CyberPower and National Security**. [sl]: Potomac Books, 2009. p. 28

armazenar e trocar informações. Atualmente, ciberespaço pode ter várias conotações, todas elas a implicar o uso da internet para conectar pessoas por meio de vídeo, voz ou texto, além de armazenar e transmitir dados ao fazer uso da eletrónica e do espectro eletromagnético. Neste sentido, adotamos o conceito de Pierre Lévy, ao conceituar o ciberespaço desta forma:

> O conjunto dos sistemas de comunicação eletrônicos (aí incluídos os conjuntos de redes hertzianas e telefônicas clássicas), na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização. Insisto na codificação digital, pois ela condiciona o caráter plástico, fluido, calculável com precisão e tratável em tempo real, hipertextual, interativo e, resumindo, virtual da informação que é, parece-me, a marca distintiva do ciberespaço. Esse novo meio tem a vocação de colocar em sinergia e interfacear todos os dispositivos de criação de informação, de gravação, de comunicação e de simulação. A perspectiva da digitalização geral das informações provavelmente tornará o ciberespaço o principal canal de comunicação e suporte de memória da humanidade a partir do próximo século.[8]

Nesse sentido, podemos concluir que o ciberespaço não é apenas uma simples via onde trafegam informações, mas um ambiente virtual amparado pelas tecnologias da informação, onde poderemos conservar e lembrar atos, fatos, nomes e reputação dos indivíduos e empresas e tudo o que se passou em relação a esses indivíduos e empresas.

Trata-se, de fato, como apontado acima, de uma memória da humanidade e, por esse aspeto, torna-se, cada vez mais, um local de competição estratégica. Sua acessibilidade a baixo custo e sua difusão torna-o o local ideal para a proliferação de novas e antigas ameaças, ao mesmo tempo em que forma um mundo em que empresas multinacionais, corporações e cibercriminosos se enfrentam numa verdadeira guerra pela conquista de dados e informações, uma vez que, conforme já assinalado, esses dados e essas informações contêm valor económico.

De acordo com Nazli Choucri[9], as peculiaridades do ciberespaço podem ser caracterizadas sob sete aspetos, quais sejam: (1) temporalidade, em que a temporalidade convencional é praticamente substituída pela instantaneidade das informações, dados etc.; (2) flexibilidade, quando a ausência de restrições da geografia e localização física é observada; (3) permeabilidade, pois é possível penetrar fronteiras e jurisdições; (4) fluidez, que se refere à facilidade com que ocorrem mudanças nos padrões de interação, com configurações e reconfigurações associadas, bem como o surgimento de novos atores e novas modalidades de interação; (5) participação, uma vez que ficam reduzidas as barreiras ao ativismo e à expressão política; (6) anonimato,

[8] LÉVY, Pierre – **Cibercultura.** Tradução de Carlos Irineu da Costa. São Paulo: 34 Editora, 2008. p. 92-93.
[9] CHOUCRI, Nazli – **Cyberpolitics in International Relations**. Cambridge: MIT Press, 2012. p. 4

quando são obscurecidas as identidades de atores e links; e, por fim, podemos notar a característica da quase (7) ausência de mecanismos de responsabilidade daqueles que trafegam no ciberespaço.

De outro lado, podemos notar que os diplomas legais vigentes possuem uma relação de pertinência com as características acima enumeradas. Podemos citar, por exemplo, as características da flexibilidade e permeabilidade estampadas no artigo 2º, números 1 e 2, alíneas 'a' e 'b' da Lei n.º 58/2019, ou, ainda, a proteção à participação no número 1 do artigo 24 da citada Lei. A par dos indiscutíveis benefícios que a informatização traz para a sociedade, existem também vulnerabilidades. A segurança do ciberespaço deve ser uma grande preocupação de todos os atores envolvidos, especialmente no âmbito institucional.

É nesse amplo e complexo universo que os nossos dados pessoais trafegam e são armazenados, sujeitos a todos os tipos de incidentes cibernéticos. É importante mencionar a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia (UE). Assim, ao lado do direito de pessoas singulares poderem controlar o uso de seus dados pessoais[10], a proteção de dados concretiza, portanto, medida indiscutível para a realização de resolução de disputas online (ODR).

1.1.2 Dados pessoais

O conceito de dados pessoais é compreendido de forma abrangente nos dias atuais. Assim, vamos nos ater aos textos legais para definir a expressão. A lei brasileira sobre proteção de dados[11] os conceitua como a "informação relacionada a pessoa identificada ou identificável"[12].

Identificável é quando a identidade da pessoa pode ser revelada pela combinação de informações dispersas. Assim, para este diploma legal, um dado é considerado pessoal quando propicia a identificação, direta ou indireta, da pessoa natural por trás do dado, por exemplo: nome, sobrenome, data de nascimento, documentos pessoais, tais como CPF (ou NIF, em Portugal), Registro Geral (RG), Carteira Nacional de Habilitação (CNH ou

[10] De acordo com o número 7 do Considerando do Regulamento n.º 2016/679 do Parlamento e do Conselho da União Europeia.
[11] Lei n.º 13.709, de 14 de agosto de 2018.
[12] Artigo 5º, inciso I, da Lei n.º 13.709, de 2018 – LGPD/Brasil.

Carteira de Condução, em Portugal), Carteira de Trabalho, dados da Previdência Social (no Brasil) ou dos Recibos Verdes (em Portugal), passaporte e título de eleitor, endereço residencial ou comercial, telefone, e-mail, *cookies*, endereço de IP etc.

A Lei brasileira diferencia, ainda, os dados pessoais, por meio dos quais um indivíduo pode ser identificável, dos dados pessoais sensíveis[13], pois estes se referem às características próprias de cada um, isto é, são aqueles dados que o distingue dos demais integrantes da sociedade, seja em relação à raça, opinião política, filiação, dados de saúde ou vida sexual, por exemplo. O tratamento dos dados pessoais sensíveis, por ser de maior potencial lesivo, observa regras mais rígidas de resguardo e proteção.

Na União Europeia e, por via de consequência, em Portugal e em todos os países que integram a União Europeia, o conceito de dados pessoais[14] encontra-se previsto no artigo 4º do Regulamento Geral sobre a Proteção de Dados (RGPD). Diferentemente da lei brasileira, não encontramos a subdivisão em dados pessoais e dados pessoais sensíveis, ao considerar que na definição do RGPD as características peculiares de cada indivíduo, previsto em seu artigo 4º, já as incluem como dados singulares da pessoa, tais como sua identidade física, fisiológica, genética, económica, social, dentre outros. Não obstante, nas alíneas do citado artigo 4º do RGPD há a previsão diferenciada para os dados genéticos, biométricos e relativos à saúde dos indivíduos (alíneas 13, 14 e 15 do citado artigo 4º, bem assim o considerando número 35 do RGPD relativo aos dados da saúde do titular de dados, e o considerando número 34 do RGPD, referente aos dados genéticos da pessoa singular). No entanto, em 1981, foi assinado pelo Comitê de Ministros do Conselho da Europa, o Convênio para a proteção daspessoas com respeito ao tratamento automatizado de dados de caráter pessoal, denominado Convenção 108, que conferiu proteção mais adequada ao tratamento de dados denominados "sensíveis" de uma pessoa, ou seja, aqueles relativos à raça, opinião política, religião, vida sexual, antecedentes penais, entre outros. Esse Convênio foi atualizado pelo Protocolo CETS n.º 223, pelo Comitê de Ministros do Conselho da Europa, em 18 de abril de 2018.

Segundo Catarina Sarmento e Castro[15], dados pessoais equivalem a todos aqueles utilizados para indicar a natureza e as características distintivas das pessoas, desde os

[13] Artigo 5º, inciso II, da Lei n.º 13.709, de 2018 – LGPD/Brasil.

[14] Artigo 4º do Regulamento Geral sobre a Proteção de Dados União Europeia – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativos à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. A União Europeia adotou também o Regulamento Geral de Proteção de Dados quando são utilizados pelas autoridades policiais e judiciárias e à livre circulação desses dados, nos termos da Diretiva 2016/680/UE.

[15] CASTRO, Catarina S. e – **Direito da informática, privacidade e dados pessoais**. Coimbra: Edições Almedina, 2005. p. 74.

dados biométricos, assim como aqueles relativos à saúde física e económica. Por sua vez, Maria Eduarda Gonçalves[16] define dados pessoais em conformidade com a Convenção do Conselho da Europa, sendo necessário destacar nesta definição a característica da temporalidade do ciberespaço, pois se a identificação da pessoa carecer de tempo ou custos, a pessoa física não será considerada identificável. Podemos apurar da doutrina, portanto, que existem definições mais e menos detalhistas sobre o que se consubstancia "dado pessoal", no sentido de indicar mais ou menos informações para identificar o titular dos dados, bem assim, temos também conceitos extremamente objetivos, como aquele utilizado por William Smith Kaku, ao afirmar que "tudo que trafega na Internet é dado"[17]. Para nosso estudo, utilizaremos como parâmetro o conceito contido no artigo 4º, número 1, do RGPD.

Outro termo de importância para o assunto é o que significa "controlador de dados" – expressão utilizada no Brasil – ou "responsável pelo tratamento" – expressão empregada pelo número 7 do artigo 4º do RGPD que, ao abrigo do direito interno, deve assumir a responsabilidade final pelas atividades relacionadas ao tratamento de dados pessoais e, como veremos adiante, será responsável pelos ciclos de vida do tratamento dos dados pessoais. O responsável pelo tratamento é a parte legalmente competente para decidir sobre o conteúdo e o uso dos dados, independentemente de tais dados serem ou não recolhidos, armazenados, processados ou disseminados por essa parte ou por um agente em seu nome. Pode ser uma pessoa física ou jurídica, autoridade pública, agência ou qualquer outro órgão.[18]

Necessário registrar, ainda, a designação da autoridade de controlo nacional para os efeitos de tratamento de dados. Em Portugal, trata-se da Comissão Nacional de Proteção de Dados (CNPD), criado pela Lei n.º 43/2004, de 18 de agosto. Posteriormente, a Lei n.º 58/2019, designou a CNPD a autoridade de controlo nacional para efeitos do RGPD e estabeleceu diretrizes em seus artigos 4º ao 7º. O Brasil também adota a figura da autoridade pelo tratamento de dados, com atribuições semelhantes ao órgão europeu, e foi criado pela Lei n.º 13.709, de 2018, alterada pela Lei n.º 13.853, de 2019, em seu artigo 55-A. Trata-se da Autoridade Nacional de Proteção de Dados (ANPD), órgão da

[16] GONÇALVES, Maria E. – **Direito da informação: novos direitos e formas de regulação na sociedade da informação**. Coimbra: Almedina, 2003. p. 89

[17] KAKU, William S. – Internet e comércio eletrónico: pequena abordagem sobre a regulação da privacidade, *apud*, ROVER, Aires J. (org.) – **Direito, Sociedade e Informática: limites e perspectivas da vida digital**. Florianópolis: Fundação Boiteux, 2000. p. 90.

[18] OCDE – **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível em www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. [Consult. 29 mar. 2021].

administração pública federal eintegrante da Presidência da República do Brasil.

Isso posto, outro conceito correlato ao tema e que deve ser estabelecido é o de "proteção de dados". A proteção de dados é composta por todas as medidas adotadas, tanto em nível técnico como jurídico, para garantir que as informações dos utilizadores de uma empresa, entidade ou qualquer base de dados, fiquem protegidas de qualquer violação de dados ou tentativa de acesso por parte de pessoas ou entes não autorizados. A violação de dados deve ser entendida nos termos da alínea 12, do art. 4º do RGPD [19].

1.1.3 Cibersegurança

A Lei n.º 46/2018, de 13 de agosto, transpôs a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, com o fim de estabelecer o regime jurídico da segurança do ciberespaço, isto é, medidas destinadas a assegurar um alto nível de segurança das redes e da informação em toda a União. Trata-se de envolver todos os agentes engajados na comunicação em rede e estabelecer os respectivos requisitos de segurança. Trata-se, portanto, de cibersegurança, isto é, a segurança das informações que trafegam nas redes e nos sistemas de informação. A cibersegurança sempre foi objeto de atenção por parte dos usuários das redes, sejam as pessoas físicas, as pessoas coletivas ou a administração pública e os governos.

Até pouco tempo um "vírus de computador"[20] levava até três meses para infectar aparelhos telemáticos pelo mundo. Atualmente, a possibilidade de infecção generalizada pode acontecer em alguns cliques, pois a dinâmica do planeta conectado mudou rapidamente, em especial devido à pandemia do vírus SARS-COV-2 e o movimento de *home office*. Nesse contexto, os dados pessoais passaram a ficar cada vez mais sujeitos a ataques cibernéticos que podem alterá-los e torná-los suscetíveis a malfeitos. Como consequência, as empresas governamentais e não-governamentais têm investido em medidas de segurança, visando obstaculizar as ações dos cibercriminosos.

---

[19] RGPD, Art. 4º, alínea 12: "Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;"

[20] Vírus de computador é um tipo de programa ou código malicioso criado para alterar a forma como um computador e/ou outros aparelhos telemáticos funcionam. São desenvolvidos para se propagar de um computador e/ou aparelhos telemáticos para outro. Disponível em https://br.norton.com/internetsecurity-malware-what-is-a-computer-virus.html. [Consult. 28 out. 2021].

1.1.3.1 Cibersegurança em Portugal

O Observatório de Cibersegurança, do Centro Nacional de Cibersegurança (CNCS) de Portugal, divulgou seu Relatório, em dezembro de 2020[21]. Segundo o documento, Portugal ainda está abaixo da média da UE no que tange a uma melhor proteção possível contra as ameaças do ciberespaço. O Relatório apresenta indicadores e análise global que permitem estabelecer visão panorâmica sobre os pontos fortes e fracos dos indivíduos e das organizações quanto às boas práticas de cibersegurança.

Não obstante, os dados absolutos e as tendências anuais são, em parte, positivos. Além disso, a educação e a sensibilização dos utilizadores melhoraram em vários aspetos, apresentando indicadores também mais favoráveis, o que demonstra um potencial de crescimento em outros domínios.

1.1.3.2 Cibersegurança no Brasil

No Brasil a situação não difere muito de Portugal. O país carece de uma política governamental que enquadre a cibersegurança quase como um objetivo nacional. Os cibercriminosos têm agido com muita liberdade ao comprometer o sigilo e o uso abusivo de dados em atividades diferentes daquelas para os quais foram coletados.

Verdadeira análise sobre como o Brasil lida com a segurança cibernética foi apresentada em Relatório divulgado em 2020 pela Organização dos Estados Americanos (OEA). Intitulado "Revisão de capacidade de cibersegurança – República Federativa do Brasil", a publicação analisa avanços na área obtidos desde 2010, assim como os desafios para os próximos anos[22]. O documento traz, entre outros fatos, a necessidade de o país promover efetivamente a cultura da segurança na internet, além de listar como um grande problema a falta de mão de obra especializada em cibersegurança.

1.2 O DIREITO À PRIVACIDADE E O DIREITO À PROTEÇÃO DE DADOS

Conhecer a distinção entre o Direito à Privacidade e o Direito à Proteção de Dados é importante a fim de repelir confusões e mal-entendidos sobre as obrigações e os direitos legais. Também é essencial que as empresas e organizações compreendam que têm obrigações

[21] **Relatório Cibersegurança de 2020**. Disponível em www.cncs.gov.pt. [Consult. 10 abr. 2021].
[22] OEA-**Revisão de capacidade de cibersegurança – República Federativa do Brasil**. Disponível https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf. [Consult. 10 abr. 2021].

com a proteção de dados, bem assim os indivíduos, na medida em que devem proteger seus dados pessoais e respeitar os dados de outrem. A maioria dos instrumentos jurídicos de proteção de dados identifica a proteção do direito à privacidade como uma das principais justificativas para a sua promulgação. Contudo, trata-se de conceitos diferentes.

O conceito de privacidade sofreu modificações ao longo do tempo, o que torna difícil determinar uma definição exata para ele, segundo Joana de Moraes Souza Machado[23]. As acepções sobre a privacidade iniciaram-se com uma abordagem individualista baseada no artigo "The Right to Privacy", de Samuel D. Warren e Louis Brandeis[24], publicado em 1890, na *Harvard Law Review* nº 4, em que defendiam a existência de um direito garantido à pessoa para repelir e evitar intromissões indevidas em sua intimidade, resguardando a sua tranquilidade pessoal para uma visão mais ampla, como expõe Danilo Doneda[25]: "[…] a privacy, hoje, compreende algo muito mais complexo do que o isolamento ou tranquilidade – algo de que o próprio Brandeis, tendo se ocupado do assunto posteriormente, tinha ciência".

Do mesmo modo, Carlos Alberto Bittar[26] ressalta a relevância do citado direito de proteger a privacidade em seus inúmeros pontos de vista; por exemplo, sob o caráter familiar, pessoal ou relativo aos negócios desenvolvidos pelo titular dos dados. Parece-nos que, nesse conceito, o direito à privacidade é definido sob o seu aspeto mais objetivo.

Patrícia Cardoso Dias esclarece que o direito à proteção de dados é mais amplo do que o direito à reserva sobre a intimidade da vida privada, "projetando-se a tutela relativamente a todas as operações e categorias de dados pessoais tratados independentemente da relação que se estabelece com a privacidade"[27]. Carlos Alberto da Mota Pinto entende que a privacidade é "merecedora da tutela do conteúdo da vida privada de uma pessoa, englobando os seus sacrifícios familiares e pessoais, ou mesmo seus sentimentos"[28]. Rabindranath Capelo de Sousa também destaca a proteção do direito à privacidade voltado ao plano íntimo do titular dos dados, relativos à "assunção de sua

[23] MACHADO, Joana de M. S. – **A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados**. Disponível em http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/viewFile/206/142. [Consult. 20 mar. 2021]

[24] WARREN Samuel; BRANDEIS Louis – The Right to Privacy. Boston. **Harvard Law Review**, n. 4, 1890. Disponível em https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. [Consult. 19 abr. 2021].

[25] DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006. p. 8-10

[26] BITTAR, Carlos Alberto – **Os Direitos da Personalidade**. 8ª. ed. São Paulo: Saraiva, 2015. p. 172.

[27] DIAS, Patrícia C. – Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos éticos-jurídicos relevantes da protecção de dados de saúde no âmbito da emergência de saúde pública. **JULGAR Online**. Janeiro 2021, p. 1-45. Disponível em http://julgar.pt/author/patricia-cardoso-dias/. [Consult. 22 jun. 2022].

[28] MOTA PINTO, Carlos Alberto da – **Teoria Geral do Direito Civil**. 4ª. ed. Reimpressão. Coimbra: Coimbra Editora, 2017. p. 212.

escala de valores"[29], ou seja, àqueles relativos à sua prática e condução de seu comportamento.

Há de se notar dos conceitos acima, que a doutrina portuguesa destaca com afinco a proteção aos sentimentos e valores do titular do direito. Porém, no plano prático, parece não existir diferença quanto à proteção do direito à privacidade, seja em Portugal ou no Brasil. Os conceitos, enfim, são equivalentes.

Privacidade, por fim, significa o direito de o indivíduo manter o controlo sobre informações relativas à sua vida privada, familiar, doméstica e de suas comunicações.

Em 1997, Roger Clarke[30] dividiu a privacidade em quatro categorias: (1) a privacidade do indivíduo (entendida em termos físicos); (2) a privacidade de comportamento humano; (3) a privacidade das comunicações pessoais; e (4) a privacidade dos dados pessoais. Outros juristas[31], baseados no modelo de Clarke, expandiram o conceito de privacidade ao abranger outras características e o dividiram em sete tipos: (1) a privacidade das pessoas; (2) a privacidade de pensamentos e sentimentos; (3) a privacidade do local e espaço; (4) a privacidade de dados pessoais e imagens; (5) a privacidade de comportamento e de ações; (6) a privacidade das comunicações; e (7) a privacidade de associação.

Embora não haja consenso a respeito de um significado preciso e definitivo sobre o direito à privacidade, suas várias conceituações têm encontrado aplicação na proteção de dados pessoais. Por exemplo: os direitos de o titular dos dados ao apagamento ou ao esquecimento; ou o tratamento especial a certos tipos de dados sensíveis, tais como a saúde ou a vida sexual, podem ser vistos como esforços para limitar o acesso aos mais íntimos detalhes pessoais. Nenhum dos conceitos de privacidade consegue, no entanto, abranger todos os direitos e todas as obrigações estabelecidas na legislação de proteção de dados.

O direito à proteção de dados, de seu lado, compreende a proteção em relação à recolha, ao uso e aos demais tratamentos de dados pessoais relativos a um indivíduo identificado ou identificável, independentemente de serem informações privadas, profissionais ou mesmo publicamente disponíveis. O direito à proteção de dados é

[29] CAPELO DE SOUSA, Rabindranath – **O Direito Geral da Personalidade**. Coimbra: Coimbra Editora, 1995. p. 317.
[30] CLARKE, Roger – **Introduction to Dataveillance and Information Privacy, and Definitions of Terms.** Xamax Consultancy. Disponível em http://www.rogerclarke.com/DV/Intro.html. [Consult. 29 mar. 2021].
[31] FINN Rachel L; WRIGHT David; FRIEDEWALD, Michael – **Seven Types of Privacy**. Disponível em https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.827.5418&rep=rep1&type=pdf. [Consult. 29 mar. 2021].

relativo, portanto, à divulgação, à segurança e ao tratamento dispensado a esses dados pessoais.

Outra consideração sobre os dois direitos refere-se ao tipo de liberdades que representam. A privacidade é considerada uma "liberdade negativa", no sentido de não sofrer interferência alheia, não poder ser violada nem desrespeitada. A privacidade está lá posta, estática, à espera de uma violação. É uma liberdade que aguarda que o seu titular defina quais informações suas podem ser levadas ao público ou não, conforme expõe Gabriela Machado Vergili[32].

De outro lado, o direito à proteção de dados é uma "liberdade positiva". Ao contrário do direito à privacidade, trata-se de um direito dinâmico. É uma liberdade positiva no sentido de que há um espaço a ser construído. E é neste contexto, por exemplo, que as leis que regulamentam a proteção de dados asseguram ao titular o direito a ter acesso aos seus dados, o direito de retificá-los e, ainda, garantem ao titular a possibilidade de revogação de seu consentimento ou portabilidade de seus dados, conforme explica Cris Beux.[33]

Em última análise, a privacidade se estende para além do mero controlo de dados, com o objetivo de proteger o direito de seu titular ser deixado sozinho, o direito ao isolamento, o direito ao livre desenvolvimento da personalidade e assim por diante. Por outro lado, o direito à proteção de dados identifica, de forma autónoma, valores dignos de proteção nem sempre considerados no âmbito da vida privada, como a segurança dos sistemas de informação, a qualidade dos dados, o princípio da não discriminação, a liberdade de informação e comunicação.

Compreender a diferença entre os dois direitos é essencial para a construção de uma sólida cultura de proteção de dados responsável[34], bem assim de importância

---

[32] VERGILI, Gabriela M. – **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados.** Disponível em https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados. [Consult. 19 abr. 2021].

[33] BEUX, Cris – **Privacidade e proteção de dados são coisas diferentes**. Disponível em https://www.linkedin.com/pulse/privacidade-e-prote%C3%A7%C3%A3o-de-dados-s%C3%A3o-coisas-diferentes-cris-eux?articleId=6673216800903229440#:~:text=O%20direito%20%C3%A0%20prote%C3%A7%C3%A3o%20de,livremente%20desenvolver%20a%20sua%20liberdade.&text=%C3%89%20uma%20liberdade%20positiva%20no,um%20espa%C3%A7o%20a%20ser%20constru%C3%ADdo. [Consult. 19 abr. 2021].

[34] KOKOTT, Juliane; SOBOTTA, Christoph – The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. **International Data Privacy Law**, Volume 3, Issue 4, November 2013. p. 222–228. Disponível em https://academic.oup.com/idpl/article/3/4/222/727206. [Consult. 25 mar. 2021].

fundamental para balizar as relações na vida atual, e, no caso deste estudo, para se admitir a adequada resolução de disputas online.

Não obstante, esses dois direitos possuem diferenças, conforme exposto acima. O direito à privacidade e o direito à proteção de dados encontram-se intimamente ligados, pois a observância deste garante, ao fim e ao cabo, que o seu titular desfrute e veja respeitado o seu direito personalíssimo à vida privada, de acordo com os termos e conclusões da Advogada- Geral Eleanor Sharpston no âmbito dos processos C-92/09 e C-93/09, n.º 72[35].

O artigo 8º da Convenção Europeia dos Direitos Humanos (CEDH)[36] define e reconhece o direito à privacidade. A Declaração Universal dos Direitos Humanos (DUDH), em seu artigo 12º, prevê a proteção legal a todo ser humano à ausência de "interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação"[37]. Obsta-se, portanto, qualquer intromissão estatal na vida privada dos cidadãos, salvo se houver previsão legal ou em algumas circunstâncias designadas, tais como para proteger a segurança pública ou o bem-estar económico do país, entre outras situações previstas.

Em Portugal, o artigo 35º da Constituição de 1976 prevê a garantia ao acesso de dados informatizados pelos cidadãos, desde que lhe digam respeito, bem como o direito à retificação e atualização, além de conhecer a destinação que lhe será atribuída. O direito à utilização da informática encontra-se incluso no Título II, nominado como direitos, liberdades e garantias, e sob a Parte I, relativo aos direitos e deveres fundamentais, a demonstrar que a proteção de dados foi alçada à categoria de direito fundamental. Esta garantia constitucional deve ser conjugada com a proteção prevista no artigo 26º, número 1, da Constituição da República Portuguesa (CRP) que, entre outros direitos, assegura expressamente o direito à reserva da intimidade da vida privada e familiar. Em Portugal,

---

[35] Disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=80291&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=11269075. [Consult. 23 nov. 2021].

[36] "Artigo 8.º– Direito ao respeito pela vida privada e familiar.

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros." Convenção Europeia dos Direitos do Homem. Disponível em https://www.echr.coe.int/documents/convention_por.pdf. [Consult. 1º abr. 2021].

[37] Disponível em https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. [Consult. 1º abr. 2021].

portanto, a proteção de dados e as garantias para utilização da informática estão expressamente previstas.

No Brasil, o artigo 5º, inciso X, da Constituição, estabelece a inviolabilidade à intimidade, vida privada, honra e imagem das pessoas e, na hipótese de violação desses bens jurídicos, estabelece o direito à indenização, seja pelo dano moral, seja pelo dano material. Em fevereiro de 2022, foi promulgada a Emenda à Constituição n.º 115/2022, que acrescentou o inciso LXXIX ao artigo 5º da Constituição da República Federativa do Brasil (CF), de 1988, a fim de assegurar "nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais", do que se pode concluir – quanto à proteção constitucional inicial da intimidade e vida privada – que o legislador brasileiro avançou no sentido de abranger também os dados pessoais.

De fato, o avanço exponencial da tecnologia nas sociedades globalizadas acaba por impingir modificações nas relações pessoais e comerciais a provocar novas indagações jurídicas sobre o direito à privacidade e aos dados pessoais. A transformação dessas relações configura um novo desafio aos operadores do direito e aos legisladores, tanto em Portugal como no Brasil.

1.2.1 Princípios do direito à proteção de dados em Portugal

Em 2016, a União Europeia adotou um diploma legal sobre a proteção de dados com validade em todos os países da União denominado Regulamento Geral sobre a Proteção de Dados (RGPD), objeto do Capítulo III deste trabalho. O RGPD contém um conjunto único de regras disciplinadoras da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados no âmbito da União Europeia. O RGPD foi acolhido pela ordem jurídica portuguesa em 8 de agosto de 2019, ocasião na qual a Assembleia da República aprovou a Lei n.º 58/2019 e estabeleceu em seu artigo 1º a proteção no tocante ao tratamento de dados pessoais[38].

O artigo 5º do RGPD estabelece os princípios que o tratamento de dados pessoais deve observar. Neste sentido, o Princípio da licitude, lealdade e transparência determina ao responsável pelo tratamento a transparência no processamento de dados em relação ao titular dos dados. Já o Princípio da limitação das finalidades visa garantir que os dados

[38] "Artigo 1.º – Objeto. A presente lei assegura a execução, na ordem jurídica interna, do 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, doravante designado abreviadamente por Regulamento Geral de Proteção de Dados (RGPD)."

pessoais devem ser recolhidos e tratados apenas para uma utilização específica e legítima, correspondendo às missões do estabelecimento ou do responsável pelos dados. O uso indevido ou fora desse propósito é punível com penalidades criminais. Este princípio estabelece que os dados pessoais recolhidos não possam posteriormente, e de forma inconciliável com esses objetivos, ser novamente tratados, salvo exceções previstas no texto legal, quais sejam: na hipótese de o tratamento posterior à finalidade inicial ser necessário para o arquivamento com fundamento no interesse público ou para a investigação científica, histórica ou a coleta de dados estatísticos, desde que cumprida a norma do artigo 89º, número1.

De outro lado, o RGPD exige que os dados sejam recolhidos apenas para um processamento muito específico e claramente definido. É o Princípio da minimização dos dados. O RGPD visa garantir, ainda, que os dados tratados sejam exatos e, quando necessário, objeto de atualização, além de serem tomadas todas as medidas adequadas para que os dados considerados inexatos sejam apagados (Princípio da Exatidão). O Princípio da limitação da conservação, por sua vez, determina que as informações devem ser mantidas em arquivos de computador, conforme o objetivo de cada arquivo. Além desse limite, os dados devem ser excluídos ou tornados anónimos. A adequada e correta proteção de dados pessoais está garantida pelo Princípio da integridade e confidencialidade. Por fim, o Princípio da responsabilidade é direcionado ao responsável pelo tratamento, no sentido de que deveobservar os princípios supra-referidos.

Infere-se dos princípios do RGPD, portanto, um conjunto de normas que visa assegurar a proteção de dados para legitimar seu uso adequado e a sua segurança ao longo de seu ciclo de vida, isto é, desde a sua obtenção até que sejam finalmente destruídos, eliminados ou apagados. Estes princípios, pode-se afirmar, encontram amparo nos documentos internacionais de proteção de dados[39].

1.2.2 Princípios do Direito à Proteção de Dados no Brasil

À semelhança do RGPD, o Brasil aprovou a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709, de 14 de agosto de 2018[40], com vigência a partir de

[39] Por exemplo, a Declaração Universal dos Direitos do Homem (artigo 12º), o Pacto Internacional de Direitos Civis e Políticos (artigo 17º), a Convenção Europeia dos Direitos do Homem (artigo 8º), a Carta dos Direitos Fundamentais da União Europeia (artigos 7º e 8º), entre outros.

[40] Lei nº13.709, de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. [Consult. 10 abr. 2021].

agosto de 2020. A Lei, que também será analisada com maiores detalhes no Capítulo III, prevê dez princípios norteadores[41] contra os sete princípios do RGPD.

Não obstante a diferença numérica de princípios vigentes em Portugal (RGDP) e no Brasil (LGPD) podemos inferir que existe quase uma concordância entre os princípios que preservam a proteção de dados nos dois países.

De modo geral, percebe-se em ambos os ordenamentos jurídicos que os princípios regentes da utilização de dados pessoais se preocupam em garantir ao titular desse direito segurança, lealdade e transparência na utilização de seus dados, além de fixar que o tratamento destes dados tenha objetivo definido e limitado, bem como visam delimitar responsabilidades àqueles que se utilizam dos dados pertencentes a outrem. Por exemplo, podemos citar o Princípio da finalidade e da necessidade previstos na LGPD como similar ao Princípio da limitação das finalidades do RGPD.

Esta coincidência de princípios revela, de fato, um mesmo tecido jurídico, isto é, um mesmo encadeamento de normas de forma a resultar maior segurança no tratamento dos dados pessoais. Ora, em um mundo globalizado, onde é possível aceder informações quase imediatamente e em qualquer lugar do planeta, a similitude dos preceitos legais que regulamenta a proteção de dados significa um avanço e, portanto, maior proteção ao direito à privacidade dos cidadãos.

[41] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I– finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II– adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
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;
IV– livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V– qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI– transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII – segurança: 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;
VIII– prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX– não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X– responsabilização e prestação de contas: 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."

1.2.3 Direitos dos titulares de dados pessoais

Os dados pessoais, como o próprio nome indica, são de propriedade das pessoas que eventualmente os cedem para a prática de determinadas operações, mas os seus titulares continuam a exercer os direitos incidentes sobre os seus próprios dados. Tanto o RGPD como a LGPD garantem a titularidade desses direitos. O direito à proteção de dados nos países- membros da UE pode ser dividido em três categorias[42]. Alguns países incluíram em seus textos constitucionais o direito à proteção de dados como um direito independente (i); outros entenderam que este é derivado do direito à privacidade (ii), este sim previsto nas respectivas Constituições; e, finalmente, os países cuja Constituição não faz nenhuma alusão à proteção de dados (iii). Portugal faz parte do primeiro grupo, pois o artigo 35º e o artigo 26º, número 1, ambos da CRP, são explícitos ao reconhecer esse direito.

Além do direito manifestado explicitamente na CRP, aos proprietários dos dados são reconhecidos os direitos compreendidos no artigo 15º[43] e seguintes do RGPD. Entre esses direitos nota-se a prerrogativa de ter conhecimento, isto é, informação sobre a sucessão de tratamento sobre seus dados pessoais e, neste caso, obter informações sobre o uso e o armazenamento dos referidos dados (Direito de confirmação e acesso). Decorre, ainda, a possibilidade de o titular retificar seus dados pessoais colhidos de forma incorreta, errônea ou inverídica (Direito de retificação) ou, ainda, solicitar que os seus dados sejam apagados (Direito ao apagamento dos dados ou Direito a ser esquecido).

O RGPD permite que o titular de dados exerça concretamente suas prerrogativas, em consonância com o Princípio da licitude, lealdade e transparência, bem como com o Princípio da exatidão, ao conferir ao titular de dados amplo domínio e exercício sobre os seus dados (Direito de oposição). O Direito de portabilidade dos dados e o Direito de não ser submetido a decisões automatizadas encerram a gama de direitos que outorga ao titular dos dados o monitoramento efetivo no que diz respeito aos dados que lhe são atinentes.

O Brasil recentemente ingressou no grupo de países onde a Constituição Federal contempla a proteção de dados pessoais como direito fundamental autónomo e explícito, com

[42] Categorias, expressão utilizada no sentido filosófico do termo, isto é: " 6) FILOSOFIA conceito muito geral que exprime as diversas relações que podemos estabelecer entre as ideias e os factos" Porto Editora – *categoria* no Dicionário infopédia da Língua Portuguesa. Porto: Porto Editora. [Em linha]. [Consult. 2022-06-29]. Disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/categorias.

[43] RGPD – DIREITOS DO TITULAR DOS DADOS. Capítulo III. Artigo 15º e seguintes. Disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?qid=1559291025147&uri=CELEX:32016R0679#d1e2468-1-1. [Em linha]. [Consult. 10 abr. 2021].

a promulgação da Emenda à Constituição n.º 115/2022, em fevereiro de 2022. Esta recente alteração constitucional encontra fundamento na literatura jurídica, bem assim em diversas ações judiciais que ensejaram decisões judiciais[44], inclusive oriundas do Supremo Tribunal Federal (STF), favoráveis à proteção de dados pessoais antes mesmo da citada modificação do texto constitucional.

De se notar que a LGPD, de maneira praticamente idêntica ao RGPD[45], estabelece os seguintes direitos para os titulares de dados pessoais: Direito a ser informado; Direito de contestar; Direito de acesso; Direito de não ser sujeito a discriminação para desfrutar seus direitos; Direito à portabilidade de dados e Direito de apagamento de dados (ou Direito de esquecimento de dados).

No que concerne ao Direito de apagamento de dados, porém, existe uma diferença fundamental entre os dois países.

Em Portugal, o apagamento de dados está ligado ao Direito ao esquecimento. Pedro Trovão do Rosário, ao analisar o Direito ao esquecimento e o RGPD, conclui pela ampliação e afirmação do Direito a ser esquecido nomeadamente sobre fatos que "já não tenham interesse público"[46]. Neste caso, é necessário exemplificar e comentar o conhecido processo judicial referente ao pedido de Mario Costeja González, cidadão espanhol, que pretendia fossem alteradas ou excluídas as páginas eletrónicas do motor de busca Google com informações relativas a um antigo processo de execução (hasta pública) sofrido em 1998, umavez que já havia sido extinto. Inicialmente, ingressou com pedido administrativo junto ao jornal (2009) e ao Google Spain (2010), sem obter êxito. Posteriormente, entrou com o pedido administrativo perante a Agência Espanhola de Proteção de Dados (AEPD), em março de 2010, contra a empresa *La Vanguardia Ediciones SL,* que publica periódico com nome idêntico na Catalunha e, também, contra o Google Spain e o Google Inc.

