Universidade de Brasília – UnB

Faculdade de Direito

JADE CASTRO RODRIGUES BERNARDES

REGULAÇÃO DE RISCO NA LEI GERAL DE PROTEÇÃO DE DADOS: ANÁLISE DE VARIÁVEIS JURÍDICAS RELACIONADAS AO MODELO TEÓRICO DA REGULAÇÃO DO RISCO SOB O ENFOQUE COMPARADO DO MODELO TLICS.

Risk regulation in the General Data Protection Law: Analysis of legal variables related to the theoretical model of risk regulation under the comparative approach of the TLICS Model.

Brasília

2022

REGULAÇÃO DE RISCO NA LEI GERAL DE PROTEÇÃO DE DADOS: ANÁLISE DE VARIÁVEIS JURÍDICAS RELACIONADAS AO MODELO TEÓRICO DA REGULAÇÃO DO RISCO SOB O ENFOQUE DO MODELO TLICS.

Autor: Jade Castro Rodrigues Bernardes.

Orientador: Prof. Dr. Márcio Iorio Aranha

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel, no Programa de Graduação da Faculdade de Direito da Universidade de Brasília, linha de pesquisa de *Transformações da Ordem Social e Econômica e Regulação*.

Brasília, 29 de abril de 2022.

FOLHA DE APROVAÇÃO

JADE CASTRO RODRIGUES BERNARDES

Regulação de risco na lei geral de proteção de dados: análise de variáveis jurídicas relacionadas ao modelo teórico da regulação do risco sob o enfoque do modelo TLICS.

Monografia apresentada como requisito parcial à obtenção do grau Bacharel Graduação da Faculdade de Direito da Universidade de Brasília, linha de pesquisa de *Transformações da Ordem Social e Econômica e Regulação*.

Aprovada em: ___ de _____ de _____.

BANCA EXAMINADORA

_____

Prof. Dr. Márcio Iorio Aranha
(Orientador – Presidente)

_____

Prof. Me. Adriano Drummond Trindade

(Membro)

_____

Prof. Me. Fernando Barbelli Feitosa
(Membro)

_____

Prof. Dr.
(Suplente)

Agradecimentos

Em primeiro lugar, agradeço a Deus pelo dom da vida, pelas oportunidades e por ter me dado força para superar as adversidades.

A minha mãe, Solange, por seu amparo, compreensão e paciência. A meu pai, Carlos, pelo seu apoio e incentivo. A minha avó, Francisca Maria, que foi um grande exemplo de fé, força e dedicação. Ao meu avô, Salvador, e a toda a minha família.

Ao meu orientador, professor Dr. Márcio Iorio Aranha, pelo seu compromisso, dedicação e por sempre estar disposto a me ajudar e a contribuir para meu aprendizado.

Às minhas colegas Clarice, Flávia e Larissa, pelo seu auxílio durante a fase de elaboração do projeto de monografia.

Por fim, agradeço aos membros da banca, professor Me. Adriano Trindade e professor Me. Fernando Feitosa, por aceitarem prontamente o convite para examinar este trabalho.

FICHA CATALOGRÁFICA

BB522r Bernardes, Jade

Regulação de risco na lei geral de proteção de dados: análise de variáveis jurídicas relacionadas ao modelo teórico da regulação do risco sob o enfoque do modelo TLICS. / Jade Bernardes; orientador Marcio Iorio Aranha. -- Brasília, 2022.

77 p.

Monografia (Graduação - Direito) -- Universidade de

Brasília, 2022.

1. Lei Geral de Proteção de Dados Pessoais. 2. Regulação de risco. I. Iorio Aranha, Marcio , orient. II. Título.

REFERÊNCIA BIBLIOGRÁFICA

BERNARDES, J. C. R. (2022). Regulação de risco na lei geral de proteção de dados: análise de variáveis jurídicas relacionadas ao modelo teórico da regulação do risco sob o enfoque do modelo TLICS. Monografia Final de Curso, Faculdade de Direito, Universidade de Brasília, Brasília, DF, p. 77.

Sumário

INTRODUÇÃO..... 1

CAPÍTULO 1 – EVIDÊNCIAS DA EMERGÊNCIA DE UM MODELO DE PROTEÇÃO DE DADOS CENTRADO NO RISCO 4

1.1 RELAÇÃO ENTRE O MODELO TEÓRICO DA REGULAÇÃO DO RISCO E PROTEÇÃO DE DADOS NA LEGISLAÇÃO EUROPEIA..... 5

1.1.1 Regime de regulação do risco 8

1.1.2 Elementos componentes de um regime de regulação do risco na legislação europeia.....11

1.1.3 Orientações relativas às decisões automatizadas e definição de perfis do Grupo de Trabalho do Artigo 29.º 16

1.1.4 Regulação baseada no risco 21

1.1.5 Regulação baseada no risco na legislação europeia.....23

1.1.6 Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento.....25

1.2 EVIDÊNCIAS DE UM MODELO CENTRADO NO RISCO NA LEGISLAÇÃO BRASILEIRA 32

1.2.1 Lei nº 8.078/1990 - Código de Defesa do Consumidor.....33

1.2.2 Lei nº 12.214/2014 - Marco Civil da Internet.....40

CAPÍTULO 2 - RELAÇÃO ENTRE A LEI GERAL DE PROTEÇÃO DE DADOS E O MODELO TEÓRICO DA REGULAÇÃO DO RISCO, COM O USO DO MODELO TLICS..... 46

2.1 MODELO TLICS..... 46

2.2 VARIÁVEIS JURÍDICAS RELACIONADAS AO MODELO TEÓRICO DA REGULAÇÃO DO RISCO NA LGPD..... 49

2.2.1 Variáveis relacionadas ao regime de regulação do risco..... 49

2.2.2 Variáveis relacionadas à regulação baseada no risco..... 60

2.3 COMPARAÇÃO ENTRE LGPD E RGPD QUANTO ÀS VARIÁVEIS DO RISCO..... 65

CONCLUSÃO..... 69

REFERÊNCIAS BIBLIOGRÁFICAS..... 72

Resumo

O presente trabalho se dedica a investigar as relações existentes entre a regulação de risco e a proteção de dados no Brasil. Para isso, busca-se identificar elementos da regulação baseada em riscos e do regime da regulação do risco na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados). Como suporte teórico, utilizam-se as teorias da regulação baseada em riscos e do regime da regulação do risco para avaliar o processo de "risquificação" da proteção de dados. Além dessas teorias, usa-se o Modelo TLICS para identificar variáveis jurídicas relacionadas à regulação do risco e à regulação baseada no risco. Assim, primeiro demonstram-se evidências do processo de "risquificação" da proteção de dados na Europa, por meio da análise de elementos da regulação do risco no Regulamento Geral de Proteção de Dados e em outros dispositivos normativos. Ademais, apontam-se elementos que sugerem a abertura para um modelo de regulação do risco na em normas brasileiras que regulavam o tratamento de dados antes da LGPD - a Lei nº 12.965/16 (Marco Civil da Internet) e a Lei nº 8.078/90 (Código de Defesa do Consumidor). Em seguida, com o auxílio do Modelo TLICS, são identificadas variáveis jurídicas relacionadas ao regime de regulação de risco e à regulação baseada em riscos para verificar se a Lei Geral de Proteção de Dados reflete um processo de "risquificação" semelhante ao observado na legislação europeia.

Palavras-chaves: Privacidade; Proteção de dados; Regulação do risco; Regulação baseada no risco.

Abstract

This final project investigates the relationship between risk regulation and data protection in Brazil. We identify elements of risk-based regulation and risk regulation regime in Law 13,709/2018 (General Data Protection Law). The theories of risk-based regulation and risk regulation regime are used to evaluate the "riskification" of data protection. Besides, the TLICS Model is used to identify commensurable legal variables related to risk regulation and risk-based regulation. First, we expose the signs of the "riskification" of data protection in Europe, which can be perceived in the General Data Protection Regulation and other normative statements. We also denote elements that suggest an open to a risk regulation in Brazilian laws that regulated data protection before the GDPL - Law 12.965/16, known as Marco Civil da Internet, and Law 8.078/90 (Consumer Protection Code). Finally, we identify the legal variables related to risk regulation and risk-based regulation to measure the "riskfication" in the General Data Protection Law.

Keywords: Privacy; Data Protection; Risk regulation; Risk-based regulation.

Lista de Figuras

Figura 1	–	Ilustração de processo iterativo genérico para realização de uma AIPD	30
Figura 2	–	Diagrama com a metodologia, teorias de suporte e ferramentas operacionais do Modelo TLICS.....	47

Lista de Tabelas

Tabela 1 – Categorias de perfis de consumidores..... 19

Tabela 2 – Resumo sobre a AIPD..... 31

Tabela 3 – Resumo sobre as obrigações do controlador em contexto de realização de uma AIPD..... 32

Tabela 4 – Princípios identificados na LGPD..... 52

Tabela 5 – Bases legais identificadas na LGPD..... 55

Tabela 6 – Bases legais para tratamento de dados sensíveis identificadas na LGPD..... 56

Tabela 7 – Variáveis jurídicas relacionadas aos elementos componentes de um regime de regulação de risco identificadas na LGPD 60

Tabela 8 – Variáveis jurídicas relacionadas a regulação baseada no risco identificadas na LGPD..... 64

Lista de siglas e abreviaturas

AIPD *Avaliação de Impacto sobre a Proteção de Dados*

CDC *Código de Defesa do Consumidor*

LGPD *Lei Geral de Proteção de Dados*

RGPD *Regulamento Geral sobre a Proteção de Dados*

TLICS *Telecommunications Law Indicators for Comparative Studies*

INTRODUÇÃO

As discussões sobre o direito à privacidade mantêm relação próxima com o desenvolvimento tecnológico. As novas técnicas e instrumentos influenciaram de tal modo a esfera privada que motivaram os primeiros debates doutrinários acerca do tema (MENDES, 2014). Essa relação - entre privacidade e tecnologia – intensificou-se com revolução técnico-informacional, que consolidou uma sociedade em rede, na qual as atividades de coleta, transferência e uso de dados são essenciais (WILSON, 2006). Assim, o direito à privacidade transformou-se para incluir a proteção de dados pessoais e responder aos desafios emergentes do crescente tratamento informatizado de dados (DONEDA, 2006).