A AEPD, em julho de 2010, rejeitou o pedido de Mario Costeja González em face da agência de notícias, uma vez que o jornal era tão-somente o meio de divulgação da hasta pública. Em relação ao Google Spain e Google Inc., a AEPD decidiu que o motor de busca sesubmete à legislação relativa à proteção de dados pessoais porque abrangeria também o direito de o requerente resguardar os seus dados pessoais para que não fossem

[44] ADI 6.387 MC-Ref/DF, Min Relatora: Rosa Weber, julgado em 6 e 7 de maio de 2020, STF, voto conjunto com as ADIs 6.389, 6.390, 6.393, 6.388 e 6.387.
[45] ROSÁRIO, Pedro T. – O Direito a ser esquecido. Revista de Direito Santa Cruz do Sul. V. 3, n. 53, set./dez. 2017, p. 121-139. Disponível em https://online.unisc.br/seer/index.php/direito/issue/view/496. [Consult. 11 jul. 2022].

conhecidos por outrem. Portanto, o Google Spain e Google Inc. deveriam retirar de suas páginas eletrónicas as informações relativas ao requerente, com fundamento no direito fundamental da proteção de dados e, também, em observância ao Princípio da dignidade da pessoa humana em sentido amplo.

O Google Spain e o Google Inc. impugnaram a decisão da AEPD junto à Audiência Nacional, órgão pertencente ao Poder Judiciário espanhol, com atribuições sobre todo o território do país, cujas decisões cabem recurso ao Supremo Tribunal de Espanha. Neste caso, a Audiência Nacional decidiu que seria necessário devolver o processo para julgamento perante o Tribunal de Justiça da União Europeia (TJUE), por considerar que a matéria envolvia a aplicação da Diretiva 95/46, de 1995, do Parlamento Europeu e do Conselho da União, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

O TJUE, em 13 de maio de 2014, julgou a ação, cujo pedido envolvia a interpretação do artigo 2°, alíneas 'b' e 'd'; artigo 4°, inciso 1, alíneas 'a' e 'c'; artigo 12º, alínea 'b', e artigo 14º, parágrafo primeiro, alínea 'a', todos da Diretiva 95/46, de 1995, bem como do artigo 8° da Carta dos Direitos Fundamentais da União Europeia.

Inicialmente, o TJUE entendeu, em relação à natureza das atividades dos motores de busca, que estes realizam tratamento de dados na forma do artigo 2°, alínea 'b', da Diretiva 95/46, bem assim possuem a qualidade de responsáveis pelos dados que trafegam em suas páginas, nos termos do artigo 2°, alínea 'd', da citada Diretiva. O entendimento foi que a atividade dos motores de busca pode afetar sensivelmente "os direitos fundamentais à vida privada e à proteção dos dados pessoais", de modo que:

> [...] o operador desse motor, como pessoa que determina as finalidades e os meios dessa atividade, deve assegurar, no âmbito das suas responsabilidades, das suas competências e das suas possibilidades, que essa atividade satisfaça as exigências da Diretiva 95/46, para que as garantias nela previstas possam produzir pleno efeito e possa efetivamente realizar-se uma proteção eficaz e completa das pessoas em causa, designadamente do seu direito ao respeito pela sua vida privada.[46]

O TJUE também considerou que, apesar de o Google Inc. ter sua sede localizada nos Estados Unidos da América e o Google Spain no país europeu, a Diretiva não pode ter interpretação restritiva, ao menos em território europeu, pois deve assegurar liberdades e direitos fundamentais de maneira completa. Assim, quanto ao direito à

[46] Disponível em https://curia.europa.eu/juris/document/document.jsf?doclang=PT&text=&pageIndex=1&part=1&mode=req&docid=152065&occ=first&dir=&cid=201752. [Consult. 22 nov. 2021]

oposição do titular de dados, o TJUE ponderou sua aplicação e determinou que será aplicável quando os dados (a) forem inexatos; (b) inadequados; (c) impertinentes ou (d) excessivos. Essa qualificação deverá considerar os seguintes fatores: (a) atualização do tratamento de dados ou (b) conservação dos dados por tempo superior ao necessário, "a menos que a sua conservação se imponha para finalidades históricas, estatísticas ou científicas". Nota-se designadamente, nesta parte da decisão do TJUE, a aplicação concreta dos princípios do RGPD.

Neste caso em particular, vale destacar a atribuição de peso ao quesito temporal na fundamentação do acórdão, pois verificou-se que "mesmo um tratamento inicialmente lícito de dados exatos se pode tornar, com o tempo, incompatível com esta diretiva, quando esses dados já não sejam necessários atendendo às finalidades para que foram recolhidos ou tratados". O processo de Mario Costeja González é um exemplo evidente dessa inadequação superveniente, uma vez que as informações sobre a hasta pública deixaram de ser adequadas com o passar do tempo.

No Brasil, já houve apreciação semelhante pelo Poder Judiciário, ou seja, divulgação de informações ampla e legalmente divulgadas que, com o longo passar do tempo, o(s) interessado(s) solicita(m) o apagamento dessas informações na mídia ou no motor de busca. No caso brasileiro, um crime que causou grande impacto na sociedade na década de 1950 foi reconstituído por um programa televisivo em 2004. Os familiares ingressaram com a ação judicial contra a emissora requerendo uma reparação, uma vez que não houve autorização dos familiares para a reconstituição do crime abjeto que, ao final, acabaria expondo de maneira vexatória a imagem e os dados da vítima.

Em 11 de fevereiro de 2021, o STF julgou por maioria que o Direito ao esquecimento fere a Constituição brasileira. A tese de repercussão geral, firmada no aludido julgamento, foi a seguinte:

> É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo a, divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social – analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível.[47]

[47] Recurso Extraordinário (RE) 1010606 – STF conclui que direito ao esquecimento é incompatível com a Constituição Federal. Resumo das teses afiançadas pelos Ministros disponível em http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1. [Consult. 11 abr. 2021].

Infere-se das transcrições acima que o RGPD (vigente em Portugal) e a LGPD (vigente no Brasil) possuem disposições parecidas em relação aos seus princípios e às suas finalidades atinentes à proteção da privacidade e à proteção de dados pessoais. De outro lado, verifica-se que o entendimento do TJUE e do STF não são coincidentes, mesmo ainda em relação ao quesito temporal. No caso do Google Spain, a passagem do tempo serviu para proteger o direito do requerente. No caso brasileiro, a passagem do tempo não pôde ser utilizada para inibir o direito à informação e à memória coletiva.

1.2.4 Ciclo de vida do tratamento dos dados pessoais

Para bem usufruir os direitos relativos aos dados pessoais, seja em Portugal ou no Brasil, torna-se forçoso conhecer o ciclo de vida dos dados pessoais[48]. Inicialmente, registre- se que os dados pessoais são coletados para atender a uma finalidade específica e podem, por exemplo, ser eliminados a requerimento de seu titular ou na finalização de seu tratamento. Dessa forma, a configuração de um ciclo de vida se inicia com a recolha e termina com a sua exclusão. Com o intuito de representar o ciclo destacado acima, é proposto ciclo de vida de dados pessoais em cinco fases: recolha, retenção, processamento, compartilhamento e eliminação.[49]

Ao conhecer as fases do ciclo de vida dos dados pessoais poderemos relacionar, a cada fase, a aplicação concreta dos direitos do titular de dados previstos na RGPD e na LGPD. Por exemplo, se é solicitado o compartilhamento dos dados pessoais do cidadão quando utiliza o serviço médico, é importante que o titular possua absoluta ciência de que se trata da recolha de seus dados pessoais, que examine com atenção o tempo de armazenamento e as suas finalidades, e, sobretudo, que o seu consentimento seja livre, informado, específico e explícito, a fim de que os princípios expostos na RGPD e LGPD sejam de fato e concretamente cumpridos.

[48] As fases do ciclo de vida referem-se, basicamente, ao tratamento de dados, cuja definição consta no artigo 4º, alínea 2 do RGPD. O tratamento de categorias especiais de dados pessoais está previsto no artigo 9º; aquele relativo às condenações penais, no artigo 10º e o que não exige identificação no artigo 11º, todos do RGPD. O tratamento dos dados pessoais é regulamentado pelo RGPD, em especial nos artigos 13º a 22º e 34º.

[49] É importante notar que na literatura sobre o assunto há um número diferente de fases (entre quatro e sete). Geralmente, todos eles descrevem as mesmas coisas, mas combinam fases semelhantes ou quando existem alternativas (por exemplo, destruir ou arquivar). Nesta dissertação o número de fases foi baseado no trabalho da Escola de Nacional de Administração Pública do Brasil (ENAP). Disponível em https://enap.gov.br/pt/. [Consult. 10 mar. 2021].

1.2.4.1 Fases do ciclo de vida

a) Recolha ou Coleta[50]

A recolha é o primeiro passo do ciclo de vida, sempre iniciada por um problema ou uma necessidade específica. A criação de dados pode ser motivada por muitas e variadas fontes. O modo de coleta pode ser importante para o procedimento relativo à proteção dos dados, uma vez que formulários eletrónicos apresentam riscos diferentes de documentos em papel, por exemplo. Assim, essa também é uma informação relevante nas definições de privacidade. A coleta deve ser guiada pelos limites de privacidade bem definidos e captar apenas os dados que foram declarados necessários para as finalidades almejadas.

b) Retenção ou Armazenamento

Os dados devem ser armazenados e preservados em determinado dispositivo, a partir do momento de sua criação. É importante armazená-los corretamente e em local adequado para garantir a sua viabilidade e evitar qualquer perda. O armazenamento pode ser feito de diferentes maneiras, por exemplo: disco rígido, servidor, nuvem. O importante é que o ambiente seja seguro ou mesmo qualificado, a depender da atividade e da espécie dos dados obtidos.

Uma vez que a obrigação de segurança faz parte dos princípios de proteção de dados, o responsável deve oferecer infraestrutura necessária para garantir sua proteção. Da mesma forma, apenas pessoas autorizadas devem ter acesso aos dados. O essencial é manter a conformidade, integridade, disponibilidade e capacidade de auditoria dos dados.

c) Tratamento de dados

O tratamento de dados deve ser entendido como qualquer operação, ainda que realizada sem meio eletrónico, de coleta, consulta, processamento, conservação, organização, modificação, comparação, utilização, comunicação, divulgação, transferência, cancelamento, destruição de dados, mesmo que não registrada em um banco de dados.

O processamento deve responder ao chamado Princípio da necessidade, isto é, a

[50] Nota-se que a legislação portuguesa utiliza a expressão “recolha” e, no Brasil, o termo usual é “coleta”. Entretanto, ao consultar o dicionário virtual www.infopedia.pt, foi verificado que em Portugal o termo coleta também significa arrecadação de bens, objetos, dados etc.; recolha, colheita.

utilização de dados pessoais e de identificação deve ser minimizada, de forma a excluir o tratamento quando o fim perseguido, em casos individuais, possa ser alcançado por meio de dados anónimos ou métodos que permitam identificar o titular dos dados apenas em caso de necessidade.

O tratamento de dados não é um procedimento isento de problemas. Ele, *de per si*, não prejudica os titulares desses dados, mas os principais problemas levantados pelo processo estão relacionados a abusos, tais como discriminações pessoais ou advindos da aplicação de determinada norma em que o justo e o errado são de difícil definição. Por exemplo, há quem considere que as seguradoras de automóveis e/ou viaturas agem corretamente ao aumentar o valor do prêmio para motoristas que habitam regiões consideradas perigosas em determinada localidade. Outros veem isso como uma penalidade injusta, pois entendem que a sua privacidade é prejudicada quando as seguradoras monitoraram seus dados pessoais.

A principal preocupação dos legisladores deve ser criar normas que regulem quais tipos de dados afetam, realmente, a privacidade dos seus detentores, juntamente com regras claras que permitam a aplicação de leis para prevenir e processar abusos, como crimes cibernéticos, fraude e discriminação. Isso permitirá que o processo beneficie as pessoas sem prejudicar a sua privacidade – um bem tão precioso nos tempos atuais.

Trata-se, portanto, da etapa mais abrangente do ciclo de vida do uso de dados pessoais.É a etapa em que é definida como o dado será utilizado, pois quando necessário, os dados deverão ser processados para fornecer informações. Em conclusão, a escolha do meio de tratamento deve respeitar a integridade dos dados e não ultrapassar os limites, as finalidades eas necessidades que fundamentaram a recolha e o armazenamento dos dados.

d) Compartilhamento

O compartilhamento de dados consiste na divulgação dos dados a outros atores. Na maior parte das vezes, o compartilhamento de dados ocorre internamente entre diferentes departamentos de uma mesma empresa. No entanto, esse compartilhamento pode ser externo, ou seja, partilhado com atores confiáveis, porém, fora da estrutura da empresa que recolheu e realizou o tratamento dos dados. Em resumo, trata-se de qualquer transação que envolva reprodução, transmissão, distribuição, comunicação, transferência e difusão de dados. De toda forma, esse compartilhamento deve ser estritamente harmonioso, enquadrado e regulamentado, a fim de evitar qualquer alteração ou ataque malicioso.

e) Eliminação

A quantidade de dados arquivados aumenta inevitavelmente, o que torna impossível salvar os dados por tempo indeterminado. Ademais, os custos de armazenamento e os problemas de conformidade exercem pressão para eliminar dados que não são mais necessários.

Destruição ou eliminação de dados é a operação que visa apagar ou excluir dados pessoais. Essa fase também contempla o descarte dos ativos organizacionais nos casos necessários ao negócio da instituição, bem assim a remoção de todas as cópias de determinados dados de uma organização. Normalmente, inicia-se em um local de armazenamento de arquivo. O desafio dessa fase do ciclo de vida é garantir que tais dados tenham sido destruídos adequadamente. Antes da destruição, porém, é importante assegurar que os itens de dados excederam o período de retenção regulamentar exigido.

1.2.4.2 Consentimento no Regulamento Geral sobre a Proteção de Dados e na Lei Geral de Proteção de Dados Pessoais

Durante as etapas do ciclo de vida é importante que fique bem definido os termos de consentimento e as políticas de privacidade, de forma que o titular possa ter ciência e controlo sobre os próprios dados.

O consentimento do titular dos dados na União Europeia é definido em Portugal pelo art. 4º, número 11[51], e, também deve ser observado o considerando número 42 do RGPD[52]. Por sua vez, no Brasil, o consentimento do proprietário dos dados está previsto no artigo 5º, inciso XII, da LGPD[53]. Percebe-se, portanto, que as definições para o consentimento nos dois países são praticamente idênticas ao conferir ao cidadão algum

[51] "(11) Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento."

[52] "(42) Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Em conformidade com a Diretiva 93/13/CEE do Conselho (1), uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado."

[53] "XII – consentimento: a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada."

poder de controlo sobre dados que lhe digam respeito. Para a validação do consentimento, devem ser cumpridos os seguintes requisitos cumulativos[54]: (i)-manifestação de vontade inequívoca, ou seja, o consentimento exige do titular dos dados uma declaração inequívoca, o que significa uma ação positiva ou declaração, isto é, não há lugar a autorizações tácitas ou consentimento baseado no silêncio; (ii)-consentimento livre, isto é, o titular não pode sofrer coação ou ser influenciado. Uma escolha real deve ser oferecida a ele, sem sofrer consequências negativas na hipótese de recusa ou, ainda, de outro modo: a recusa de consentimento para o processamento de dados não deve resultar em qualquer consequência na execução de um contrato ou na prestação de determinado serviço. Quanto a esse consentimento livre há de se registrar uma observação, uma vez que muito aplicativos para telemóveis gratuitos não funcionam se não houver o consentimento com a política de tratamento de dados da empresa que desenvolveu o aplicativo, o que contraria esse requisito; (iii)-finalidade específica, ou seja, cada consentimento deve corresponder a um único tratamento, a um único objetivo específico. Portanto, para realizar o processamento que tenha várias finalidades, os titulares de dados devem consentir com cada um deles, de maneira independente; (iv)-consentimento informado, a validação do consentimento deve vir acompanhado de informação prévia, suficiente e bastante à elucidar o titular de dados sobre seus termos. Além das obrigações de transparência, deve ser fornecido aos titulares dos dados a identidade do controlador, os objetivos perseguidos, as categorias de dados coletados, e a existência do direito de retirar o consentimento para alcançar o consentimento informado; e, por fim, (v)-consentimento explícito, isto é, o consentimento esclarecido deve ser expresso de forma escrita, em linguagem clara, acessível, positiva, isenta de juízos de valor e deve permitir a compreensão e a autonomia do titular dos dados. Esse requisito se assemelha muito à manifestação da vontade inequívoca do titular de dados. A respeito do consentimento informado, vale consignar também as Diretrizes 05/2020 relativas ao consentimento na

[54] Minutas de Consentimento Informado. Universidade de Coimbra. Disponível em https://www.uc.pt/protecao-de-dados/minutas_consentimento_informado. [Consult. 23 abr. 2021].

[56] Para que o consentimento seja informado, é necessário informar o titular dos dados acerca de determinados elementos cruciais para se poder escolher. Por conseguinte, o CEPD considera que, pelo menos, as informações seguintes são necessárias para se obter um consentimento válido: i. a identidade do responsável pelo tratamento, ii. a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento,
iii. Que (tipo de) dados serão recolhidos e utilizados, iv. Existência do direito de retirar o consentimento, v. informações acerca da utilização dos dados para decisões automatizadas em conformidade com o artigo 22.º, n.º 2, alínea c)36, quando pertinente, e vi. Sobre os possíveis riscos de transferências de dados devido à inexistência de uma decisão de adequação e de garantias adequadas, tal como previsto no artigo 46.º Disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. [Consult. 28 jun. 2022].

aceção do Regulamento 2016/679, adotado em 4 de maio de 2020.

O consentimento surge, portanto, como uma forma de autorizar e legitimar os procedimentos ligados ao processamento dos dados. Visa conceder algum poder de controlo ao cidadão, de forma que ele não seja, segundo Stefano Rodotà, um mero "fornecedor de dados"[55]. Dessa forma, o titular de dados figura como elemento central no decorrer da evolução dos meios de proteção de dados, a ponto de essa proteção ser equiparada ao "direitode o cidadão autogerenciar as suas informações pessoais".

Um exemplo corriqueiro sobre o consentimento na coleta de dados é o que ocorre em uma compra online. Após realizar o pedido, para completar a compra, o adquirente deve fornecer seu nome, endereço de entrega e detalhes sobre o pagamento, inclusive sobre o seu cartão de crédito, para que o processo seja completado. A depender dos termos do site, o consentimento pode eventualmente estar inserido de maneira dissimulada, isto é, sem que o consumidor perceba pode conter uma permissão para o envio de e-mails de propaganda. Para ser válida, todavia, essa autorização deve ser obtida mediante o consentimento expresso e inequívoco, resultante de um ato positivo do titular dos dados, observando-se todos os requisitos acima expostos.

Por fim, confira um exemplo de termo de consentimento utilizado em Portugal[56]. É possível notar que os atributos são encontrados, de forma cumulativa, no termo citado.

1.3 DIREITO À PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL EM PORTUGAL E NO BRASIL

A proteção de dados possui alcance amplo e deve ser examinada sob vários aspetos. Neste momento, será destacada a qualidade de direito fundamental. A interação com outros direitos será analisada, sob outros aspetos, no Capítulo III.

As origens da proteção de dados pessoais podem ser registradas a partir da sociedade da informação. Nos anos 1970, a industrialização passou a fazer parte do cotidiano das pessoas. Para os governos, entretanto, emergiu uma nova preocupação em face do crescente uso da Tecnologia da Informação e Comunicação (TIC), que resulta no fomento da produção de riqueza a partir da utilização de informações pessoais. Surge, afinal, o que se conhece atualmente como tratamento de dados pessoais.

[55] RODOTÀ, Stefano – **A vida na sociedade da vigilância – a privacidade hoje**. MORAES, Maria C. B. (org). Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 76

[56] https://www.lisboa.pt/fileadmin/special_areas/pedal/declaracao_de_consentimento_cartao_cidadao_RL_e_crianca2021_PAAB21_VF.pdf. [Consult. 14 abr. 2021]

Antes de prosseguir, necessário registrar breve síntese do que se entende por direitos fundamentais para explicar como a proteção de dados é inserida. Existem duas construções acerca dos direitos fundamentais que importa destacar neste momento: uma estreita e exata, no sentido de defender que tais direitos se apresentam como regras; e outra, ampla e holística, que os entende como princípios, segundo Robert Alexi[57]. Para Cristina M. M. Queiroz[58], os sistemas jurídicos que categorizam os direitos fundamentais como regras são aqueles fechados e vinculados ao positivismo ou ao legalismo; já os sistemas jurídicos que classificam os direitos fundamentais como princípios são ordenamentos abertos e vinculados ao constitucionalismo.

Vale relembrar: os princípios são disposições a ordenar que algo seja feito na medida do possível, dentro das possibilidades legais existentes. Assim, os princípios são mandatos de otimização. Já as regras, ao contrário, impõem a obrigação de segui-las ou não. Se uma regra for válida, esta deve ser executada com precisão. Portanto, as regras contêm determinações no campo do possível, tanto de fato como de direito.

A caracterização do direito fundamental mais usual, contudo, é aquela que os divide em direitos fundamentais formais e materiais. Para Jorge Miranda[59], os direitos fundamentais formais são as posições jurídicas subjetivas protegidas pela Constituição formal, por estarem nela inscritas. Do mesmo modo, Konrad Hesse define o que se denomina direitos fundamentais formais, ou seja, "aqueles direitos que o direito vigente qualifica de direitos fundamentais"[60].

Os direitos fundamentais materiais, por seu lado, são aqueles direitos constitucionais que não foram definidos no texto constitucional pelo poder constituinte originário ou derivado como direitos fundamentais, embora possuam fundo fundamental. Na interpretação de Ingo Wolfgang Sarlet:

> [...] direitos fundamentais em sentido material são aqueles que, apesar de se encontrarem fora do catálogo, por seu conteúdo e por sua importância, podem ser equiparados aos direitos formalmente (e materialmente) fundamentais.[61]

Ao considerar a divisão dos direitos fundamentais em formais e materiais,

---

[57] ALEXY, Robert – Direitos Fundamentais, Ponderação e Racionalidade. Tradução de Luís Afonso Heck. **Revista de Direito Privado**, São Paulo: RT, n. 24, out./dez. 2005. p. 334-337.
[58] QUEIROZ, Cristina M. M. – **Direitos fundamentais: teoria geral.** Coimbra: Coimbra Editora, 2002, p. 127.
[59] MIRANDA, Jorge – **Manual de Direito Constitucional.** Tomo IV, 5.ª ed. Coimbra: Coimbra Editora, 2000. p. 9.
[60] HESSE, Konrad – **Elementos de Direito Constitucional da República Federal da Alemanha**. Tradução de Luíz Afonso Heck. Porto Alegre: Sergio Antonio Fabris Editor, 1998. p. 225.
[61] SARLET, Ingo W – **A eficácia dos direitos fundamentais–Uma teoria geral dos direitos fundamentais na perspectiva constitucional**. Porto Alegre: Livraria do Advogado, 2009. p. 80.

verificamos uma dicotomia entre Portugal e Brasil quanto ao direito de proteção de dados. Em Portugal, o artigo 35º, número 1, da Constituição de 1976, estabelece que os cidadãos têm direito de acesso aos dados informatizados que lhes digam respeito.[62] Exceção interessante consta no mesmo artigo 35º, número 6. Nota-se a preocupação em resguardar dados que possam colocar em risco a soberania nacional. Esse dispositivo constitucional é complementado pelo artigo 18º, que dá aplicabilidade e eficácia aos preceitos constitucionais.

Como se depreende do que consta do texto constitucional português, há o reconhecimento expresso do direito de obter todas as informações sobre a própria pessoa. Garante, ao fim e ao cabo, a faculdade de o próprio sujeito obter ciência específica sobre o uso e tratamento concedido aos seus dados pessoais. Por via de consequência, o direito à proteção de dados é apreendido como direito fundamental formal, pois consta do texto constitucional, fato que tornou Portugal pioneiro nessa questão no cenário mundial.

No ordenamento jurídico brasileiro a situação é bem mais complexa. O direito à proteção de dados até bem pouco tempo atrás não integrava o texto constitucional, portanto, era considerado direito fundamental material. Nessa medida, mesmo antes da EC n.º 115/2022, o Supremo Tribunal Federal o considerou como direito fundamental em 2020 por ocasião do julgamento da declaração de inconstitucionalidade da Medida Provisória 954/2020[63], e o classificou como um direito fundamental de "ricochete", isto é, um direito proveniente do desdobramento de outros direitos fundamentais. Tal fato é evidenciado no voto do Ministro Gilmar Mendes:

> A autonomia do direito fundamental em jogo na presente ADI exorbita, em essência,de sua mera equiparação com o conteúdo normativo da cláusula de proteção ao sigilo. A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa.[64]

---

[62] No que importa para este trabalho, é necessário mencionar o artigo 26º, número 1 da CRP, que reconhece, entre outros direitos, o direito à reserva da intimidade da vida privada.

[63] A Medida Provisória n.º 954/2020 previa o compartilhamento de dados dos usuários de telecomunicações (sejam eles: nomes, números de telefone e endereços dos consumidores, pessoas físicas ou jurídicas – Artigo 2º da MP) com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de uma estatística oficial durante a pandemia do novo coronavírus, fundamentada na impossibilidade de o IBGE realizar visitas presenciais, como de costume. Ela foi julgada inconstitucional por dez dos onze Ministros da Corte.

[64] ADI 6388, disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895166 e http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902. [Consult. 14 abr. 2021]

A partir desse entendimento maioritário do mais alto tribunal do país, os demais passaram a reconhecer o direito à proteção de dados pessoais como direito fundamental implícito ou derivado dos direitos à privacidade, à liberdade e à intimidade, conclui Ana Amélia Geleilate[65]. Atualmente, com a recente alteração constitucional ocorrida em fevereiro de 2022, o direito à proteção de dados no Brasil passará também a ser considerado direito fundamental formal.

1.3.1 O *Habeas Data* no direito brasileiro

O texto constitucional brasileiro evidencia, ainda com respeito ao direito à proteção de dados, o instituto do *Habeas Data.* Logo após o término da ditadura militar no Brasil (1964- 1985), a Assembleia Constituinte se reuniu para elaborar a nova Constituição Federal da República Federativa do Brasil. A instituição do *Habeas Data* foi um desdobramento do término do período de exceção, pois permite aos cidadãos requisitar, conhecer, e, até mesmo, retificar seus dados pessoais armazenados pelas entidades governamentais para usos não condizentes com os direitos humanos.

O instituto está previsto no artigo 5°, inciso LXXII, da Constituição Federal de 1988[66]e foi regulamentado pela Lei n.º 9.507, de 12 de novembro de 1997. *Habeas Data*, enfim, é o direito de os titulares de dados solicitarem informações sobre seus próprios dados pessoais para tomar conhecimento e, se for o caso, para que "sejam retificados os dados inexatos ou obsoletos ou que impliquem em discriminação"[67].

No que diz respeito à proteção de dados, a aplicação do *Habeas Data* pode ser visto como uma tutela deste direito, amparada pela Constituição. Vale destacar que, embora o texto faça referência apenas aos órgãos públicos, esse instituto vem sendo empregado em situações previstas pelo Código de Defesa do Consumidor (CDC) brasileiro.

Não obstante, parece-nos que no tocante à proteção de dados, o *Habeas Data* possui limitações que não se coadunam com a modernidade requerida pela TIC. Isso pode ser explicado, inicialmente, pelo fato de existir três modalidades de *Habeas Data*,

---

[65] GELEILATE, Ana Amélia – **A proteção de dados pessoais como um direito fundamental**. Disponível em https://www.conjur.com.br/2020-nov-11/ana-geleilate-proteção-dados-pessoais. [Consult. 04 abr. 2021].

[66] "Artigo 5º. LXXII – conceder-se-á habeas data:
a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo."

[67] MORAES, Alexandre de – Direito Constitucional. São Paulo: Atlas, 2001. p. 146.

categorizado conforme a sua finalidade, quais sejam: quando destinado ao conhecimento de informações relativas à pessoa do impetrante, denomina-se "*Habeas Data* cognitivo"; quando impetrado para a retificação de dados, designa-se "*Habeas Data* retificatório". Por fim, quando a intenção do impetrante é que a notícia sobre a sua pessoa seja complementada por uma explicação ou justificação, têm-se o "*Habeas Data* completivo".

Em princípio, há de se acordar que essas três modalidades cobrem os matizes de dados possíveis. Contudo, um óbice ainda não pacificado entre os juristas é se o pedido pode ser cumulativo, isto é, o *Habeas Data* pode ser a um só tempo cognitivo, retificatório e completivo?

José Eduardo Carreira Alvim[68] nega tal possibilidade, pois segundo o seu entendimento, o rito do processo de *Habeas Data* não permite formulação de pedido genérico.Por sua vez, José Afonso da Silva discorda em razão da agilidade e facilidade de se corrigir dados pessoais, de forma que não seriam "necessários dois *habeas data* para que uma mesma pessoa tome conhecimento dos dados e proponha sua retificação. Sustentar o contrário é pretender instituto novo em velhos esquemas de um procedimentalismo superado".[69]

Infere-se, portanto, entendimentos divergentes entre doutrinadores sobre o *Habeas Data* cumulativo ou não e, em última análise, resulta que, em termos práticos, dependerá do entendimento do órgão demandado, que poderá rapidamente adequar e retificar os dados do interessado, independentemente do tipo de *Habeas Data* impetrado e, dessa maneira, mais condizente com a modernidade requerida pela TIC.

1.3.2 Marcos da legislação da proteção de dados

A proteção de dados pessoais, hoje fortemente enraizada em diversos ordenamentos jurídicos, ofereceu fundamentos para que hoje esse direito fosse elevado à condição de direito fundamental.

A edição de leis que visam a proteção dos dados pessoais – no contexto do uso extremamente numeroso – começa a se formar, de fato, nas últimas décadas do século XX.[70] A análise geracional de Victor Mayer-Schönberger[71] explica esse processo de

[68] "O processo de habeas data não comporta pedido genérico, do tipo 'se erradas ou equivocadas sejam corrigidas', porquanto tem-se que delimitar os termos em que se dará a correção ou retificação." ALVIM, José E. C. – ***Habeas data***. Rio de Janeiro: Forense, 2001. p. 104-107.
[69] SILVA, José A. – **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros, 2002. p. 432.
[70] MENDES, Laura S. – **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo**

produção normativa em "gerações" de leis de proteção de dados.

A primeira geração surgiu na década de 1970, quando se pensava na centralização dos dados em grandes bancos de dados nacionais. Contudo, essa centralização não se efetivou de fato. O avanço da tecnologia possibilitou que organizações governamentais ou privadas criassem seus próprios bancos de dados. Estes são alguns exemplos de normas da primeira geração: as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Todas essas normas podem ser consideradas de primeira geração por sua estrutura e linguagem, segundo Laura Schertel Mendes[72].

A segunda geração de leis de proteção de dados nasce da insuficiência das normas anteriores para alcançar um conjunto de bancos de dados públicos e privados, que se tornaram cada vez mais fragmentados. Desse modo, surgiu a necessidade de alteração legislativa e assistiu-se ao surgimento de normas que visavam regulamentar prioritariamente o direito à privacidade ao invés de normatizar procedimentos.

O receio, então existente, pela criação de um banco de dados único e centralizado foi substituído pela possibilidade de que redes de bancos de dados menores dispersas pelo mundo pudessem "conversar" entre si e trocar informações. A característica principal das normas de segunda geração reside na faculdade de o indivíduo interferir diretamente no processo de coleta e de processamento de dados, mediante o seu consentimento ou a sua ausência, enfatiza Laura Schertel Mendes.[73] Como consequência, a privacidade voltada à área da informática é inserida nos textos das Constituições da Áustria, Espanha e Portugal, sendo esta última pioneira no assunto.

A decisão de 1983 do Tribunal Constitucional alemão, ao declarar a inconstitucionalidade parcial da Lei do Censo daquele país, marca a terceira geração de leis de proteção de dados.[74] Naquele caso, o Tribunal Constitucional defendeu o direito à "autodeterminação informativa" ao estabelecer a participação dos indivíduos no controlo sobre o processamento de seus dados, uma vez que a lei respectiva não afiançava esse direito. A decisão foi fundamental para a afirmação do direito à proteção de dados. São exemplos

---

direito fundamental. São Paulo: Saraiva, 2014. 248 fls.

[71] MAYER-SCHÖNBERGER, Viktor – Generational Development of Data Protection in Europe. *In* AGRE, P. ROTENBERG, M., Eds. **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 219-236.

[72] *Op. cit.* p.221.

[73] *Op. cit.* p. 223.

[74] MARTINS, Leonardo, Org. – **Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Montevidéu: Fundação Konrad Adenauer, 2005. p. 233-245.

dessa geração, além do marco citado, as alterações da lei da Áustria de 1986, a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda.

Por fim, a quarta geração de leis de proteção de dados consolidou a ideia de que fosse mais factível o exercício dessas garantias protetoras do indivíduo contra a exposição de seus dados pessoais. A leis passaram a erguer o padrão coletivo da proteção, pois a simples adoção de medidas que identifica o direito à autodeterminação informativa não era suficiente.[75]

Essa geração é bem representada pelo RGPD da União Europeia, bem como pelas Diretivas que o antecederam. Nesse contexto, necessário destacar a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, denominada Convenção 108 do Conselho da Europa, em 1981. Essa Convenção foi alterada pelo Protocolo de Modificação CETS n.º 223, de 18 de abril de 2018. Trata-se de um instrumento internacional que vincula os Estados signatários que a tenham ratificado no campo de atribuições da proteção de dados.

O direito à proteção de dados pessoais está consagrado em várias leis internacionais e nacionais, e podemos citar algumas delas em ordem cronológica: em 1948, foi promulgada a Declaração Universal dos Direitos Humanos (UDHR), da Organização das Nações Unidas (ONU) que, pela primeira vez, firmou esse direito em seu artigo 12º, e, por consequência, influenciou o nascimento de instrumentos legislativos subsequentes. Em 1950, foi publicada a Convenção Europeia dos Direitos Humanos (CEDH) que, em seu artigo 8º, assegurou o respeito à vida privada. Em 1973, a Suécia aprovou a primeira lei sobre Proteção de Dados, e, em 1977, a Alemanha se tornou o primeiro estado a publicar uma lei de privacidade que protege os dados dos seus cidadãos e prevê restrições à coleta dessas informações. Em 1980, a Organização para a Cooperação e Desenvolvimento Económico (OCDE) publicou as diretrizes para a proteção da privacidade e o fluxo transfronteiriço de dados; em 1995, o Parlamento Europeu e o Conselho aprovaram a Diretiva de Proteção de Dados. Mais recentemente, em 2013, a Assembleia Geral das Nações Unidas (AGNU) adotou a Resolução n.º 68/167 sobre o Direito à privacidade na era digital; e no mesmo ano a OCDE revisou as diretrizes de 1980, ao estabelecer a gestão de riscos e o fornecimento de notificações sobre a violação de dados; em 2016, a União Europeia aprovou o RGPD e, finalmente, em 2018, esse Regulamento entrou em vigor.

[75] DONEDA, Danilo – A proteção dos dados pessoais como um direito fundamental. Disponível em https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. [Consult. 29 mar. 2021].

Sob esse âmbito, importa ressaltar a atuação do Comité Europeu para a Proteção de Dados (CEPD), órgão europeu independente, cujo objetivo é promover a cooperação entre as autoridades de proteção de dados da União Europeia (UE) a fim de assegurar a aplicação sólida do RGPD dentro da UE, mediante orientações gerais, pareceres e apoio às autoridades nacionais de proteção de dados.[76]

Em janeiro de 2021, o Mercado Comum do Sul (Mercosul)[77] por meio do Conselho do Mercado Comum (CMC), órgão superior do bloco, estabeleceu o Acordo sobre Comércio Eletrónico do Mercosul, mediante a publicação da Decisão n.º 15/20[78]. Esse acordo apresentaregras específicas sobre a proteção de dados que criam obrigações para os Estados-partes que deverão adotar ou manter leis, regulamentos e medidas administrativas para a proteção da informação pessoal dos titulares envolvidos no comércio eletrónico. Para tais fins, os países do MERCOSUL levarão em consideração os padrões internacionais existentes nessa matéria e envidarão esforços para assegurar que o marco legal para a proteção dos dados pessoais dos titulares do comércio eletrónico não tenha caráter discriminatório.

A Decisão n.º 15/20 também se refere ao estabelecimento de medidas comuns de proteção de dados e sua livre circulação no MERCOSUL, e acrescenta, à intrínseca e necessária livre circulação de bens, serviços e fatores produtivos dentro do bloco, a livre circulação de dados. Destarte, o MERCOSUL também consolida sua posição de instituição que fomenta desenvolvimentos normativos fundamentais no Brasil referentes à matéria. Infere-se, deste relato, que a relevante questão da proteção de dados pessoais ocupa atualmente lugar de destaque na agenda do MERCOSUL.

Em 2018, Manuel David Masseno[79] publicou longo artigo em que apresenta uma exposição sintética da evolução das leis de proteção de dados em Portugal.

Entre os diplomas infraconstitucionais mais importantes, o autor cita a Lei n.º 10/91, de 29 de abril, que regulamentou o disposto no art. 35º da CPR. Em seguida,

---

[76] Disponível em https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en. [Consult. 11 jul. 2022].

[77] Mercosul é o bloco de comércio formado por países da América do Sul divididos da seguinte maneira: Países-membros do Mercosul: Argentina, Brasil, Paraguai e Uruguai. Países associados: Bolívia, Chile, Colômbia, Equador, Peru, Guiana e Suriname. Países observadores: México e Nova Zelândia. A Venezuela faz parte bloco, mas devido ao seu regime político encontra-se com suas atividades suspensas dentro do Mercosul.

[78] Acordo sobre Comércio Eletrónico do Mercosul. Disponível em http://siscomex.gov.br/wp-content/uploads/2021/02/82753_DEC_015-2020_PT_Acordo-Comercio-Eletronico.pdf. [Consult. 29 mar. 2021].

[79] MASSENO, Manuel D. – **A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa, uma cartografia das Fontes Legislativas**. Disponível em http://direitoeti.com.br/artigos/a-protecao-de-dados-pessoais-em-portugal-e-nos-outros-paises-de-lingua-portuguesa-uma-cartografia-das-fontes-legislativas/. [Consult. 17 abr. 2021].

surgiu a na Lei n.º 67/1998, de 26 de outubro, que transpôs para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação de dados.

O autor ainda cita, em relação ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas, a Lei n.º 41/2004, de 18 de agosto, atualizada pela Lei n.º 46/2012, de 29 de agosto, as quais transpuseram para o ordenamento jurídico português a Diretiva relativa à privacidade e às comunicações eletrónicas. Em outro campo, a Lei Geral Tributária, aprovada pelo Decreto-Lei nº 398/1998, de 17 de dezembro, incluiu as regras relativas ao tratamento e à segurança dos dados dos contribuintes.

Finalmente, o citado autor menciona a Lei n.º 58/2019, que assegura a execução na ordem jurídica portuguesa do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

No Brasil, a proteção dos dados passou a constar explicitamente da Constituição de 1988, conforme já aludido anteriormente, com a emenda EC n.º 115/2022, no inciso LXXIX, art. 5º, bem assim a CF também prevê expressamente a inviolabilidade da intimidade, da vida privada e da imagem das pessoas (art. 5º, inciso X); dispõe sobre a inviolabilidade da correspondência e das comunicações telegráficas, de dados e das comunicações telefónicas (art. 5º, inciso XII); e, por fim, garante a todos o direito de receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral.

No caso especial dos sigilos de dados fiscais e bancários, estes estão protegidos pelo inciso XII do art. 5º da CF. O sigilo fiscal é amparado pelo art. 198 do Código Tributário Nacional (CTN), instituído pela Lei n.º 5.172, de 15 de outubro de 1966, e o sigilo bancário é pela Lei Complementar n.º 105, de 10 de janeiro de 2001, bem como o Decreto n.º 4.489, de 28 de novembro de 2002.

Ainda a respeito da previsão de proteção dos dados pessoais no Brasil, a faculdade de se aceder aos dados pessoais sigilosos armazenados pelos órgãos públicos encontra apoio no art. 5º, inciso XXXIII da Constituição, na Lei nº 12.527, de 2011, em especial nos arts. 55 a 62, que dispõem sobre as condições de acesso a documentos pessoais detidos pelos órgãos e entidades.

Outro dispositivo infraconstitucional brasileiro que prevê a proteção dos dados é o

Código de Defesa do Consumidor (CDC), aprovado pela Lei n.º 8.078, de 11 de setembro de 1990.

Na área penal, existe o tipo penal previsto no artigo 313-A, denominado "inserção de dados falsos em sistema de informações", acrescentado pela Lei n.º 9.983, de 2000, ao Código Penal (CP), que sanciona a inserção de dados falsos, alteração ou exclusão indevida de dados corretos nos sistemas informatizados ou nos bancos de dados da administração pública, com o fim de obter vantagem indevida para si ou para outrem ou para causar danos, além dos artigos 154-A, 154-B e 266, todos do Código Penal, relativos à invasão de dispositivo informático alheio.

Finalmente, em setembro de 2020, foi aprovada no ordenamento jurídico brasileiro a lei fundamental para a proteção de dados, muito semelhante ao RGPD adotado por Portugal, qual seja a Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709, de 14 de agosto de 2018.

Assim, podemos concluir que, com a alteração recentemente realizada na Constituição brasileira, a garantia de proteção dos dados pessoais emerge de dispositivos dela própria, além de leis esparsas brasileiras, tais como do CDC, do CTN, do CP, e encontra-se, portanto, em situação similar à previsão expressa prevista na CRP.

1.3.3 Decisões judiciais sobre a proteção de dados

1.3.3.1 Decisões judiciais sobre a proteção de dados em Portugal

Os tribunais de Portugal e do Brasil têm tomado decisões em questões que englobam a proteção de dados baseadas na jurisprudência específica do RGPD e na LGPD.

Alexandre Sousa Pinheiro[80] analisa o julgamento acerca das decisões judiciais. Ao tomar conhecimento que os dados do Censo de 2021 estavam a ser enviados para os Estados Unidos por intermédio da empresa Cloudflare Inc[81], a Comissão Nacional de Proteção de Dados (CNPD) emitiu a Deliberação 2021/533, de 27 de abril, determinando

[80] PINHEIRO, Alexandre S. – **Dados pessoais, Censos 2021 e o Tribunal de Justiça da União Europeia**. Disponível em https://www.jornaldenegocios.pt/opiniao/colunistas/detalhe/dados-pessoais-censos-2021-e-o-tribunal-de-justica-da-uniao-europeia. [Consult. 30 abr. 2021].

[81] A Cloudflare é uma empresa com sede na Califórnia. Pelo tipo de serviços que fornece, está diretamente sujeita à legislação norte-americana de vigilância para fins de segurança nacional, a qual lhe impõe a obrigação legal de dar acesso irrestrito às autoridades dos Estados Unidos aos dados pessoais que tenha em sua posse, à sua guarda ou custódia, sem que possa disso dar conhecimento aos seus clientes.

que o Instituto Nacional de Estatística (INE) suspendesse imediatamente o envio desses dados, não apenas para os Estados Unidos, como para outros Estados que não garantissem proteção adequada no tratamento de dados pessoais.

A decisão da CNPD se baseou no Acórdão do Tribunal de Justiça da União Europeia (TJUE) relativo ao Processo C-311/2018, de 15 de julho de 2020 (Schrems II)[82], em que se inferiu que o ordenamento jurídico americano acarreta uma intromissão desproporcional nos direitos fundamentais dos proprietário dos dados à luz do direito da União Europeia, e não assegura, portanto, grau de proteção de dados essencialmente equivalente ao garantido na UE.

O TJUE considerou, ainda, que as autoridades responsáveis pela proteção de dados estão obrigadas a suspender ou a proibir transferências de dados, mesmo quando assentes em contratos baseados no modelo aprovado pela Comissão Europeia, como é o caso das cláusulas subscritas pelo INE, se não houver garantias que estas possam ser respeitadas no país terceiro. A CNPD tomou a decisão, pois entendeu que estavam em causa dados pessoais de um universo quase total dos cidadãos residentes em Portugal, incluindo dados sensíveis, como os relativos à religião ou à condição de saúde.

O fundamento da decisão pauta-se na determinação de que os titulares de dados devem gozar de direitos oponíveis e de medidas jurídicas eficazes por ocasião da transferência de dados pessoais de um país a outro, ou para uma organização internacional, nos termos do artigo 46, número 1 do RGPD.

1.3.3.2 Decisões judiciais sobre a proteção de dados no Brasil

Recentemente, uma empresa de *e-commerce* foi processada pelo uso indevido de dados pessoais.[83] Na ação, o autor provou que a empresa atuou como intermediária de comercialização em grandes proporções de dados pessoais ao oferecer cadastros e banco de dados, em geral, mediante retribuição pecuniária.

O tribunal baseou sua decisão em princípios relevantes da LGPD, como o da privacidade, do consentimento e da inviolabilidade do sigilo de dados, ao considerar que

[82] Schrems II se baseia numa queixa apresentada por Maximilliam Schrems, em 2013, na Irlanda, para que fosse suspensa ou proibida a transferência de seus dados pessoais para os Estados Unidos, a partir da Facebook Ireland para o Facebook Inc.

[83] LEGAL CLOUD – **Decisões Judiciais sobre a LGPD nos Tribunais.** 2020. Disponível em https://legalcloud.com.br/decisoes-judiciais-lgpd-tribunais/. [Consult. 30 abr. 2021].

as pessoas naturais eram identificáveis e o uso compartilhado de dados foi realizado irregularmente. A fundamentação da decisão do tribunal foi baseada diretamente na LGPD, Lei n.º 13.709, de 2018.[84]

Por fim, o juiz deferiu a tutela de urgência postulada na inicial e determinou à ré, empresa largamente conhecida de *e-commerce*, que se abstivesse de disponibilizar dados dos indivíduos, seja de forma gratuita ou onerosa, sob pena de multa de dois mil reais (R$ 2.000,00) a cada descumprimento.

Logo, apesar de esse processo estar no início de seu desenrolar e, portanto, sem sentença de mérito, ainda assim a liminar já demonstra na prática como o Brasil está atento e preocupado com a proteção de dados pessoais.

[84] Trechos da ementa: 9. Com efeito, os elementos de prova coligidos aos autos revelam a comercialização de dados pessoais de terceiros pelo réu, vale dizer, informações relacionadas com pessoa natural identificada ou identificável (artigo 5º, I, da Lei 13.709/2018). 10. Registre-se, ainda, inexistir indícios de concordância dos titulares dos dados, a revelar a irregularidade na indistinta comercialização promovida pelo réu, na forma do artigo 44 da Lei 13.709/2018.11. Tal prática, portanto, está em patente confronto com o princípio constitucional da inviolabilidade do sigilo de dados, insculpido no artigo 5º, XII, da Constituição Federal e o fundamento do respeito à privacidade, previsto no artigo 2º, I, da Lei Geral de Proteção de Dados Pessoais, sem prejuízo de outros Diplomas Legais aplicáveis à espécie, a demonstrar a probabilidade do direito invocado. 12. O perigo de dano, por sua vez, da persistente violação à privacidade dos titulares dos dados, a tornar impositiva a suspensão do comércio erigido pelo réu.

2. ONLINE DISPUTE RESOLUTION E MEIOS INFORMÁTICOS

2.1 PANORAMA GERAL DA ONLINE DISPUTE RESOLUTION EM PORTUGAL E NO BRASIL

A pandemia causada pelo vírus SARS-CoV-2 modificou de maneira peculiar as relações entre as pessoas. Além de provocar desafios relativos à saúde da população e à atividade económica, ocasionou mudanças no convívio entre as pessoas. Foi necessário reinventar o exercício das atividades cotidianas, notadamente no campo laboral, uma vez que o modo convencional de trabalho, com a presença física em escritórios e fábricas, foi alterado e, em algumas situações, abolido. Destarte, as atividades online se sobrepuseram ao atendimento presencial, tais como as atividades escolares ou o atendimento médico, com o advento da telemedicina, entre outros.

Nesse contexto, o Poder Judiciário não poderia deixar de ser afetado. A pandemia gerou nos tribunais uma dependência sem precedentes da Tecnologia da Informação e Comunicação (TIC), com o apoio e o uso de plataformas online e de videoconferência para garantir o acesso à Justiça e à prestação contínua de serviços, em que as audiências e interações pessoais foram interditadas, devido às restrições governamentais de saúde pública. Assim, as audiências, que anteriormente eram realizadas no modo presencial, passaram a ser conduzidas em meio virtual. O uso da tecnologia para a realização de audiências, depoimentos e mediações em tribunais obviamente aumentou de forma significativa com a pandemia do novo coronavírus, e parece que tal uso necessariamente continuará no futuro, em maior ou menor proporção.

O sucesso dessa nova realidade na aplicação das leis e da Justiça acabou por impactar positivamente um procedimento já conhecido há algum tempo no contexto da Resolução Alternativa de Litígios (RAL)[85] e que tomou um novo impulso com a utilização do ciberespaço para solucionar questões jurídicas, qual seja a denominada Disputa de Resolução em Linha ou, como é universalmente conhecida pela sua denominação em inglês: Online Dispute Resolution (ODR). A ODR caracteriza outra modalidade de solução adequada de conflitos, cujo diferencial é o seu desenvolvimento total ou, por vezes, parcial no ciberespaço.

O estudo da abrangência dos métodos de autocomposição dos conflitos, seja a

[85] No Brasil, atualmente utiliza-se a expressão "adequada' ao invés de "alternativa" (Resolução Adequada de Litígios).

RAL ou a ODR, pode ser visto sob vários aspetos. Entre eles, os impactos causados no Sistema Judiciário em geral ou sobre um ramo do direito em particular. No Sistema Judiciário, a contribuição para a sua melhoria é expressiva, pois é fato que em quase todos os países democráticos a cultura do litígio cresceu ao mesmo tempo em que as Constituições asseguraram e, muitas vezes ampliaram, os meios de acesso à Justiça. O acesso à Justiça constitui tema particularmente relevante em Portugal e no Brasil, bem como para as respectivas sociedades no que diz respeito à observância dos direitos humanos e fundamentais e, entre estes, em especial, à efetivação do acesso à Justiça[86] e à cultura de paz.

É sabido que o acesso à Justiça pelos cidadãos tem sido comprometido por inúmeros obstáculos, tais como: a morosidade do Poder Judiciário em dar uma decisão final aos judicantes, as custas judiciais e os honorários advocatícios, entre outros mencionados por Mauro Cappelletti e Bryant Garth[87], que também discorrem sobre procedimentos alternativos para efetivar o acesso à Justiça, que podem ser utilizados por particulares e pela administração pública. É importante destacar, todavia, o uso de meios adequados de composição de lides, qual seja o "sistema multiportas", expressão cunhada por Frank Sander, em 1976[88], ao descrever um "centro geral de Justiça" onde seria realizada a triagem dos conflitos e onde seria verificado o procedimento mais adequado à sua solução.[89]

Mariana França Gouveia define a Resolução Alternativa de Litígios (RAL)[90] como os procedimentos adotados para a solução do conflito fora do âmbito judicial, e justifica que a "definição é propositadamente vaga, na medida em que não existe qualquer tipologia fechada"[91]. Nessa esteira, seja por meio da RAL ou, no caso deste estudo, por meio da ODR, as formas adequadas de acesso à Justiça caracterizam-se pela maior celeridade para se chegar a uma solução para as partes envolvidas no litígio. Trata-se de procedimento

[86] Artigo 20º da CRP – Constituição da República Portuguesa, e, artigo 5º, inciso XXXV, da CF-Constituição da República Federativa do Brasil, de 1988.
[87] CAPPELLETTI, Mauro; GARTH, Bryant – **Acesso à Justiça**. Tradução Ellen Gracie Northfleet. Porto Alegre: Sérgio Antonio Fabris Editor, 1988, p. 10. Disponível em https://www.irib.org.br/app/webroot/publicacoes/diversos003/pdf.PDF. [Consult. 24 jan. 2020].
[88] O conceito foi apresentado na palestra de abertura da Global Pound Conference, em 1976, em Saint Paul, Minnesota, Estados Unidos.
[89] SALES, Lilia; SOUSA, Mariana – O Sistema de Múltiplas Portas e o Judiciário Brasileiro. **Revista Brasileira de Direitos Fundamentais & Justiça**. Porto Alegre. Ano 5, n.º 16, jul/set, 2011. p. 204-220. Disponível em https://www.researchgate.net/publication/326707190_O_Sistema_de_Multiplas_Portas_e_o_/judiciario_brasileiro. [Consult. 27 jan. 2020].
[90] Ou Resolução Adequada de Litígios para a doutrina brasileira.
[91] GOUVEIA, Mariana F. – **Curso de Resolução Alternativa de Litígios**. 3ª. ed. Lisboa: Almedina, 2015. p. 17.

para alcançar o efetivo acesso à Justiça, com segurança e, no que interessa a este trabalho, com a preservação do direito fundamental à proteção dos dados pessoais dos envolvidos.

Entre os métodos utilizados pela RAL, encontram-se a conciliação, a mediação e a arbitragem, além dos Julgados de Paz que fazem parte da estrutura judiciária de Portugal.[92]

No Brasil, os métodos de autocomposição dos conflitos são todos voluntários.[93] Em Portugal, são "voluntários a negociação, a mediação, a conciliação e arbitragem voluntária. É obrigatória a arbitragem necessária. Os Julgados de Paz serão voluntários ou obrigatórios conforme a posição que se tome sobre sua competência"[94].

Kazuo Watanabe esclarece a proposição, pois quando "se pensa na estrutura da RAL de conflitos dentro de um sistema judicial: [pensa-se] a busca pela solução adequada a partir da natureza do conflito e levando em conta a característica especial das partes envolvidas"[95]. É certo que o envolvimento em conflitos exige (1) facilitar a comunicação entre as partes; (2) auxiliar no manuseio de informações e dados, e (3) gerenciar a dinâmica de grupo.

Do mesmo modo, quando os recursos da Tecnologia da Informação e Comunicação (TIC) são utilizados, aparecem novas oportunidades, tais como: (1) abrir novos canais de comunicação; (2) oferecer novas maneiras de lidar com informações, e (3) criar novos métodos de gerenciar a dinâmica de grupo (e ainda permite que o praticante redefina o "grupo", integrando novos interessados ou modificando-o conforme o desenvolvimento da controvérsia). Neste capítulo iremos examinar o comportamento da ODR.

2.1.1 Online Dispute Resolution

O desenvolvimento da Online Dispute Resolution (ODR) data de 1995, quando a Villanova University, localizada na Filadélfia, deu início ao Virtual Magistrate (VM)[96],

---

[92] Art. 209, número 2, CRP.
[93] Cf. Resolução n.º 125, de 29/11/201, do CNJ- Conselho Nacional de Justiça (Brasil).
[94] GOUVEIA, Mariana F. *Op. cit,* p. 19.
[95] WATANABE, Kazuo – Acesso à justiça e meios consensuais de solução de conflitos. CRESPO, Maria Hernandez (Org.) *In* **Tribunal Multiportas – Investindo no capital social para maximizar o sistema de solução de conflitos no Brasil.** Rio de Janeiro: FGV Editora, 2012. p. 89.
[96] O projeto do Magistrado Virtual era um serviço de arbitragem baseado na Internet que auxiliava a resolução inicial rápida de disputas de rede de computadores. O projeto começou a funcionar em março de 1996, e oferecia um meio de resolução rápida e provisória de disputas envolvendo (1) usuários de sistemas online, (2) aqueles que alegaram ter sido prejudicados por mensagens, postagens e arquivos errados e (3) operadores de sistema. LUDLOW, Peter – **Virtual Magistrate Project Press Release**. *In* Crypto Anarchy, Cyberstates, and Pirate

que era um procedimento de arbitragem online voluntário destinado a resolver disputas entre provedores de serviços e usuários internet. Pablo Córtes[97] divide o desenvolvimento da ODR em quatro fases: amadora, experimental, empreendedora e institucional. A ODR alcançou sucesso, porém, com a resolução de disputas referentes ao *e-commerce*.[98]

Em 2004, Alan Gaitenby[99] conceituou a ODR como a aplicação da RAL em meio virtual. Segundo Daniel Arbix, o conceito de ODR vai além da utilização do meio virtual na solução do conflito, pois não se limita à substituição de canais de comunicação tradicionais, ao contrário, revela-se "um procedimento a dar direção à melhor resolução de determinado conflito"[100].

A Comissão das Nações Unidas para o Direito Comercial Internacional

---

Utopias, MIT Press, 2001. p. 339-342.

[97] Fase amadora: foi o período compreendido desde a criação da Internet até 1995. Nesse interregno não existia a ODR, as disputas aconteciam num modo informal.
Fase experimental: esta fase decorreu entre 1995 a 1998. Em razão da expansão da Internet, o número de disputas cresceu e surgiram iniciativas da sociedade civil para resolver estas disputas, mediante as organizações sem fins lucrativos. A fase pode ser exemplificada com o Magistrado Virtual.
Fase empreendedora: entre os anos de 1998 a 2002, quando a indústria de ODR começou a se desenvolver e empresas comerciais tiveram projetos de sucesso, por exemplo, SquareTrade.
Fase institucional: esta fase representa o desenvolvimento de 2002 até o presente. É caracterizada pela adoção do ODR pelas autoridades públicas. A institucionalização do ODR em órgãos públicos pode ser vista no processo da Comissão Europeia para criar a Diretiva 2013/11/EU do Parlamento Europeu e do Conselho, de 21/05/2013, sobre Resolução alternativa de litígios de consumo, e o Regulamento 524/2013 sobre litígios online. CORTÉS, Pablo – **Online dispute resolution for consumers in the European Union**. Abingdon: Routledge, 2011. p. 54.

[98] "Um passo fundamental no desenvolvimento do ODR veio através do site eBay. Desde 1999, o gigante do mercado online fornece um sistema interno para que as partes envolvidas em uma transação resolvam suas disputas online. Hoje, esse sistema ajuda as partes a resolver mais de 60 milhões de disputas a cada ano – um número que se assemelha ao volume anual total de casos arquivados em todos os tribunais civis dos EUA. Esse tipo de capacidade demonstra do que o ODR é capaz, tanto em termos do número de casos tratados quanto na capacidade de capacitar as partes a resolver rapidamente suas próprias disputas. Nos dias de hoje, os tribunais no mundo todo têm adotado e defendido os ODR, da mesma forma que outrora recorreram ao RAL como um meio de gerenciar sua carga de trabalho, melhorar os resultados e atender mais rapidamente os litigantes. Nos últimos anos, nos Estados Unidos, vários grupos ligados a aplicação da justiça pediram mudanças ousadas e substanciais no sistema de justiça civil para incorporar o ODR. Vários escritórios administrativos dos tribunais estaduais propuseram planos que pedem o estabelecimento de ODR. E alguns estados, como Michigan e Utah, já adotaram programas de ODR em suas operações. À medida que a tecnologia continua avançando, é lógico que o ODR continuará a proliferar." In **Resolution Systems Institute – Online Dispute Resolution**. Disponível em https://www.aboutrsi.org/special-topics/online-dispute-resolution. [Consult. 02 abr. 2020].

[99] "Resolução de disputas on-line é a aplicação de práticas e teorias de resolução alternativa de disputas (RAL) com tecnologia da informação em rede para gerenciar conflitos. Composto principalmente por sistemas de mediação, negociação ou arbitragem on-line, o ODR também inclui ferramentas de gerenciamento de informações para gerenciamento informal de conflitos por indivíduos e organizações." GAITENBY, Alan – **Wiley and Sons InternetEncyclopedia**, 2004. Disponível em https://onlinelibrary.wiley.com/doi/abs/10.1002/047148296X.tie129. [Consult. 02 abr. 2020].

[100] A ODR é, portanto, a resolução de controvérsias em que as tecnologias de informação e comunicação não se limitam a substituir canais de comunicação tradicionais, mas agem como vetores para oferecer às partes ambientes e procedimentos ausentes em mecanismos convencionais para dirimir conflitos. Mais, são "uma nova porta" para solucionar conflitos que talvez não possam ser dirimidos por mecanismos tradicionais de resolução de controvérsias". ARBIX, Daniel A. – **Resolução Online de Controvérsias**. São Paulo: Editora Intelecto, 2017. p. 4.

(UNCITRAL)[101], que é o órgão subsidiário da Assembleia Geral, refere-se à ODR como um "mecanismo de resolução litígio", ou seja, uma série de procedimentos intercalados e dependentes entre si, com o uso das comunicações eletrónicas para alcançar um consenso que satisfaça as partes envolvidas.

Das definições acima, algumas conclusões podem ser apresentadas. Em primeiro lugar, os mecanismos de ADR que simplesmente se valham das facilidades das TICs – como videoconferências ou e-mails para evitar o deslocamento das partes – não podem ser considerados um processo de ODR. A ODR deve estar submetida necessariamente a um procedimento, ou seja, submetida a fases subordinadas e relacionadas entre si. Em segundo lugar, conforme destaca Daniel Arbix, deve existir pelo menos uma ou mais contestações envolvidas na disputa, ou seja, a recuperação de créditos sem resistência do devedor, realizada com a assistência das TICs, por exemplo, não se qualifica como ODR.[102]

De fato, a utilização da ODR deve significar, além da facilidade de acesso e o baixo custo para os litigantes resolverem definitivamente a contenta, a forma compreendida como "ótima" para a resolução da disputa. A solução ótima do litígio pode ser percebida ao comparar a sua deliberação junto aos tribunais com aquela resolvida por meio da ODR. Assim, se a controvérsia fosse levada aos tribunais, o interessado deveria perceber que não configuraria um bom custo-benefício, seja pelo valor envolvido na disputa, pelo tempo dispendido, pelo valor dos respectivos honorários advocatícios, entre outras razões. Isto é, ao comparar a resolução do conflito por meio dos tribunais com aquela solucionada por intermédio da ODR, esta deve se mostrar mais vantajosa, tornando-se a melhor opção, ou, a opção "ótima" para a solução do conflito. O que Daniel Arbix ressalta, e com o que concordamos neste aspeto, é que determinados litígios serão melhor resolvidos pela ODR do que pelo Poder Judiciário. Nesse sentido, a ODR atua indubitavelmente como fator facilitador para a aplicação efetiva do princípio fundamental de acesso à Justiça.

Em resumo, o processo da RAL exige a presença física do terceiro (mediador/conciliador/árbitro) interagindo em tempo real com as partes, enquanto a ODR

[101] "O termo ODR refere-se a um mecanismo de resolução litígio facilitado pelo uso de comunicações eletrônicas e outras tecnologias de informação e comunicação." UNCITRAL – **Résolution des litiges en ligne dans les opérations internationales de commerce électronique. Note du Secrétariat, Résolution des litiges en ligne**, 2015. p.6. Disponível em https://www.uncitral.org/pdf/french/workinggroups/wg_iii/crp3-f.pdf. [Consult. 12 fev. 2021].

[102] ARBIX, Daniel A. *Op. cit*, p. 85.

utiliza a tecnologia da informação e comunicação (TIC) como o seu elemento diferenciador e fator de desenvolvimento para a consequente resolução da demanda, sempre submetendo a controvérsia entre as partes a um determinando procedimento, com fases intercaladas e relacionadas entre si. Assim, a aplicação da TIC expande as ferramentas utilizadas na RAL aotrocar o contato humano direto pelo contato a distância, por meio da ODR.

De outro lado, o mercado de tecnologia encontra-se em crescimento, uma vez que as ferramentas utilizadas para efetivar a ODR mudam fundamentalmente a experiência daqueles que a adotam. Necessário que essa experiência seja eficaz, com ótima resolução e velocidade, de forma a satisfazer os litigantes para, ao final, acelerar de fato a resolução das disputas. Assim, além do aparato tecnológico, resulta que a ODR deve estar submetida também a uma proteção jurídica eficaz, a fim de que os seus usuários possuam segurança para utilizá-la. Nessa esteira estão os direitos fundamentais da proteção dos dados, a RGPD em Portugal, a LGPD no Brasil, além das respectivas legislações subjacentes.

Necessário registrar, ainda, breve comentário no sentido de que o acesso à Justiça constitui um dos pilares essenciais ao exercício e à proteção dos direitos fundamentais dos cidadãos, cuja proteção é assegurada pela Constituição de Portugal e do Brasil. Ademais, como é sabido, a ONU instituiu a Agenda 2030, que visa atingir os Objetivos de Desenvolvimento Sustentável (ODS), e incluiu em seu objetivo 16 – Paz, Justiça e Instituições Eficazes – a oferta de acesso à Justiça para todos ao lado da construção de instituições eficazes. Nesse objetivo, destaca-se o subitem 16.3, no sentido de "promover o Estado de Direito, em nível nacional e internacional, e garantir a igualdade de acesso à Justiça para todos"[103]. Ou seja, a adoção da RAL e, no caso deste estudo, especificamente a adoção da ODR, contribuem efetivamente para o cumprimento do Objetivo 16 da Agenda 2030 da ONU.

Nesse sentido, qual seja, de que a adoção da ODR promove o acesso à Justiça e, portanto, assegura maior proteção aos direitos fundamentais dos cidadãos, importa ressaltar as avaliações realizadas pelo Resolution Systems Institute (RSI) em inúmeros casos envolvendo a adoção da ODR, o que proporcionou significativo aumento nas oportunidades para os interessados chegarem a um acordo, bem como alcançarem mais rapidamente um acordo, além de se sentirem mais satisfeitos com a solução dada ao

[103] Disponível em https://brasil.un.org/pt-br/sdgs/16. [Consult. 18 abr. 2022].

conflito.[104]

No tocante às características da ODR, quanto aos aspetos da voluntariedade, confidencialidade, igualdade e imparcialidade, podemos verificar a semelhança entre as regras da ODR com as regras da RAL entre Portugal[105] e Brasil[106]. Para além dessas características, dependerá das leis de cada administração pública, princípios constitucionais e legislação pertinentes à matéria, que poderão impingir mais ou menos requisitos e garantias aos envolvidos. A peculiaridade de cada sociedade, enfim, limitará outras características da ODR,que deverá ser regulamentada pela respectiva legislação.

De outro lado, seja em Portugal ou no Brasil, notamos que a ODR respeita alguns mandamentos gerais e comuns àqueles que a adotam. Esses mandamentos são compreendidos como pilares basilares para a constituição da ODR, quais sejam: (a) custo proporcional à demanda para a utilização da ODR; (b) suporte off-line para a resolução do litígio; (c) assistência individualizada para os litigantes; (d) sistemas de Justiça integrados; (e) regras claras, precisas e objetivas, sob a supervisão dos usuários; e (f) aprimoramento constante do sistema de ODR (g) para a manutenção da boa qualidade do sistema.[107]

2.1.2 Princípios orientadores da Online Dispute Resolution

A RAL e a ODR possuem princípios que regem a sua atuação. Muito deles são coincidentes, tais como os princípios da igualdade, justiça e imparcialidade; ou da honestidade, da participação informada, da transparência, da neutralidade, entre outros que podem variar de acordo com a legislação de cada país.[108] Neste capítulo, serão listados alguns princípios característicos da ODR.

Os sistemas e as práticas de ODR nas esferas pública e privada necessitam seguir

---

[104] Disponível em https://www.aboutrsi.org/publications/program-evaluations#Online%20Dispute%20Resolution. "Resolução de Disputas on-line para casos de direito de família pós-julgamento: um relatório para o condado de Ottawa, Michigan, amigo do Tribunal". [Consult. 02 jul. 2022].

[105] Lei n.º 29/2013, de 19 de abril, artigos 4º; 5º; 6º, e 7º.

[106] Lei n.º 13.140, de 2015, artigo 2º.

[107] **ODR and the Courts: The promise of 100% access to justice?** Disponível em: https://www.hiil.org/projects/trend-report-4-odr-and-the-courts-the-promise-of-100-access-to-justice/. [Consult. 10 mar. 2021].

[108] Lei n.º 29/2013, de 19 de abril (Portugal) e Lei n.º 13,140, de 2015, artigo 2º, e Resolução n.º 125/CNJ (Brasil). Muito embora as legislações de Portugal e do Brasil nomeiem um outro princípio da RAL com designações diferentes, podemos perceber a identidade desses princípios, por exemplo: o princípio da independência, previsto no artigo 7º, n. 1, da Lei n.º 29/2013 (Lei da mediação Portuguesa) é equivalente ao princípio da imparcialidade previsto no artigo 2º, inc. I, da Lei n.º 13.140, de 2015 (Lei da Mediação Brasileira).

princípios[109] que, além de estruturar as operações, estabeleçam valores éticos que devem ser observados. Nesse sentido, destacamos o (a) princípio da acessibilidade, que no campo da ODR significa adaptar o acesso da ODR aos usuários, considerando as capacidades económica e de compreensão de sua utilização, bem como o custo envolvido, uma vez a ODR deve facilitar e ampliar a sua utilização, e não limitar a atuação das partes em litígio. Isso significa, por exemplo, que a incapacidade de um usuário em utilizar o sistema informático inviabiliza a ODR como vetor ótimo de solução da contenda. O (b) princípio da adaptabilidade e inovação da utilização dos meios tecnológicos, por exemplo, o uso da Inteligência Artificial (IA), bem como o (c) o princípio da integração da ODR com outros sistemas de resolução de disputas, que deve ser diuturnamente observado. Finalmente, cabe destacar o (d) princípio da segurança e proteção de dados, uma vez que é absolutamente imprescindível a segurança do sistema virtual para o correto funcionamento da ODR, preservando-se o sistema de eventuais invasões não autorizadas que impliquem no comprometimento do processamento de dados pessoais, os quais devem ser rigorosamente protegidos.

Em resumo, a concepção e implementação da ODR procura prevenir e minimizar os danos e riscos para as pessoas envolvidas nos processos de resolução de disputas online, com particular atenção aos mais marginalizados e com menos acesso à Justiça. Além dessas características, Esther van den Heuvel[110] cita a importância de o procedimento da ODR ser conduzido sob o comando da confiança entre as partes e o mediador. Outro requisito fundamental é a certeza e segurança a respeito da identidade dos envolvidos. Por consequência, faz-se necessário utilizar as ferramentas da TIC, tal como a assinatura eletrónica para assegurar a identidade dos envolvidos. Destaca, ainda, a importância sobre a confidencialidade e a privacidade da comunicação durante o processo de ODR.

O princípio da segurança e proteção de dados é entendido, no nosso sentir, como essencial para a admissibilidade da ODR, seja em Portugal ou no Brasil. Isso porque o eventual rompimento da privacidade e da confidencialidade dos trâmites havidos durante a ODR ou a divulgação indesejada de dados pessoais no ambiente virtual pode comprometer os envolvidos com a difusão de informações que poderão, eventualmente,

[109] **The International Council for Online Dispute Resolution**. Disponível em http://odr.info/ethics-and-odr/. [Consult. 15 fev. 2021].

[110] HEUVEL, Esther van den – **Online dispute resolution as a solution to cross-border e-disputes. An introduction to ODR**. Disponível em https://www.oecd.org/digital/consumer/1878940.pdf. p. 13-16. [Consult. 12 jul. 2022].

ficar disponíveis indefinidamente na rede mundial de computadores. A prevalência do princípio da segurança e proteção de dados não significa que os demais princípios não sejam igualmente importantes para a ODR, apenas optou-se por destacar esse princípio dos demais, haja visto (1) o avanço acelerado dos meios informáticos nos últimos anos; (2) a disseminação de meios eletrónicos etelemáticos por toda a população, inclusive pela parcela mais vulnerável. Não é raro encontrar pessoas de baixíssimo poder aquisitivo que possuam, por exemplo, telemóvel (ou celular, no Brasil). Em conclusão, a oportunidade de levar a Justiça, por meio da ODR, mesmo para os estratos mais necessitados da sociedade, significa – ao nosso sentir – avanço na disponibilização do acesso à Justiça a toda a sociedade, com consequente pacificação social, não obstante faça-se necessário a estrita observância às regras de proteção dos dados pessoais dos envolvidos.