Nesse contexto, surgem as primeiras normas de proteção de dados pessoais (MENDES, 2014). Essa primeira geração de legislações preocupava-se com a criação e o controle dos bancos de dados centrais. A próxima a geração abandona o enfoque nos bancos de dados e se dedica a garantir a escolha do cidadão em fornecer ou não seus dados pessoais, logo entende a privacidade como uma liberdade negativa. A terceira geração supera essa perspectiva ao ampliar as liberdades do cidadão para buscar a efetividade da participação do indivíduo no processo de tratamento dos dados e consolida a autodeterminação informativa como aspecto central da proteção de dados pessoais (DONEDA, 2020). Esse modelo regulatório, centrado na autodeterminação informacional, predomina nas atuais legislações de proteção de dados pessoais, porém, diante dos avanços tecnológicos, surgem questionamentos acerca da necessidade de uma alteração em sua moldura teórica.

As novas tecnologias da informação criam um cenário de incerteza ao potencializarem a assimetria informacional e possíveis consequências negativas à privacidade e a outros direitos fundamentais. Big Data, Internet das Coisas, Reconhecimento Facial, Sistemas de I.A. e decisões automatizadas são exemplos de tecnologias capazes de facilitar atividades cotidianas, mas também que trazem riscos e ameaças à privacidade e às garantias individuais. Dessa forma, os avanços nos sistemas de inteligência artificial ensejam dúvidas quanto à implementação de uma regulação capaz de equilibrar a necessidade de *accountability* com os benefícios gerados pela aplicação desses sistemas (DOSHI-VELEZ e KORTZ, 2017). As decisões

automatizadas, cada vez mais presentes no cotidiano, afetam as esferas pessoal e profissional do indivíduo o que torna necessária a previsão legal de novos direitos para garantir a proteção à privacidade, como o direito à explicação e à revisão de decisões automatizadas (MONTEIRO, 2018).

A definição de perfis é outra fonte de riscos a direitos, uma vez que pode contribuir para a discriminação de determinados grupos e perpetuação de desigualdades (ZANATTA, 2019; PASQUALE, 2015). Além das possíveis violações de direitos, a assimetria informacional aumenta, pois, os riscos tornam-se menos cognoscíveis e mais difíceis de controlar diante da superioridade informacional dos responsáveis pelo tratamento de dados em relação aos demais agentes (BIONI; LUCIANO, 2019).

Com base nesse cenário de incertezas e riscos, defende-se uma gradual mudança no centro da regulação da proteção de dados pessoais. Nesse sentido, Kurner identifica o Regulamento Geral de Proteção de Dados como uma "revolução Copernicana na legislação europeia de proteção de dados pessoais" (KURNER, p. 14, 2012). Antes da mudança legislativa, indícios da "risquificação" da proteção de dados pessoais poderiam ser observados no julgamento casos a C-293/12 e C-594/12 "*Digitals Rights Ireland and Seitlinger and others*", apreciados pela Corte Europeia, em que se verifica a adoção de uma perspectiva baseada em riscos para assegurar a proteção de direitos fundamentais em face da coleta massiva de dados (SPINA, 2014).

Esse gradual processo de "risquificação" da legislação de proteção de dados pessoais na Europa é identificado por dois elementos principais: a) o reconhecimento da proteção de dados pessoais como um regime de regulação de risco, dado que surge como uma resposta aos riscos à privacidade e a direitos fundamentais decorrentes do desenvolvimento tecnológico (GELLERT, 2015; SPINA, 2017) b) a adoção de instrumentos da regulação baseada em riscos na nova legislação, o Regulamento Geral de Proteção de Dados (GELLERT, 2015; QUELLE, 2018; MACENAITE, 2017).

Essa discussão sobre a construção de um modelo regulatório centrado nos riscos não é exclusiva de autores europeus. No Brasil, Zannata analisa a emergência de um modelo de regulação de risco (ZANATTA, 2017) e Bioni e Luciano estudam a possibilidade de as leis gerais de proteção de dados serem uma abertura para aplicação do princípio da precaução - elemento característico da regulação de risco (BIONI;

LUCIANO, 2019). É nesse âmbito que se situa o presente trabalho, que se dedicou a investigar as relações existentes entre a regulação de risco e a proteção de dados no Brasil. Para isso, os esforços se concentraram na identificação de elementos da regulação baseada em riscos e do regime da regulação do risco na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).

Embasaram a presente pesquisa as teorias da regulação baseada em riscos, que prioriza ações regulatórias de acordo com os riscos apresentados pelos agentes (BALDWING; CAGE; LODGE, 2012), e do regime de regulação de risco, que se concentra nos processos básicos de reunião de informação e cognição de riscos, criação de regras e padrões de conduta, *enforcement* e monitoramento da modificação do comportamento social (BALDWING; HOOD e ROTHSTEIN, 2001). De forma mais específica, na aplicação dessas teorias na proteção de dados pessoais desenvolvida por Rapahel Gellert, Claudia Quelle e Milda Macenaite (GELLERT, 2015; QUELLE, 2018; MACENAITE, 2017).

Além dessas teorias de referência, recorreu-se, como papel instrumental, ao Modelo TLICS, baseado na hermenêutica prescritiva, na teoria institucional do direito e no conceito de garantias institucionais (ARANHA, 2011; MENDES, L. S.; BIONI, B. R.; OLIVEIRA, F. M. G. S.; LIMA, J. A. de O.; ARANHA, M. I, 2019). Com esse suporte teórico, busca-se responder a seguinte pergunta de pesquisa: Qual a relação existente entre o modelo teórico de regulação do risco - representado pelo regime de regulação do risco e pela regulação baseada em riscos - e a Lei Geral de Proteção de Dados Pessoais?

Com a análise e comparação da LGPD e do RGPD, por meio das variáveis jurídicas identificadas com o uso do Modelo TLICS, o objetivo do trabalho era demonstrar a tendência de adoção do regime de regulação do risco e da regulação baseada no risco no modelo regulatório brasileiro de proteção de dados pessoais. Outra alternativa era que não houvesse previsão suficiente de mecanismos de gerenciamento de risco na legislação brasileira, ou que estes não fossem compatíveis pelos adotados pelo regulamento europeu.

Para enfrentar essa problematização, utilizou-se como base empírica a Lei Geral de Proteção de Dados, o Regulamento Geral de Proteção de Dados, o Marco civil da

Internet, o Código de Defesa de Consumidor e outros dispositivos normativos europeus aptos a comprovar o processo de "risquificação" – "Orientações sobre a Avaliação de Impacto de Privacidade (AIPD) e sobre quando determinar quando o processamento "pode resultar em um alto risco" para os efeitos do Regulamento (EU) 2016/679"; e "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679". Ressalte-se que a LGPD e o RGPD foram o foco da análise, sendo as outras normas – brasileiras e estrangeiras – usadas para levantar evidências de abertura para um modelo de regulação do risco.

Esta monografia estruturou-se da seguinte forma: a) no primeiro capítulo, foram abordadas evidências da emergência de um modelo de regulação de risco na proteção de dados pessoais. Assim, apresentam-se os mecanismos de gerenciamento de riscos adotados pelo Regulamento Geral de Proteção de Dados que demonstram a passagem de um modelo centrado na autodeterminação informacional para um com enfoque na regulação do risco. Ademais, foram utilizados outros dispositivos normativos para evidenciar o processo de "risquificação"; b) no segundo capítulo, identificam-se as variáveis jurídicas que demonstram a "risquificação" da proteção de dados pessoais, as quais são usadas para comparação entre as leis gerais de proteção de dados da União Europeia e do Brasil e averiguar se a LGPD adota uma perspectiva baseada em riscos do mesmo modo que o RGPD; c) com isso, concluiu-se que a LGPD apresenta disposições que possibilitam reconhecer a proteção de dados no Brasil como um regime de regulação de risco e que revelam a adoção de ferramentas da regulação baseada no risco. Isso permite afirmar que também se encontram evidências da emergência de um modelo centrado no risco entretanto, quando é feita a comparação com o RGPD, demonstre-se que no Brasil o processo de "risquificação" ocorre em um grau menor do que o verificado na legislação europeia.

CAPÍTULO 1 – EVIDÊNCIAS DA EMERGÊNCIA DE UM MODELO DE PROTEÇÃO DE DADOS CENTRADO NO RISCO

Nesse primeiro capítulo, abordam-se evidências que demonstram a emergência de um modelo de regulação de risco na proteção de dados pessoais. Adota-se a perspectiva de que, com o Regulamento Geral de Proteção de Dados, opera-se uma mudança pautada em dois níveis relacionados ao risco: regime de regulação de risco e regulação baseada no risco (MACENAITE, 2017).

Primeiramente, apresentam-se as características e os elementos que compõem um regime de regulação do risco e analisa-se o Regulamento Geral de Proteção de Dados pessoais para identificá-los a fim de caracterizar a regulação da proteção de dados como tal regime. Ademais, destaca-se a Orientação do Conselho Europeu para definição de perfis como outro indicativo da relação entre regulação do risco e proteção de dados.

Em seguida, concentram-se os esforços no outro nível da mudança: a regulação baseada em risco. Após uma breve explicação teórica dessa forma de regulação, utiliza-se o Regulamento Geral de Proteção de Dados (RGPD) para demonstrar os indicativos do surgimento de um modelo de proteção de dados pessoais centrado no risco. Para aprofundar esse estudo, recorre-se à Orientação para Avaliação de Impacto de Proteção de Dados (AIPD).

Após apresentar as evidências da "risquificação" da proteção de dados, que é considerado um processo eminentemente europeu conforme consenso na doutrina (ZANATTA, 2017), inicia-se a investigação acerca da possibilidade de ocorrência do fenômeno no Brasil. Antes de se buscar esses indicativos da na Lei Geral de Proteção de Dados (LGPD), verifica-se o papel do risco em legislações anteriores e que continuam a complementar à lei geral – o Código de Defesa do Consumidor e o Marco Civil da Internet.

1.1 RELAÇÃO ENTRE O MODELO TEÓRICO DA REGULAÇÃO DO RISCO E PROTEÇÃO DE DADOS NA LEGISLAÇÃO EUROPEIA

Primeiro, cabe estabelecer o contexto em que se analisa a relação entre o modelo teórico da regulação do risco e a proteção de dados. Nos últimos anos, surgiram estudos na Europa, principalmente na Bélgica, Holanda e Inglaterra, sobre uma nova perspectiva da proteção de dados pessoais, baseada na regulação do risco (ZANATTA, 2017).

Nesse sentido, investiga-se a passagem para um modelo de proteção de dados pessoais com enfoque no risco. Destaca-se que essa mudança ocorre no campo teórico, isto é, como uma nova moldura teórica para se analisar debates relacionados à proteção de dados pessoais e não para substituir a matriz de direitos e garantias fundamentais

(ZANATTA, 2017). Assim, busca-se verificar se a legislação brasileira possibilita que seja feita essa interpretação, de modo semelhante à abordagem baseada no risco verificada na legislação europeia.

Esse destaque deve ser feito porque existem dúvidas sobre a crescente centralização do papel do risco na legislação de dados pessoais, especialmente sobre os seus efeitos nos direitos dos titulares de dados. Para esclarecer isso, recorre-se a um parecer do Grupo de Trabalho do Artigo 29.º[1] sobre o papel da regulação baseada em riscos na legislação de proteção de dados pessoais, realizado em meio às discussões que precederam à reforma legislativa.

Nesse documento, explicita-se que a abordagem baseada no risco consiste em uma forma flexibilizar a regulação de proteção de dados no sentido de utilizar o risco para escalar a *compliance*. Desse modo, as obrigações do controlador e a forma de registro das operações de tratamento de dados variam de acordo com o risco envolvido. Entretanto, esclarece-se que os direitos dos titulares de dados e os princípios fundamentais devem respeitados independentemente do grau de risco da atividade (GRUPO DE TRABALHO DO ARTIGO 29.º, 2014).

Segundo o Grupo de Trabalho do Artigo 29.º, os riscos devem ser avaliados segundo a gravidade e a probabilidade de afetar direitos e liberdades fundamentais, e também conforme critérios objetivos - como a natureza do dado pessoal, a categoria do titular de dados e o número de titulares de dados afetados (GRUPO DE TRABALHO DO ARTIGO 29.º, 2014). No parecer também se apresentam medidas adicionais a serem tomadas em caso de operações de elevado risco e, dessa forma, introduz mecanismos de gerenciamento de risco que constam no RGPD.

[1] O Grupo de Trabalho do Artigo 29.º (GT ART. 29.º) consistia em um grupo de trabalho europeu independente que era responsável pelas questões relacionadas à proteção de dados pessoais – suas tarefas estavam descritas no artigo 30 da Diretiva 95/46/EC e no artigo 15 da Diretiva 2002/58/EC - até 25 de maio de 2018, quando o RGPD começou a vigorar. A partir disso, suas atividades passaram a ser de responsabilidade do Comité Europeu para a Proteção de Dados (CEPD), o qual é composto por representantes nacionais para proteção de dados e pela Autoridade Europeia de Proteção de Dados (AEPD). Entre outras funções, o Comité fornece orientação acerca da legislação europeia de proteção de dados, na forma diretrizes, recomendações e melhores práticas sobre o RGPD.

Além disso, o GT ART. 29.º apresenta diversos dispositivos do rascunho do RGPD relacionados à regulação baseada no risco, como a avaliação de impacto e a previsão de *privacy by design*, e aborda as funções a serem desenvolvidas pela autoridade de proteção de dados: atualizar lista de atividades que apresentam riscos determinados, desenvolver orientações sobre outras ferramentas de prestação de contas, procedimentos de reforço em caso de não cumprimento e direcionar ações para áreas com maiores riscos (GRUPO DE TRABALHO DO ARTIGO 29.º, 2014).

Esses aspectos centrais do parecer demonstram que a abordagem baseada no risco estava no cerne da elaboração da nova legislação europeia de proteção de dados pessoais de modo a representar uma mudança na forma de interpretar e aplicar as suas normas, sem isso implique em um prejuízo à garantia de direitos fundamentais dos titulares de dados.

Nessa senda, diversos autores investigam essa mudança na moldura teórica da regulação da proteção de dados. Alessandro Spina foi o primeiro deles a se referir a esse processo como "risquificação" da legislação de proteção de dados pessoais. Esse termo foi retirado de estudos no campo da segurança e proporciona percepções que interessam à proteção de dados, principalmente quando relacionadas a riscos da segurança da informação (MACENAITE, 2017). Entre essas percepções, encontram-se os desafios enfrentados diante de cenários em que predominam incertezas, a aplicação princípio da precaução, a identificação dos agentes que classificam o risco de uma atividade e mecanismos de gerenciamento de risco (CLAPTON, 2011; CORRY, 2012;).

Spina afirma que se observa uma gradual "risquificação" na legislação europeia de proteção de dados e que essa mudança se direciona a um modelo de auto-regulação para gerenciar inovações tecnológicas em cenários em que predominam a incerteza. Para Spina, a "risquificação" é muito mais complexa e profunda do que uma abordagem mais flexível para garantir o cumprimento da lei, pois postula que as disposições do RGPD fornecem ferramentas para que os riscos sejam controlados e mitigados (SPINA, 2017).

Outro autor que analisa a relação entre regulação de risco e proteção de dados nas mudanças legislativas ocorridas na União Europeia é Raphäel Gellert, que aponta

os seguintes indicativos para comprovar sua tese: a recomendação de 2010 do Conselho da Europa de que a definição de perfis pode levar a "riscos significantes para liberdades e direitos individuais"; o relatório sobre a aplicação dos princípios da Convenção 108 sobre coleta e tratamento de dados biométricos, que sustenta a necessidade do uso do princípio da precaução, o qual pertence ao campo da regulação do risco (GELLERT, 2015; ZANATTA, 2017).

Percebe-se que o foco desses estudos são o Regulamento Geral de Proteção de Dados Pessoais e a adoção de uma abordagem baseada no risco nele. Por isso, reconhece-se esse processo gradual de "risquificação" da proteção de dados pessoais como eminentemente europeu (ZANATTA, 2017).

Diante desse contexto, percebe-se relação entre risco, regulação e proteção de dados pessoais enseja diversas discussões e questionamentos, o que justifica a existência de diferentes abordagens do tema. Nesse sentido, Claudia Quelle observa que:

> O "risco" e a proteção de dados encontram-se de muitas formas. Embora haja um consenso aproximado sobre a significado da abordagem baseada no risco, esta é facilmente confundida com uma série de outros usos do "risco". Deve ser cuidadosamente distinguida da regulação do risco, regulação baseada no risco, meras avaliações de conformidade assim como da pura análise de risco ou gerenciamento do risco. (QUELLE, 2018, p. 508, tradução nossa)

Destarte, o presente trabalho adota as perspectivas de regulação do risco e regulação baseada no risco, fundamentado nos estudos de Milda Macenaite, segundo a qual houve a "risquificação" do RGPD ocorreu nesses dois níveis (MACENAITE, 2017). Também se recorre aos estudos de Gellert e Quelle para tratar da caracterização da proteção de dados como um regime de regulação do risco e para tratar da nova ótica de prestação de contas e *compliance* no RGPD. (GELLERT, 2015; QUELLE, 2018).

1.1.1 Regime de regulação do risco

Primeiro, apresenta-se a relação entre a regulação de risco e a proteção de dados. Raphäel Gellert caracteriza proteção de dados pessoais é um regime de regulação de riscos desde sua origem, porquanto se constitui como uma forma de intervenção na sociedade a fim de controlar potenciais efeitos negativos de uma atividade que se situa em um contexto de incertezas. No caso, a proteção de dados é um meio para enfrentar

os riscos, provocados pelo desenvolvimento tecnológico, à privacidade e a outros direitos e liberdades dos indivíduos (GELLERT, 2015).

A primeira geração de leis de proteção de dados confirma essa caracterização, uma vez que o foco dessas normas era controlar o uso da tecnologia diante da preocupação com a coleta e armazenamento de dados dos cidadãos pelo governo, devido ao crescimento da burocracia, e por grandes corporações. A utilização de computadores e banco de dados gerou tamanho temor que essas primeiras legislações destinavam seus esforços ao aspecto funcional do tratamento de dados, para regular essa tecnologia, de modo que os direitos individuais da privacidade eram colocados em segundo plano (MAYER-SCHÖNBERGER, 1998).