Ou seja, é preciso observar que a ODR, ao tempo que facilita o acesso à Justiça por toda a gente, deve também ter por objeto a confidencialidade, segurança e proteção de dados de seus usuários, considerando-se a ausência de um ambiente virtual cem por cento seguro, bem como a garantia de confidencialidade. Nesse contexto, a RGPD e a LGPD devem servir notadamente de arcabouço jurídico inicial[111] infraconstitucional para a sua corretaimplementação.

2.2 INTERAÇÃO ENTRE A ONLINE DISPUTE RESOLUTION, OS TRIBUNAIS E A ADMINISTRAÇÃO PÚBLICA

Podemos visualizar quatro interações de cooperação entre a ODR e os procedimentos dos tribunais.

Inicialmente, podemos imaginar a utilização da ODR como uma fase anterior ao início do processo judicial, permitindo a redução no número de casos no Poder Judiciário, a resultar na economia de custos e tempo das partes. A segunda possibilidade seria a utilização da ODR para substituir as intervenções judiciais; seria praticamente uma concorrência entre o Poder Judiciário e a ODR. Por óbvio, o acesso aos tribunais não pode ser impedido à vista do artigo 20° da Constituição Portuguesa e, também, pelo artigo 5°, inciso XXXV, da Constituição do Brasil. O que queremos reiterar, porém, é que a ODR deve ser entendida como uma ferramenta efetiva para instrumentalizar, tornar concreto aos cidadãos, o direito fundamental ao acesso à Justiça dentro dos parâmetros

[111] Diz-se legislação inicial, pois cada Administração pode entender necessário regulamentação mais detalhista, conforme veremos no item seguinte.

institucionais, isto é, de acordo com as leis vigentes. José Joaquim Gomes Canotilho e Vital Moreira evidenciam este raciocínio:

> O direito de acesso ao direito e à tutela jurisdicional efectiva (nº 1 e epígrafe) é, ele mesmo, um direito fundamental constituindo uma garantia imprescindível da protecção de direitos fundamentais, sendo, por isso, inerente à ideia de Estado de direito. É certo que carece de conformação através da lei, ao mesmo tempo em que lhe é congénita uma incontornável dimensão prestacional a cargo do Estado (e, hoje, também da União Europeia), no sentido de colocar à disposição dos indivíduos – uma organização judiciária e um leque de processos garantidores da tutela judicial efectiva. A sua natureza de direito prestacionalmente dependente e de direito legalmente conformado é visível, quer quanto ao direito de acesso ao direito através das vias não-jurisdicionais (ex.: serviços de informação jurídica, <<cidadão>>em questões de direito), quer quanto ao direito de acesso aos tribunais (patrocínio judiciário). De qualquer modo, ninguém pode ser privado de levar a sua causa (relacionada com a defesa de um direito ou interesse legítimo e não apenas de direitos fundamentais) à apreciação de um tribunal, pelo menos como último recurso. Por isso, o art. 20º consagra um direito fundamental independentemente da sua recondução a direito, liberdade e garantia ou a direito análogo aos direitos, liberdades e garantias.[112]

De fato, a ODR deve servir para ampliar o acesso à Justiça de maneira mais célere e menos custosa aos envolvidos. Porém, nessa hipótese de cooperação entre a ODR e o Poder Judiciário, a utilização da ODR em casos específicos poderia, porventura, mostrar-se mais vantajosa aos litigantes e, assim, por hipótese e apenas para demonstrar nosso argumento, a ODR poderia eventualmente concorrer com a atuação dos tribunais, sem obviamente impedir o acesso a eles. A utilização da ODR, nessas hipóteses, portanto, deveria deixar claro, ainda, as situações nas quais os envolvidos poderiam recorrer aos tribunais, caso resultassem insatisfeitos com a resolução do conflito obtida por meio da ODR.

Interação também teórica, e apenas para fins de conjectura, poderíamos pensar em um modelo de integração completa entre os procedimentos da ODR e os processos judiciais. Essemodelo poderia permitir que as partes evoluíssem durante o procedimento litigioso e buscassem ora a atuação dos tribunais, ora a resolução por meio da ODR, tornando o processo dinâmico. Claramente, essa hipótese não se adequa às estruturas dos atuais sistemas jurídicos, seja em Portugal ou no Brasil.

O uso da ODR como uma solução de litígios de mercado, voltada ao direito do consumidor, por outro lado, tem sido utilizada pela plataforma Resolução de Litígios em

[112] CANOTILHO, José J. G.; MOREIRA, Vital.(Eds.) – **Constituição da República Portuguesa anotada.** Volume 1. Artigos 1º a 107. 1ª edição brasileira – São Paulo: Revista dos Tribunais; 4. ed. portuguesa revista. Coimbra: Coimbra Editora, v. 1, 2007. p. 408-409.

Linha (RLL)[113] desenvolvida pela Comissão Europeia para resolver disputas entre consumidores e fornecedores. Esse aspeto é um bom exemplo prático do uso da ODR. Trata- se de um sistema que permite ao reclamante inserir sua queixa online na plataforma e, imediatamente, a outra parte é cientificada. As partes têm noventa dias para chegar a um acordo ou trinta dias para concordar com o prosseguimento da disputa em uma entidade de resolução de litígios devidamente aprovada.[114]

Em quaisquer das interações da ODR, regidas por entidade gestora de mediação da administração pública ou por ente privado, necessário a existência de um código de conduta que norteie os princípios de gestão ODR, não apenas submetendo essas entidades a regras claras e/ou leis que limitem e regulamentem a sua atuação, mas também por meio de metodologias e tecnologias.

Na opinião de Faye Fangfei Wang[115], o modelo proposto de códigos de conduta para lidar com disputas online deve incluir pelo menos quatro principais provisões: (1) disposições gerais, que compreendam mecanismos de controlo do sistema ODR e seus serviços, além de alcançar princípios fundamentais, tais como responsabilidade, imparcialidade, transparência, confidencialidade, acessibilidade e segurança; (2) disposições específicas para regulamentar os procedimentos a serem observados pelas câmaras privadas ou públicas que conduzirão a ODR, tais como procedimentos, prazos, arquivamentos eletrónicos e compromissos com a tecnologia; (3) mecanismo de acreditação para assegurar a legitimação da ODR; e, por fim, (4) mecanismo de aplicação, isto é, regulamentação de acordos resultantes da ODR.

2.2.1 A Online Dispute Resolution na administração pública

Muitos países desenvolvidos consideram estabelecer o chamado governo eletrónico uma estratégia essencial para modernizar a administração pública. Sem dúvida, dentro do âmbito deste estudo, para que essa estratégia se concretize, é imperativo que a ODR seja incorporada como um de seus objetivos. No entanto, existem alguns óbices a

[113] Disponível em https://ec.europa.eu/consumers/odr/main/?event=main.home.howitworks. [Consult. 15 fev. 2021].

[114] Esta entidade aprovada para resolução de conflitos, no âmbito da Administração pública em Portugal é referida no artigo 31º da Lei n.º 29/2103, de 19 de abril, podendo a RAL ser exercida também por entidades privadas. No Brasil, no âmbito do Poder Judiciário, existe o Centro Judiciário de Resolução de Conflitos e Cidadania – CEJUSC, referido no artigo 8º da Resolução n.º 125 do Conselho Nacional de Justiça-CNJ, e no âmbito privado, as Câmaras Privadas, previstas no art. 12-C da aludida Resolução nº 125.

[115] WANG, Faye F. – **Online Dispute Resolution. Technology, management and legal practice from an international perspective**. Oxford: Chandos Publishing Limited, 2008. p. 85.

serem transpostos, dentre eles a exclusão digital, dificuldade que ataca mesmo alguns países e impede a plena utilização da ODR. A exclusão digital, como designa o próprio nome, é a dificuldade de acesso de indivíduos de uma mesma sociedade à tecnologia (aparelhos, redes de internet, compreensão sobre TIC, entre outros) e à sua adequada utilização, e esse impedimento (parcial ou em grande escala) decorre de algumas variáveis, tais como desenvolvimento de políticas públicas, existência de um quadro jurídico adequado, fundos e infraestrutura disponíveis, fatores técnicos e de segurança e, sobretudo, melhoria das condições sociais, culturais e de educação da população, no sentido de o cidadão ter acesso a equipamentos eletrónicos, mas sobretudo possuir pleno desenvolvimento intelectual e ciência de seus direitos, além de ser dotado de um conjunto de princípios, valores e normas sociais que lhe permitam a ampla discussão sobre os direitos que lhe são próprios. Tais fatores são agravados nos países em desenvolvimento ou subdesenvolvidos.

O que se quer dizer é que não basta ao cidadão comum ter um telemóvel (ou celular, como se denomina no Brasil) em mãos para que a ODR consiga ser incorporada às estratégias do governo eletrónico. É necessário ter educação, em seu sentido amplo, que resulte em um cidadão com mais ciência e consciência de seus direitos e deveres para que o estratagema do governo eletrónico alcance suas metas. Somente quando as providências necessárias para suplantar essas dificuldades forem tomadas pelos governos é que a ODR poderá ser amplamente difundida e utilizada pela administração pública. Todavia, essa mudança de paradigma não ocorre de maneira rápida. Trata-se de um processo de desenvolvimento sujeito a adversidades, com avanços e retrocessos. De toda forma, ainda que se considerem todos esses percalços, a adoção de meios de ODR pela administração pública, no nosso entender, facilita o acesso à Justiça e faz parte desse percurso, cujo objetivo é aprimorar as instituições, tornar mais simples o acesso à Justiça e, ao final, fomentar a cultura de paz.

Trata-se, portanto, de um processo em andamento no sentido de superar essas dificuldades. Os governos, de seu lado, têm um papel importante a desempenhar no funcionamento do sistema de ODR. Por meio da ação governamental, a difusão e a confiança na ODR podem ter um aumento significativo, se provido por um contexto de autorregulação confiável e seguro, seja sob o aspeto tecnológico, seja pelo aspeto jurídico. Obviamente, não se pode prescindir da iniciativa privada no campo da ODR. Seja em Portugal ou no Brasil, existem várias plataformas particulares. Contudo, o Governo e os atores privados não têm as mesmas funções e capacidades. O Governo tem

competências que atores privados não possuem e vice-versa; são ambos os atores complementares. De toda forma, quer nos parecer que a ODR necessitará de regulação estatal, tal como a Lei de Mediação[116] em Portugal, ou o Marco Civil da Internet[117] e a Lei de Mediação[118] no Brasil.

De acordo com Thomas Schultz, a "ODR precisa de uma arquitetura de confiança"[119], ou seja, normas que criarão características tangíveis, contextos sociais e soluções previsíveis –no caso de eventuais impedimentos ou obstáculos –, e que deve ser regulamentado pelo respectivo Governo. Ou seja, em breve, a fim de que a Administração pública regulamente a utilização da ODR, pode-se aventar a promulgação de atos normativos específicos (leis, decretos, portarias etc) para a utilização da ODR.

De outro lado, uma questão fundamental – quando se pensa na utilização da ODR pela administração pública, além dos quatro princípios específicos da ORD citados[120] – é o interessante questionamento que diz respeito à delimitação das situações nas quais a administração poderia atuar em uma ODR, isto é, em quais situações seria possível transigir com o interesse público, uma vez que a administração pública é o guardião desse interesse?[121] Tal assunto certamente poderia ser objeto de um estudo aprofundado, o que não é o mister neste trabalho. Não obstante, faz-se necessário tão-somente registrar alguns parâmetros, dada a essencialidade do tema.

Primeiramente, portanto, necessário repetir que o princípio da voluntariedade[122] (ou da autonomia da vontade[123], no caso brasileiro) regulamentado por lei e dirigido à RAL, como dissemos acima, também se aplica à ODR. Esse conceito é importante, pois ao contrário do que é permitido aos particulares, a administração pública somente pode fazer e realizar suas atividades estritamente de acordo com os dispositivos legais que determinam o seu modo de agir e autorizam a realização de suas funções específicas.

---

[116] Lei n.º 29/2013, de 19 de abril, que estabelece princípios gerais aplicáveis à mediação realizada em Portugal, bem como os regimes jurídicos da mediação civil e comercial, dos mediadores e da mediação pública.
[117] Lei n.º 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.
[118] Lei n.º 13.140, de 26 de junho de 2015, que dispõe sobre a mediação entre particulares como meio de solução de controvérsias e sobre autocomposição de conflitos no âmbito da administração pública.
[119] SCHULTZ, Thomas – **Does Online Dispute Resolution Need Governmental Intervention? The Case for Architectures of Control and Trust.** [sl] N.C. J.L. & TECH, 2004. p. 71-73.
[120] (1) disposições gerais; (2) disposições específicas; (3) mecanismo de acreditação; e (4) mecanismo de aplicação, segundo Faye F. Wang, *op. cit*
[121] Art. 266, números 1 e 2 da CRP, art. 37, *caput*, da Constituição do Brasil.
[122] Artigo 4º da Lei n.º 29/2013
[123] Artigo 2º, inciso V, da Lei n.º 13.140, de 2015.

Marcelo Alexandrino e Vicente Paulo[124] discorrem que aos particulares, a regra é a autonomia da vontade, ao passo que a administração pública não tem vontade autônoma, estando adstrita à lei, a qual expressa a "vontade geral", manifestada pelos representantes do povo, único titular originário da "coisa pública". A propósito da voluntariedade da mediação, é necessário registrar seus aspetos fundamentais, destacados por Dulce Lopes e Afonso Patrão, quais sejam: "(i) na liberdade de escolha da mediação; (ii) na liberdade de abandono da mediação; (iii) na liberdade de conformação das partes no acordo; (iv) na liberdade de escolha do mediador"[125]. Tais aspetos devem também estar presentes quando a administração pública participa de resoluções alternativas de conflito; em especial, nas RALs e ODRs.

De outro lado, é de amplo conhecimento que o uso da discricionariedade pelo gestor público não significa agir com arbitrariedade e, portanto, a possibilidade de o agente público participar de uma ODR deve estar expresso em um comando normativo fundamentado na busca do interesse público, em razões de ordem económica ou outras que, concretamente, e sempre considerando as circunstâncias peculiares de cada caso concreto, leve à conclusão de que o acordo obtido em eventual procedimento de ODR será mais proveitoso à administração do que a opção usualmente utilizada ou mais comumente encontrada pelos gestores.

Em conclusão, inicialmente há a necessidade de (a) autorização legislativa para que a administração pública participe da RAL e/ou ODR. Após a autorização legal, há de se ter uma (b) decisão balizada e fundamentada da autoridade responsável, que permita realizar negociação intrínseca à consecução da mediação pelo órgão público em cada caso concreto. Nesse caso, há de se buscar o consenso dentro da esfera de discricionariedade do gestor público, e, nesse consenso, o que denominamos "autonomia regulada da administração", que nada mais é do que a obediência ao princípio da legalidade na administração pública, que determina que a atuação administrativa deve, sempre, obrigatoriamente, ser fundamentada na lei. Para todas as ações do Estado é imprescindível a subordinação à lei; à autorização legal. Esse entendimento, ou seja, a possibilidade de reconhecer à autoridade pública uma medida de discricionariedade na composição de litígios, "seja a discricionariedade procedimental ou substantiva"[126], tem

[124] ALEXANDRINO, Marcelo; PAULO, Vicente – **Direito Administrativo Descomplicado** 23.ª ed. São Paulo: Método, 2013. p. 187.
[125] LOPES, Dulce; PATRÃO, Afonso – **Lei da Mediação Comentada**, Coimbra: Almedina: 2014, p. 28-29.
[126] MARTINEZ, Gerardo C. – **La Mediación Administrativa y el Defensor del Pueblo**. Cizur Menor, Editora: Thomson Aranzadi, 2008. p. 61 e seguintes.

sido defendida por alguns autores. Ou seja, nessa decisão balizada da autoridade responsável deve ficar evidenciado o interesse público perseguido e as razões pelas quais, dentro do espaço da discricionariedade, a participação na ODR se mostrou mais vantajosa do que outras escolhas administrativas e/ou judiciais. Por fim, de acordo com a legislação de cada órgão público, pode ser necessário um (c) comando normativo expedido pela autoridade responsável, dirigido especificamente a cada caso concreto que, enfim, materialize e detalhe a participação da administração na ODR de acordo com a decisão e os parâmetros expostos pela autoridade responsável em sua decisão fundamentada anterior, que autorizou a participação da administração na ODR.

Ao fim e ao cabo, ao negociar concretamente a solução de determinado conflito, tendo de um lado a autorização legislativa e, de outro, o espaço de discricionariedade demonstrado pela autoridade pública mediante decisão fundamentada – e, quando for o caso, dirigida ao gestor público mediante comando normativo expedido por essa mesma autoridade – restará demonstrada a "autonomia regulada da administração" e, portanto, a possibilidade concreta de a administração pública participar da ODR.[127]

2.2.2 A Online Dispute Resolution na administração pública em Portugal

Em nossa pesquisa pudemos perceber que a RAL em Portugal, especificamente a mediação, ainda se encontra em um "estado embrionário de discussão" [128]. De fato, não existem notícias explícitas sobre a aplicação da RAL e, portanto, também sem notícias sobre a aplicação da ODR na administração pública portuguesa. Não obstante, é possível inferir que os mecanismos alternativos de conflitos podem ser utilizados, uma vez que há diversos diplomas legais do ordenamento jurídico português a recomendar o uso dos métodos da RAL na administração pública, desde que observados os demais princípios desse mesmo ordenamento jurídico português. Assim, a CRP, em seu art. 202, número 4, ao dispor sobre a função jurisdicional, autoriza que a "lei poderá institucionalizar instrumentos e formas de composição não jurisdicional de conflitos", o que pode vir a ser o fundamento constitucional para que futura lei autorize específica e expressamente a RAL e/ou ODR e, eventualmente, outras formas de resoluções alternativas de conflitos na

[127] Esse raciocínio foi primeiramente exposto pela autora no artigo Resolução de conflitos on-line e os desafios para a Administração Pública. WATANABE, Kazuo *et al*. (Coords.) *In* **Desjudicialização, Justiça Conciliativa e Poder Público.** São Paulo: Thomson Reuters Brasil, 2021. p. 513-531.

[128] SILVA, Artur Flamínio. O Novo Regime Jurídico da Resolução de Conflitos Desportivos no Direito Administativo: sobre a Arbitragem Necessária e a Mediação no Tribunal Arbitral do Desporto. GOMES, Carla A. *et al.* (Coords). *In* **Arbitragem e Direito Público.** Lisboa: AAFDL, 2018. p. 423.

administração pública. Não obstante, já existem outros normativos que autorizam a utilização da RAL e/ou da ODR pela administração pública portuguesa. O exemplo mais manifesto de resoluções alternativas em Portugal é a arbitragem, que não é objeto deste estudo. Porém, no tocante à arbitragem, podemos citar, por exemplo, o art. 180º do Código do Processo nos Tribunais Administrativos (CPTA), ou, ainda o artigo 187º desse mesmo CPTA, que autoriza o Estado instalar Centros de Arbitragem Permanentes (CAPs) para atuar nas áreas relativas a contratos, responsabilidade civil da administração, funcionalismo público, sistemas públicos de proteção social e urbanismo. Admite, ainda, que os CAPs – nos casos de impugnação administrativa – possam realizar as outras modalidades da RAL.[129] De outro lado, ainda temos o Regime Jurídico das Empreitadas de Obras Públicas (RJEOP- Decreto-Lei n.º 59/99, de 2 de março) que, em seu artigo 260º, número 1, determina sejam as ações sobre interpretação, validade ou execução do contrato administrativo de empreitada de obras públicas de competência da Justiça administrativa, obrigatoriamente precedidas de uma tentativa de conciliação perante uma comissão composta por um representante de cada uma das partes e presidida pelo presidente do Conselho Superior de Obras Públicas e Transportes.

Como já dito antes, o ordenamento jurídico português não prevê de modo explícito a aplicação da RAL ou da ODR em conflitos da administração pública, entretanto, existe a previsão constitucional do artigo 202, número 4, bem assim leis esparsas que contêm recomendações para o uso da mediação e arbitragem. Nesse sentido, Artur Flamínio da Silva[130] cita três dispositivos do CPA, quais sejam os artigos 12º; 56º e 57º. O autor alerta, porém, que, para a consecução da mediação no âmbito do direito administrativo, faz-se necessário a atuação de um terceiro que auxilie as partes a alcançar um consenso, ou seja, é preciso a figura do mediador imparcial (e, portanto, segundo o autor, esse espaço não deve ser preenchido pelo Provedor de Justiça, uma vez que exerce a função de fiscalização, "colidindo com a neutralidade exigida ao mediador"), bem como questiona se os "acordos celebrados no âmbito do procedimento administrativo podem ou não vincular juridicamente a Administração na sua decisão final no âmbito de um procedimento administrativo" e dos conflitos administrativos multipolares. Quanto à dimensão processual, o autor exemplifica essa possibilidade citando o artigo 87º-C, números 1, 2 e 3 do CPTA, e a utilização subsidiária do CPC, nos termos do seu art. 273º,

[129] CARVALHAL, Ana P. Z. – A arbitragem administrativa em Portugal. **Revista FMU Direito**. São Paulo, ano 24, n.º 33, 2010. p.1-18. Disponível em www.revistaseletronicas.fmu.br. [Consult. 15 mar. 2021].
[130] *Op. Cit.* p. 427-436.

mas ainda assim aponta dúvidas jurídicas, por exemplo: no curso de ação judicial, a quem caberá desempenhar o papel de mediador (poderá ser o próprio juiz da causa?), e, ainda, a aplicação dos princípios previstos nos artigos 3º e seguintes da Lei de Mediação à Administração, além da questão de eventual (in)compatibilidade da mediação com o direito fundamental à tutela jurisdicional efetiva, nos termos do art. 268º, número 4, da CRP.

De todo o exposto, pode-se extrair que, muito embora não exista uma lei específica que discipline e solucione as questões jurídicas levantadas pelos estudiosos, conforme relatado acima, em relação à possibilidade de a administração pública de Portugal participar de RAL (em especial, a mediação) e, por conseguinte, da ODR, o ordenamento jurídico prevê esta possibilidade em leis diversas, além de a Lei de Mediação, em seu artigo 3º[131], ao estabelecer que os princípios ali consagrados são aplicáveis a todas as mediações realizadas em Portugal, bem assim porque não restringe a sua aplicação à natureza do litígio, e, portanto, poderia em tese abranger as mediações a serem efetuadas pela administração pública portuguesa. Não obstante, pensamos que a publicação de lei que discipline a atuação da administração pública nas RALs e, consequentemente, na ODR, poderá assegurar maior tranquilidade jurídica àqueles que recorrerem a essa modalidade de resolução alternativa de conflitos em Portugal.

2.2.3 A Online Dispute Resolution na administração pública no Brasil

No Brasil, a ODR vem sendo utilizada como meio de fomentar e solucionar eventuais conflitos surgidos entre a administração e o cidadão, bem como tem sido utilizado como medida pré-judicial[132] também pelo Poder Judiciário, estando em causa litígios entre cidadãos, entre cidadãos e administração pública ou entre dois ou mais entes de natureza jurídica pública.

Como é sabido, no Brasil a Federação é composta pela União, pelos Estados, Municípios e Distrito Federal, nos termos dos artigos 1º e 18 da Constituição Federal do Brasil. Assim, em relação ao uso da ODR, cada ente pode decidir se adere ou não à

[131] Lei n.º 29/2013 – Princípios da mediação. Os princípios consagrados no presente capítulo são aplicáveis a todas as mediações realizadas em Portugal, independentemente da natureza do litígio que seja objeto de mediação.

[132] Neste caso, durante a pandemia, os atos judiciais, as conciliações e as mediações, que seriam realizadas de maneira presencial, foram realizadas por meio virtual, conforme a Resolução CNJ n.º 313, de 19 de março de 2020, e modificações posteriores, incluindo a instalação da plataforma de videoconferência denominada "Balcão Virtual", pela Resolução CNJ n.º 372, de 12 de fevereiro de 2021.

autocomposição. Necessário fazer essa distinção, uma vez que Portugal é um país unitário, conforme o art. 6º, número 1, da Constituição da República portuguesa. No caso brasileiro, portanto, caberá a cada ente estimar a conveniência e a oportunidade de celebrar acordos institucionais com a finalidade de aplicar uma política pública de desjudicialização e acesso à Justiça, voltada, enfim, ao estímulo da consensualidade e à rápida solução dos conflitos.

O ordenamento jurídico brasileiro permite o uso da ODR pela administração pública[133], notadamente com a finalidade de evitar a judicialização de questões de baixa complexidade, outras vezes para solucionar questões extremamente complicadas[134]. É possível, ainda, aproveitar as etapas já desenvolvidas anteriormente em um eventual processo judicial, com fundamento na cláusula geral de negociação processual do artigo 190[135] do Código de Processo Civil (CPC). Por exemplo, podemos citar a página na rede mundial de computadores da Advocacia-Geral da União, onde é possível solicitar a negociação online para encerrar litígios contra a União.[136]

A aplicação da ODR na administração pública brasileira, na opinião desta signatária, está ajustada ao princípio de acesso à Justiça previsto no inciso XXXV do art. 5º da Constituição de 1988[137]. Novamente, necessário ressaltar, que não se trata de mera situação administrativa de gerenciamento de banco de dados, conforme já salientado por Daniel Arbix.[138] Ademais, a Resolução n.º 125 do CNJ[139] disciplinou sobre a Política Judiciária Nacional de tratamento adequado dos conflitos de interesses no âmbito do

---

[133] Artigo 1º; e arts. 32 ao 40 da Lei n.º 13.140, de 2015.

[134] Como exemplo, TOMAZELLI, Idiana – **Prefeitura de SP e União fecham acordo para encerrar disputa por Campo de Marte**. Rio de Janeiro: O Globo, 2022.

[135] Art. 190. – Versando o processo sobre direitos que admitam autocomposição, é lícito às partes plenamente capazes estipular mudanças no procedimento para ajustá-lo às especificidades da causa e convencionar sobre os seus ônus, poderes, faculdades e deveres processuais, antes ou durante o processo. Parágrafo único. De ofício ou a requerimento, o juiz controlará a validade das convenções previstas neste artigo, recusando-lhes aplicação somente nos casos de nulidade ou de inserção abusiva em contrato de adesão ou em que alguma parte se encontre em manifesta situação de vulnerabilidade.

[136] GOVERNO FEDERAL. **Solicitar Negociação para Prevenir ou Encerrar Litígios (Judiciais ou Extrajudiciais) Contra a União**. Brasília, DF: [sn], [sd]. Disponível em: https://www.gov.br/pt-br/servicos/solicitar-negociacao-online-para-prevenir-ou-encerrar-litigios-judiciais-e-extrajudiciais-contra-a-uniao. [Consult. 19 abr. 2022].

[137] "Artigo 5º – […] XXXV – A lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;"

[138] "Uma ponderação persistente neste trabalho diz respeito ao equilíbrio entre efetividade e justiça. A judicialização de controvérsias é a resposta corriqueira esperada em regimes democráticos, nos quais a cultura de direitos individuais e de acionamento de órgãos judiciais por grupo de interesse convive com letargia ou delegação consentida dos Poderes Legislativo e Executivo. Mecanismos de ODR eficientes podem ser cruciais para órgãos judiciais, dando vazão a uma pluralidade de demandas similares cuja equação por formas tradicionais de resolução de disputas não seria possível – assim, a absorção de mecanismos de ODR por órgãos judiciais é imprescindível para viabilizar mais acesso à justiça". ARBIX, Daniel A. *Op. cit.* p. 14

[139] Resolução n.º 125 CNJ, atualizado pelas Emendas n.º 01/2013 e n.º 02/2016, e pelas Resoluções n.º 290/2019 e n.º 326/2020.

Poder Judiciário, bem assim a Lei de mediação, além dos atos normativos expedidos por cada um dos entes da Federação que compõem um conjunto normativo, cujo objetivo comum é o acesso à Justiça e, através dele, pacificação social e a promoção da paz, que se ajusta, vale repisar, ao Objetivo 16 da Agenda 2030 da ONU – Paz, Justiça e Instituições Eficazes. Nesse sentido, a ODR deve obrigatoriamente observar os princípios que regem a administração pública[140] e, acrescente-se a essa modalidade, a ambientação virtual e o gerenciamento de informações em grande porte.

O gerenciamento de informações constitui mecanismo de fundamental importância para a implementação da ODR, pois significa dissolver assimetrias de informação, aclarar regras de procedimento, entre outras providências, até que, em um exemplo extremo, seja crível alcançar um metódico e sistemático conjunto de soluções possíveis, em casos de processos em massa.[141] Dessa forma, ao manejar as informações de maneira a compreender amplamente os "dados brutos" das demandas mais comuns que acometem a administração pública e, ao mesmo tempo, beneficiar-se das técnicas de RAL, pode-se alcançar um leque de opções para solucionar tais conflitos, judiciais ou não, em ambiente virtual, ou seja, mediante o uso da ODR.

Ressalte-se, por oportuno, que não se trata de abandonar as técnicas da RAL no ambiente virtual e transformar as demandas em um "grande banco de dados", conforme já citado. O apropriado e confiável gerenciamento dessas informações é que irá permitir às partes aprenderem a melhor forma de resolver seus conflitos (Res 125 CNJ – Anexo III, art. 1º, inc. VII), obterem informações seguras e simétricas de forma mais rápida (Res 125 CNJ – Anexo III, art. 1º,inc. II); permitir ao mediador ser fiscalizado publicamente, ocasião que qualquer cidadão poderá se certificar sobre sua competência (Res 125 CNJ – Anexo III, art. 1º, inc. III), sua imparcialidade (Res 125 CNJ – Anexo III, art. 1º, inc. IV), sua independência e autonomia (Res 125 CNJ – Anexo III, art. 1º, inc. V) e legalidade,

---

[140] Conforme artigo 37 da CF: "Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência […]."

[141] Em análise similar voltada à iniciativa privada, mais uma vez Daniel Arbix opina: "Quanto mais aprimoradas as tecnologias, mais universais elas serão. Isso significa que as partes que lidam com muitos conflitos que hoje se tornam processos judiciais (como empresas de telecomunicações, do setor financeiro ou de aviação civil) estão na dianteira, por terem acesso aos dados brutos sobre múltiplas controvérsias. Se souberem analisar esses dados, identificar padrões, moldar comunicações e, sobretudo, ajustar suas práticas e políticas, estas empresas podem economizar, melhorar seus produtos e serviços e reconquistar seus consumidores. Conflitos que possuem feições semelhantes, embora envolvam partes diferentes, também são terreno fértil para experimentação com a resolução online: de cobranças (Money Claim Online no Reino Unido) a divórcios (Uitelkaar na Holanda, wevorce nos EUA), os exemplos vêm se multiplicando." CABRAL, Rubia. **A Transformação do Direito na Era Digital e a Simplificação do Acesso à Justiça**. Rio de Janeiro: [sn], 2017. Entrevista concedida em 31/10/2017, disponível em https://justto.com.br/blog/daniel-arbix-transformacao-do-direito-na-era-digital-e-simplificacao-do-acesso-justica/. [Consult. 19 abr. 2022]

pois deve agir com respeito à ordem pública e às leis vigentes (Res 125 CNJ – Anexo III, art. 1º, inc. VI)[142].

Em conclusão, a adoção da ODR pela administração pública traz benefícios a administração, aos contribuintes e aos interessados que se utilizam dessa ferramenta.

2.3 AS PLATAFORMAS PÚBLICAS E PARTICULARES UTILIZADAS NA ONLINE DISPUTE RESOLUTION

2.3.1 A Plataforma Resolução de Litígios em Linha ou Plataforma Online Dispute Resolution

Nos países democráticos o Poder Judiciário constitui o órgão estatal responsável pela manutenção da ordem e da paz social.[143] Não obstante, modernamente, novos procedimentos têm sido introduzidos, quais sejam: a RAL, e, em alguma medida, a ODR, com a finalidade de também contribuírem para a pacificação social. Nesse contexto, observa-se uma adaptação das técnicas da RAL, acrescidas dos instrumentos da TIC, para criar um modo menos custoso, mais rápido e informal para solucionar as controvérsias que surgem em sociedade, isto é, a ODR. As modificações nas rotinas que buscam solucionar os conflitos já são sentidas, motivadas ultimamente pela pandemia de SARS-COV-2, em especial a partir de março de 2020. Contudo, essas alterações, já há algum tempo, têm obtido algum sucesso no tratamento dos litígios decorrentes do comércio eletrónico. Ou seja, como já foi citado anteriormente, as questões ligadas ao direito do consumidor encontraram inicialmente maior aplicação da ODR; por exemplo, nos sites eBay, Alibaba, entre outros. Nesse caso, utilizam-se as "plataformas eletrónicas', ou seja, trata-se da utilização da Tecnologia da Informação (TI), em meio digital, que suporta a execução de tarefas e/ou procedimentos seriados a fim de solucionar demandas entre partes antagónicas decorrentes do mercado digital, isto é, entre consumidores e comerciantes.

A União Europeia[144] devido à sua abrangência e aos seus numerosos sistemas judiciários, além do crescimento cada vez maior do comércio eletrónico dentro de suas fronteiras e o consequente aumento de litígios nesse campo, normatizou o uso da

[142] FIGUEIRA, Denise C. *Op. cit.* p. 524-525.
[143] CRP – Artigo 20º, número 1; CF- artigo 5º, inciso XXXV.
[144] A União Europeia é uma união económica e política atualmente composta por vinte e sete países-membros, firmada inicialmente pelo Tratado de Maastricht, de 1992, inicialmente composta pelos sete países que constituíam a antiga Comunidade Europeia. Foi assinado em 7 de fevereiro de 1992 e entrou em vigência em 1º de novembro de 1993.

ODR para pôr termo às pendências relativas ao comércio ao disponibilizar uma plataforma eletrónica para resolver tais conflitos, mediante a edição da Diretiva 2013/11/UE[145] do Parlamento Europeu e do Conselho, de 21 de maio, relativa à resolução alternativa de litígios de consumo (Diretiva RAL), e o Regulamento 524/2013/UE[146], do Parlamento Europeu e do Conselho, de 21 de maio, sobre a resolução de litígios de consumo em linha (Regulamento RLL ou Regulamento ODR). Tais soluções visam, portanto, cooperar para a construção de um mercado único digital da União Europeia, no sentido de diminuir resistências à livre circulação de bens entre os Estados-Membros da União.

Em suma, a Plataforma RLL facilitou o acesso à solução de controvérsias, tornando mais célere a composição entre os litigantes, com alcance transfronteiriço, ao eliminar custos financeiros e de transporte e, ao fim e ao cabo, aumentou a segurança do processo de resolução de conflitos. Nesse sentido, Teresa Moreira atesta e aplaude a disponibilização da plataforma como um marco na defesa do direito do consumidor, mediante o acesso a uma "justiça simples e fácil"[147].