O atual nível de desenvolvimento tecnológico é um dos fatores que podem justificar a perspectiva da proteção de dados pessoais como uma regulação do risco. As ameaças e inseguranças trazidas pela modernização contribuíram para a constituição de uma sociedade do risco (BECK, 1992). Assim, se no passado os riscos e ameaças aos indivíduos decorriam da falta de tecnologia, hoje eles provêm do excesso de tecnologia (BECK, 1992).

Nesse contexto, as novas tecnologias da comunicação e da informação justificam a afirmação de que houve um crescimento das ameaças à privacidade, tanto em número quanto em nível de gravidade. A proteção de dados pessoais almeja assegurar a privacidade e, desse modo, tutelar a personalidade dos indivíduos. A relação entre proteção de dados e privacidade é tão próxima atualmente que é difícil analisá-las separadamente.

A privacidade pode ser ameaçada e violada de formas diversas, de acordo com Westin: vigilância física, vigilância psicológica e vigilância de dados (WESTIN, 1967). Além disso, outros autores se referem a mais direitos que podem ser ameaçados, como Vance Packard que aponta para os riscos aos direitos de ser diferente, de esperar pela tolerância ou perdão ou erros e de um novo começo (PACKARD, 1964). Portanto, isso evidencia como violações à privacidade podem afetar diferentes esferas da vida de um indivíduo.

Essas ameaças se potencializaram com a evolução tecnológica. Em 2015, um relatório da Comissão Federal de Comércio dos Estados Unidos (FTC) apresentou os

riscos aos consumidores trazidos por dispositivos com tecnologia IoT - Internet das Coisas. Identificaram-se esses dispositivos como dotados de um elevado potencial de riscos à segurança em razão de possibilitarem o acesso não autorizado a informações pessoais ou seu uso inadequado, facilitarem ataques em outros sistemas e criarem riscos de segurança. Além disso, como os dispositivos com tecnologia IoT coletam diversos dados, também geram riscos à privacidade. Inclusive pode haver a coleta de informações sensíveis, como geolocalização, informações de saúde e dados financeiros. Os dados dos consumidores são coletados de forma massiva e, se por um lado possibilitam que sejam realizadas inferências que podem trazer benefícios ao consumidor, por outro podem ser usadas de forma inadequada. O relatório também aponta possíveis usos desses dados para orientar decisões de empresas, como análises de crédito, seguro e até seleção de empregados. Nesse sentido, preocupa-se a possibilidade de sua utilização sistemática contra determinados grupos e com fins discriminatórios (FEDERAL TRADE COMMISSION, 2015).

Além disto, uma questão importante dentro dessa temática é a coleta de dados durante atividades desenvolvidas na internet, sendo que esses dados podem ser submetidos a tratamentos de modo a revelar outras informações, inclusive sobre aspectos sensíveis da personalidade.

Nessa perspectiva, há diversos estudos que se dedicam a investigar como as informações compartilhadas em redes sociais podem ser usadas. Um deles demonstra que as curtidas do Facebook podem ser utilizadas para predizer automaticamente e de forma acurada aspectos da vida privada de um indivíduo que geralmente não são compartilhados. Registros básicos de comportamentos humanos em redes sociais podem ser usados para estimar corretamente informações sensíveis sobre a vida pessoal das pessoas. Entre os atributos selecionados, encontraram-se: orientação sexual, origem étnica, opiniões políticas, religião, personalidade, inteligência, satisfação com a vida, se os pais permaneceram juntos até a idade de 21 anos (BACHRACH, KOSINSKI, *et al.*, 2012).

Segundo os pesquisadores, essas predições contribuem para melhorar produtos e serviços, com uma personalização maior destes. Entretanto, destacam-se suas possíveis consequências negativas, que incluem ameaças ao bem-estar liberdade e até

a vida. É fundamental para compreender a extensão desses riscos que essas informações são coletadas sem que os indivíduos tenham consentido ou tenham sido notificados (BACHRACH, KOSINSKI, *et al.*, 2012).

Ademais, dados, fornecidos diretamente pelos indivíduos ou coletados de forma semelhante à descrita acima – comportamento em redes sociais, por exemplo, podem ser utilizados para a definição de perfis. Esses perfis podem ser usados para orientar decisões em diversas áreas, desde análises para concessão de empréstimos até para seleção para uma vaga de trabalho (ZANATTA, 2019).

Esses foram apenas alguns exemplos, que demonstram que o ritmo do desenvolvimento tecnológico impõe desafios cada vez maiores no campo da privacidade e da proteção de dados. Após apresentar alguns dos riscos trazidos pelas novas tecnologias no campo da privacidade e da proteção de dados, resta demonstrar os elementos que permitem classificar a proteção de dados como um regime de regulação do risco, conforme a definição de Hood, Hothstein e Baldwin para regime de regulação de risco e seus elementos componentes.

1.1.2 Elementos componentes de um regime de regulação do risco na legislação europeia

A regulação de risco é definida como uma forma de intervenção governamental, por meio de processos de mercado e sociais, a fim de exercer o controle sobre riscos à saúde (HOOD, HOTHSTEIN e BALDWIN, 2001). Apesar de inicialmente se usar esse modelo regulatório em áreas relacionadas à saúde, verificou-se sua expansão para outras áreas. Nesse sentido, Hood Hothstein e Baldwin investigam como esses regimes de regulação de risco se estruturam e funcionam (HOOD, HOTHSTEIN e BALDWIN, 2001).

Hood, Hothstein e Baldwin explicitam que inexiste um modelo uniforme de um regime de regulação de risco, uma vez que sua configuração varia de acordo com as estruturas regulatórias, instituições, cultura e contexto de cada país. Entretanto, em seus estudos sobre diferentes regimes de regulação de risco, evidenciam três elementos presentes em todo regime de regulação do risco: I. criação de regras e padrões de conduta (*standard-setting*); II. reunião de informações e cognição de riscos (*information-gathering/monitoring*); 3. *enforcement* e monitoramento da modificação

do comportamento social (*behaviour-modification/control*) (HOOD, HOTHSTEIN e BALDWIN, 2001).

O primeiro elemento consiste em estabelecer padrões, objetivos, metas e orientações para definir as condições em que a atividade regulada é considerada segura. Muitos estudos sobre o risco concentram seus esforços nesse elemento, pois é o responsável por fornecer valores e níveis aceitáveis de risco bem como tratar de sua distribuição. Existem diversas formas de definir padrões e os regimes também podem adotar formas combinadas (HOOD, HOTHSTEIN e BALDWIN, 2001).

Hood, Hothstein e Baldwin apresentam alguns exemplos: I. simples direções*:* padrões definidos por julgamento direto e geralmente não separado de outros componentes; II. controle homeostático: especificam-se níveis de risco em termos quantitativos e qualitativos de modo a manter o sistema nesse nível ou abaixo; III. padrão de calibração*:* objetivos contrários são mantidos sob alguma tensão e há pontos de equilíbrio (HOOD, HOTHSTEIN e BALDWIN, 2001).

A reunião de informações e cognição de riscos é essencial para esses os regimes de regulação, porquanto a noção de risco abrange conhecer perigos e ameaças de forma a usar esse conhecimento para controlá-los (GELLERT, 2015). O risco auxilia decisões sobre eventos futuros, que são caracterizados pela incerteza, por meio da formação de conhecimento de modo a transformar sua incerteza característica em certeza e possibilitar o seu controle. Utilizam-se estatísticas e probabilidades para atingir esse fim (GELLERT, 2015).

Portanto, a reunião de informações é fundamental para gerar o conhecimento necessário para compreender e controlar os riscos e pode ser feita por métodos distintos, como demonstram Hood, Hothstein e Baldwin: I. ativo: os próprios reguladores verificam o ambiente e buscam e reúnem informações; II. reativo: reguladores dependem de outros atores para coletar as informações; III. interativo: método intermediário entre os dois anteriores e no qual os reguladores impõem relatórios periódicos a outros atores e pautam suas ações no conteúdo deles (HOOD, HOTHSTEIN e BALDWIN, 2001).

O terceiro elemento - *enforcement* e monitoramento da modificação do comportamento social - é bastante desafiador, pois envolve a problemática de como

modificar o comportamento de indivíduos e organizações. Os autores apontam como desafios a possibilidade de preferências e estruturas de incentivo causarem distorções e as influências de crenças e atitudes dos regulados nos resultados das medidas que visam ao controle e à alteração de comportamentos (HOOD, HOTHSTEIN e BALDWIN, 2001).

A partir desses elementos, Hood, Hothstein e Baldwin realizaram um amplo estudo comparativo de regimes de regulação de risco, com uma variedade de objetos regulados, como gás rádon em casa e em locais de trabalho, benzeno no ar e em locais de trabalho, segurança em estradas locais e exposição a pesticidas presentes na água e em alimentos (HOOD, HOTHSTEIN e BALDWIN, 2001). Como o foco desse trabalho é utilizar os três elementos componentes para caracterizar a proteção de dados como um regime de regulação de risco, não se abordam os parâmetros usados pelos autores na comparação de diferentes regimes.

Com base nesse referencial teórico, Gellert identifica esses três elementos na Diretiva 95/46/CE. Primeiro, a criação de padrões e regras de conduta seriam representadas pelos dispositivos que estabelecem os princípios e as bases legais, dado que os dois determinam as condições de um tratamento seguro de dados. Na Diretiva, eles estão previstos no artigos 6º, que contém os princípios, e no artigo 7º, que estabelece as bases legais para o tratamento de dados[2] (GELLERT, 2015). No RGPD, os princípios e as bases legais se encontram, respectivamente nos artigos 5º e 6º.