Em resumo, a Diretiva da RAL teve atuação fundamental na proteção dos consumidores[148], localizados dentro dos limites dos Estados-Membros, uma vez que a "fragmentação do mercado interno é prejudicial para a competitividade, para o crescimento e para a criação de emprego na União"[149]. De outro lado, o Regulamento 524/2013 criou uma plataforma de ODR que auxiliou a solucionar disputas relativas às vendas online. O êxito dessa plataforma, entretanto, esteve atrelada à atuação dos Estados-Membros[150] no sentido de implementar de maneira efetiva essa ferramenta, uma vez que a plataforma RLL proporciona o contato entre os litigantes e a possibilidade de acompanhamento online das demandas, além de oferecer serviço de tradução de documentos, porém, cada Estado-Membro deve habilitar entidades de Resolução Alternativa de Litígios de Consumo (RAL) em seu respectivo território para solucionar o conflito. Sob esse aspeto, a plataforma ODR da UE não é uma plataforma ODR *stricto*

[145] Esta Diretiva alterou o Regulamento (CE) n.º 2006/2004 e a Diretiva 2009/22/CE.
[146] Este Regulamento também alterou o Regulamento (CE) n.º 2006/2004 e a Diretiva 2009/22/CE.
[147] MOREIRA, Teresa – Novos desafios para a contratação à distância a perspectiva da defesa do consumidor. **Estudos do Direito do Consumidor**. n.º 9. Coimbra, 2015. p. 19-36.
[148] Considerando (4) da Diretiva 2013/11/EU.
[149] Considerando (3) da Diretiva 2013/11/EU.
[150] Segundo Nicolas Vermeys, há a necessidade de preencher conjuntamente três critérios para o sucesso de plataformas eletrónicas: material, tecnológico e geográfico, conforme consta em Les modes privés de prévention et de règlement des differends em ligne. ROUSSEAU, Stéphane (Coord.) *In* **Juriste dans fronteires – Mélanges Ejan Mackaay**. Montreal: Ed. Thémis, 2015.p. 471 e seguintes.

sensu, onde os consumidores podem solucionar seus questionamentos apenas mediante a sua utilização, pois é a entidade (RAL), previamente credenciada, que resolverá a disputa. Vale observar que as matérias sujeitas à resolução, por meio da Plataforma RLL, devem estar em harmonia com o disposto no artigo 2º da Diretiva 2013/11/UE do Parlamento Europeu e do Conselho. O procedimento da plataforma pode ser visualizado nas figuras abaixo:

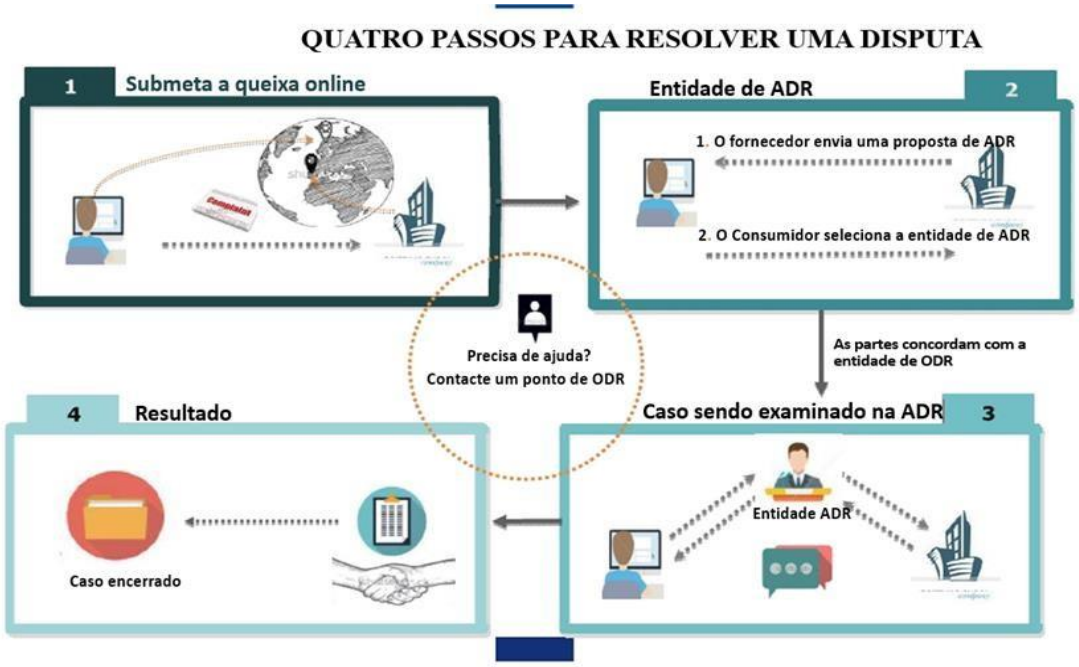

Figura 1. Imagem que demonstra o funcionamento resumido da Plataforma RLL "Reimpressa de https://www.europarl.europa.eu/meetdocs/2014_2019/" por Parlamento Europeu, 03/03/2021.

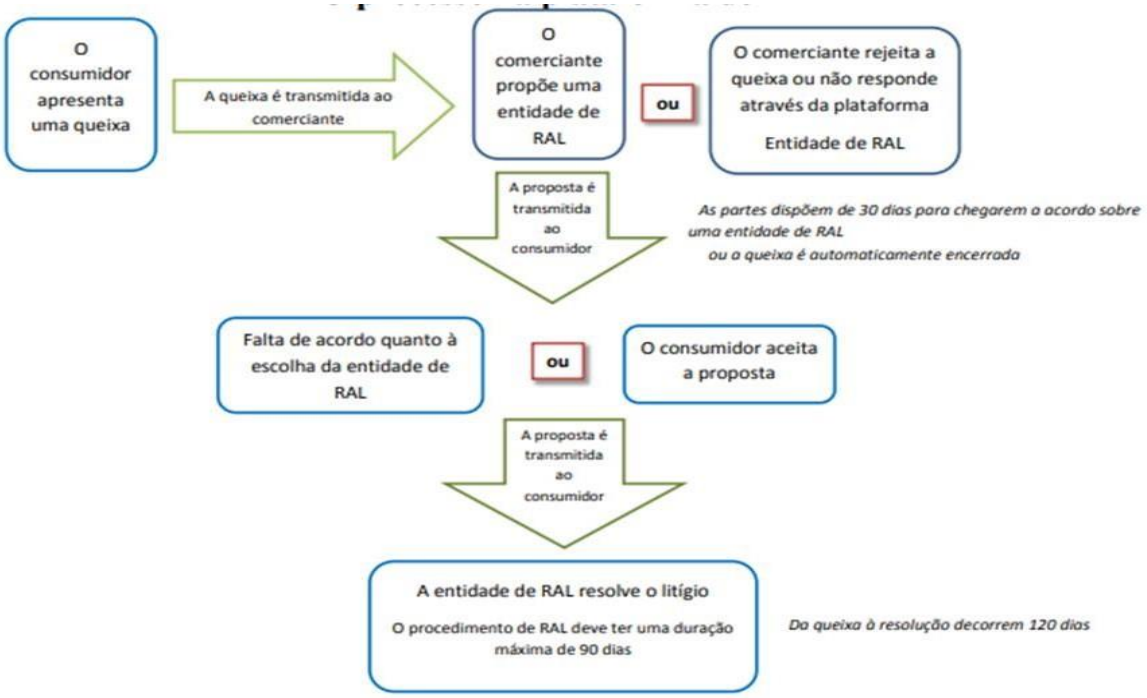

Figura 2. Imagem que demonstra o funcionamento Detalhado da Plataforma RLL. Relatório da Comissão ao Parlamento Europeu e ao Conselho sobre o Funcionamento da Plataforma Europeia de Resolução de Litígios em

Linha Criada ao Abrigo do Regulamento (UE) n.º 524/2013 sobre a Resolução de Litígios de Consumo em Linha. Bruxelas: [sn], 2017 "Reimpressa de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017DC0744&from=en" pela Comissão Europeia, 17/02/2021.

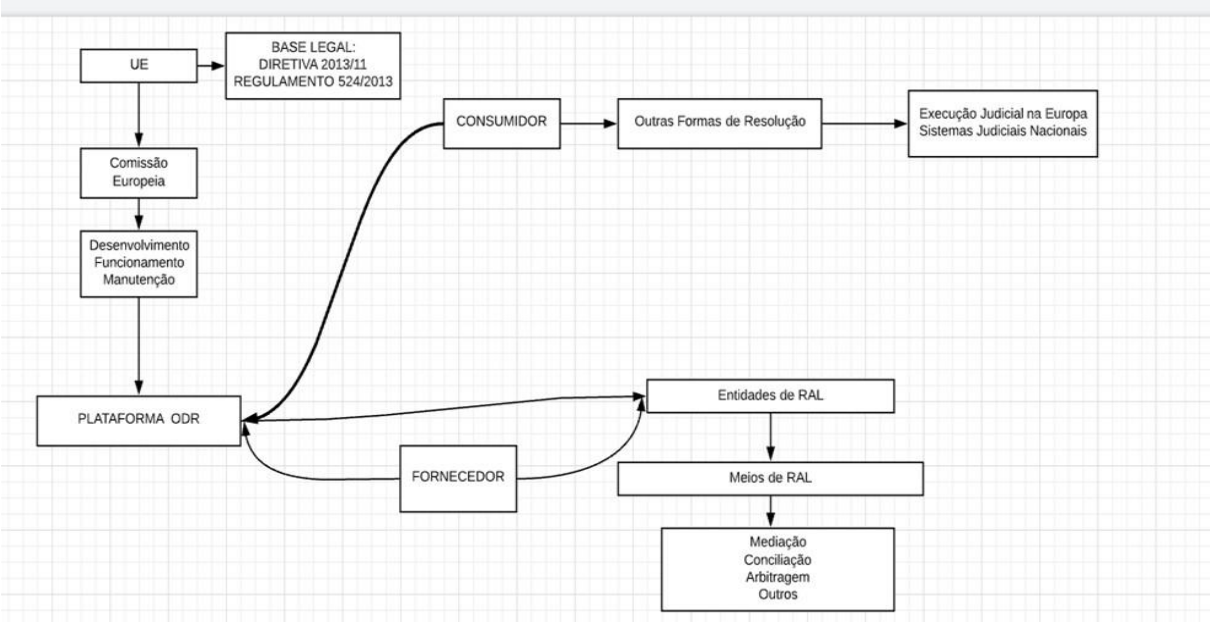

Figura 3. Mapa Conceitual da Plataforma RLL, construído e elaborado pela própria autora.

A Plataforma RLL, juntamente com outros normativos, como a Diretiva de Direitos do Consumidor (Dir. 2011/83/UE), tem por objetivo incrementar a confiança do consumidor no comércio online.[151] De fato, podemos destacar como vantajosa a utilização da Plataforma RLL, ao considerar a possibilidade de traduzir documentos; a centralização das demandas emum único endereço eletrónico; o acompanhamento online das etapas pelos litigantes e a gratuidade do procedimento. Todavia, o fato de a Plataforma RLL se constituir em um centro de receção de demandas para a distribuição das reclamações nos respectivos RAL acaba por restringir a solução completa das lides por meio online, além de ter sua atuação restrita aos territórios dos Estados-Membros da União. Ou seja, sua atuação poderia ser mais abrangente se a resolução dos conflitos fosse realizada integralmente por meio da plataforma RLL, constituindo verdadeira ODR, bem como pudesse extrapolar os limites territoriais da União Europeia.

Existem, portanto, obstáculos a serem enfrentados para a utilização da Plataforma RLL, notadamente no que diz respeito ao desconhecimento de sua utilização pela população em geral e a ausência de confiança para solucionar as questões por meio

[151] LÓPEZ, Manuel J. M. – La Directiva 2011/83/UE: esquema general, ámbito de aplicación, nivel de armonización y papel de los Estados Miembros *in* **Revista CESCO de Derecho de Consumo**. N.º 1, 2012. Disponível em: https://revista.uclm.es/index.php/cesco/article/view/7. [Consult. 22 abr. 2022].

eletrónico. Não obstante, considerando os benefícios que a ODR proporciona, a busca por estratégias para superar esses óbices, segundo Pablo Córtes[152], deve continuar.

2.3.2 A Plataforma Resolução de Litígios em Linha em Portugal

Portugal realizou em 2015 a transposição para o direito português a Diretiva 2013/11/UE, por meio da publicação da Lei n.º 144/2015[153], de 8 de setembro, sobre a resolução alternativa de litígios de consumo.[154]

O artigo 2º, n. 1, da Lei 144/2015, determina que o seu escopo é a utilização da RAL para resolver pendências entre contratos de compra e venda ou prestação de serviços entre consumidores residentes em Portugal e na União Europeia, e, em seu artigo 6º, a Lei determina que as entidades de RAL devem aderir à plataforma RLL criada pelo Regulamento n.º 524/2013, bem assim os procedimentos devem estar disponíveis por meios convencionais ou online (artigo 10º). A plataforma encontra-se em vigor desde fevereiro de 2016, conservada e financiada pela Comissão Europeia, conforme estabelecido no artigo 5º, número1, do Regulamento 524/2013[155].

A citada Lei cria a Rede de Arbitragem de Consumo (artigo 4º), formada por entidades de RAL previamente qualificadas, com o objetivo de harmonizar os procedimentos de RAL e a recolha de informações estatísticas, além de determinar a manutenção de sítios eletrónicos na rede mundial de computadores, a fim de facilitar o acesso dos envolvidos às informações relativas ao procedimento da RAL (artigo 6º).

---

[152] O autor sugere algumas estratégias: campanhas de educação e conscientização para empresas e consumidores; investimento em prevenção de disputas; resolução de disputas o mais rápido possível; linhas de financiamento: taxas públicas/setoriais/comerciantes/processos etc.; estabelecimento de padrões mínimos de atuação para garantir resultados justos; tornar o uso obrigatório da plataforma em certos setores ou em litígios transfronteiriços; incentivos para os fornecedores usarem a plataforma. CÓRTES, Pablo – What should the ideal ODR system for e-commerce consumers look like? **The Hidden World of Consumer ADR: Redress and Behaviour**. [sl], [sn], oct., 2011. p. 1-2. Disponível em https://www.law.ox.ac.uk/sites/default/files/migrated/dr_pablo_cortes.pdf. [Consult. 10 mar. 2021].

[153] Lei n.º 144/2015. **Diário da República, Série I**. N.º 175 (08-09-2008), p. 7251-7258. Disponível em https://dre.pt/dre/detalhe/lei/144-2015-70215248. [Consult. 16 fev. 2021].

[154] A Lei n.º 144/2015 foi objeto de duas modificações, ambas pontuais: a primeira pelo Decreto-Lei n.º 102/2017, de 23 de agosto, e a segunda pela Lei n.º 14/2019, de 12 de fevereiro.

[155] Artigo 5º – Criação da plataforma de RLL. "1. A Comissão cria uma plataforma de RLL e é responsável pelo seu funcionamento, incluindo todas as funções de tradução necessárias ao objetivo do presente regulamento, à sua manutenção, ao seu financiamento e à segurança dos dados dela constantes. A plataforma de RLL deve ser de fácil utilização. A criação, o funcionamento e a manutenção da plataforma de RLL devem assegurar que a privacidade dos seus utilizadores seja respeitada desde a fase de conceção, e que a plataforma de RLL seja acessível e utilizável por todos os utilizadores, incluindo, na medida do possível, os utilizadores vulneráveis." REGULAMENTO (UE) 524/2013. **Jornal Oficial da União Europeia**. (21-05-2013), p. L165/1-165/12. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013R0524&from=EL. [Consult. 16 fev. 2021].

Em Portugal, a Rede de Arbitragem de Consumo é composto por nove[156] Centros de Arbitragem de Conflitos de Consumo, divididos em razão de sua localização territorial, e mais três[157] Centros de competência nacional, divididos de acordo com suas competências finalísticas. A respeito dos Centros de Arbitragem, Cátia Marques Cebola alerta sobre as condições de seu funcionamento:

> Pelo contrário, a Lei 144/2015 tentou implementar em Portugal um sistema de acreditação e controlo absoluto sobre entidades que podem resolver disputas consumo neste país. Consequentemente, após a transposição da Diretiva ADR, todas as entidades que pretendem oferecer serviços de resolução extrajudicial para Litígios de consumo por meio de mediação, conciliação ou arbitragem devem solicitar autorização da Direção-Geral de Consumo e, respeitando os requisitos de qualidade da Lei 144/2015, passam a fazer parte da lista de entidades RAL de Portugal. Caso a autorização não seja solicitada, a entidade não pode resolver disputas de consumo fora do tribunal. Consequentemente, a Lei Portuguesa estabelece sanções pecuniárias em caso de incumprimento dos requisitos legal ou para entidades que promovem a resolução disputas extrajudiciais de consumo sem autorização.[158]

O site da UE contém dados que permitem avaliar o comportamento da plataforma de acordo com a disposição do artigo 21º do Regulamento 524/2013/UE, relativo à Resolução deLitígios em Linha (RLL ou ODR), cujo desempenho podemos observar nos dois gráficos:

[156] (1) Centro de Arbitragem da Universidade Autónoma de Lisboa; (2) Centro de Arbitragem de Conflitos de Consumo da Região Autónoma da Madeira; (3) Centro de Arbitragem de Conflitos de Consumo de Lisboa; (4) Centro de Informação de Consumo e Arbitragem do Porto; (5) CIAB – Centro de Informação, Mediação e Arbitragem de Consumo (Tribunal Arbitral de Consumo); (6) CIMAAL- Associação Centro de Informação, Mediação e Arbitragem de Conflitos de Consumo do Algarve; (7) CNIACC – Centro Nacional de Informação e Arbitragem de Conflitos de Consumo; (1) Centro de Arbitragem da Universidade Autónoma de Lisboa; (2) Centro de Arbitragem de Conflitos de Consumo da Região Autónoma da Madeira; (3) Centro de Arbitragem de Conflitos de Consumo de Lisboa; (4) Centro de Informação de Consumo e Arbitragem do Porto; (5) CIAB – Centro de Informação, Mediação e Arbitragem de Consumo (Tribunal Arbitral de Consumo); (6) CIMAAL- Associação Centro de Informação, Mediação e Arbitragem de Conflitos de Consumo do Algarve; (7) CNIACC – Centro Nacional de Informação e Arbitragem de Conflitos de Consumo; (8) Centro de Arbitragem de Conflitos de Consumo do Ave, Tâmega e Sousa; (9) Associação de Arbitragem de Conflitos de Consumo do Distrito de Coimbra.

[157] (1) Centro de Arbitragem do Sector Automóvel; (2) CIMPAS – Centro de Informação, Mediação, Provedoria e Arbitragem de Seguros; (3) Provedor da APAVT- Provedor do Cliente das Agências de Viagens e Turismo.

[158] MARQUES CEBOLA, Cátia – Mediación y arbitraje de consumo: una visión comparada de los modelos portugués y español. **Revista de Internet, Derecho y Política**. N.º 25, Sept. 2017, p. 6-16. Disponível em https://www.redalyc.org/articulo.oa?id=78852903003. [Consult. 10 mar. 2021].

Figura 4. Imagem que demonstra o Desempenho da Plataforma RLL. Functioning of the European ODR. Platform Statistical report, dezembro de 2020 "Reimpressa de https://ec.europa.eu/info/sites/info/files/odr_report_2020_clean_final.pdf" pela Comissão Europeia, 10/03/2021.

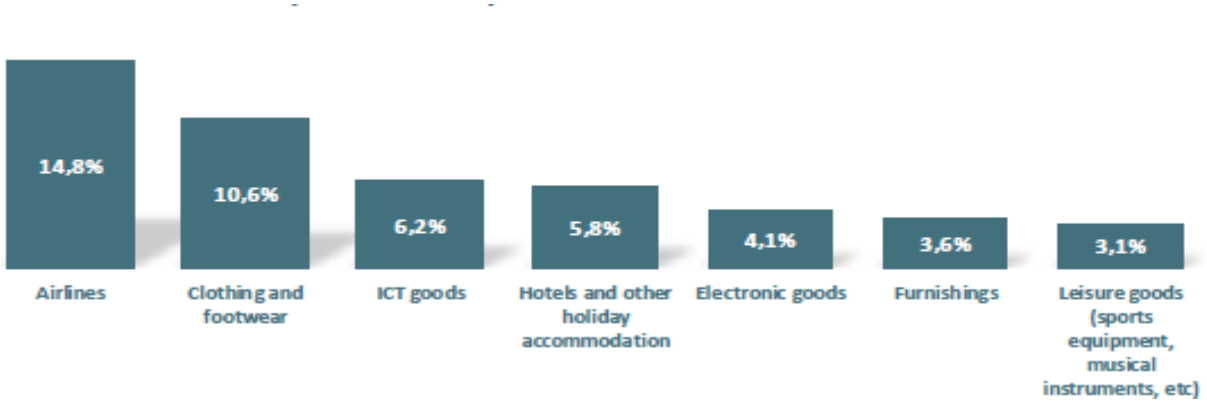

Figura 5. Imagem que demonstra os sete segmentos mais demandados da Plataforma RLL no ano de 2019. Functioning of the European ODR. Platform Statistical report, dezembro de 2020 "Reimpressa de https://ec.europa.eu/info/sites/info/files/odr_report_2020_clean_final.pdf" pela Comissão Europeia, 10/03/2021.

Essa estatística servirá para eventual adaptação da Plataforma RLL (ou ODR), conforme dispõe o número 2 do artigo 21º do citado Regulamento. Uma breve leitura desses dados oferece uma ideia do aproveitamento da Plataforma[159]. Por exemplo, em 2019, pode-se observar pela informação disponibilizada no site da UE[160], que 83% das demandas foram concluídas após o prazo de 30 dias; 11% das reclamações foram refutadas pelos comerciantes; 20% informaram que sua disputa foi resolvida na plataforma ou fora dela, e outros 18% responderam que continuavam a discutir com o comerciante. Apenas 2% das reclamações foram apreciadas por um órgão da RAL, o que nos leva a concluir que os obstáculos a serem enfrentados para a utilização da Plataforma RLL, conforme relatado precedentemente, ainda se mostram bastante desafiadores e requerem uma atuação mais eficiente dos Estados-Membros para tornar eficaz o livre comércio, a geração de empregos e a efetiva proteção dos consumidores no âmbito da União Europeia.

É possível concluir, também, no tocante aos princípios da ODR mencionados, que o número 2 do artigo 21º do citado Regulamento, que visa a eventual adaptação do sistema, encontra amparo no citado princípio da adaptabilidade e inovação da utilização dos meios tecnológicos, bem assim no princípio da integração da ODR com outros sistemas de resolução de disputas. Nesse último caso, é de se notar que a informação trazida pela Plataforma RLL relata que 20% dos demandantes resolveram a sua pendência pela plataforma ou

[159] Portugal ocupa o sétimo lugar entre os países demandantes, sendo que 1.059 foram provenientes de litígios internos e 526 foram transfronteiriços.
[160] Disponível em https://ec.europa.eu/info/sites/info/files/odr_report_2020_clean_final.pdf. [Consult. 10 mar. 2021].

fora dela, e 18% ainda permaneciam em contato com o comerciante. Ou seja, esses dados permitem afirmar que a integração do sistema ODR, nesse caso a Plataforma RLL (que, como dissemos, sequer pode ser caracterizada como uma Plataforma ODR *strictu sensu*) com outras modalidades de RAL de fato se mostra proveitosa, no sentido de promover o consenso e a resolução de disputas.

Vale registrar, nesse contexto, que em julho de 2019, segundo o citado endereço eletrónico da UE, alterações já foram introduzidas na Plataforma RLL, qual seja: a oferta de um formulário para que o interessado identifique qual solução melhor o atende para reparar sua demanda. Ao final de 2019, a quantidade de consumidores por mês que interagiram com a plataforma quadruplicou, atingindo o número de vinte mil consumidores mensais. O número de reclamações formalmente registrados na plataforma também diminuiu consideravelmente, conforme se pode apurar na figura a seguir:

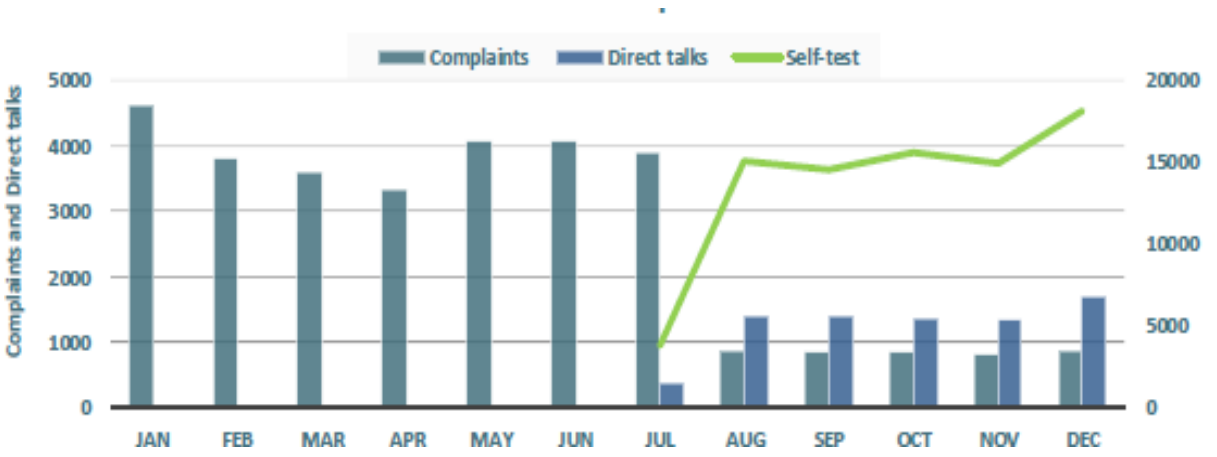

Figura 6. Imagem que demonstra o número de submissões à Plataforma RLL em 2013. O gráfico mostra que a partir do mês de julho – data do lançamento das modificações na Plataforma RLL – a quantidade de queixas submetidas à plataforma diminuiu consideravelmente "Reimpressa de https://ec.europa.eu/info/sites/info/files/odr_report_2020_clean_final.pdf" pela Comissão Europeia, 10/03/2021.

Assim, muito embora ainda hoje a solução de controvérsias por meios virtuais possa soar estranha aos ouvidos mais conservadores, é de se registrar que existe um aparato legal que fundamenta essa escolha, bem assim o meio virtual, que aos poucos tem se mostrado eficaz e com tendência de crescimento entre os europeus.

2.3.3 Utilização de plataformas em Portugal

Necessário registrar que a pandemia da COVID-19, de um lado, afetou profundamente o funcionamento do Poder Judiciário, e, de outro, acelerou o uso dos

meios informáticos no campo judicial. Tomemos, por exemplo, a atuação da Assembleia da República que aprovou a Lei n.º 4-A/2020, de 6 de abril, e alterou a Lei n.º 1-A/2020, de 19 de março, regulamentando "medidas excecionais e temporárias de resposta à situação epidemiológica provocada pelo coronavírus SARS-CoV-2 e da doença COVID-19". Entre outras medidas, essa Lei incentivou a utilização da ODR notadamente ao dispor, em seu artigo 2º, a alteração do artigo 7º da Lei n.º 1-A/2020, e no que se refere ao número 5 (b), a possibilidade de prática de atos processuais "quando todas as partes entendam ter condições para assegurar a sua prática através das plataformas informáticas que possibilitam a sua realização por via eletrónica ou através de meios de comunicação à distância adequados, designadamente teleconferência, videochamada ou outro equivalente". Nota-se, portanto, que a lei estimulou o uso de plataformas informáticas sempre que possível diante da emergência sanitária, bem como preservou o princípio da voluntariedade da ODR no aludido inciso 5(b).

Houve, ademais, a disponibilização de um conjunto de recursos online por meio do site eportugal.gov.pt[161], bem como a divulgação de sítios para melhorar o acesso à Justiça, como a CITIUS (https://www.citius.mj.pt/), destinado à gestão processual dos Tribunais Judiciais de Portugal, com o objetivo de desmaterialização dos processos judiciais e, portanto, criação de processos digitais, com várias iniciativas de acesso à Justiça eletrónica.

Em conclusão, podemos perceber que a utilização dos meios informáticos, seja para a proteção dos consumidores, para assegurar o acesso à Justiça em meio à pandemia ou, sobretudo para facilitar o acesso à Justiça, vem se tornando comum e cada vez mais habitual, sendo certo arriscar que a ODR poderá ocupar em breve uma posição de destaque nos meios judiciais e promotores do acesso à Justiça e pacificação social.

2.3.4 Utilização de plataformas no Brasil

No Brasil existem várias plataformas particulares e estatais. Também no Brasil, os litígios envolvendo o direito do consumidor são aqueles mais favoráveis a serem resolvidos por meio da ODR. Em virtude desse fato, os *softwares* de ODR vem ganhando espaço, segundo dados da Associação Brasileira de Lawtechs & Legaltechs (AB2L).[162]

[161] Exemplos de serviços disponibilizados: registar nascimento; renovação online do Cartão de Cidadão; solicitar agendamento; solicitar e consultar registro criminal de pessoas; solicitar certidão judicial eletrónica, entre outros.
[162] No Brasil, existem dezessete empresas de desenvolvimento de *softwares* para os métodos de ODR, segundo ROSA, Camila da; SPALER, Mayara G. – Experiências Privadas de ODR no Brasil. **Revista Jurídica da**

Entre as plataformas particulares, a mais antiga é a Reclame Aqui[163]. Trata-se de uma plataforma de uso gratuito, e, embora não possamos denominá-la como uma plataforma de ODR, uma vez que a sua atuação se restringe a colocar em contato o consumidor e a empresa prestadora de serviços e/ou venda para solucionarem a demanda do interessado, transformou-se em um local de pesquisa sobre a reputação das empresas que estão no mercado, isto é, são utilizadas precedentemente pelo consumidor (antes de firmar o contrato de compra e venda e/ou serviços) para investigar a atuação da empresa com os seus clientes. Outra plataforma que inclui a negociação e a conciliação eletrónica é a Sem Processo[164]. Trata-se de plataforma acessível apenas aos advogados das partes, a fim de resolver demandas, sem e com processo judicial instalado, e abrange integralmente todas as tratativas empenhadas entre as partes, representadas por seus advogados.

Os entes estatais brasileiros, ou seja, a União, os Estados e os Municípios, conforme já esclarecido, possuem competência para legislar sobre a sua própria política de utilização dos meios adequados de resolução de conflitos (RAL). Assim, serão destacados apenas os meios utilizados pela União. Nesse sentido, a plataforma institucional mais relevante é a consumidor.gov.br[165], que se apresenta como um sítio de negociação ligada ao Ministério da Justiça. É um serviço público que permite a comunicação direta entre consumidores e empresas para solução de conflitos típicos do comércio eletrónico.[166] Não constitui um procedimento administrativo e não substitui o atendimento prestado por outros órgãos de defesa do consumidor. Trata-se de um serviço que valoriza a comunicação recíproca entre consumidores e fornecedores, e, portanto, a participação de empresas e de seus clientes é voluntária. Ambos devem se comprometer formalmente ao serviço e se empenhar para solucionar os problemas apresentados.

A plataforma consumidor.gov.br tem por objetivos: (1) ampliar o atendimento aos consumidores e incentivar a competitividade pela melhoria da qualidade de produtos, serviçose do relacionamento entre consumidores e empresas; (2) aprimorar as políticas de prevenção de condutas que violem os direitos do consumidor; e (3) fortalecer a promoção

Escola Superior de Advocacia da OAB-PR. Ano 3, n.º 3 – Dezembro de 2018, p. 1-46. Disponível em http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista_esa_8_10.pdf. [Consult. 14 mar. 2021].

[163] Disponível em www.reclameaqui.com.br. [Consult. 14 mar. 2021].

[164] Disponível em https://www.semprocesso.com.br. [Consult. 14 mar. 2021].

[165] Disponível em https://www.consumidor.com.br. [Consult. 14 mar. 2021].

[166] É necessário registrar que o Governo Federal tem investido na digitalização dos serviços públicos e, por essa razão, tem incentivado que os cidadãos brasileiros tenham uma conta no site www.gov.br, que disponibiliza diversos serviços em um único endereço eletrónico. Não se trata de uma plataforma de resolução de conflitos, mas indica a orientação de utilizar, cada vez mais, o meio digital para atender ao público.

da transparência nas relações de consumo canais tradicionais de atendimento.[167]

O funcionamento da plataforma é bem simples e muito parecido com o da Reclame Aqui: o consumidor envia a sua manifestação à empresa contra a qual visa solucionar uma demanda e que deve estar cadastrada na aludida plataforma. Caso a empresa não esteja cadastrada, o cliente deve procurar os órgãos do Sistema Nacional de Defesa do Consumidor, que poderão orientá-lo e auxiliá-lo na resolução de seu problema de consumo. Registrada a reclamação, a empresa tem o prazo de dez dias para apresentar uma resposta. Após esse prazo, o consumidor classificará a demanda como resolvida ou não resolvida, e ainda indicar o seu nível de satisfação com o atendimento recebido.

Como se pode perceber também nesse caso, e igualmente como a Plataforma RLL, não se trata de uma plataforma de negociação que utilize as técnicas da RAL e/ou ODR para solucionar eventuais pendências entre consumidor e empresa. Não obstante, como dissemos antes, a transformação dos hábitos em meio digital constitui um processo longo, sujeito a avanços e retrocessos. Assim, toda e qualquer tentativa de incentivar a comunicação entre as partes de uma demanda, seja de consumo ou não (porque a RAL e ODR podem ser utilizadas para resolver pendências em outros campos de desavença), acaba por influenciar positivamente no aprimoramento da RAL ou ODR, bem como na aproximação dos demandantes, que pavimentam o caminho da consciência de direitos dos cidadãos e deveres das empresas prestadoras de serviços, o que pode resultar em um ambiente mais confiável e, portanto, mais favorável ao comércio eletrónico ou físico.

Da mesma forma que a Plataforma RLL, as informações sobre as demandas na plataforma consumidor.gov.br são endereçadas a uma base de dados pública, onde é possível a recolha de informações e, consequentemente, a elaboração de ranking sobre o seu desempenho.

Para melhor elucidar a questão, disponibilizamos duas figuras que mostram dados estatísticos sobre a plataforma consumidor.gov.br[168]:

---

[167] CONSUMIDOR.GOV. **Conheça o Consumidor.gov.br**. Brasília, DF: [sn], [sd]. Disponível em https://www.consumidor.gov.br/pages/conteudo/publico/1. [Consult. 09 mar. 2021].

[168] Gráficos disponíveis em https://consumidor.gov.br/pages/indicador/infografico/abrir. [Consult. 09 mar. 2021].

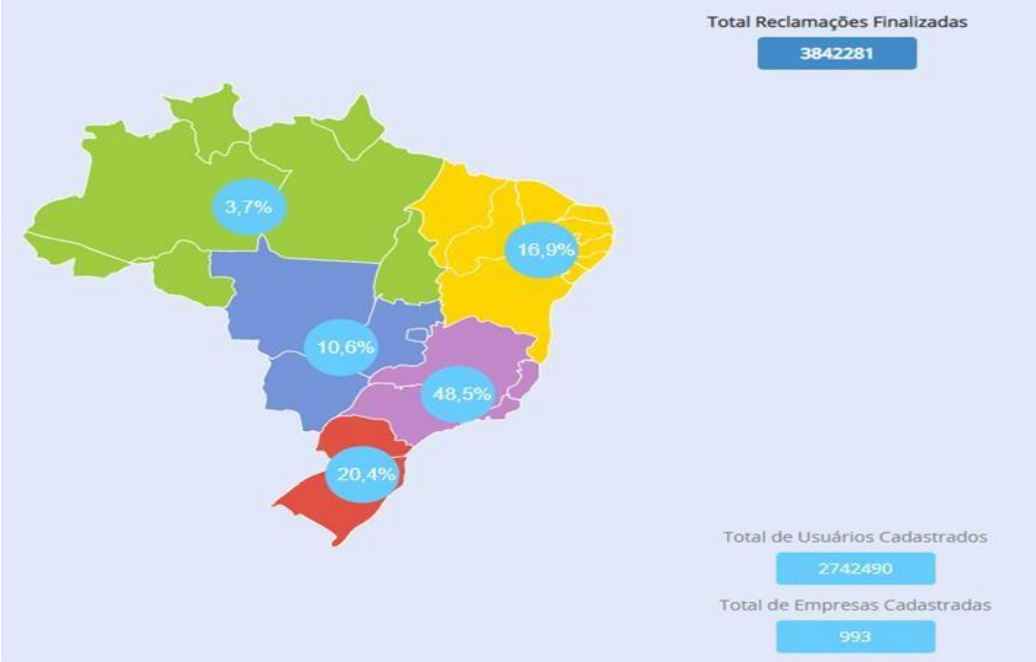

Figura 7. Imagem que demonstra as porcentagens de acessos no site consumidor.gov.br por região do Brasil. "Reimpressa de em https://consumidor.gov.br/pages/indicador/infografico/abrir." Pelo Governo Federal do Brasil, 09/03/2021.

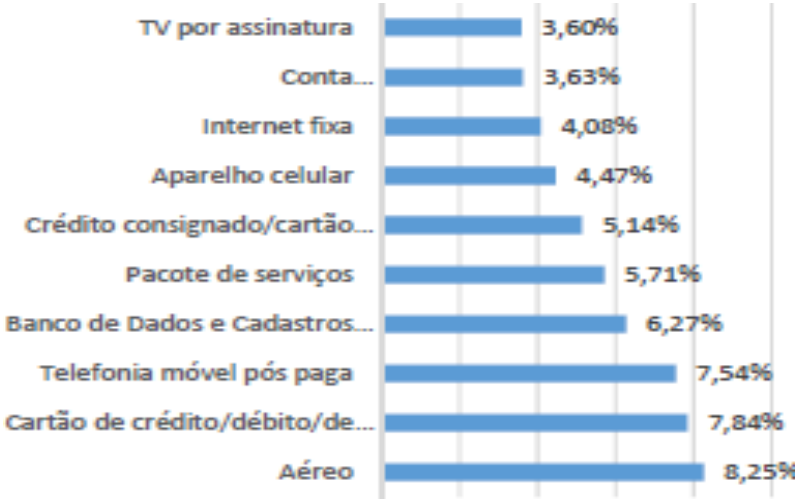

Figura 8. Imagem que demonstra os segmentos mais demandados de janeiro a abril de 2020 no site consumidor.gov.br. "Reimpressa de em https://consumidor.gov.br/pages/indicador/infografico/abrir" Pelo Governo Federal do Brasil, 09/03/2021.

Verifica-se, inicialmente, a porcentagem de acessos por região brasileira, bem como percebe-se que os acessos advindos da região Sudeste praticamente correspondem à metade do total de acessos. Além disso, pode-se visualizar o número significativo de reclamações finalizadas (3.842.281), o número de usuários cadastrados (27.424.490) e de empresas cadastradas (993). Quanto à diferença nominal entre usuários e empresas cadastradas, pensamos que essa diferença evidencia o tamanho do desafio para a

construção de um local seguro e confiável, em meio virtual, para resolver definitivamente as demandas de consumo, ou seja, constata-se a situação fática ainda desconfortável para a completa implementação de uma plataforma integralmente dedicada à ODR.

2.3.4 Comparação entre a plataforma da União Europeia e a plataforma consumidor.gov.br

Após o relato sobre o funcionamento das plataformas utilizadas na União Europeia e no Brasil, mostra-se interessante realizar uma breve comparação entre ambas, utilizando como parâmetro as principais características de cada uma.

Inicialmente, necessário registrar que a Plataforma RLL (ou ODR) da União Europeia atende a todos os vinte e sete países da União, cuja população atinge mais de 447 milhões de habitantes[169] com regras de comércio, sistemas jurídicos, idiomas diferentes, sendo que dezenove deles fazem parte da "Zona Euro", ou seja, em alguns casos, as moedas não são coincidentes.

De outro lado, a Plataforma consumidor.gov.br é uma plataforma para um único país, que utiliza o mesmo idioma e moeda, e abrange cerca de 213 milhões de habitantes[170], subordinados a um único sistema jurídico, que proporciona, portanto, um contexto mais homogéneo à plataforma. Em verdade, ao analisar o quadro abaixo, pode-se inferir agrande similitude entre as plataformas.

Características	**Consumidor.gov.br**	**UE**
Fornecedores	Exige registro	Exige registro
Consumidores	Exige registro	Não exige registro
Tempo para resposta	10 dias	30 dias
Taxa para consumidores	Não	Pode existir, se for usado uma entidade de RAL

[169] COUNTRY ECONOMIC. União Europeia. Disponível em https://pt.countryeconomy.com/paises/grupos/uniao-europeia. [Consult. 23 abr. 2022].
[170] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. População: Pirâmide Etária: 2010. Disponível em: https://cidades.ibge.gov.br/brasil/panorama. [Consult. 23 abr. 2022].

Taxas para fornecedores	Não	Pode existir, se for usado umaentidade de RAL
Tipos de transações	Online e offline	Online
Intermediários	Não	Entidade de RAL

Figura 9. Tabela que apresenta uma síntese comparativa entre as plataformas brasileira e da União Europeia, utilizando como parâmetro as principais características de cada uma. SCHMIDT-KESSEN M.J.; NOGUEIRA R.; CANTERO, G. – **Success or Failure? Effectiveness of Consumer ODR Platforms in Brazil and in the EU**. "Reimpressa de https://link.springer.com/article/10.1007/s10603-020-09448-y." aos 16/03/2021.

Vale notar, porém, a ausência de intermediários na consecução da RAL na plataforma brasileira, em contraposição à plataforma europeia, o que se justifica tendo em vista, como mencionado acima, o variado número de países atendidos pela Plataforma RLL. De toda forma, também podemos concluir que, apesar de destinadas a públicos diferentes, tanto a plataforma brasileira como a europeia parecem caminhar na mesma direção e velocidade, enfrentando idênticos obstáculos e, em ambas, parece-nos que a utilização integral e absoluta da ODR para solucionar as questões entre os interessados ainda não foi alcançado.

Entretanto, em 2020, realizou-se pesquisa com trinta e dois operadores de trinta países sobre a plataforma ideal para se utilizar a ODR. Do resultado da pesquisa, pode-se concluir que as plataformas RLL e a consumidor.gov.br aproximam-se bastante uma da outra.[171] Podemos concluir, também, que as respostas harmonizam-se com os princípios orientadores da ODR, já mencionados precedentemente neste trabalho.

Em conclusão, de um lado temos o uso ainda incipiente da ODR e das respectivas plataformas, com expectativa de crescimento de sua utilização, uma vez que os sistemas de ODR podem gerar altos níveis de satisfação dos interessados, devido, notadamente, à sua rapidez, ao baixo custo e à facilidade de acesso. De outro lado, não temos pesquisa e/ou informação segura sobre (1) os dados definitivos sobre a durabilidade dos resultados alcançados por meio da ODR; (2) a adequação das técnicas de ODR, ao se considerar as

[171] Uma das perguntas feitas foi: quais seriam as propriedades de uma plataforma ideal? Os pontos comuns nas respostas foram: (1) maior eficiência da tecnologia da informação; (2) fácil acesso, baixo custo, mas não sem custo (para evitar o uso e/ou o comércio de dados); (3) baseado na web (sem necessidade de instalar qualquer *software* adicional em qualquer computador ou smartphone); (4) uso seguro; (5) sem necessidade de licenças especiais ou *software*; (6) possuir vídeo de boa resolução que permita produzir documentos legais; e (7) possuir vínculo com centros de arbitragem e tribunais. MATTEUCCI, Giovanni. **ODR in 30 Countries**, 2020: Mediation in the COVID-19 Era. [sl]: [sn], [sd]. Disponível em https://mgimo.ru/library/publications/odr_in_30_countries_2020_mediation_in_the_covid_19_era/. [Consult. 17 mar. 2021].

necessidades emocionais e psicológicas dos envolvidos, por exemplo, a necessidade ou não do encontro físico entre as partes; (3) a qualidade de justiça oferecida pela ODR é equivalente àquela que é realizada presencialmente; e (4) as auditorias frequentes realizadas nos processos submetidos à ODR para garantir que o sistema está atuando de forma ética e conforme o pretendido, segundo Colin Rule[172]. De toda forma, podemos constatar que a ODR possui um poder transformador no sentido de reduzir a desigualdade entre as partes e proporcionar uma justiça mais equitativa, como prega John Rawls[173].

2.3.5 Impactos da Inteligência Artificial sobre a ODR

Embora a ODR não esteja totalmente assimilada conforme vimos acima, a Inteligência Artificial surge como uma inovação que necessita ainda mais adaptação tecnológica das instituições jurídicas e de seus integrantes nesse caminho tortuoso que é a utilização do aparato tecnológico no mundo do direito. A introdução das ferramentas da Inteligência Artificial promete grandes transformações na maneira de exercer as profissões ligadas ao direito, criando, inclusive, tribunais, juízes e advogados virtuais.[174]

Esse tema poderia ensejar um estudo ainda mais aprofundado, porém, não é o objeto deste trabalho. De outro lado, não poderíamos nos furtar a, pelo menos, citar esse viés da inovação tecnológica, uma vez que acreditamos que o emprego da tecnologia entre os operadores do direito e os sistemas de Justiça não obedece a um caminho retilíneo, crescente e único. Ao contrário, como já dissemos, a inovação tecnológica, nesse caso, sofre avanços e retrocessos e depende, ademais, de circunstâncias que fogem do campo jurídico, como a educação da população, do acesso aos meios informáticos, entre outros já citados, a fim de alcançar o universo dos potenciais usuários.

De toda forma, a utilização da Inteligência Artificial (IA) no meio jurídico parece já estar se tornando realidade. Podemos citar como exemplo em Portugal o projeto da Universidade do Minho, denominado UMCourt[175]. Trata-se de um projeto que visa o

---

[172] RULE, Colin – Online Dispute Resolution and the Future of Justice. **Annual Review of Law and Social Science**. V. 16, Out. 2020. Disponível em: https://doi.org/10.1146/annurev-lawsocsci-101518-043049. [Consult. 17 mar. 2021].

[173] RAWLS, John – Justiça como equidade. Uma reformulação. São Paulo: Martins Fontes, 2003. p.89-95.

[174] CARNEIRO, Davide; NOVAIS, Paulo; ANDRADE, Francisco; ZELEZNIKOW, John; NEVES, José – Online dispute resolution: an artificial intelligence perspective *In* **Artificial Intelligence Review**. V. 41, n.º 2, 2014. p. 211-240. Disponível em https://repositorium.sdum.uminho.pt/handle/1822/32005?locale=en. [Consult. 27 fev. 2021].

[175] CARNEIRO, Davide; NOVAIS, Paulo; ANDRADE, Francisco; ZELEZNIKOW, John; NEVES, José – Using BATNAs and WATNAs in Online Dispute Resolution. **New Frontiers in Artificial Intelligence**. V.

desenvolvimento de uma arquitetura multifacetada de ODR para ser utilizada em diferentes processos jurídicos. O principal objetivo é capacitar as partes no processo de resolução de disputas, fornecendo sentido e contextualizando informações, propondo soluções, estratégias e orientações por meio de mediação e algoritmos de negociação. O *software* foi projetado para dar suporte à ODR em um sistema de apoio à resolução de conflitos trabalhistas. Nesse contexto, os agentes de *software* são usados para calcular e fornecer às partes a melhor e a pior alternativa para um acordo negociado, facilitando, portanto, a concreção de um acordo.

No Brasil, podem-se citar dois exemplos emblemáticos. O primeiro, já implantado no Distrito Federal e iniciado em 2017, é o Projeto Dra. Luzia[176], nome escolhido em homenagem às mulheres e ao primeiro fóssil humano encontrado nas Américas. Trata-se de um robô que gera petições com uma velocidade que o ser humano não consegue alcançar, além de diminuir a quantidade de erros que poderiam ser cometidos. A outra experiência denomina-se Projeto Victor[177], capitaneado pelo Supremo Tribunal Federal (STF) em conjunto com a Universidade de Brasília (UnB). O nome do projeto é um tributo ao Ministro Victor Nunes Leal, principal responsável pela sistematização da jurisprudência do STF em súmula durante o período que atuou naquele Tribunal, nos anos de 1960 a 1969, e que facilitou a aplicação dos precedentes judiciais aos recursos. O Projeto Victor auxilia o STF na análise de admissibilidade dos recursos extraordinários recebidos por Tribunais de todo o país, identificando se algum(ns) tema(s) de repercussão geral aplica(m)-se ao caso dos autos.

6284, 2010, p. 5-18. Disponível em https://link.springer.com/chapter/10.1007/978-3-642-14888-0_2. [Consult. 27 fev. 2021].

[176] PORTAL DO GOVERNO DO DISTRITO FEDERAL. **Inteligência Artificial em Execução Fiscal.** Distrito Federal: [sn], [sd]. Disponível em https://www.pg.df.gov.br/inteligenciaartificial/. [Consult. 23 abr. 2021].

[177] SUPREMO TRIBUNAL FEDERAL. **Projeto Victor Avança em Pesquisa e Desenvolvimento para Identificação dos Temas de Repercussão Geral**. Brasília, DF: [sn], 2021. Disponível em https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=471331&ori=1.[Consult. 23 abr. 2021].

3. A IMPLICAÇÃO FUNDAMENTAL DOS INSTRUMENTOS REGULATÓRIOS DE PROTEÇÃO DE DADOS NO PROCESSO DA ONLINE DISPUTE RESOLUTION EM PORTUGAL E NO BRASIL

Os avanços na expansão do acesso à internet e a disseminação do uso de dispositivos móveis têm resultado em volume, frequência e tipos de dados disponíveis cada vez maiores na esfera digital. É imprescindível, portanto, que marcos regulatórios baseados em padrões internacionais sejam estabelecidos para guiar, minimizar e neutralizar os efeitos que a recolha, o armazenamento, o tratamento, a análise e a utilização de dados pessoais possam eventualmente causar no exercício dos direitos fundamentais dos indivíduos, com reflexos nos direitos humanos e na própria democracia.

A proteção de dados pode ser compreendida como um arcabouço jurídico constituído de medidas legais e regulamentares que visam impedir abusos no tratamento dos dados pessoais e, ao mesmo tempo, assegurar aos indivíduos o direito de tê-los sob controlo. É um instrumento que estabelece regras para a atuação dos atores públicos e privados na coleta e no tratamento de dados pessoais que, como visto anteriormente, envolve pelo menos seis fases.

A proteção de dados por meio de leis tem sido uma preocupação de quase todos os países. Em agosto de 2021, quase cento e quarenta países e territórios autônomos em todo o mundo já aprovaram leis de proteção ou sobre privacidade de dados pessoais coletados por órgãos públicos e privados, conforme pode ser verificado na figura que segue:

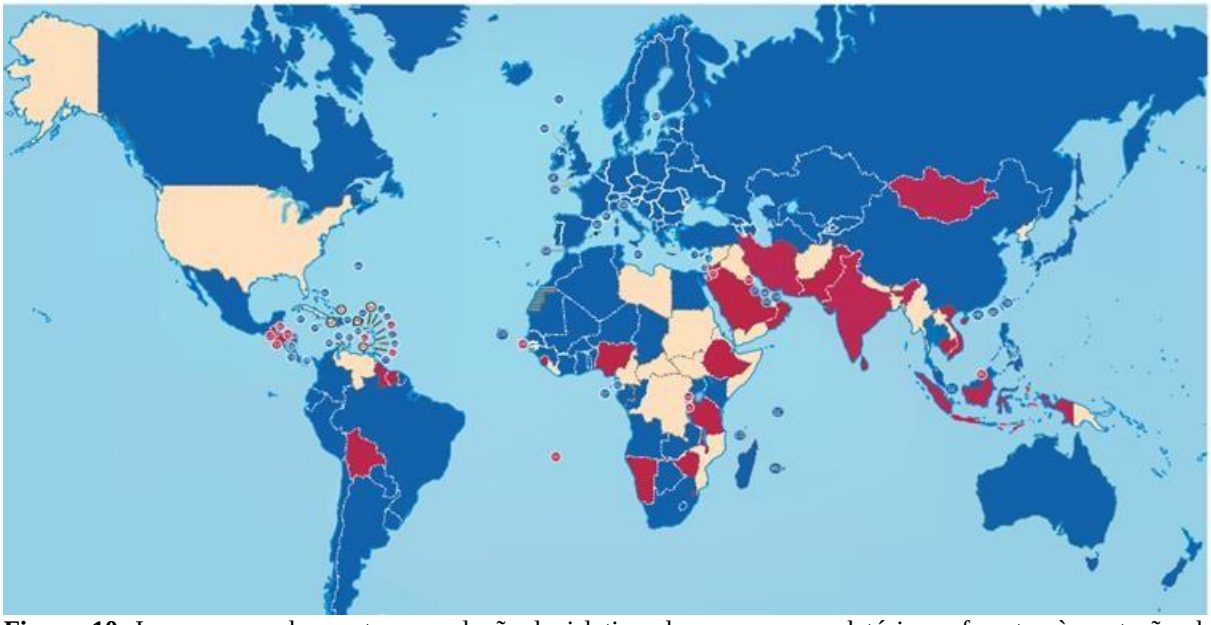

Figura 10. Imagem que demonstra a evolução legislativa dos marcos regulatórios referentes à proteção de dados no mundo. BANISAR, David – National Comprehensive Data Protection/Privacy Laws and Bills. [sl]:

[sn], 2023. “Reimpressa de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416” aos 31/09/2021.

As regiões que se encontram em azul, na imagem acima, detém uma Lei abrangente de proteção de dados já promulgada, em vermelho as regiões em que há projeto de lei ou iniciativa pendente para promulgar lei e na cor creme, as regiões em que não há lei/iniciativa atual ou nenhuma informação.

Regularizar o uso e o tratamento de dados pessoais é o mais importante objetivo das leis de proteção de dados. Estas têm em vista não apenas proteger a privacidade, mas também preservar outros direitos fundamentais e liberdades individuais, que somente podem ser exercidos em sua inteireza se houver a garantia do uso adequado (e protegido) dos dados pessoais dos indivíduos. Dessa forma, as leis de proteção de dados são como “guarda-chuvas”regulatórios que protegem outros direitos[178].

Como explanado no Capítulo I desta dissertação, a tendência global tem sido reconhecer o direito à proteção de dados pessoais como um direito fundamental que contribui para a realização de outros direitos humanos, como o da privacidade, o direito de não ser discriminado, o da liberdade de pensamento, o da liberdade e consciência, o da liberdade de expressão, o do acesso à informação, entre outros.

Nesse contexto, os estados se viram obrigados a estabelecer parâmetros legais com vistas a tornar eficaz a proteção de dados pessoais. Assim, a União Europeia estabeleceu para seus membros o Regulamento Geral de Proteção de Dados (RGPD) e, por sua vez, o Brasil aprovou a Lei Geral de Proteção de Dados (LGPD).

Essa legislação e outras correlatas[179], especificamente no caso da ODR, assumem distinta importância, uma vez que a circulação de dados pessoais, por vezes sigilosos, pode tornar o processo vulnerável com a intervenção de terceiros interessados em obter informações, as quais, se divulgadas, podem corromper e/ou desnaturar o aludido procedimento.

Para medir a influência de tais medidas no processo da ODR, tanto em Portugal como no Brasil, este capítulo propõe apreciar o RGPD e a LGPD, procurando verificar se os seus dois textos são realmente eficazes para a proteção da ODR em ambos os países.

---

[178] MONTEIRO, Renato L. – Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**. **Artigo Estratégico 39.** Dezembro de 2018, p. 1-27. Disponível em https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. [Consult. 18 maio 2022].
Este trabalho compara a LGPD e o RGPD no tocante à “existência do direito à explicação no contexto de decisões automatizadas. Conclui que a legislação nacional [brasileira], mais especificamente a lei de proteção de dados pessoais, foi além de outras regulações internacionais, como a RGPD, no que concerne a este assunto. Isso porque expandiu o escopo de exercício desse direito, quando comparada com a regulamentação europeia”.

[179] Tais como as respectivas leis de mediação em Portugal e no Brasil.

3.1 A PROTEÇÃO DE DADOS EM PORTUGAL

Como membro da UE, Portugal se sujeitou ao Regulamento Geral de Proteção de Dados (RGPD). O documento é resultado do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento e à livre circulação desses dados, transposta em Portugal pela Lei n.º 58/2019, de 8 de agosto (Lei da Proteção de Dados Pessoais), que garante a sua execução na ordem interna portuguesa.

3.1.1 O Regulamento Geral sobre a Proteção de Dados

Pode-se verificar, no Capítulo I[180], um breve histórico da implementação do Regulamento Geral de Proteção de Dados (RGPD), dispensando-se uma nova manifestação sobre este tema. Porém, merece destaque que a sua redação final resultou de intensas negociações, tanto no Parlamento Europeu como no Conselho da União Europeia, e, ao fim e ao cabo, chegou-se a um Regulamento que tem como finalidade a proteção dos direitos e das liberdades fundamentais das pessoas físicas e, em particular, o seu direito à proteção de dados pessoais.

O RGPD constitui, portanto, um instrumento legal para a proteção da privacidade e dos dados para toda a União Europeia (UE). Requer que os entes organizacionais estabeleçam proteções à privacidade, bem como acordos de proteção de dados e declarações mais detalhadas sobre as atividades relativas à privacidade dos dados com a finalidade de que sejam facilmente compreendidas pelos indivíduos.

O RGPD substituiu a antiga normativa sobre a matéria, denominada “Diretiva de Proteção de Dados” (Diretiva 95/46/CE). Essa Diretiva foi transposta para a legislação de cada um dos Estados-Membros, o que acarretou normas específicas em cada um deles e resultou em uma fragmentação legislativa à proteção de dados na UE.

O Regulamento, por outro lado, possui efeito jurídico direto em todos os Estados-Membros da UE, ou seja, para adquirir força vinculativa não necessita ser transposto para o direito nacional dos Estados-Membros da UE. Tal sistemática proporcionou coerência legislativa e consequente aplicação igualitária da proteção de dados dentro da União. Nesse sentido, o RGPD produziu novidades, entre eles: o fortalecimento dos direitos dos

[180] Item 3.2 Marcos regulatórios da legislação de proteção de dados.

indivíduos sobre seus dados; a obrigação de harmonização das normas sobre o tema e a obrigação das empresas a terem mais responsabilidade sobre a coleta de dados pessoais, com sanções mais duras para aquelas que não agirem em conformidade com as novas regras.[181]

Um dos objetivos do RGPD, portanto, é proporcionar tratamento uniforme à proteção de dados em todos os países integrantes da União Europeia. Não obstante, o RGPD permite que cada um de seus Estados-Membros adapte minimamente o texto às peculiaridades locais como a possibilidade de sancionar ou não com coimas as administrações públicas que cometam infrações nesta matéria.

Pode-se dizer, ao fim e ao cabo, que o RGPD representa uma mudança quanto à perspectiva da proteção de dados pessoais, uma vez que o Regulamento passa a considerar que as organizações, empresas e administrações públicas devem analisar os riscos e avaliar determinados comportamentos no âmbito dos direitos e das liberdades dos indivíduos, titulares de dados pessoais. Um exemplo dessa mudança está descrita no número 1 do art. 24º do RGPD. Em resumo, o Regulamento estabeleceu um quadro jurídico que contribui firmemente para gerar confiança necessária ao desenvolvimento da utilização do meio digital,seja sob o aspeto económico, jurídico, interpessoal etc., ou seja, colabora para diminuir riscos e elevar a segurança nas interações virtuais.

Nesse sentido, o RGPD exige que as organizações tratem os dados pessoais de maneira lícita, leal e transparente; recolham dados para fins específicos, explícitos e legítimos; coletem tão-somente os dados necessários à finalidade perquirida; adotem providências para assegurar sejam os dados precisos e atualizados, bem como utilizados apenas pelo tempo necessário; garantam a segurança dos dados e, ademais, sejam capazes de demonstrar conformidade com os princípios do RGPD. Em conclusão, o objetivo do RGPD[182]é dar aos usuários maior controlo sobre como seus dados pessoais são recolhidos, armazenados e usados, e ciência daqueles que os utiliza.

[181] IRAMINA, Aline – RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**. V. 12, n.º 2, Brasília: Universidade de Brasília, Outubro de 2020. p. 91-117. Disponível em https://periodicos.unb.br/index.php/RDET/article/view/34692. [Consult. 20 maio 2022].

[182] Essas diretrizes se coadunam com os princípios que regem o RGPD e a LGPD, objeto de estudo do Capítulo I deste trabalho.

3.1.2 O responsável pelo tratamento de dados e a Autoridade de Controlo

No que concerne à governança[183] e às políticas públicas a respeito da proteção de dados, o RGPD nomeia, de um lado, o "responsável pelo tratamento" (artigo 4º, número 7) e, de outro, determina o estabelecimento de uma "autoridade de controlo" (artigo 51º e seguintes). O responsável pelo tratamento de dados pode ser a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais, que tem por obrigação[184] a licitude do tratamento com o consentimento livre, específico, informado e explícito (artigo 6º, número 1); assegurar a privacidade dos dados (artigo 25º); definir políticas, procedimentos, códigos de conduta adequados (artigo 24º, número 2); contratar subcontratado adequado (artigo 28º); proceder ao registro das atividades de tratamento, quando aplicável (artigo 30º); cooperar com as autoridades de controlo (artigo 31º); assegurar o tratamento de dados com medidas técnicas que permitam a pseudonimização[185] (artigo 32º, número 1); avaliar o risco dispensado ao tratamento de dados (artigo 32º, número 2); notificar a violação de dados à Autoridade de Controlo (artigo 33º); proceder à avaliação de impacto de proteção de dados (artigo 35º); designar o encarregado da proteção de dados (artigo 37º); entre outras atribuições, que devem ser revistas e atualizadas consoante as necessidades.

As Autoridades de Controlo, por outro lado, são autoridades públicas independentes que monitoram, por meio de poderes de investigação, a adoção de medidas corretivas, a aplicação da legislação de proteção de dados, além de fornecer aconselhamento especializado em questões de proteção de dados e lidar com reclamações apresentadas sobre violações do Regulamento Geral de Proteção de Dados e das leis nacionais relevantes, segundo seu artigo 51º. Cada Estado-Membro da UE possui uma ou mais autoridade de controlo em seu território (artigo 51º, número 3).

O RGPD ainda assegura à autoridade de controlo sua independência no desempenho de suas atividades (artigo 51º, números 1 e 2), além de estabelecer

---

[183] Governança: forma de governar baseada no equilíbrio entre o Estado, a sociedade civil e o mercado, a nível local, nacional e internacional.

[184] PORTAL DO DPO. **Responsabilidades do Responsável pelo Tratamento**. [sl]: [sn], [sd]. Disponível em https://www.portaldodpo.pt/blog/service/responsavel-pelo-tratamento/. [Consult. 30 jul. 2021].

[185] RGPD – "Artigo 4º. 5) «Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;"

autonomia financeira e de pessoal (art. 51º, números 4, 5 e 6). De fundamental importância a previsão estabelecida no RGPD no sentido de que as nomeações dos membros da Autoridade de Controlo sejam realizadas mediante procedimento transparente pelo Parlamento, pelo Governo, pelo Chefe de Estado, ou, ainda, por um organismo independente incumbido desse mister (artigo 53º, número 1) e demais regras correlatas (artigo 54º), pois, não houvesse a garantia de nomeações transparentes, muito dificilmente haveria a possibilidade de a Autoridade de Controlo exercer suas atividades com independência e autonomia.

Em continuação, o RGPD ainda determina à Autoridade de Controlo sua competência, atribuições e poderes (artigos 55º; 56º; 57º; 58º), bem como a elaboração de relatório anual de atividades, com a enumeração dos tipos de violação notificadas e as providências adotadas (artigo 59º). Vale destacar, ainda, uma medida importante para a adequada aplicação do RGPD nos Estados-Membros da UE, uma vez que os artigos 60º, 61º e 62º do RGPD estabelecem cooperação, assistência mútua e operações conjuntas de controlo entre as diversas Autoridades de Controlo para que, ao fim e ao cabo, seja alcançada a necessária coerência na aplicação do RGPD (artigo 63º). Há, ainda, a previsão do Comité Europeu para a Proteção de Dados (CEPD) composto pelo diretor da Autoridade de Controlo de cada Estado-Membro e da autoridade europeia para a proteção de dados (artigo 68º, número 3), de onde se pode inferir que a legislação prevê mecanismos e organismos que visam a aplicação de suas normas de maneira igualitária e coerente em toda a União. Quanto ao CEPD, vale destacar que se trata de um organismo que expede orientações, recomendações e melhores práticas no intuito de esclarecer as disposições do RGPD, de forma a promover o seu entendimento comum entre os Estados-Membros da UE. Nesse sentido, o CEPD publica decisões vinculativas para a correta aplicação da RGPD nos termos do artigo 65º do RGPD e, quando instada pelas autoridades, de controlo nacional.[186] A Comissão Nacional de Proteção de Dados (CNPD) é a Autoridade de Controlo estabelecida em Portugal.

[186] Nesse sentido, citamos, por exemplo, a Decisão Vinculativa 1/2021 sobre o litígio decorrente do projeto de decisão da autoridade de controlo irlandesa relativo ao WhatsApp Ireland, no tocante ao cumprimento ou à ausência de cumprimento dos artigos 12º, 13º e 14º do RGPD e que envolveu as autoridades de controlo interessadas alemã, francesa, húngara, italiana, holandesa, polaca e portuguesa. EUROPEAN DATA PROTECTION BOARD. **Decisão Vinculativa do Comité (art. 65)**. Bruxelas: [sn], 2021. Disponível em https://edpb.europa.eu/system/files/2022-03/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_pt.pdf. [Consult. 11 jul. 2022].

3.1.3 A Comissão Nacional de Proteção de Dados e as Leis n.º 21/2019, n.º 58/2019 e n.º 59/2019

O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados – RGPD) entrou em vigor em 24 de maio de 2016 e tem aplicação desde 25 de maio de 2018, criando um conjunto coerente e bem ordenado de regras aplicáveis ao tratamento de dados pessoais dentro da União Europeia (UE). A Lei n.º 58/2019, de 8 de agosto, assegura a execução ao RGPD em território português. Como vimos, o RGDP teve como objetivo aumentar a proteção aos dados pessoais em qualquer localidade da UE.

Não obstante, para algumas matérias relativas à repressão penal, foram editados mais dois instrumentos jurídicos relacionados à proteção de dados pessoais: (1) a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção dos dados pessoais das pessoas singulares, efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção, repressão de infrações penais e execução de sanções penais, transposta para a ordem jurídica portuguesa pela Lei n.º 59/2019, de 8 de agosto; (2) a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registros de identificação dos passageiros (em inglês, Passenger Name Record – PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave e sobre a proteção de dados pessoais, transposta para o ordenamento jurídico português pela Lei n.º 21/2019, de 25 de fevereiro.

Quando se trata de procedimentos relativos à prevenção, investigação, deteção, repressão de infrações penais e execução de sanções penais, é aplicável o disposto na Diretiva 2016/680 e na Lei n.º 59/2019, que constituem a lei aplicável em matéria penal e da cooperação policial. A Comissão Nacional de Proteção de Dados (CNPD) é a Autoridade de Controlo responsável pela fiscalização do cumprimento da Lei n.º 59/2019, bem como da Lei n.º 58/2019 e da Lei n.º 21/2019. A designação da mesma Autoridade de Controlo para interpretar, aplicar e fiscalizar esses diplomas legislativos favorece a interpretação homogénea e coerente das leis relativas à proteção de dados pessoais em Portugal.

3.1.4 Aplicação do Regulamento Geral sobre a Proteção de Dados em Portugal

Abaixo relatamos dois acontecimentos referentes ao emprego do RGPD a fim de exemplificar sua aplicação em Portugal. O primeiro deles diz respeito à aplicação da Lei n.º 58/2019 e o seguinte sobre a fiscalização exercida, ambas as ações protagonizadas pela Comissão Nacional de Proteção de Dados (CNPD). Nesse sentido, embora a Lei n.º 58/2019 reproduza em quase a sua totalidade os artigos do RGPD, algumas de suas normas foram desaplicadas pela CNPD. Entre elas, podemos destacar as seguintes situações[187]: 1- o entendimento de que, ao considerar a existência de uma restrição legal infundada ao exercício dos direitos de informação e de acesso a dados por parte dos titulares dos dados, não se pode aplicar o artigo 20º, número 1; 2- também não se aplica o artigo 28.º, número 3, alínea "a", uma vez que essa norma desconsidera o consentimento do trabalhador sobre seus dados pessoais; 3- por contrariarem o rol taxativo das infrações previstas no RGPD e o respetivo enquadramento sancionatório, não se aplicam o artigo 37º, número 1 alíneas "a", "h" e "k" e o artigo 38º, número 1 alínea "b" e, ainda, 4- não se emprega o artigo 37º, número 2, e o artigo 38º, número 2, por estabelecerem critérios sobre a adoção de medidas sancionatórias não definidas no RGPD.

Na decisão constante na Deliberação n.º 2019/494[188], podemos verificar que se considerou "a adoção nacional de normas jurídicas em contradição com o estatuído no RGPD não só viola o princípio do primado do direito da União (Acórdão TJUE, Simmenthal, Proc. 106/77, § 21), como prejudica seriamente o funcionamento adequado do mecanismo de coerência, colocando a respetiva autoridade nacional em risco de violar uma das normas em antinomia". Inicialmente, pode-se inferir desse contexto que a não aplicação das normas constantes na Lei n.º 58/2019 acarreta necessariamente a adoção das regras constantes no RGPD. Em segundo lugar, pode-se concluir pelo surgimento de insegurança jurídica relativa às situações albergadas pelos artigos que foram desaplicados pela CNPD.

Em razão de a CNPD fixar o entendimento de que determinadas normas da Lei n.º 58/2019 são manifestamente incompatíveis com o direito da União[189], cinco parlamentares europeus portugueses solicitaram um pedido de resposta do Parlamento

---

[187] MOTA, Joana; SAMPAIO, Alexandre P. – Regulamento Geral de Proteção de Dados em Portugal – Alguns apontamentos à sua lei de execução. **Actualidad Jurídica Uría Menéndez**. V. 53, 2019, p. 142-148. Disponível em https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341. [Consult. 30 jun. 2021].

[188] COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **Deliberação/2019/494**. Lisboa: [sn], 2019.Disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2019&type=2&ent=. [Consult. 30 jun. 2021

[189] *Ibidem*

Europeu[190] sobre a aplicação plena e a efetiva vigência do RGPD em Portugal, podendo-se deduzir pelo grau de incerteza jurídica que causou tal decisão, embora, no meu entendimento, seja a decisão correta e de acordo com as leis portuguesas. O Parlamentou Europeu ainda não se manifestou. Outro caso ocorreu no primeiro semestre de 2021, quando a CNPD de Portugal, investigou e acusou o Município de Lisboa[191] de violar em cento e onze vezes o RGPD, ao comunicar os dados pessoais dos promotores de manifestações públicas ocorridas naquele município às entidades terceiras, sendo que a lei não permite a transmissão de dados pessoais, disponibilizando apenas a comunicação da informação relativa ao objeto, à data, hora, local e trajeto da manifestação.

As infrações caracterizaram a falta de licitude e a violação do princípio da necessidade, pois sendo dados especialmente sensíveis, devido ao fato de revelarem opiniões e convicções políticas, filosóficas ou religiosas, de forma que o "Município de Lisboa procedeu a um conjunto de operações sobre informação relativa a pessoas singulares, no exercício de uma atividade pública específica, da qual resulta necessariamente impacto na privacidade e na liberdade daquelas e tinha obrigação de conhecer o enquadramento legal em que poderia de facto realizar esse conjunto de operações e de conformar os procedimentos e atuações face às regras e princípios do RGPD"[192].

A CNPD considerou que o envio dos dados pessoais dos promotores às representações diplomáticas e a outras entidades estrangeiras violaram o direito fundamental à proteção de dados, o que coloca em perigo outros direitos fundamentais consagrados na Constituição portuguesa. Além do exposto, a CNPD concluiu ainda existirem outras infrações ao RGPD, notadamente, a de não informar aos promotores sobre o tratamento dos seus dados pessoais.[193] A extensa enunciação dos artigos do

[190] PEREIRA, Lídia; FERNANDES, José M.; RANGEL, Paulo; AGUIAR, Cláudia M.; AMARO, Álvaro. **Desaplicação de Normas da Lei Nacional que Adapta o RGPD em Portugal**. [sl]: [sn], 2019. Disponível em https://www.europarl.europa.eu/doceo/document/E-9-2019-003014_PT.html#:~:text=Na%20delibera%C3%A7%C3%A3o(3)%20em%20que,encarregue%20da%20aplica%C3%A7%C3%A3o%20do%20Regulamento. [Consult. 30 jun. 2022].

[191] COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **CNPD acusou município de Lisboa**. Lisboa: [sn], 2021. Disponível em https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-acusou-municipio-de-lisboa/. [Consult. 20 set. 2021].

[192] Item 140 da Deliberação 2021/1569. COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **Deliberação/2019/494**. Lisboa: [sn], 2019. Disponível em https://www.cnpd.pt/decisoes/deliberacoes/. [Consult. 30 jun. 2022].

[193] Conforme alínea 'h' da Deliberação 2021/1569. COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **Deliberação/2021/1569**. Lisboa: [sn], 2021. Disponível em https://www.uc.pt/site/assets/files/475840/20211221_deliberacao_1569_cnpd_multa_munic_lisboa.pdf. [Consult. 30 jun. 2022].

RGPD que foram violados, bem como a coima atribuída ao Município de Lisboa, encontra-se na Deliberação n.º 2021/1529.

3.2 A PROTEÇÃO DE DADOS NO BRASIL

Inspirada na lei europeia de proteção de dados, conhecida como Regulamento Geral de Proteção de Dados (RGPD), a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n.º 13.709, de 14 de agosto de 2018) tem como objetivo proteger dados pessoais das pessoas físicas, assim como os dados armazenados pelas pessoas jurídicas (ou pessoas coletivas, como é denominado em Portugal) pertencentes às pessoas físicas, sejam elas funcionários, terceirizados[194], clientes, acionistas etc., "com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[195]. Necessário observar que a proteção aos direitos fundamentais de liberdade e de privacidade foi destacada pela LGPD, mediante o tratamento de dados pessoais das pessoas naturais, visando o desembaraço do desenvolvimento da personalidade da pessoa física. A Lei n.º 13.709, de 2018, é composta por sessenta e cinco artigos e foi alterada pela Medida Provisória n.º 869, de 2018, convertida posteriormente na Lei n.º 13.853, de 8 de julho de 2019.