A reunião de informações e cognição de riscos é representada pelas obrigação dos controladores[3] de notificar a autoridade de proteção de dados antes da realização do tratamento de dados e informar determinados aspectos da atividade desenvolvida,

[2] O conceito de tratamento de dados pessoais abrange qualquer operação ou conjunto de operações realizada sobre dados pessoais, "tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição", como consta no artigo 4º (2) do RGPD (UNIÃO EUROPEIA, 2016, p. 33).

[3] Controlador é a pessoa física ou jurídica responsável por determinar as finalidades e os meios da atividade de tratamento de dados pessoais (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE, 2018).

como a identidade do processador[4], a finalidade do tratamento e as categorias de titulares de dados e de destinatários (GELLERT, 2015). A previsão da notificação à autoridade constava no artigo 18 e o seu conteúdo estava no artigo 19 da Diretiva. No RGPD, extinguiu-se essa obrigação geral de notificação para substitui-la por regras que se baseiam no risco do tratamento de dado para definir se a notificação é obrigatória, conforme o Considerando 89[5]. Essa mudança evidencia a presença abordagem baseada no risco no RGPD, que se encontra na seção 1.1.4 deste trabalho.

Os artigos 21.1 e 21.2 da Diretiva também são identificados como representantes do segundo elemento componente, uma vez que estabelecem a obrigação de publicar as operações de tratamento de dados realizadas por meio da divulgação de um registro (GELLERT, 2015). No RGPD, o registro de atividades de tratamento se encontra no artigo 30.

Por fim, Gellert reconhece restrições, medidas preventivas e regime de responsabilidade como disposições de *enforcement* e monitoramento da modificação do comportamento social, pois são formas de se buscar controlar e garantir a implementação das regras e padrões estabelecidos de modo a se verificar a mudança do comportamento dos regulados.

Em primeiro lugar, há as restrições, expressas nos artigos 8º e 16. O artigo 8º proíbe o tratamento de dados sensíveis, o qual só é permitido nos casos elencados pela Diretiva – artigo 8.2. Essa previsão legal revela uma abordagem preventiva no sentido de estabelecer uma proibição geral para o tratamento desses dados em virtude do seu

[4] Processador é a pessoa física ou jurídica que realiza o tratamento de dados, em nome do controlador, e segue as instruções estabelecidas (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE, 2018).

[5] Considerando (89): "A Diretiva 95/46/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controle. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento. " (UNIÃO EUROPEIA, 2016, p.17)

potencial de causar danos a direitos e liberdades dos indivíduos. O artigo 16, para garantir a confidencialidade dos dados, veda o seu tratamento por qualquer pessoa que atue em nome do controlador, do subcontratante, ou até mesmo o próprio subcontratante, sem que haja autorização do controlador deste (GELLERT, 2015). No RGPD, essas disposições permanecem nos artigos 9º e 28, respectivamente. Embora haja alterações no artigo 28, persiste a proibição de que o subcontratante realize operação de tratamento sem autorização do controlador.

Em segundo lugar, Gellert reconhece medidas preventivas nos artigos 17 e 20. O artigo 17 consiste em uma disposição geral sobre segurança de tratamento de dados e estabelece que medidas preventivas devem ser tomadas de modo proporcional ao risco e ao seu custo de implementação. O artigo 20 determina obrigação de um exame prévio quando as operações de tratamento de dados apresentam riscos consideráveis a direitos e liberdades do titular de dados (GELLERT, 2015). No RGPD, a disposição geral sobre segurança consta no artigo 32 e a consulta prévia no artigo 36, a qual é obrigatória em atividades de tratamento que apresentam um elevado risco.

Em terceiro lugar, há o regime de responsabilidade, previsto artigo 23, que atribui ao controlador a responsabilidade quando há violação de dados, a menos que ele prove o contrário (GELLERT, 2015). No RGPD, as instruções normativas quanto ao direito de indenização e o regime de responsabilidade se encontram no artigo 82, que dispõe sobre a responsabilidade do controlador e do subcontratante e os isenta de responsabilidade se provarem que não são responsáveis pelo evento que causou o dano.

Além desses elementos componentes, Gellert aponta a transparência, a participação pública e as autoridades independentes como fundamentais para um regime de regulação do risco. A transparência é reconhecida como característica essencial a qualquer estrutura de regulação de riscos e como uma forma de viabilizar que o titular de dados participe ativamente de atividades relacionadas ao tratamento de seus dados (GELLERT, 2015).

Na Diretiva, a transparência e a participação são asseguradas nos artigos 10, 12 (a), 12 (b) e 14 (GELLERT, 2015). No RGPD, as previsões sobre transferência do tratamento de dados constam no artigo 12 e a participação é garantida pelos direitos dos titulares de dados, apresentados nos artigos 15 a 20, como o direito de acesso e o direito

de retificação. Ademais, o Considerando (58) aborda a importância do princípio da transparência para facilitar a compreensão sobre as condições em que se realiza o tratamento de dados[6].

As autoridades administrativas independentes exercem um papel importante no regime de regulação de risco ao suprir a ausência de conhecimento específico existente no governo. Ressalte-se que a expertise e o conhecimento constituem aspectos indispensáveis para coleta de informações e cognição dos riscos (GELLERT, 2015).

O artigo 28 da Diretiva contém a forma de instituição, competências e outras regras para o desempenho de funções das denominadas autoridades de controle. Gellert destaca as previsões sobre a competência consultiva das autoridades em processos legislativos relacionados à proteção de dados, que demonstra o papel de fornecer conhecimento específico, e a elaboração de relatórios periódicos das atividades desenvolvidas pela agência, que é uma forma de disseminar informações e, assim, também contribuir para a participação pública (GELLERT, 2015).

No Regulamento Geral sobre Proteção de Dados, as competências, funções e poderes das autoridades de controle se encontram no artigo 51 e o artigo 52 dispõe sobre sua total independência no desempenho de suas atribuições e no exercício de seus poderes. O dever de publicar relatórios anuais de suas atividades está presente no artigo 59.

1.1.3 Orientações relativas às decisões automatizadas e definição de perfis do Grupo de Trabalho do Artigo 29.º

As Orientações sobre decisões automatizadas e definição de perfis estruturam-se da seguinte forma: 1. Definições, em que são apresentados os conceitos de definição de perfis e decisões automatizadas, bem como sua abordagem pelo Regulamento Geral

[6] Considerando (58), RGPD: "O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado. Essas informações poderão ser fornecidas por via eletrônica, por exemplo num sítio web, quando se destinarem ao público. Isto é especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos, como no caso da publicidade por via eletrônica. (...)" (UNIÃO EUROPEIA, 2016, p. 11).

sobre Proteção de Dados; 2. Previsões gerais sobre definição de perfis e decisões automatizadas, em que aspectos essenciais – princípios, fundamentos legais e direitos dos titulares da proteção de dados são apresentados à luz dessas operações; 3. Previsões específicas para decisões automatizadas, presentes no art. 22 do RGPD.

Primeiro, cabe destacar que a própria elaboração desse documento já é um forte indício da regulação do risco, pois um dos elementos do regime de regulação do risco (HOOD, HOTHSTEIN e BALDWIN, 2001) é o estabelecimento de padrões, que consiste na definição de orientações, diretrizes e parâmetros do que seria considerado uma atividade segura dentro do setor ou operação regulada. Portanto, a elaboração de um documento cuja a principal finalidade é explicar e fornecer condições padrões para um assunto ser tratado é uma expressão desse elemento componente. Além disso, no decorrer do texto é possível identificar outros elementos do regime de regulação do risco. Entretanto, antes disso, é importante apresentar os conceitos essenciais para compreender as disposições do Grupo do Trabalho sobre o tema.

Assim, o conceito de definição de perfis encontra-se no artigo 4º Regulamento Geral sobre Proteção de Dados[7]. As Orientações ressaltam três elementos desse conceito para compreender essa operação: procedimento automatizado, realizado sobre dados pessoais e com o objetivo de analisar dados pessoais do titular dos dados (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018).

Ademais, destacam as deduções estatísticas e a busca por analisar ou realizar predições sobre os indivíduos para sintetizar a definição de perfis da seguinte forma: trata-se da coleta de informações sobre um indivíduo ou grupo para avaliar as características ou padrões de comportamento para colocá-los em uma categoria ou grupo, especialmente com o objetivo de analisá-los e realizar predições (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018).

[7] Art. 4º (4), do RGPD: "definição de perfis: qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (UNIÃO EUROPEIA, 2016, p.33).

As decisões automatizadas possuem uma definição mais sintética e é entendida como a habilidade de realizar decisões por meios tecnológicos e sem a intervenção humana. É uma operação independente da definição de perfis, mas não necessariamente separada, tanto que o RGPD aborda a matéria da seguinte forma: definição de perfis, de forma geral; decisões baseadas na definição de perfis; e somente decisões automatizadas, que incluem a definição de perfis (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018).

O capítulo que trata das previsões gerais para essas atividades é uma clara expressão do elemento criação de regras e padrões, especialmente por apresentar a os princípios e fundamentos legais que devem ser observados na definição de perfis e nas decisões automatizadas. Os princípios e fundamentos legais foram identificados por Gellert como expressão do primeiro elemento componente de um regime de regulação do risco na Diretiva 95/46/CE (GELLERT, 2015).

As Orientações se concentram na legalidade, justiça, transparência, minimização de dados, acurácia e limitação de armazenagem como princípios essenciais para que a definição de perfis e as decisões automatizadas sejam realizadas de forma segura. Cabe ressaltar que, apesar de a seção se dedicar a previsões gerais para decisões automatizadas e definição de perfis, a explicação dos princípios concentra-se na definição dos perfis.

Assim, percebe-se uma preocupação com os riscos da formação de perfis, principalmente os relacionados a um possível uso discriminatório. O Grupo de Trabalho evidencia essa preocupação quando exemplifica as categorias de perfis vendidos por *data broker*[8] a companhias financeiras e a atribuição de score com base na vulnerabilidade econômica para demonstrar o potencial de os perfis serem utilizados para perpetuar desigualdades (ARTICLE 29 DATA PROTECTION WORKING

[8] *Data broker* (uma tradução literal poderia ser ‘corretores de dados’) se refere a indivíduos ou a companhias que vendem dados sobre mercados, empresas, de pessoas físicas, etc. *Data brokers* coletam e vendem informações para diversos propósitos e possuem uma ampla base de clientes que abrange tanto grandes empresas que são referência no setor em que atuam quanto pequenos negócios locais (UNITED STATES SENATE, 2013).

PARTY, 2018). A tabela abaixo representa uma amostra de categorias de perfis de consumidores que são oferecidos a companhias financeiras:

Tabela 1: Categorias de perfis de consumidores

"Burdened by Debt: Singles"	"Struggling Elders: Singles"	"Meager Metro Means"	"Very Elderly"
"Mid-Life Strugglers: Families"	"Retiring on Empty: Singles"	"Relying on Aid: Retired Singles"	"Rolling the Dice"
"Resilient Renters"	"Tough Start: Young Single Parents"	"Rough Retirement: Small Town and Rural Seniors"	"Fragile Families"
"Very Spartan"	"Living on Loans: Young Urban Single Parents"	"Financial Challenges"	"Small Town Shallow Pockets"
"X-tra Needy"	"Credit Crunched: City Families"	"Credit Reliant"	"Ethnic Second-City Strugglers"
"Zero Mobility"		"Rocky Road"	"Rural and Barely Making It"
"Hard Times"			
"Enduring Hardships"			
"Humble Beginnings"			

Tabela retirada de: UNITED STATES SENATE. **A Review of the Data Broker Industry: Collection, Use,and Sale of Consumer Data for Marketing Purposes**. Committee on Commerce, Science, and Transportation. Washington, DC, p. 24. 2013.

Nesse âmbito, deve ser dada uma maior atenção à observância conjunta dos princípios da minimização, limitação de finalidade e limitação de armazenagem. Assim, diante da crescente quantidade de dados coletados pelas organizações, é fundamental justificar a necessidade da coleta de dados e seu tratamento, limitar-se a finalidade inicial e limitar o tempo em que essas informações são mantidas. No contexto da definição de perfis, destaca-se que muitos dos dados utilizados nos perfis não são coletados para esse fim e que o titular não tem ciência disso (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018).

Os fundamentos legais são os mesmos que são aplicados ao tratamento de dados, como consentimento e obrigação legal. Porém, são realizadas algumas considerações em razão da natureza das operações e de suas consequências. Por exemplo, ao definir o fundamento legal do consentimento é ressaltada a importância de que o titular o conceda explicitamente para a definição de perfis ou decisões

automatizadas e que seja informado de forma exata sobre a extensão desse consentimento (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018).

Além do estabelecimento de padrões, o dever dos controladores de fornecer uma explicação clara e simples de como as operações funcionam, bem como os direitos dos titulares de dado à informação e ao acesso aliados são modos de garantir a participação pública, característica essencial em um regime de regulação do risco, conforme Gellert (GELLERT, 2015).

A seção sobre as previsões específicas para decisões automatizadas contém disposições que se correlacionam com o terceiro elemento componente de um regime de regulação do risco – o *enforcement* e monitoramento da modificação de comportamento social. Assim como no RGPD, as Orientações se referem a diversas formas de controle de riscos.

Por exemplo, o artigo 22 do RGPD [9] assegura o direito de o titular de dados não ficar sujeito a decisões tomadas exclusivamente com base em tratamento automatizado. Conquanto o artigo 22 aparente tratar sobre um direito do titular de dados, as Orientações esclarecem que se trata de uma proibição geral a processos de decisões realizados somente com base em meios automatizados, independendo da manifestação do titular de dados para que se concretize (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018). Desse modo, consiste em uma proibição, que é um tipo de *enforcement*, conforme Gellert.

A obrigação de os controladores implementarem medidas para proteger direitos dos titulares de dados, liberdades e interesses legítimos também se correlata com esse elemento. Entre essas medidas, encontram-se: o direito de obter intervenção humana (presente no considerando 71), avaliações frequentes, sistemas para examinar algoritmos e revisões regulares. O Grupo de Trabalho destaca que as atividades que envolvem o tratamento de dados de crianças geram obrigações adicionais em razão de

[9] Art. 22 (1), RGPD: " O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar" (UNIÃO EUROPEIA, 2016, p. 46).

sua vulnerabilidade, como indica o considerando 38 (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018).

Além disso, nas Orientações há um espaço para abordar categorias especiais de dados, garantindo que os dados sensíveis utilizados nas operações de definição de perfis e decisões automatizadas observem os fundamentos legais para o seu tratamento estabelecidos no artigo 9 (2) do Regulamento Geral sobre Proteção de Dados, inclusive para os dados sensíveis obtidos na definição de perfis por processos de inferência (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018). Cabe ressaltar que separar e destacar um tipo de dados conforme sua natureza em razão de ela própria significar um risco maior a direitos e liberdades é uma perspectiva associada à regulação do risco.

Por fim, menciona-se nas Orientações o relatório de avaliação de impacto e a indicação de um encarregado como ferramentas de *accountability* dos controladores. O relatório de avaliação de impacto pode ser utilizado para avaliar riscos em decisões automatizadas e definição de perfis. Além disso, pode auxiliar os responsáveis a identificar medidas a serem tomadas para lidar com riscos a proteção de dados no tratamento (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018).

O Grupo de Trabalho exemplifica algumas medidas que podem ser tomadas: informar a titular de dados sobre a existência e a lógica envolvida nas decisões automatizadas, explicar as consequências previstas para o tratamento de dados, fornecer meios para o titular se opor à decisão e permitir que o titular expresse sua perspectiva (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018).

1.1.4 Regulação baseada no risco

A estrutura de uma regulação baseada no risco varia de acordo com a perspectiva adotada pelos autores. Neste trabalho, a abordagem baseada no risco que tanto Maceinate quanto Quelle usam como referencial teórico é a presente no manual de direito regulatório de Robert Baldwin, Martin Cave e Martin Lodge (QUELLE, 2018; MACENAITE, 2017). Em função disso, nessa seção se ocupa de apresentar os elementos centrais e as características da regulação baseada em risco para esses autores.

Segundo Baldwin, Cave e Lodge, a regulação baseada em riscos tem como premissa básica a inviabilidade de controlar e eliminar todos os riscos e ameaças existentes. Assim, é necessário mapear e avaliar o risco de modo a direcionar a atenção para as atividades que apresentam maior potencial de provocar danos. Por isso, os quadros regulatórios baseados no risco se concentram em controlar riscos relevantes e estabelecer prioridades para facilitar a tomada de decisões ao fornecer uma estrutura lógica para que essas decisões sejam compreendidas (BALDWIN, CAVE e LODGE, 2012).

Um dos motivos para expansão e adoção da regulação baseada no risco em diversas áreas é que ela fornece meio para direcionar o uso de recursos e priorizar a atenção do regulador para áreas em que se encontram os riscos mais elevados por meio de uma estrutura transparência, sistemática e adequada de avaliação de riscos (BLACK e BALDWIN, 2010).

Nessa senda, identificam-se três elementos centrais dessa estrutura regulatória, relacionados a ações do regulador: I. o regulador deve identificar os objetivos e riscos que os regulados podem apresentar; II. o regulador deve desenvolver um sistema para avaliar riscos e estabelecer seus níveis; III. esse sistema de avaliação deve se relacionar com a alocação de recursos de modo a orientar o regulador para quais áreas ele deve priorizar sua atenção (BALDWIN, CAVE e LODGE, 2012).

A partir desses elementos centrais, reconhece-se cinco características de uma regulação baseada no risco: I. definição de objetivos e riscos; II. aceitação de riscos específicos; III. avaliação de riscos; IV. utilização de *scores* ou categorias par priorizar atores, atividades e assuntos; V. alocação de recursos para supervisões, inspeções e *enforcement* (BALDWIN, CAVE e LODGE, 2012).

Além disto, Baldwin, Cavel e Lodge também identificam que a regulação baseada no risco pode se configurar como uma forma de defesa para resolver problemas de ilegitimidade e *accountability*. Desse modo, pode dissipar a culpa do regulador no sentido de que se a atividade causadora do dano não era classificada como de alto risco, não há como responsabilizar o regulador. Os autores destacam essa discussão como importante diante de novas tecnologias e da inevitável defasagem de intervenção regulatória (BALDWIN, CAVE e LODGE, 2012). Isso proporciona percepções

interessantes no contexto de proteção de dados em razão justamente do desenvolvimento tecnológico que cria uma defasagem entre as normas e a realidade.

1.1.5 Regulação baseada no risco na legislação europeia

Nesta seção, aborda-se o segundo nível da "risquificação" da legislação europeia - a regulação baseada no risco. Assim, apresentam-se as disposições no Regulamento Geral sobre Proteção de Dados que revelam a presença da abordagem baseada no risco.

Em primeiro lugar, enfatiza-se que a legislação anterior, a Diretiva 95/46/CE, continha disposições sobre o risco. Nesse sentido, Macenaite identifica dois papéis exercidos pelo risco nessa legislação: ajustar obrigações e delimitar o objeto regulatório. O primeiro papel se encontrava nos artigos 13, 13 (2), 18 e 20 e também no considerando 49 e considerando 53 (MACENAITE, 2017).