3.2.1 A Lei Geral de Proteção de Dados Pessoais

Anteriormente à promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), a legislação brasileira estabelecia como preceito geral a obrigatoriedade de se obter o consentimento do titular para o acesso ou a divulgação de seus dados pessoais. Previa-se a dispensa em hipóteses limitadas, como o cumprimento de ordem judicial. Contudo, devido ao crescimento dos cibercrimes, foi promulgada a Lei n.º 12.373, de 30 de novembro de 2012, que alterou o Código Penal brasileiro (CP) e inseriu, no que importa para este estudo, três artigos que tornam crimes a invasão de dispositivo informático alheio, bem como a interrupção ou perturbação de serviço telegráfico,

[194] Terceirizado é um vocábulo utilizado no Brasil; diz-se do trabalhador que presta serviços a uma, ou mais empresas, com a qual não possui vínculo de trabalho permanente. Disponível in Porto Editora – terceirizado no Dicionário infopédia da Língua Portuguesa. Porto: Porto Editora. Disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/terceirizado. [Consult. 25 maio 2022].

[195] "Artigo 1º – Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.".

telefônico, informático, telemático ou de informação de utilidade pública (artigos 154-A, 154-B e 266 do CP).

O crime de invasão de dispositivo informático depende, para prosseguimento, de representação do ofendido, salvo se o crime for cometido contra a administração pública.[196] Com a finalidade de aperfeiçoar ainda mais a defesa da privacidade dos dados pessoais, foi promulgada a Lei n.º 12.965, de 23 de abril de 2014, conhecida como "Marco Civil da Internet", que estabeleceu princípios e garantias para o uso da internet no Brasil, além de direitos e deveres oriundos nas relações que ocorrem no ciberespaço.[197]

As providências e o alcance das medidas incluídas no Marco Civil da Internet não foram suficientes, contudo, para estancar a violação de dados. O Governo brasileiro, em vista desse quadro, optou por criar legislação específica sobre a proteção de dados pessoais, inspirando-se nas diretrizes europeias sobre esse tema. Nesse contexto, foi publicada a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709, de 14 de agosto de 2018, que disciplinou de forma específica a proteção de dados pessoais, além de alterar o Marco Civil da Internet.

Um dos objetivos da LGPD é, além da evidente regularização do uso dos dados pessoais, gerar uma cultura de respeito a esse direito fundamental ao assegurar um ambiente de proteção e segurança jurídica com a padronização de normas internacionalmente reconhecidas. Podemos tomar como exemplo as normas que preveem o uso indevido de dados, isto é, quando os dados pessoais coletados são utilizados com uma finalidade diferente daquela originalmente informada ao proprietário dos dados na época da recolha, ou seja, quando houve o seu consentimento. Assim, quando ocorre a divergência entre o consentimento e a efetiva utilização dos dados, o responsável sujeita-se à penalização, tanto segundo as normas da LGPD[198] como do RGPD[199].

A LGPD estabelece, ainda, parâmetros sobre como esses dados devem ser coletados, armazenados, processados e até destruídos. Além disso, proíbe qualquer organização de transmiti-los sem consentimento expresso dos titulares, tornando ilegal ceder ou vender informações de contato de potenciais clientes para a divulgação de produtos e/ou serviços. Os dados pessoais, portanto, devem ser tratados de forma legítima,

[196] CÓDIGO PENAL – "Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.".
[197] Notadamente, os artigos 2º-; 3º e 4º da Lei n.º 12.965, de 2014.
[198] LGPD – Artigo 7º, I; artigo 8º, § § 1º a 6º; combinada com o art. 52 e seus incisos.
[199] RGPD – Artigo 6º e artigo 7º, números 1 a 4; combinada com o art. 37º e suas alíneas, da Lei nº 58/2019

adequada e proporcional.

3.2.2 O responsáveis pelo tratamento de dados na Lei Geral de Proteção de Dados Pessoais

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por três agentes de tratamento, quais sejam: o controlador, o operador e o encarregado. A LGPD define controlador como a pessoa natural (ou pessoa singular, em Portugal) ou jurídica (ou pessoa coletiva, em Portugal), de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais (artigo 5º, VI). Por sua vez, o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador – aí incluídos agentes públicos, no sentido amplo que exerçam tal função –, bem como pessoas jurídicas diversas daquelas representadas pelo controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere (artigo 5º, VII).

Podemos distinguir, portanto, a diferença de atribuições entre o controlador e o operador, uma vez que àquele caberá a decisão, isto é, a orientação sobre o tratamento a ser dispensado aos dados recolhidos, ao passo que ao operador competirá aplicar e efetivar as decisões tomadas pelo controlador no que concerne ao ciclo de vida dos dados pessoais, ou seja, no tocante às cinco fases do ciclo de vida do tratamento dos dados pessoais.[200] Interessante notar que tanto o controlador como o operador podem ser pessoas coletivas, inclusive de naturezas jurídicas diferentes, ou seja, pode ser um de direito público e outro privado, por exemplo e, ainda, o mesmo operador poderá contratar outra pessoa coletiva (ou física) para tratar diferentes etapas do ciclo de vida do tratamento de dados, se essa possibilidade for autorizada pelo controlador, como mencionado, uma vez que a orientação sobre o tratamento de dados é definida pelo controlador, bem como em obediência ao artigo 39 da Lei.

Nessa última possibilidade, o operador poderá ter uma empresa que lhe preste os serviços de recolha, retenção e tratamento de dados e outra pessoa coletiva que cuide do compartilhamento e da eliminação dos dados arquivados. Importa ressaltar que a Lei define, em grau de igualdade, como agentes de tratamento, tanto o controlador como o operador (artigo 5º, inciso IX). De toda forma, ambos devem, ainda, manter o registro das

[200] Item 2.3.3 do Capítulo I.

operações de tratamento de dados pessoais que realizarem (artigo 37).

O controlador e o operador responderão por danos morais, patrimoniais, individuais ou coletivos, na hipótese de desobediência à legislação vigente (artigo 42 da LGPD). A responsabilidade solidária é atribuída ao controlador pelos danos causados pelo operador, se este estiver envolvido diretamente no tratamento que deu origem ao dano[201], e o operador também responderá pelo dano se descumprir a legislação e se não tiver observado as orientações do controlador (artigo 42, § 1º, I e II, LGPD).

Por fim, o encarregado é a pessoa que deverá atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)[202]. Nesse caso, o encarregado equipara-se à figura do DPO do RGPD. A Figura a seguir, demonstra resumidamente as características de cada um dos responsáveis pelo tratamento de dados previstos na LGPD:

Figura 11. Imagem que demonstra o Comparação entre controlador, operador e encarregado. (previstos no artigo 5º, incisos VI, VII e VII, da Lei n.º 13.709, de 2018). KAUER, Gisele – Controlador, Operador e Encarregado: Quem é Quem na LGPD. São Paulo: [sn], [sd]. "Reimpressa de https://www.infranewstelecom.com.br/controlador-operador-encarregado-quem-e-quem-na-lgpd/" aos 08/09/2021.

[201] Daí resulta a necessidade de se manter os registros das operações de tratamento, bem assim conhecer detalhadamente os ciclos de vida do tratamento de dados e os respectivos contratos, com outras pessoas, natural ou coletiva, se for o caso. Nota-se que a fragmentação das atividades de tratamento, neste caso, poderá causar confusão quando da atribuição da responsabilidade pela violação de dados não autorizados.

[202] Segundo o artigo 5º, inciso VIII, da LGPD, alterada pela Lei n.º 13.853, de 2019, o encarregado é a pessoa indicada pelo controlador e o operador. Não obstante, o *caput* do artigo 41, da LGPD, em sua redação original e sem qualquer mudança até o momento, determina que somente cabe ao controlador a indicação do encarregado,

3.2.3 Autoridade Nacional de Proteção de Dados Pessoais

A ANPD é um órgão da administração pública federal, integrante da Presidência da República, nos termos do artigo 55-A da Lei n.º 13.709, de 2018[203], com autonomia técnica e decisória (artigo 55-B, Lei n.º 13.709, de 2018), com jurisdição em todo o território brasileiro, responsável por elaborar as diretrizes que regulamentam o tratamento de dados pessoais, bem como por examinar a correta aplicação da LGPD. A criação de uma autoridade independente tem se mostrado eficiente e necessária para o cumprimento da legislação respectiva e facilita a fiscalização nas hipóteses de não observação do adequado tratamento de dados.

Além dessas atribuições, a ANPD também tem a função de informar e fazer com que a população tenha conhecimento das políticas de proteção aos dados, das práticas e dos direitos sobre os dados, assim como estimular o entendimento das normas pelas pessoas coletivas que fazem uso dos dados e informações pessoais. As competências da ANPD estão descritas no artigo 2º do Anexo I do Decreto n.º 10.474, de 26 de agosto de 2020.

A ANPD é constituída pelo Conselho Diretor, órgão máximo da entidade, com mandato de quatro anos, prorrogável uma única vez por igual período[204], além de um órgão consultivo, denominado Conselho Nacional de Proteção de Dados Pessoais e da Privacidade[205], e pelos órgãos de assistência direta e imediata ao Conselho Diretor, órgãos seccionais e órgãos específicos singulares, todos eles enumerados no artigo 3º do Anexo I do Decreto n.º 10.474, de 2020. Vale ressaltar que o Conselho Diretor é o órgão máximo de decisão da ANPD, bem como que ao seu Diretor-Presidente cabe a gestão e a representação institucional da ANPD (conforme § §1º e 2º do citado artigo 3º).

3.2.4 Aplicação da Lei Geral de Proteção de Dados Pessoais no Brasil

A pandemia provocada pelo vírus SARS-COV-2 causou mudanças no comportamento social de todos os países. Uma dessas mudanças foi o incremento do uso da internet para resolver situações que antes eram tratadas presencialmente, o que inclui

[203] Alterada pela Lei n.º 13.853, de 8 de julho de 2019.
[204] Artigos 3º e 6º, ambos do Decreto n.º 10.474, de 2020.
[205] A competência e a representação estão descritas nos artigos 14 e 15 do Anexo I do Decreto n.º 10.474, de 2020.

desde o acesso à Justiça até o comércio virtual. Questões várias surgiram entre consumidores, administração pública e prestadores de serviços, abrangendo o tratamento de dados e a eventual possibilidade de uso indevido de dados pessoais, muitas vezes sensíveis. Para resolver essas situações, fez-se necessário a aplicação de regras bem-estabelecidas[206], o que torna ainda mais relevante as normas da RGPD na União Europeia e LGPD no Brasil.

A entrada em vigor da LGPD, em setembro de 2020, deixou muitas empresas altamente suscetíveis ao impacto das novas diretrizes a serem seguidas. A expectativa era de que as relações comerciais e de consumo fossem muito afetadas, uma vez que surgiu o entendimento de que o tratamento de dados pessoais dos usuários fosse efetuado com o intuito de traçar o perfil dos consumidores.

Uma dificuldade comum encontrada à época diz respeito às organizações que já possuíam uma base de dados consolidada, porém, muitas vezes sem procedência identificada e, portanto, necessitariam obter um novo consentimento dos usuários para o uso daqueles dados. Tudo isso criou um cenário confuso para que as pessoas jurídicas se adaptassem às práticas e ao cumprimento da Lei. Foi realizada pesquisa sobre a adaptação das empresas coletivas à LGPD, cujos gráficos com os resultados obtidos encontram-se no Anexo I. Dessas conclusões, podemos destacar a dificuldade de as pessoas coletivas observarem as regras da LGPD, porém, sem perder a capacidade de iniciar novos negócios digitais. Por fim, percebe-se que a fiscalização e a eventual punição às pessoas jurídicas que descumpriam a LGPD naquela época também não estavam sendo observadas por parte dos agentes fiscalizadores, evidenciando a ausência de respeito e eficiência dessa normativa.

3.2.5 Comparação entre o Regulamento Geral sobre a Proteção de Dados e a Lei Geral de Proteção de Dados Pessoais

O RGPD claramente suscitou ideias, mecanismos e normas que acabaram incluídas na LGPD. Essa relação de semelhança já foi mencionada de maneira espaçada neste texto. Ainda assim, cabem algumas observações quando comparamos o RGPD e a LGPD, embora essa análise não tenha o condão de ser definitiva nem absolutamente completa, dados os numerosos artigos que compõem ambas as Leis. De toda forma,

[206] Os principais marcos regulatórios do LGPD já foram contemplados no item 3.2 do Capítulo I – Marcos da legislação da proteção de dados.

alguns aspetos que julgamos mais relevantes serão relacionados a seguir.

Inicialmente, cabe registrar que o objeto e os objetivos traçados pelo RGDP e pela LGDP são em grande parte coincidentes, uma vez que tanto em um como em outro o objeto do conjunto normativo é regulamentar a proteção de dados e a sua consequente circulação, com o objetivo de proteger o direito fundamental de liberdade das pessoas singulares, nomeadamente o direito à proteção dos dados pessoais, no caso do RGPD[207], e de privacidade e o livre desenvolvimento da personalidade da pessoa natural no caso da LGPD[208]. Quanto à definição de dados pessoais, os conceitos também são praticamente idênticos[209], sendo que ambas as leis entendem que tal conceito abrange informações de qualquer pessoa natural identificável, e a lei brasileira acrescenta também a pessoa física identificada, ou seja, daquelaque já possui sua identidade reconhecida.

No tocante ao âmbito de aplicação territorial dessas normativas, o RGPD, em seu artigo 3º, protege os dados pertencentes a cidadãos e residentes na União Europeia. Portanto, abrange também as organizações e entidades que tratam desses dados, sejam ou não organizações sediadas em território europeu. A LGPD[210] possui norma idêntica a ser aplicada a qualquer empresa ou organização que processe dados pessoais de pessoas físicas, brasileiros ou não, cujos dados tenham sido coletados ou estejam sendo processados em território brasileiro, sem levar em conta o local onde essa empresa ou organização mantém sua sede.

Os direitos do titular dos dados pessoais estão descritos no Capítulo III do RGPD, sendo possível mencionar o direito de ser informado; o direito de acesso; o direito à retificação; o direito de ser esquecido (ou direito ao apagamento dos dados); o direito de restringir o processamento; o direito à portabilidade de dados; o direito de se opor ao processamento e, finalmente, o direito em relação à tomada de decisão automatizada e a definição de perfis. Muito embora na LGPD, em seu artigo 18, sejam enumerados nove direitos dos titulares, uma breve leitura daqueles descritos no artigo 12º ao 20º do RGPD, pode-se concluir pela semelhança desses direitos.

O artigo 6º, número 1, alíneas "a" a "f" do RGPD[211], lista seis hipóteses jurídicas

---

[207] RGPD – Artigo 1º, números 1 a 3.
[208] LGPD – Artigo 1º.
[209] V. RGPD – Artigo 4º, número 1; LGPD artigo 5º, I.
[210] LGPD – Artigo 3º.
[211] "Artigo 6º – Licitude do tratamento 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento

para a realização de processamento de dados pessoais. A LGPD, por sua vez, em seu artigo 18, acresceu aos seis fundamentos do RGPD mais quatro hipóteses para realizar o tratamento de dados, quais sejam: (i) quando necessário aos estudos de órgão de pesquisa; (ii) no exercício de direitos em processos judiciais, arbitrais ou administrativos; (iii) a fim de proteger a saúde do titular (nesse caso, procedimento realizado tão-somente pelos profissionais de saúde; serviços de saúde ou autoridade sanitária) e, por fim, (iv) visando a proteção ao crédito.

No tocante à fiscalização empreendida pela autoridade de controlo, o RGPD estabelece seja realizado um relatório de violação de dados dentro de setenta e duas horas após o conhecimento do fato (artigo 33º, número 1). De seu lado, a LGPD não define um prazo conclusivo e determina seja realizada a comunicação da ocorrência de incidente de segurança em prazo razoável, a ser determinado pela ANPD, além de enumerar as informações que deverão fazer parte tal comunicação (artigo 48, § 1º).

Um aspeto importante da fiscalização – que tem como objetivos confiar eficácia à legislação sobre a proteção de dados e, simultaneamente, coibir novos incumprimentos legais - diz respeito à aplicação de coimas (ou multas[212] no Brasil). Tanto o RGPD como a LGPD preveem a incidência de coimas quando há a transgressão de suas regras. O RGPD foi mais seletivo e específico na aplicação dessas penas estabelecendo dois patamares para a sua aplicação, conforme a violação cometida, nos termos do artigo 83º, notadamente no número 4, onde se prevê o valor de até dez milhões de euros (10 000 000 EUR) para pessoas naturais ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, e no número 5 do mesmo artigo, cujos valores são dobrados, conforme a violação ali descrita.

Já a LGPD previu uma série de restrições administrativas e deu liberdade para a ANPD aplicar as multas pecuniárias, uma vez que o valor inicia em até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a cinquenta milhões de reais (R$ 50.000.000,00) por infração, nos termos do artigo 52 e seus incisos. Pode-se

esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança."

[212] Em Portugal também é aceita a expressão "multa"; porém, é menos usual. Porto Editora – *coima* no Dicionário infopédia da Língua Portuguesa. Porto: Porto Editora. Disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/coima. [Consult. 26 maio 2022].

inferir, entretanto, que ambas as legislações trataram de impor coimas altíssimas, a fim de que suas regras fossem respeitadas. As diferenças quanto às autoridades de controlo já foram expostas anteriormente neste capítulo. Ao fim e ao cabo, pode-se perceber, portanto, a quase similitude das legislações em Portugal e no Brasil sobre a proteção de dados pessoais.

3.3 O IMPACTO DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS E DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO PROCESSO DE ONLINE DISPUTE RESOLUTION

Na utilização dos métodos da ODR, conforme vimos no Capítulo II deste trabalho, devem ser observados o tipo de conflito, a melhor estratégia e outras variantes que sejam específicas com cada caso concreto, tais como custos, tempo despendido e análise económica do direito, ou seja, faz-se necessário analisar a denominada arquitetura de confiança[213], isto é, o adequado e seguro embasamento jurídico para o caso concreto específico, bem assim, no caso da administração pública, a adoção da respectiva autonomia regulada da administração, o que torna o processo de escolha da ODR bastante complexo, seja para as pessoas físicas ou jurídicas, seja para as pessoas de direito público. Há de se observar, ainda, a imprescindível necessidade do sigilo, pois durante a execução da ODR circula pela rede todos os tipos de dados, inclusive os pessoais, muitas vezes de caráter sensível e que o titular não deseja sejam expostos a terceiros. Portanto, devido a esse cenário, o processo de ODR deve ser submetido às restrições impostas tanto pela RGPD, em Portugal, quanto pela LGPD, no Brasil, além de outras leis, decretos e portarias que regulam a matéria.

Entre os diversos aspetos a serem considerados na apreciação dos sistemas de ODR, destacam-se por sua importância a privacidade, a confiabilidade e a segurança do processo[214], itens imprescindíveis, no nosso sentir, para o abrigo do direito fundamental à proteção de dados. Portanto, essa dissertação, cingir-se-á a analisar o impacto do RGPD e da LGPD sob esses três aspetos.

---

[213] Item 2.2 do Capítulo II.

[214] BRAGA NETO, Adolfo; CARDOSO, Christiana B.; ANDREOTTI, Cristina M.; BORGES, Fernanda T. T.; FERREIRA, Silmara Z. A.; PEDROTI, Silvia R. G. – Resolução de disputas on-line (ODR), mediação e a advocacia. **OAB-SP**. [sd], p. 1-24. Disponível em https://www.oabsp.org.br/comissoes2010/mediacao-conciliacao/artigos/RESOLUC2560oA2560aO%20DE%20DISPUTAS%20ON-LINE%20-ODR-%20MEDIAC2560oA2560aO%20E%20A%20ADVOCACIA.pdf. [Consult. 03 ago. 2021].

3.3.1 Conceitos fundamentais: segurança, privacidade e confidencialidade

Certos conceitos devem ser estabelecidos antes de entrar no cerne do capítulo. Neste capítulo[215], faz-se necessário distinguir a segurança, a privacidade e a confidencialidade. Essas três definições possuem muitos pontos convergentes, mas se diferenciam quando aplicados a um sistema online. A segurança diz respeito à proteção dos dados, enquanto a privacidade à proteção da identidade do usuário. Eventualmente, haverá áreas de sobreposição entre as duas. O importante, porém, é saber que a segurança se refere à proteção contra o acesso não autorizado aos dados, a fim de proteger a privacidade do titular dos dados. Isto é, implementam-se controlos de segurança para limitar quem pode acessar informações pessoais.

A privacidade, por seu lado, é o direito de o indivíduo manter seus dados pessoais com acesso restrito, ou seja, o direito de o titular não tornar público seus dados pessoais, de não querer que seus dados sejam divulgados e impossibilitar que sejam expostos na internet ou vendidos para terceiros. A privacidade pode ser dividida em duas categorias[216]: trata-se da privacidade desde a conceção (*Privacy by Design*), que significa considerar o risco de privacidade desde o início do processo de conceção de um novo produto ou serviço, em vez de considerar as questões de privacidade apenas posteriormente; e a privacidade padrão ou por defeito (*Privacy by Default*), ou seja, assegurar-se que são colocados em prática, dentro de uma organização, mecanismos para garantir que apenas será recolhida, utilizada e conservada para cada tarefa a quantidade necessária de dados pessoais.

Podemos listar outras duas distinções sobre os conceitos de segurança e privacidade. A segurança está sempre relacionada à proteção de dados, já a privacidade diz respeito à proteção da identidade do usuário. A segurança de uma informação pode ser realizada sem privacidade, já a privacidade não pode ser assegurada sem segurança. Vale exemplificar para distinguirmos a diferença entre esses dois conceitos: consideremos um hospital que utiliza sistemas seguros para se comunicar com os pacientes sobre a sua saúde. Esse tipo de transmissão de dados é um exemplo de segurança. De outro modo, as disposições de privacidade podem limitar o acesso ao registro de saúde do paciente somente a determinados integrantes específicos de uma mesma equipa do hospital.

[215] No primeiro capítulo do presente trabalho, diferenciamos o direito à privacidade e o direito à proteção de dados.
[216] Art. 25 e Considerando 78, ambos do RGPD.

Contudo, se um dos profissionais de saúde divulgar um dado do paciente sem a sua autorização, a segurança do sistema foi mantida, mas a privacidade foi violada.[217]

A confidencialidade, por sua vez, está ligada às situações em que o provedor de serviços, responsável pelos dados pessoais de terceiros, tem a obrigação de salvaguardar o acesso a esses dados por pessoas não autorizadas. A confidencialidade também está ligada à recolha de dados, quando a identidade do titular dos dados deve ser preservada.

Privacidade e confidencialidade são conceitos que muitas vezes se sobrepõem, mas existem diferenças entre essas definições. A privacidade está relacionada ao direito de limitar o acesso público sobre determinados dados, permitindo a sua divulgação conforme o desejo do titular dos dados, ou seja, refere-se ao indivíduo. A confidencialidade, por sua vez, refere-se a afiançar determinados documentos e informações, normalmente, às organizações e pessoas coletivas, consubstancia-se em um ajuste de vontades entre interessados para manter o sigilo desses documentos e informações. Em geral, a privacidade refere-se a uma escolha pessoal do titular, enquanto a confidencialidade tem como fundamento uma relação profissional e legal.[218]

3.3.2 Segurança, privacidade e confidencialidade no processo da Online Dispute Resolution

Para que o processo da ODR alcance sucesso, os aspetos da segurança, privacidade e confidencialidade são essenciais para o seu desenvolvimento e devem ser observados em todas as etapas do sistema de ODR. Contudo, a utilização do ODR gera desafios. O principal deles diz respeito à necessária confiança na tecnologia e na segurança de dados, abrangendo nesse caso a privacidade e a confidencialidade das informações pessoais, uma vez que essas informações são digitalizadas e transferidas online. Esse procedimento pode ser violado e, eventualmente, acessado por terceiros não autorizados ou, ainda, as informações podem ser liberadas de forma maliciosa ou negligente por uma das partes. Ademais, a proteção e a segurança dos dados é uma das questões que os legisladores têm necessariamente prestado grande atenção.

Quando nos referimos à ODR, o aspeto tecnológico vem logo à lembrança, principalmente no que diz respeito à infraestrutura da Tecnologia da Informação e

---

[217] JAVA T POINT. **Difference between Security and Privacy**. India: [sn], sd]. Disponível em https://www.javatpoint.com/security-vs-privacy. [Consult. 30 ago. 2021].

[218] SURBHI, S. – **Difference between Privacy and Confidentiality**. [sl]: [sn], 2018. Disponível em https://keydifferences.com/difference-between-privacy-and-confidentiality.html. [Consult. 03 set. 2021].

Comunicação (TIC). Paradoxalmente, é essa infraestrutura que traz a desconfiança aos usuários, pois está sujeita a constantes fraudes e problemas devido às violações que ocorrem na rede mundial de computadores. Por essa razão, os orçamentos estatais aportam cada vez mais recursos económicos direcionados à pesquisa e ao desenvolvimento de mecanismos eletrónicos e virtuais que podem fornecer maior proteção da TIC contra tais ameaças, a fim de reduzir a insegurança em relação aos dispositivos eletrónicos e os meios de comunicação.

No que diz respeito à segurança, é necessário registrar que esse conceito deve ser entendido sob várias perspectivas, tais como: confidencialidade, transparência, sigilo, autenticação, assinatura, integridade, privacidade e controlo de informação. O aspeto mais importante da segurança é proteger as informações de violações não autorizadas, tarefa que envolve a transmissão e o armazenamento de dados pessoais. A segurança leva ao aumento da confiança dos usuários e pode-se estabelecer nesse sentido, um círculo virtuoso. No entanto, é necessário ponderar que nenhum método de comunicação é capaz de garantir segurança absoluta.

A segurança é tratada com detalhes no RGDP[219], que disciplina como devem ser implementadas as medidas técnicas e organizacionais para assegurar um nível de segurança apropriado ao risco, levando em consideração as técnicas mais avançadas, os custos de aplicação face aos riscos, à probabilidade e à gravidade variável. Além da segurança dos dados, outro fator de importância para garantir a segurança na ODR é a confidencialidade ou o sigilo. A questão da confidencialidade é complexa e varia de acordo com a situação e o tipo de informação trocada entre as partes. Uma preocupação que ocorre durante os métodos da ODR é a publicação ou não das soluções encontradas. Normalmente, as partes preferem não ter as informações durante o processo comunicados, exceto com a sua permissão. Na verdade, a não divulgação estabelece um ambiente de confiança e segurança entre as partes e protege a sua reputação.

Não obstante, os provedores de ODR têm uma política de confidencialidade de informações dispondo sobre o seu sigilo absoluto ou mesmo a sua disponibilidade. A Organização Mundial de Propriedade Intelectual (WIPO), por exemplo, adotou a transparência e determinou a publicação de resoluções em seu site, onde todos os usuários da internet podem obter acesso a ele[220]. Essa recomendação da WIPO pode

[219] RGPD. Secção 2 – Segurança dos dados pessoais. Artigo 32. Segurança do tratamento

[220] PECNARD, C. – The issue of security in ODR. **Berkeley Electronic Press**. V. 7, 2004, p. 1-5. Disponível em http://epublications.bond.edu.au/adr/vol7/iss1/1/. [Consult. 05 set. 2021].

conduzir o leitor desavisado a um aparente antagonismo, pois a confidencialidade é obviamente o oposto da publicidade, devido ao fato de que a confidencialidade protege a privacidade das partes para resolver os assuntos de forma mais fácil e rápida por meio da ODR.

Não obstante, todo ajuste necessário sobre o alcance e a profundidade das informações disponibilizadas pode ser objeto de acordo entre os envolvidos. Ou seja, os envolvidos em uma ODR podem definir a medida da transparência de acordo com a sua vontade e o seu caso concreto, por exemplo, fazendo publicar os resultados de casos ou apenas informações gerais sobre a ODR realizada. Essa solução parece harmonizar dois princípios aparentemente incompatíveis entre si, quais sejam, a transparência do procedimento (publicizando o resultado obtido) e a confidencialidade das informações tratadas durante o procedimento. No tocante às pessoas coletivas, a utilização da ODR tem a confidencialidade como um dos fatores importantes a serem considerados para utilizar essa ferramenta, pois a combinação "confidencialidade-transparência" pode protegê-la em conflitos envolvendo a sua reputação.

Como vimos, a confidencialidade está relacionada à proteção de dados em geral, enquanto a privacidade concentra-se na proteção de dados pessoais.[221] Para alguns usuários da ODR, é importante que todas as suas informações pessoais e declarações de casos fiquem privadas, muito embora em sistemas ODR, informações pessoais sobre usuários possam ser coletadas. Portanto, esse é outro aspeto importante para que os provedores de ODR mantenham um equilíbrio entre a privacidade das informações e a transparência do procedimento, além da segurança das informações. De fato, as diretrizes de segurança, privacidade e confidencialidade constituem uma base sólida e atrativa para a resolução de conflitos por meio da ODR.

As medidas de privacidade para sistemas ODR podem incluir[222]: (i) a criação de diretrizes éticas de privacidade para sistemas neutros e tomadores de decisão, que incluem leis e regras para restringir a publicação de dados pessoais das partes; ou ainda, (ii) a publicação de casos sem identificar os detalhes das partes, por exemplo, divulgar apenas informações estatísticas e resumos de casos anônimos, com fatos e nomes removidos; e, ainda, (iii) o estabelecimento de um serviço protegido, seguro e certificado para

[221] ABEDI, Fahimeh; ZELEZNIKOW, John; BRIEN, Chris. – Developing regulatory standards for the concept of security in online dispute resolution systems. **Computer Law & Security Review**. V. 35, n.º 5, 2019. p. 1-8. Disponível em https://www.researchgate.net/publication/334056927_Developing_regulatory_standards_for_the_concept_of_security_in_online_dispute_resolution_systems. [Consult. 05 set. 2021].
[222] ABEDI, Fahimeh *et al. Op. cit*, p. 4.

declarações de privacidade. Isso pode incluir o uso de *softwares* que permitam a criptografia de senhas e de outras informações.

Em conclusão, os sistemas de ODR deverão possuir diversas tecnologias que se enquadrem nas diferentes medidas de proteção e que vão desde a proteção genérica, para mitigar ataques de *malware*, até a encriptação de dados passando por sistemas de autenticação de dois fatores, de forma a evitar violações no acesso aos sistemas e aos dados.

3.3.3 O impacto do Regulamento Geral de Proteção de Dados sobre o processo de Online Dispute Resolution

O RGPD, ao regulamentar o tratamento de dados pessoais e à livre circulação desses dados, expressou a sua preocupação com a eventual vulnerabilidade dos endereços eletrónicos, sítios etc., que podem ficar expostos no sistema virtual de informação, ou seja, os dados de pessoas singulares ou coletivas podem ficar vulneráveis na rede mundial de computadores. Essa condição está bem caracterizada no RGPD, ao disciplinar em seus artigos como devem ser conduzidos os quesitos de segurança, privacidade e confidencialidade. Por exemplo, o artigo 5º, número 1, alínea f, diz respeito à integridade e confidencialidade dos dados pessoais, nestes termos:

> Os dados pessoais são: [...] f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»)

Os artigos que tratam especificamente de segurança estão reunidos na secção 2 do capítulo IV, do RGPD, do artigo 32º ao artigo 34º. O artigo 32º indica que é essencial implementar medidas de segurança adequadas para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais. Especifica que as medidas a serem tomadas devem ser adaptadas aos riscos e estabelece o princípio de responsabilidade para o controlador de dados e o subcontratado, além de vedar a transferência de responsabilidade pela segurança para outrem. Fornece, ademais, orientações específicas relacionadas à segurança de dados e notificação de violação.

Entre outras coisas, os controladores e processadores de dados são aconselhados a incluir: (a) a pseudonimização e criptografia de dados pessoais; (b) a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos

sistemas e serviços de processamento; (c) a capacidade de restaurar a disponibilidade e o acesso aos dados pessoais em tempo hábil, no caso de um incidente físico ou técnico; e (d) um processo para testar regularmente, apreciar e avaliar a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento.[223]

O artigo 33.º indica que é obrigatório notificar a autoridade de controlo em caso de violação de dados pessoais e descreve as informações mínimas que deve conter a respectiva notificação, a fim de que a autoridade de controlo tenha condições de avaliar a situação de violação de dados. O artigo 34 descreve os procedimentos para notificar os titulares dos dados na hipótese de violação dos dados pessoais.

Considerando essas normativas por fundamento, os desenvolvedores de sistemas de ODR deverão, portanto, fornecer endereço eletrónico (ou programas ou aplicativos) que sejam seguros, notadamente melhorados com base na *privacy by design*, bem assim devem respeitar a privacidade dos dados, o que exige ajustes contínuos nesse processo de desenvolvimento.

Outro impacto que o RGPD pode ter sobre os sistemas de ODR resulta na constante reorganização dos métodos, utilizando as mais recentes ou avançadas ferramentas, com vistas a fortalecer a segurança de dados do próprio sistema ODR. Essas ferramentas permitirão, em particular, (1) identificar e corrigir as eventuais fragilidades ao longo do ciclo de vida; (2) criptografar dados, armazenados ou em trânsito, ou na nuvem; (3) fortalecer a autenticação de usuários; (4) garantir a integridade dos dispositivos utilizados pelos usuários; e (5) impedir ou mitigar ataques que visem a violação de dados.

Assim que os sistemas de ODR iniciem a coleta e a transmissão de dados pessoais, é indispensável que a privacidade de dados esteja inserida em sua estratégia operacional de modo que haja uma reavaliação contínua dos requisitos do RGPD, a fim de aumentar a inviolabilidade de dados, e, portanto, para melhorar a própria segurança cibernética. Uma dessas ferramentas atualmente utilizada, por exemplo, é a criptografia, tecnologia necessária (mas não a única) para aumentar a segurança virtual. A criptografia pode auxiliar no fenómeno da pseudonimização ao impedir que o titular dos dados seja identificado.

Além disso, o artigo 25º obriga que os controladores implementem medidas técnicas e organizacionais adequadas para fornecer as garantias necessárias ao

[223] RGPD – Artigo 32, n. 1, alíneas 'a' a 'd'.

processamento de dados pessoais que não foram tornados anônimos. A eficácia das medidas implementadas deve ser avaliada e documentada regularmente.

Deve-se salientar, mais uma vez, que o processo de ODR pode estar sujeito à violação de dados por meio de ataques de *hackers*. Devido a isso, é importante que a avaliação de impacto sobre a proteção de dados seja um fator essencial do procedimento. O RGPD faz essa imposição no artigo 35º, número 1[224]. Outro aspeto importante trata do impacto do RGPD sobre os sistemas de ODR automatizados, fundado em *softwares* e programas de computador especializados na resolução objetiva de conflitos, programados com base na experiência multidisciplinar da ciência, utilizando a matemática, a filosofia, o direito e, sobretudo, a inteligência artificial.[225] Nesse caso, o artigo 22º do RGPD garante ao titular de dados que não seja submetido a nenhuma decisão totalmente automatizada, "incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar."No entanto, o número 2 do artigo 22 permite exceções em três casos: para viabilizar a celebração de um contrato entre sujeito e controlador de dados – item 2(a); na hipótese de autorização pela legislação da União ou do Estado-Membro, com as medidas adequadas para salvaguardar os direitos do titular dos dados – item 2(b); e, por fim, em razão do consentimento livre e informado do titular dos dados – item 2(c).

Por fim, vale consignar que o texto do artigo 22º traz em seu bojo certa incongruência com o direito do titular de ser informado sobre o tratamento de seus dados. A autora portuguesa Inês da Silva Costa[226] cita que o titular dos dados se encontra vulnerável, pois a "caixa preta" do algoritmo impede que ele tenha acesso aos seus dados e a maneira como são coletados, e tal situação deixa o titular em uma posição desequilibrada em relação ao responsável pelo tratamento.

---

[224]RGPD- Artigo 35 "1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação."

[225] CARNEIRO, David R.; NOVAIS, Paulo; ANDRADE, Francisco C. P.; ZELEZNIKOW, John; NEVES, José - Online dispute resolution: an artificial intelligence perspective **Artificial Intelligence Review**. V. 41, n.º 2, 2014. p. 211-240. Disponível em https://hdl.handle.net/1822/32005. [Consult. 30 set. 2021].