Esses dispositivos legais tratam do conhecimento dos riscos, da adoção de medidas de segurança adequadas e da obrigação de consulta prévia à autoridade de controle. De modo geral, demonstram que o risco é um parâmetro a ser adotado para escalar obrigações dos controladores. Assim, as operações com risco mais elevado a direitos e garantias exigem mais ações dos controladores do que aquelas que apresentam riscos menores (MACENAITE, 2017).

O segundo papel – delimitar o objeto regulatório – se refere ao uso do risco como critério para estabelecer categorias especiais de dados. Desse modo, percebe-se que o risco se encontra implícito na caracterização dos dados sensíveis no artigo 8º, uma vez que a Diretiva dispensa um tratamento mais rígido ao seu tratamento em função do potencial de causar danos graves a direitos dos titulares de dados (MACENAITE, 2017).

Conquanto a presença do risco não seja em si uma novidade, o risco assume uma posição mais central no RGPD e não há dúvidas de que o RGPD contém mais referências ao risco do que a Diretiva. Nesse ínterim, destacam-se dois novos papéis atribuídos ao risco no RGPD: elemento central do princípio de responsabilização e prestação de contas, e desencadeador de novas obrigações dos controladores (MACENAITE, 2017).

Segundo o artigo 24, os controladores devem implementar o RGPD de modo que os riscos a direitos e liberdades sejam levados em conta. Nesse sentido, para além de determinarem as medidas técnicas e organizacionais a serem implementadas, estabelecem que elas devem ser adequadas com os riscos existentes (QUELLE, 2018). Além das medidas de segurança, os controladores devem adotar todas as medidas para cumprir todos os princípios da proteção de dados e ser responsável nos termos do artigo 5º (2) (MACENAITE, 2017).

Por isso, Quelle afirma que o artigo 24 define a responsabilidade dos controladores baseada no risco. A autora ainda afirma que as disposições contidas nos artigos 24, 25 e 35 formam um "triângulo do risco", pois a responsabilidade baseada no risco – artigo 24 - e a avaliação de impacto sobre a proteção de dados – artigo 35 – criam as condições para se atingir a proteção de dados desde a concepção e por defeito (*data protection by design* e *data protection by default*) - artigo 25 (QUELLE, 2018).

O art. 35 dispõe sobre a avaliação de impacto sobre a proteção de dados (AIPD), que é uma das novas obrigações dos controladores desencadeadas pelo risco, conforme Macenaite (MACENAITE, 2017). Dessa forma, a realização da AIPD só é obrigatória para operações de tratamento de dados como um elevado nível de risco. A AIPD é tratada com mais profundidade na seção 1.1.3 que estuda as Orientações do Grupo de Trabalho do Artigo 29.º sobre o tema. Além da AIPD, o risco também desencadeia outras obrigações, como a indicação de encarregados, que é tratada nos artigos 37 a 39, e a notificação de violação de dados pessoais a autoridades de controle – artigos 33 e 34(MACENAITE, 2017).

A proteção de dados desde a concepção (*data protection by design*) se baseia no dever de os controladores e processadores avaliarem os efeitos do tratamento sobre direitos e liberdades antes mesmo do início da operação. Assim, eles são obrigados a projetar o tratamento de dados de modo a minimizar os riscos e a implementar, em todas as fases do tratamento, medidas técnicas e organizacionais que considerem o impacto sobre a privacidade e a proteção de dados pessoais (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE, 2018).

A proteção de dados por padrão (*data protection by default*) significa que as configurações predefinidas devem respeitar a proteção de dados e que somente os dados

necessários para cada finalidade específica devem ser coletados. Destarte, os controladores aplicam medidas técnicas e organizacionais para que só os dados necessários serão tratados por defeito. Isso estabelece uma maior proteção, que abrange obrigações relativas ao tempo e acesso limitado para o tratamento, destacando que os dados não devem ser acessíveis a um número indeterminado de pessoas (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE, 2018).

Em síntese, no RGPD a noção de risco é concretizada por disposições que se relacionam à análise e gestão do risco de modo a avaliar o potencial de danos a direitos e liberdades dos titulares de dados para tomar decisões para reduzir e controlar, visto que o risco zero é impossível. Nesse sentido, direciona-se a atenção às operações de tratamento com elevados risco para promover uma proteção real e prática (GELLERT, 2018).

Outrossim, o risco no RGPD assume um papel importante na responsabilização e prestação de contas ao escalar obrigações e influenciar na responsabilidade dos controladores. Com base nisso, Quelle afirma que o risco desempenha uma função essencial no que a autora denomina *Compliance 2.0* da proteção de dados e Kurner defende que as alterações trazidas pelo RGPD representam um giro copernicano na regulação de proteção de dados, em que os regulados exercem uma função ativa e o cumprimento deixa de ser um mero preenchimento de obrigações determinadas pela lei (QUELLE, 2018; KUNER, 2012).

1.1.6 Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento

As Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados organizam-se para explicar a AIPD de forma a responder as seguintes perguntas:

a) O que abrange uma AIPD?
b) Quais são as operações de tratamento que estão sujeitas a uma AIPD?
c) As operações já existentes também estão sujeitas a uma AIPD?
d) Como realizar uma AIPD?
e) Quando a autoridade de controle deve ser consultada?

O artigo 35 do Regulamento Geral de Proteção de Dados é a principal fonte sobre a qual se debruça as Orientações para responder a essas e outras questões a fim de examinar essa ferramenta tão importante para a gestão do risco e para a responsabilização e prestação de contas[10] (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Assim, a Avaliação de Impacto sobre a Proteção de Dados pode ter como objeto uma única operação de tratamento de dados ou um conjunto de operações semelhantes em termos de natureza, contexto, finalidade e riscos, conforme explicita o Grupo de Trabalho. Cabe destacar que o principal objetivo da avaliação de impacto é avaliar novas situações e seus riscos, portanto, não são necessárias em operações cujos riscos já foram examinados. Além disso, evidencia-se que a avaliação ainda pode ter como objeto um produto tecnológico, como um equipamento ou programa informático, que possa ser utilizado por diferentes responsáveis (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

A resposta para a segunda pergunta – quais operações estão sujeitas à AIPD – encontra-se no artigo 35 (1), (3) e (4)[11]. De modo geral, a AIPD deve ser realizada quando uma operação de tratamento de dados apresenta um elevado risco a direitos e liberdades dos indivíduos, especialmente quando são usadas novas tecnologias. O artigo 35 (1) e os considerandos 89 e 91 corroboram para esse entendimento, conforme

---

[10] Art. 35 (1), RGPD: "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" (UNIÃO EUROPEIA, 2016, p.53).

[11] Art. 35 (3), RGPD: "A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o nº 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, nº 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º; ou c) Controle sistemático de zonas acessíveis ao público em grande escala" (UNIÃO EUROPEIA, 2016, p.53)

Art. 35 (4), RGPD: "A autoridade de controle elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do nº1. A autoridade de controlo comunica essas listas ao Comité referido no artigo 68" (UNIÃO EUROPEIA, 2016, p. 56).

o Grupo de Trabalho explicita. Caso haja dúvida sobre a necessidade de realização da avaliação, deve se optar pela sua realização (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Além disso, o Grupo de Trabalho destaca que o Regulamento exemplifica casos em que a AIPD é obrigatória no artigo 35 (3): avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis; operações de tratamento em grande escala de categorias especiais de dados (dados sensíveis); e controle sistemático de zonas acessíveis ao público em grande escala (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

O artigo 35 (4) também é importante para entender quais operações estão sujeitas à avaliação, pois determina que as autoridades de proteção de dados devem elaborar listas em que constem as operações de tratamento que exigem a AIPD – casos em que é obrigatória. Entretanto, esclarece-se que tanto os casos especificados no artigo 35 (3) quanto essas listas são exemplificativas, isto é, não exaurem as operações em que a avaliação é obrigatória. Nesse sentido, o Grupo de Trabalho desenvolve e apresenta critérios para avaliar se uma operação é considerada de elevado risco e a partir deles analisa-se o caso concreto para verificar a obrigatoriedade de uma avaliação de impacto (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Dessa forma, para ser considerada uma operação de elevado risco, devem ser preenchidos pelo menos dois desses critérios, porque quanto mais critérios, maior a probabilidade de a operação resultar em um alto risco a direitos e liberdades. Porém, o Grupo de Trabalho admite a possibilidade de situações em que, apesar de verificar-se só um dos critérios, é necessário realizar a avaliação em virtude dos riscos do caso concreto. Também é possível que seja necessária uma avaliação quando está presente apenas um critério (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Os casos em que a AIPD é obrigatória – tanto na definição geral quanto nos exemplos e critérios a serem utilizados – evidenciam a abordagem baseada no risco, uma vez que a avaliação do impacto não é necessária em todas operações, mas apenas naquelas consideradas mais problemáticas da perspectiva de riscos a direitos e liberdades do titular de dados. Além disso, quando o Grupo de Trabalho apresenta os

critérios e exemplifica a sua utilização resta claro uma das características da regulação baseada no risco que é o *scoring*, a avaliação do nível do risco (BALDWIN, CAVE e LODGE, 2012), pois quanto mais critérios presentes, maior a probabilidade de gerar consequências negativas aos indivíduos.