[226] COSTA, Inês S. – A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. **Revista Electrónica de Direito**. N.º 1, V. 24, fev 2021. p. 33-82. Disponível em https://www.scilit.net/article/ddced605c9ef7599a70db1ec27af88be. [Consult. 30 set. 2021].

3.3.4 O impacto da Lei Geral de Proteção de Dados Pessoais sobre o processo de Online Dispute Resolution

Do mesmo modo que o RGPD tem impactos sobre o processo de ODR, a LGPD também influencia esse procedimento adequado de resolução de conflitos por meio virtual no Brasil. Segundo Richard Susskind[227], o futuro dos serviços legais será composto por tribunais virtuais, negócios jurídicos online e a produção de documentos por meio da internet. Contudo, podemos dizer que esse futuro já se iniciou, seja pelo próprio Poder Judiciário que tem editado normas para regular a adequação da LPGD, ou, ainda, mediante a utilização da ODR.

No tocante à ODR desenvolvida no Brasil, necessário sublinhar, inicialmente, que as precauções acima delineadas para a ODR sob a regulamentação da RGPD em grande parte se aplicam também à ODR no Brasil, visto a similaridade das legislações; por exemplo, as providências relativas aos aspetos de segurança, privacidade e confidencialidade descritas.

De outro lado, é sabido que as ferramentas digitais utilizadas durante o processamento da ODR são responsáveis pelo gerenciamento dos dados pessoais das partes envolvidas no processo, portanto, nesse caso, faz-se a interação com a LGPD. Por exemplo, o artigo 52, § 7º da LGPD[228] possibilita a conciliação direta entre o controlador e o titular para a resolução sobre violações ou acessos não autorizados a dados pessoais. Ou seja, no nosso exemplo, na eventual hipótese de violação de dados de um sistema de ODR, o titular de dados poderá entrar em contato diretamente com o controlador desse sistema e realizar uma conciliação sobre o ocorrido. Certo é que, durante a condução do processo de ODR, muitos dados são gerados, coletados e armazenados, sendo que aqueles considerados sensíveis podem ficar fragilizados a uma interferência externa, cabendo, portanto, às empresas e aos órgãos públicos envolvidos proteger qualquer tipo de informação sigilosa fornecida em um processo ODR.

De outro lado, quando a empresa conhece as regras da LGPD, que cercam a segurança, a privacidade e a confiabilidade do processo, resulta na redução da possibilidade de uma sanção por tratamento irregular de dados pessoais. Para que

[227] SUSSKIND, Richard – **Tomorrow's Lawyers: An Introduction to Your Future**. 2ª. ed. Oxford: Oxford University Press, 2013. p. 12.

[228] Art. 52. (...) "§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo"

nenhuma informação sigilosa seja violada, o sistema que irá abrigar a ODR precisa ser embasado em eficiente política de segurança de dados. Hoje, muitas aplicações operam com sistemas confiáveis, como o *blockchain* e a criptografia, pois ambos dificultam o acesso de criminosos virtuais e reduzem possíveis brechas na segurança, tal como já lembrado no item anterior quanto à RGPD. Quando a estrutura virtual da empresa é construída com base em uma boa equipa de Tecnologia da Informação (TI), tecnologias e profissionais jurídicos, a ODR sai fortalecida, ficando mais difícil que o processo de ODR descumpra as regras da LGPD.

Duas questões interessantes devem ser enfatizadas. A primeira ligada à previsão expressa de proteção das informações físicas e digitais em território brasileiro, em decorrênciado artigo 3º da LGPD; e a segunda aponta a faculdade das partes, junto com o terceiro imparcial, considerarem as vantagens e desvantagens do uso de ferramentas tecnológicas.

Cada vez mais utilizados, esses métodos online precisam encontrar, nas Câmaras de Conciliação e Mediação e nas instituições privadas que utilizam a ODR, uma estrutura organizada que incorpore a compreensão da importância da proteção de dados desde o desenvolvimento de seus sistemas, bem assim durante seus processos e práticas.

Uma das maneiras que a LGPD pode impactar a privacidade do processo de ODR é por meio da anonimização[229] de dados, isto é, o procedimento de alterar ou apagar de uma base de dados todas as informações pessoais que identificam uma pessoa natural, como nome completo, RG (Carteira do Cidadão em Portugal), CPF (ou NIF em Portugal), endereço ou telefone. Essa previsão aproxima-se da pseudonimização prevista no RGPD.

Pode-se inferir, portanto, que a LGPD permite que cada pessoa coletiva que pretenda gerir processos de ODR tenha em mãos inúmeras ferramentas, sejam elas legais ou tecnológicas, a fim de assegurar a segurança, a privacidade e a confiabilidade dos procedimentos de ODR de seu sistema.

No tocante ao Poder Judiciário brasileiro, o Conselho Nacional de Justiça (CNJ) editou a Resolução n.º 363, de 12 de janeiro de 2021, que estabeleceu medidas para o processo de adequação à LGPD, tais como a criação de Comitê Gestor de Proteção de Dados no âmbito de cada tribunal de sua estrutura organizacional; a criação de Grupo de Trabalho Técnico para a revisão de formulários, a revisão do fluxo de atendimentos, de

[229] Artigo 5º, XI – "anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.".

contratos, entre outras providências administrativas; a criação de site com informações sobre a aplicação da LGPD; a disponibilização de informações, conforme o artigo 9º da LGPD; além de implementar medidas de segurança e manter registros sobre o tratamento de dados, de forma a dar eficácia à LGPD no âmbito do Poder Judiciário.

Todo esse aparato legal foi necessário, também, para que os Centros Judiciários de Solução de Conflitos e Cidadania (CEJUSCS) – instituídos pelo artigo 8º da Resolução CNJ N.º 125, de 2010, que dispôs sobre tratamento adequado dos conflitos de interesses no âmbito do Poder Judiciário e que estavam atendendo de maneira virtual durante a pandemia de SARS-COV-2[230] – pudessem se adequar à LGPD e, também, à conciliação não presencial realizada nos Juizados Especiais Cíveis[231] (similares aos Julgados de Paz, em Portugal).

Necessário destacar que o CNJ, mediante a publicação da Portaria n.º 61, de 2020[232], criou uma plataforma para a realização de sessões de julgamento durante o distanciamento social provocado pela pandemia. Assim, infere-se que o Poder Judiciário brasileiro tem se adaptado às inovações tecnológicas e oferecido soluções para exercer o seu ofício.

[230] TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. **Conciliação e Mediação**. São Paulo: [sn], [sd]. Disponível em https://www.tjsp.jus.br/Conciliacao. [Consult. 30 maio 2020].
[231] Lei n.º 13.994, de 24 de abril de 2020.
[232] CONSELHO NACIONAL DE JUSTIÇA. **Plataforma Emergencial de Videoconferência para Atos Processuais.** Brasília, DF: [sn], [sd]. Disponível em https://cnj.jus.br/plataforma-videoconferencia-nacional/. [Consult. 13 maio 2020].

CONCLUSÃO

O acesso à Justiça pelos cidadãos tem sido dificultado por inúmeros fatores, por exemplo: a morosidade do Poder Judiciário em dar uma decisão final aos judicantes, às custas judiciais e aos honorários advocatícios, entre outros mencionados por Mauro Cappelletti e Bryant Garth[233]. As administrações públicas, a fim de dar cumprimento ao direito de acesso à Justiça aos cidadãos, conforme previsto na Constituição de Portugal e na Constituição do Brasil, visam cumprir com os compromissos internacionais assumidos notadamente junto a ONU com a Agenda 2030, que implementou os Objetivos de Desenvolvimento Sustentável (ODS) e incluiu em seu objetivo 16 – Paz, Justiça e Instituições Eficazes – a oferta de acesso à Justiça para todos ao lado da construção de instituições eficazes. Nesse sentido têm sido utilizado os procedimentos adequados de solução de controvérsias denominado 'sistema multiportas'[234], expressão cunhada por Frank Sander, em 1976, ao descrever um "centro geralde Justiça"[235] onde seria realizada a triagem dos conflitos e onde se verificaria o procedimentomais adequado à sua solução. Entre os métodos utilizados pela RAL, encontram-se a conciliação, a mediação e a arbitragem e, entre esses métodos, conforme visto no Capítulo II do presente texto, avançou-se para o sistema de mediação online, denominado ODR. Em termos gerais, a ODR é um processo de incorporação da tecnologia que facilita os procedimentos adequados de resolução de disputas. A ODR economiza tempo por meio de procedimentos simplificados, tende a diminuir gastos com honorários advocatícios e minimiza custos com deslocamentos. No entanto, o mais importante é constatar o seu poder transformador que reduz a desigualdade entre as partes, proporcionando uma Justiça mais equitativa, como relata John Rawls[236].

De outro lado, a transmissão de dados e informações é um processo básico para a organização socioeconómica em um mundo globalizado, em que as redes de comunicação não respeitam as fronteiras geopolíticas dos Estados. Por esse motivo, publicam-se leis que visamconferir a necessária e suficiente proteção legal aos usuários

---

[233] CAPPELLETTI, Mauro; GARTH, Bryant – **Acesso à Justiça**. Trad. Ellen Gracie Northfleet. Porto Alegre: Sergio Antonio Fabris Editor, 1988. p. 10.
[234] O conceito foi apresentado na palestra de abertura da Global Pound Conference, em 1976, em Saint Paul, Minnesota, Estados Unidos.
[235] SALES, Lilia M. M.; SOUSA, Mariana A. – *Op. cit*, p. 204-220. [Consult. 27 jan. 2020].
[236] RAWLS, John. *Op. cit*, p. 89-95.

que lhes confira privacidade, segurança e confiabilidade no sistema. Nesse sentido, o RGPD e a LGPD constituem forte instrumento de proteção ao direito fundamental à proteção de dados, analisado no Capítulo I.

No Capítulo II, podemos analisar o desenvolvimento da ODR junto aos Poderes Judiciários e nas administrações públicas em Portugal e no Brasil e, muito embora a utilização da ODR constitua uma prática ainda em desenvolvimento, há grandes avanços na sua utilização.

No Capítulo III, podemos constatar a similitude entre a RGPD e a LGPD, bem como verificar que em ambas as legislações os aspetos da segurança, privacidade e confidencialidade no processo das ODRs são essenciais para fomentar essa modalidade de solução alternativa de conflitos e, ainda, podemos examinar que no plano jurídico existe a possibilidade de que a ODR seja adotada pelas administrações públicas de Portugal e do Brasil, assim como por entidades privadas de mediação nos dois países. A ODR, portanto, configura importante ferramenta, eficaz e económica, na resolução de conflitos.

Não devemos temer a evolução digital, que já é uma característica contundente desse início de século. Deixemos que a tecnologia resolva as questões afinadas com a sua natureza, como o arquivamento e o gerenciamento das informações de grande vulto. Aos usuários caberá, com inteligência e criatividade próprias dos seres humanos, utilizar essas informações para encontrarmos soluções *à la carte* para solucionar pendências jurídicas.[237]

[237] FIGUEIRA, Denise C. –*Op. Cit.* p. 530.

REFERÊNCIAS BIBLIOGRÁFICAS

AGRE, P. ROTENBERG, M. (Eds.) – **Technology and privacy: the new landscape**.Cambridge: MIT Press, 1997. ISBN 978-0262511018.

ALEXANDRINO, Marcelo; PAULO, Vicente – **Direito Administrativo Descomplicado**.23ª Edição, São Paulo: Editora Método, 2013. ISBN 978-6559642595.

ALVIM, José E. C. – ***Habeas data.*** Rio de Janeiro: Forense, 2001. ISBN 8530913620.

ARBIX, Daniel A. – **Resolução Online de Controvérsias**. São Paulo: Editora Intelecto,2017. ISBN 978-8558270168.

BITTAR, Carlos A. – **Os Direitos da Personalidade**. 8ª Ed. São Paulo: Saraiva, 2015. ISBN978-8502208278.

CALVÃO, Filipa U. – **Direito da Proteção de Dados Pessoais**. Lisboa: Almedina, 2018.ISBN 978-9898835406.

CANOTILHO, José J. G.; MOREIRA, Vital. (Eds.) – **CRP. Constituição da República Portuguesa anotada.** Volume 1. Artigos 1º a 107. 1ª edição brasileira – São Paulo: Revista dos Tribunais; 4. ed. portuguesa revista, v. 1. Coimbra: Coimbra Editora, 2007. ISBN: 978- 8520330449.

CAPPELLETTI, Mauro; GARTH, Bryant – **Acesso à Justiça**. Trad. Ellen Gracie Northfleet. Porto Alegre: Sérgio Antonio Fabris Editor. 1988. ISBN: 978-8588278295.

CASTRO, Catarina S. – **Direito da informática, privacidade e dados pessoais**. Coimbra: Edições Almedina, 2005. ISBN: 978-9724024240.

CHOUCRI, Nazli – **Cyberpolitics in International Relations**. Cambridge: MIT Press. 2012.ISBN: 978-0262517690.

CORDEIRO, António B. M. – **Direito da Proteção de dados à Luz do RGPD e da Lei nº58/2019**. Lisboa: Almedina, 2021. ISBN 978-9724083049.

CORTÉS, Pablo – **Online dispute resolution for consumers in the European Union.** Abingdon: Routledge, 2011. ISBN: 978-0415813280.

DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. 3ª Edição. Rio de Janeiro: Renovar, 2006. ISBN: 978-6559917969.

FERNANDES, Luís A. C.– **Teoria Geral do Direito Civil**. Vol. I, 6ª Ed., Lisboa: Universidade Católica Editora, 2012. ISBN 978-972-54-0361-7.

FIGUEIRA, Denise C. – **Resolução de Conflitos on-line e os desafios para a administração pública.** *In* WATANABE, Kazuo et al. Desjudicialização, justiça conciliativae Poder Público. São Paulo: Thomson Reutes Brasil, 2021. p. 513-531. ISBN 978- 6556144504.

GONÇALVES, Maria E. – **Direito da informação: novos direitos e formas de regulação na sociedade da informação**. Coimbra: Almedina, 2003. ISBN: 9789724019086.

GOUVEIA, Mariana F. – **Curso de Resolução Alternativa de Litígios**. 3ª Ed. Lisboa: Almedina, 2015. ISBN: 978-9724019086.

HESSE, Konrad – **Elementos de Direito Constitucional da República Federal da Alemanha.** Tradução de Luíz Afonso Heck. Porto Alegre: Sergio Antonio Fabris Editor, 1998. ISBN: 978-8588278059.

KAKU, William S. – **Internet e comércio eletrónico: pequena abordagem sobre a regulação da privacidade.** *In*: ROVER, Aires J. – Direito, Sociedade Informática: Limites e perspectivas da vida digital. Florianopolis: Fundação Boiteux, 2000, p. 81-93. ISBN: 8587995022.

LÉVY, Pierre – **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2008. ISBN: 978-8573261264.

LOPES, Dulce; PATRÃO, Afonso (Coords.) – **Lei da Mediação Comentada.** Coimbra: Almedina, 2014. ISBN: 978-6555155136.

LUDLOW, Peter – **Crypto Anarchy, Cyberstates, and Pirate Utopias**. USA: MIT Press, 2001. ISBN: 978-0262256582.

MARTINS, Leonardo. (Coord.) – **Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Montevidéu: Fundação Konrad Adenauer, 2005. ISBN 9974-7942-1-8.

MIRANDA, Jorge – **Manual de direito constitucional.** Tomo IV. 5ª Edição. Coimbra: Coimbra Editora, 2000. ISBN: 978-9723220100.

____, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada.** Vol. I, 2ª Ed. Revista. Lisboa: Universidade Católica Editora. 2017. ISBN: 978-9725405413.

MOREIRA, Teresa – Novos desafios para a contratação à distância a perspectiva da defesa doconsumidor. *In* **Estudos do Direito do Consumidor**. Nº 9. Coimbra, 2015, p. 19-36. ISSN 1646-0375.

NOVAIS, Jorge R.**– Jurisdição Constitucional e Direitos Fundamentais – Estudos em Homenagem a Jorge Reis Novais**. Belo Horizonte: Arraes Editora, 2015. ISBN: 978- 8582381526.

PINTO, Carlos A. Mota – **Teoria Geral do Direito Civil**. 4ª Ed. Reimpressão. Coimbra: Coimbra Editora, 2017. ISBN: 978-9723221022.

QUEIROZ, Cristina M. M. – **Direitos fundamentais: teoria geral.** Coimbra: CoimbraEditora, 2002, ISBN: 978-9723211368.

RAWLS, John – **Justiça como equidade – Uma reformulação**. São Paulo: Martins Fontes, 2003. ISBN: 978-8533617520.

RODOTÀ, Stefano – **A vida na sociedade da vigilância – a privacidade hoje.** Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. ISBN: 978- 8571476882.

ROSÁRIO, Pedro T. (pref.); DA SILVA, Henrique D. (introd)- **Constituição da República Portuguesa e legislação complementar.** Lisboa: Legit, 2018. ISBN: 978-9728973520.

ROSÁRIO, Pedro T.; DAL RI, Luciene; HAMMERSCHMIDT, Denise – **Direito Constitucional Luso e Brasileiro na Contemporaneidade.** Curitiba: Ed. Juruá, 2019. ISBN:978-8536285528.

SALDANHA, Nuno – **Novo Regulamento Geral de Proteção de Dados. O que é? A quemse aplica? Como implementar?** Lisboa: FCA- Editora de Informática, 2018. ISBN: 978- 9727228898.

SARLET, Ingo W. – **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.** Porto Alegre: Livraria do Advogado, 2009. ISBN: 978-8573486230.

SILVA, Artur F. – O Novo Regime Jurídico da Resolução de Conflitos Desportivos no Direito Administrativo: sobre a Arbitragem Necessária e a Mediação no Tribunal Arbitral do Desporto. *In* GOMES, Carla Amado et al. **Arbitragem e Direito Público**. Lisboa: AAFDL, 2018. p.395-436. ISBN: 978-9726292166.

SILVA, José A. – **Curso de Direito Constitucional Positivo.** São Paulo: Ed. Malheiros, 2002. ISBN: 8574204463.

SOUSA, Rabindranath Capelo de – **O Direito Geral da Personalidade**. Coimbra: Coimbra Editora, 1995. ISBN: 9723206773.

SUSSKIND, Richard – **Tomorrow's Lawyers – An Introduction to Your Future**. 2º Ed. USA: Oxford University Press, 2013. ISBN: 978-0199668069.

WANG, Faye F. – **Online Dispute Resolution. Technology, management and legal practice from an international perspective.** Oxford: Chandos Publishing Limited, 2008. ISBN: 978-1843345190.

WATANABE, Kazuo – Acesso à justiça e meios consensuais de solução de conflitos *In* **Tribunal Multiportas – Investindo no capital social para maximizar o sistema de solução de conflitos no Brasil**. CRESPO, Maria H.; ALMEIDA, Tânia; ALMEIDA, Rafael A. (Coords.). 2012. Rio de Janeiro: FGV Editora. ISBN: 978-8522509591.

REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTOS LEGAIS (INTERNET)

ABEDI, Fahimeh; ZELEZNIKOW, Jonh; BRIEN, Chris – **Developing regulatory standards for the concept of security in online dispute resolution systems**. Computer Law & Security Review, nº 35, Junho 2019, p.1-8. Disponível em https://www.researchgate.net/publication/334056927_Developing_regulatory_standards_for_the_concept_of_security_in_online_dispute_resolution_systems. [Consult. 05 set. 2021]. DOI:10.1016/j.clsr.2019.05.003.

ACORDO SOBRE COMÉRCIO ELETRÔNICO DO MERCOSUL – Disponível em http://siscomex.gov.br/wp-content/uploads/2021/02/82753_DEC_015-2020_PT_Acordo- Comercio-Eletronico.pdf. [Consult. 29 mar. 2021].

ADI 6.387 MC-Ref/DF, Min Relatora: Rosa Weber, julgado em 6 e 7 de maio de 2020, STF, voto conjunto com as ADIs 6.389, 6.390, 6.393, 6.388 e 6.387. Recurso Extraordinário (RE) 1010606. Resumo das teses afiançadas pelos Ministros disponível em http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1. [Consult. 11 abr. 2021].

ADI 6388, disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895166 e http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902. [Consult. 14 abr. 2021].

ALEXY, Robert – Direitos fundamentais, ponderação e racionalidade. Tradução de Luís Afonso Heck. in **Revista de Direito Privado**, n.º 24, out/dez 2005, p. 334-344. Disponível em https://www.conhecerparareconhecer.com.br/imprime.php?id=45. [Consult. 04 abr. 2021].

BANISAR, David - **National Comprehensive Data Protection/Privacy Laws and Bills 2021**. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416. [Consult. 30 set. 2021].

BEUX, Cris – **Privacidade e proteção de dados são coisas diferentes.** Disponível em https://www.linkedin.com/pulse/privacidade-e-prote%C3%A7%C3%A3o-de-dados-s%C3%A3o-coisas-diferentes-cris-eux?articleId=6673216800903229440#:~:text=O%20direito%20%C3%A0%20prote%C3%A7%C3%A3o%20de,livremente%20desenvolver%20a%20sua%20liberdade.&text=%C3%89%20uma%20liberdade%20positiva%20no,um%20espa%C3%A7o%20a%20ser%20constru%C3%ADdo. [Consult. 19 abr. 2021].

CARBALLO MARTÍNEZ, Gerardo – **La Mediación Administrativa y el Defensor del Pueblo**. Cizur Menor, Editora: Thomson Aranzadi, 2008. Disponível em https://dialnet.unirioja.es/servlet/articulo?codigo=3333250. [Consult. 07 dez. 2021].

CARNEIRO, Davide et al. – **Online dispute resolution: an artificial intelligence perspective**. Artificial Intelligence Review, V. 41, 2012, p. 211-240. Disponível em https://ddd.uab.cat/pub/artpub/2014/202519/air_a2014v41n2p211iENG.pdf. [Consult. 07 abr. 2021].

CARVALHAL, Ana P. Z. – **A arbitragem administrativa em Portugal.** Revista FMU Direito, ano 24, n.º 33, 2010, p.1-18. Disponível em www.revistaseletronicas.fmu.br. [Consult. 15 mar. 2021].

CEPD - Disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. [Consult. 28 jun. 2022].

CLARKE, Roger – **Introduction to Dataveillance and Information Privacy, and Definitions of Terms.** Xamax Consultancy. Disponível em http://www.rogerclarke.com/DV/Intro.html. [Consult. 29 mar. 2021].

CNPD – **Exposição de dados pessoais de redes sociais afeta milhões de utilizadores em Portugal.** Disponível em https://www.cnpd.pt/media/wq2pjyyc/informa%C3%A7%C3%A3o-da-cnpd-e-recomenda%C3%A7%C3%B5es_fb-e-linkedin_abril-2021.pdf. [Consult. 11 abr. 2021].

COMPARING PRIVACY LAWS: GDPR v. LGPD. **One Trust Data Guidance**. Disponível em https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-lgpd-0. [Consult. 10 abr. 2021].

CONSELHO EUROPEU DE PROTEÇÃO DE DADOS - Disponível em https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en. [Consult. 11 jul. 2022].

CÓRTES, Pablo – **What should the ideal ODR system for e-commerce consumers look like? The Hidden World of Consumer ADR: Redress and Behaviour.** Disponível em www.law.ox.ac.uk . [Consult. 10 mar. 2021].

COSTA, Inês S.- **A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas.** Revista Electrónica de Direito, n.º 1, vol. 24, fevereiro 2021, p. 35-82. Disponível em www.cije.up.pt/revistared. [Consult. 30 set. 2021].

DIAS, Patrícia C. – **Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública.** Revista Julgar OnLine. Jan 2021, p. 1-45. Disponível em http://julgar.pt/author/patricia-cardoso-dias/. [Consult. 22 jun. 2022].

_____, Patrícia C. – **Medidas de Prevenção e vigilância no contexto do surto de COVID-19 consistentes em operações de tratamento de dados pessoais no contexto das relações laborais.** Galileu -Revista de direito e Economia. Vol. XXI, jun- jul-2020, p. 188-190. Disponível em https://www.academia.edu/44928960/REVISTA_DE_DIREITO_E_ECONOMIA. [Consult. 22 jun. 2022].

DIREITOS DO TITULAR DOS DADOS. RGPD. Capítulo III. Art 15º e seguintes. Disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?qid=1559291025147&uri=CELEX:32016R0679#d1e2468-1-1. [Consult. 10 mar. 2021].

Difference between Security and Privacy. Disponível em https://www.javatpoint.com/security-vs-privacy. [Consult. 30 ago. 2021].

DONEDA, Danilo – **A proteção dos dados pessoais como um direito fundamental.** Disponível em https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. [Consult. 17 abr. 2021].

FIDELIS, Aline et al. – **The Impact of Covid-19 on Data Protection in Brazil.** Disponível em https://www.mayerbrown.com/en/perspectives-events/blogs/2020/04/the-impact-of-covid19-on-data-protection-in-brazil. [Consult. 24 abr. 2021].

FINN Rachel L.; WRIGHT David; FRIEDEWALD, Michael – **Seven Types of Privacy.** Disponível em https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.827.5418&rep=rep1&type=pdf. [Consult. 29 mar. 2021].

GAITENBY, Alan – **Wiley and Sons Internet Encyclopedia.** 2004. Disponível em https://onlinelibrary.wiley.com/doi/abs/10.1002/047148296X.tie129. [Consult. 02 abr. 2020].

GALLINDO, Sergio P. G. et al. – **Proteção de dados pessoais como direito fundamental autônomo e competência legiferante privativa da União.** Disponível em https://www.migalhas.com.br/depeso/314538/protecao-de-dados-pessoais-como-direito- fundamental-autonomo-e-competencia-legiferante-privativa-da-uniao. [Consult.24 abr. 2021].

GELEILATE, Ana A. – **A proteção de dados pessoais como um direito fundamental. Consultor Jurídico.** Disponível em https://www.conjur.com.br/2020-nov-11/ana-geleilate- proteção-dados-pessoais. [Consult. 04 abr. 2021].

GOMES, Carla A.- **Mediação e Arbitragem Administrativa e Direito do Ambiente: qualquer semelhança é mera coincidência.** Revista da Faculdade de Direito da Universidade Federal de Uberlândia, Vol. 42, nº 2, 2014, p. 204-223. Disponível em https://seer.ufu.br/index.php/revistafadir/article/view/29037. [Consult. 25 maio 2021].

HEUVEL, Esther van den – **Online dispute resolution as a solution to cross-border e- disputes.** An introduction to ODR. Disponível em https://www.oecd.org/digital/consumer/1878940.pdf. [Consult. 12 de jul. 2022].

IRAMINA, Aline – RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**. V. 12, nº 2, Out de 2020, p. 91-117. Brasília: Universidade de Brasília. Disponível em https://periodicos.unb.br/article. [Consult. 06 jun. 2021].

KOKOTT, Juliane; SOBOTTA, Christoph – **The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law**, Vol. 3, Issue 4, November 2013. p. 222–228. Disponível em https://academic.oup.com/idpl/article/3/4/222/727206. [Consult. 25 mar. 2021].

KUEHL, D. – **Cyberspace and Cyberpower: Defining the Problem. KRAMER, Franklin D. et al. Cyberpower and National Security**. Washington DC, NDU, 2009, Cap. II. Disponível em https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/. [Consult. 07 ago. 2020].

LEGAL CLOUD. **Decisões Judiciais sobre a LGPD nos Tribunais**. Disponível em https://legalcloud.com.br/decisoes-judiciais-lgpd-tribunais/ . [Consult. 30 abr. 2021].

MACHADO, Joana M. S. – **A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados.** Disponível em http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/viewFile/206/142 [Consult. 20 mar. 2021].

MARÍN LÓPEZ, M. J – La Directiva 2011/83/UE: esquema general, ámbito de aplicación, nivel de armonización y papel de los Estados Miembros. **Revista CESCO De Derecho De Consumo**. Disponível em https://revista.uclm.es/index.php/cesco/article/view/7 [Consult. 22 abr. 2022].

MARQUES CEBOLA, Cátia – Mediación y arbitraje de consumo: una visión comparada de los modelos portugués y español. **Revista de Internet, Derecho y Política**, núm. 25, septiembre, 2017. p. 6-16. Disponível em https://www.redalyc.org/articulo.oa?id=78852903003 . [Consult. 10 mar. 2021].

MARTÍN DE LLANO, Maria Isabel – **Teoría Y realidad constitucional.** Cizur Menor, Editora: Fundação Dialnet, nº 26, 2010, p. 544-549. ISSN 1139-5583 Disponível em https://reformafederal.files.wordpress.com/2013/05/n27_reducido.pdf [Consult. 10 mar. 2021].

MASSENO, Manuel D. – **A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa, uma cartografia das Fontes Legislativas.** Disponível em http://direitoeti.com.br/artigos/a-protecao-de-dados-pessoais-em-portugal-e-nos-outros-paises-de-lingua-portuguesa-uma-cartografia-das-fontes-legislativas/. [Consult. 17 abr. 2021].

MENDES, Laura S. **– Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. ASIN: B076CL4XXW (e-book). Disponível em https://seer.ufu.br/index.php/revistafadir/article/view/29037. [Consult. 25 maio 2021].

MINUTAS DE CONSENTIMENTO INFORMADO. Universidade de Coimbra. Disponível em https://www.uc.pt/protecao-de-dados/minutas_consentimento_informado. [Consult. 23 abr. 2021].

MONTEIRO, Renato L. – **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?** Instituto Igarapé. Artigo Estratégico 39, Dezembro de 2018. Disponível em https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. [Consult. 18 maio 2022].

MOTA, Joana; SAMPAIO, Alexandre P. – **RGPD em PORTUGAL** – Alguns apontamentos à sua lei de execução. Actualidad Jurídica Uría Menéndez. 2019. p. 142-148. Disponível em https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341. [Consult. 30 jun. 2021].

NETO, Adolfo B. et al. – **Resolução de disputas on-line (ODR), mediação e a advocacia**. São Paulo: OAB-SP. p. 8. Disponível em https://www.oabsp.org.br/comissoes2010/mediacao-conciliacao/artigos/RESOLUC2560oA2560aO%20DE%20DISPUTAS%20ON-LINE%20-ODR-%20MEDIAC2560oA2560aO%20E%20A%20ADVOCACIA.pdf. [Consult. 03 ago. 2021].

OCDE. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. ODR and the Courts: The promise of 100% access to justice?** Disponível em https://www.hiil.org/projects/trend-report-4-odr-and-the-courts-the-promise-of-100-access-to- justice/. [Consult. 29 mar. 2021].

ODR IN 30 COUNTRIES, 2020. Disponível em https://mgimo.ru/library/publications/odr_in_30_countries_2020_mediation_in_the_covid_1 [Consult. 17 mar. 2021].

OEA. **REVISÃO DE CAPACIDADE DE CIBERSEGURANÇA** – República Federativa do Brasil. Disponível em https://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da- Capacidade-de-Ciberseguranca.pdf. [Consult. 10 abr. 2021].

PECNARD, C – **The issue of security in ODR. Berkeley Electronic Press 2004**; 7(1): p. 1-5. Disponível em http://epublications.bond.edu.au/adr/vol7/iss1/1/. [Consult. 05 set. 2021].

PINHEIRO, Alexandre S. – **A COVID-19 e a proteção de dados pessoais**. Disponível em https://observatorio.almedina.net/index.php/2020/04/28/a-covid-19-e-a-protecao-de-dados- pessoais/. [Consult. 24 abr. 2021].

_____, Alexandre S. – **Dados pessoais, Censos 2021 e o Tribunal de Justiça da União Europeia** – Disponível em https://www.jornaldenegocios.pt/opiniao/colunistas/detalhe/dados- pessoais-censos-2021-e-o-tribunal-de-justica-da-uniao-europeia. [Consult. 30 abr. 2021].

RELATÓRIO CIBERSEGURANÇA DE 2020 – Disponível em www.cncs.gov.pt. [Consult. 10 abr. 2021].

RESOLUTION SYSTEMS INSTITUTE – **Resolução de Disputas on-line para casos de direito de família pós-julgamento: um relatório para o condado de Ottawa, Michigan, amigo do Tribunal.** Disponível em https://www.aboutrsi.org/publications/program-evaluations#Online%20Dispute%20Resolution. [Consult. 12 jul. 2022].

RESOLUTION SYSTEMS INSTITUTE. **Online Dispute Resolution**. Disponível em https://www.aboutrsi.org/special-topics/online-dispute-resolution. [Consult. 02 abr. 2020].

ROSA, Camila da; SPALER, Mayara G. – Experiências Privadas de ODR no Brasil. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**. Ano 3 – Número 3 – Dezembro de 2018. Disponível em http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista_esa_8_10.pdf. [Consult. 14 mar. 2021].

ROSÁRIO, Pedro T. – O Direito a ser esquecido. **Revista de Direito Santa Cruz do Sul**, V. 3, n. 53, p. 121-139, set./dez. 2017. Disponível em https://online.unisc.br/seer/index.php/direito/issue/view/496. [Consult. 11 jul. 2022].

RULE, Colin – **Online Dispute Resolution and the Future of Justice.** Annual Review of Law and Social Science. 2020. Disponível em www.annualreviews.org. [Consult. 17 mar. 2021].

SALES, Lilia; SOUSA, Mariana – **O Sistema de Múltiplas Portas e o Judiciário Brasileiro.** Revista Brasileira de Direitos Fundamentais & Justiça. Porto Alegre. Ano 5, n.º 16, jul/set-2011, p. 204-220. Disponível em https://www.researchgate.net/publication/326707190_O_Sistema_de_Multiplas_Portas_e_o_/judiciario_brasileiro. [Consult. 20 jan. 2020].

SCHULTZ, Thomas – **Does Online Dispute Resolution Need Governamental Intervention? The Case for Architectures of Control and Trust in North Carolina**. Journal of Law & Technology, v. 6, 2004, p. 71-106. Disponível em

http://cedires.com/index_files/Schultz_ODR_2004.pdf. [Consult. 09 mar. 2020].

SURBHI, S – **Difference Between Privacy and Confidentiality.** 2018. Disponível em https://keydifferences.com/difference-between-privacy-and-confidentiality.html. [Consult. 03 set. 2021]

THE INTERNATIONAL COUNCIL FOR ONLINE DISPUTE RESOLUTION – THE RIGHT TO PRIVACY. **Harvard Law Review** n.º 4. 1890. Disponível em https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. [Consult. 19 abr. 2021].

THE INTERNATIONAL COUNCIL FOR ONLINE DISPUTE RESOLUTION – Disponível em http://odr.info/ethics-and-odr/. [Consult. 15 fev. 2021].

UNCITRAL. **Résolution des litiges en ligne dans les opérations internationales de commerce électronique.** Note du Secrétariat, Résolution des litiges en ligne, 2015. p.6. Disponível em https://www.uncitral.org/pdf/french/workinggroups/wg_iii/crp3-f.pdf. [Consult. 12 fev. 2021].

VERGILI, Gabriela M.- **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados.** Disponível em https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados. [Consult. 19 abr. 2021].

REFERÊNCIAS LEGISLATIVAS

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Disponível em http://www.planalto.gov.br . [Consult. 21 dez. 2020].

CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA DE 1976. Disponível em https://www.parlamento.pt. [Consult. 12 dez. 2020].

DECRETO-LEI n.º 59/99, de 2 de março. Disponível em https://www.pgdlisboa.pt. [Consult.08 ago. 2021].

DIRETIVA 2013/11/EU. Disponível em https://eur-lex.europa.eu. [Consult. 10 set. 2021].

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD. Tribunal de Justiça de São Paulo. Disponível em https://www.tjsp.jus.br/LGPD/LGPD/ALGPD. [Consult. 08 set. 2021].

LEI n.º 29/2013, de 19 de abril. Disponível em https://www.pgdlisboa.pt. [Consult. 02 abr. 2021].

LEI n.º 13.709, de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. [Consult. 10 abr. 2021].

LEI n.º 12.965, de 23 de abril de 2014. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. [Consult. 02 abr. 2021].

LEI n.º 13.140, de 2015. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2015/lei/l13140.htm. [Consult. 10 jun. 2021].

LEI nº 13.994, de 24 de abril de 2020. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13994.htm. [Consult. 10 set.

2021].

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA.
Disponível em https://portal.oa.pt. [Consult. 10 abr. 2020].

RESOLUÇÃO Nº 125, de 29/11/201, do CNJ- Conselho Nacional de Justiça/Brasil. Disponível em http://www.gr.unicamp.br/legislacao/resolucao_cnj_125-2010.pdf. [Consult. 22 maio 2021].