Ademais, o Grupo de Trabalho também apresenta as situações em que não é necessária a avaliação: tratamento não é "suscetível de implicar um elevado risco para os direitos e liberdades de pessoas singulares"; natureza, âmbito, o contexto e as finalidades forem muitos semelhantes ao tratamento em relação ao qual tenha sido realizada uma AIPD; operações de tratamento tiverem sido previamente controladas por uma autoridade de controle antes de maio de 2018 em condições específicas que não tenham se alterado; quando um Estado-membro ou a União Europeia possuem um fundamento legal e a AIPD já tenha sido realizada para atender a esse fundamento; quando a operação de tratamento é incluída em uma lista opcional (estabelecida pela autoridade de tratamento) de operações em que a AIPD é exigida (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Em relação às operações de dados já existentes, existem situações em que a avalição de impacto é exigida e outras em que não é necessária. Assim, não é necessária AIPD em operações de tratamento previamente controladas por uma autoridade de controle ou pelo encarregado da proteção de dados nos termos do artigo 20 da Diretiva 95/46/C.E, conforme explicita o considerando 171, caso essas operações não tenham sofrido alterações (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

A AIPD é obrigatória em operações já existentes quando há uma mudança nas condições de aplicação que pode implicar um elevado risco a direitos e liberdades. Também é exigida a avaliação quando ocorrem outras alterações que modifiquem e aumentem os riscos da operação de tratamento, como a introdução de uma nova tecnologia, finalidade ou contexto organizacional diferentes (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Outrossim, caso haja alterações que diminuam os riscos, a realização de uma AIPD não é mais obrigatória. Por isso, é evidente que a Avaliação de Impacto da Proteção de Dados dever ter uma revisão contínua e uma reavaliação regular, uma vez

que as operações de tratamento de dados ocorrem em um contexto de constante mudança (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Em seguida, as Orientações se dedicam a explicar como uma avaliação de impacto de proteção de dados deve ser realizada. Para isso, utilizam-se os seguintes aspectos como direcionadores: o momento, o responsável por efetuar a AIDP, e a metodologia. Primeiro, quanto ao momento, a AIPD deve ser conduzida antes da operação de tratamento, o que corrobora para a concepção da AIPD como um instrumento de apoio à tomada de decisão. Entretanto, cabe ressaltar que a AIPD não é realizada uma única vez, mas sim deve ser entendida como um processo contínuo, com atualizações ao longo do ciclo de vida de seu objeto de exame (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

O controlador é responsável por efetuar uma AIPD, assim como o encarregado e o subcontratante, de acordo com as circunstâncias do caso concreto. Primeiro, sobressai-se a obrigação do controlador por garantir a realizar de uma AIPD, conforme prevê o artigo 35 (2) do RGPD. Conforme esse dispositivo, mesmo que a avaliação seja efetuada por qualquer outro agente, que esteja dentro ou fora da organização, o controlador permanece como a responsabilidade, logo, é o responsável último pela efetivação do procedimento (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

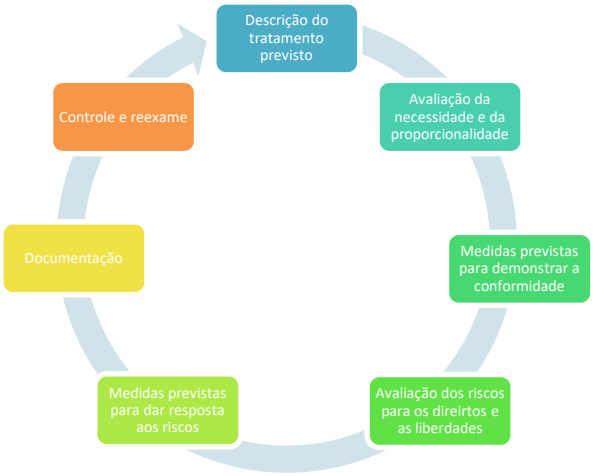
Além do momento da realização e da definição dos agentes responsáveis por uma Avaliação de Impacto de Proteção de Dados, é necessário explicar qual metodologia deve ser usada para realizar uma AIPD. Confere-se liberdade para o responsável pelo tratamento dos dados escolher a metodologia que será utilizada, no entanto ela deve estar em conformidade com critérios comuns, presentes no Anexo nº 2 das Orientações. Esses critérios esclarecem e se baseiam em requisitos mínimos estabelecidos no artigo 35 (7) e nos considerandos 84 e 90 do RGPD (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Esses elementos mínimos são: a descrição das operações de tratamento previstas e a finalidade do tratamento; a avaliação da necessidade e proporcionalidade das operações de tratamento; a avaliação dos riscos para os direitos e liberdades dos titulares; medidas previstas para enfrentar os riscos e demonstrar a conformidade com o regulamento (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017). Nesse sentido, o

Anexo 2 traz critérios comuns que servem para avaliar se uma AIPD ou uma metodologia é compatível com esses elementos presentes no RGPD.

Entretanto, cabe ressaltar que esses critérios são amplos e, assim, possibilitam diferentes formas de implementação, uma vez que é garantida aos controladores a flexibilidade necessária para definir uma estrutura e forma de AIPD que se adeque às condições de sua organização. Nesse âmbito, o Grupo de Trabalho destaca que uma característica da execução da AIPD é que ela é dimensionável. Conquanto existem regras gerais para a sua realização, a sua execução é complementada por orientações práticas do contexto da operação de tratamento objeto da avaliação (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Figura 1: Ilustração de processo iterativo genérico para realização de uma AIPD



Fonte: GRUPO DE TRABALHO DO ARTIGO 29.º. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679**. 2017.

Em síntese, a AIPD permite que o controlador avalie genuinamente os riscos e assim tome as medidas necessárias para enfrentar esses riscos e reduzi-los a um nível aceitável. Nos casos em que os riscos residuais, após a adoção das medidas previstas, permanecerem elevados, os responsáveis devem consultar a autoridade de controle. As Orientações exemplificam esses riscos residuais elevados como situações em que quando os titulares dos dados podem sofrer consequências significativas ou irreversíveis, com grande probabilidade de concretização avaliação (GRUPO DE TRABALHO DO ARTIGO 29.º, 2017).

Quando o controlador não conseguir reduzir esses riscos para um nível aceitável, a AIPD deve ser comunicada integralmente, conforme o artigo 36 (3), alínea "e" do RGPD. Em relação à publicação da AIPD, nos demais casos ela não é obrigatória, apesar de ser vista como uma boa prática. Destarte, recomenda-se a publicação de um resumo ou até de uma declaração de realização de AIPD, porque essa pode conter informações específicas sobre os riscos ou revelar segredos comerciais ou informações altamente sensíveis.

Por fim, as Orientações apresentam conclusões e recomendações sobre a realização da AIPD, com uma síntese da AIPD e sugestões sobre o modo de agir de um responsável por tratamento de dados quando se deparar com uma operação de elevado risco. A seguir apresentam-se quadros resumos desses conteúdos:

Tabela 2: Resumo sobre a AIPD

Avaliação de Impacto de Proteção de Dados (AIPD)	• Forma útil de os responsáveis aplicarem sistemas de tratamento de dados que estejam em conformidade com o RGPD; • Em determinados operações de tratamento, sua realização é obrigatória; • Dimensionável; • Diferentes formas (metodologias); • RGPD define requisitos básicos de uma AIPD eficaz; • Atividade útil e positiva; • Auxilia a conformidade jurídica.

Fonte: GRUPO DE TRABALHO DO ARTIGO 29.º. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679**. 2017.

Tabela 3: Resumo sobre as obrigações do controlador em contexto de realização de uma AIPD

Obrigações do controlador	• Escolher uma metodologia para a AIPD que satisfaça os critérios comuns do Anexo 2; • Aplicar um procedimento sistemático de AIPD que esteja em conformidade com os critérios do anexo 2, seja integrado a processos já existentes de concepção, desenvolvimento, alteração, reavaliação de risco e reavaliação operacional, envolva as partes interessadas e defina as responsabilidades;

	• Fornecer o relatório da AIPD à autoridade de controle quando for solicitado; • Consultar a autoridade de controle quando não conseguir atenuar riscos elevados; • Reavaliar periodicamente a AIPD e o tratamento que ela avalia (quando houver uma alteração do risco colocado pela operação de tratamento); • Documentar as decisões tomadas.

Fonte: GRUPO DE TRABALHO DO ARTIGO 29.º. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679**. 2017.

A abordagem baseada em risco é perceptível não só nas previsões legais sobre a AIPD, mas também nas Orientações do Grupo de Trabalho do Artigo 29, pois ao longo de todo o documento verificam-se referências ao risco como parâmetro para definir quando a AIPD é obrigatória. Além disso, a própria realização da AIPD é característica de uma regulação baseada no risco, uma vez que os riscos são avaliados e examinados para que as respostas a eles sejam mais adequadas de modo a exercer um controle mais efetivo sobre os regulados e reduzir os potenciais efeitos negativos aos titulares dos dados.

1.2 EVIDÊNCIAS DE UM MODELO CENTRADO NO RISCO NA LEGISLAÇÃO BRASILEIRA

Após apresentar as evidências da "risquificação" na legislação de proteção de dados europeia, investiga-se a existência fenômeno no ordenamento jurídico brasileiro, por meio da análise da Lei nº13.708/2018, a Lei Geral de Proteção de Dados (LGPD), que é o foco do presente trabalho e objeto pergunta orientadora. Entretanto, antes de examinar o referido diploma legal, analisou-se a presença da estrutura regulatória do risco em legislações anteriores que disciplinavam a proteção de dados pessoais no Brasil antes da LGPD.

Cabe ressaltar que a normatização da proteção de dados pessoais no Brasil não era inexistente antes da elaboração e vigência da LGPD. O cenário legislativo era composto por várias disposições em normas dispersas e, por tanto, a Lei Geral de Proteção de Dados surgiu com os objetivos de reunir, conferir abrangência e preencher lacunas legislativas relacionadas ao tema. Dentre essas normas, a Lei nº 8.078/1990, o

Código de Defesa do Consumidor, assumiu um papel precursor na regulação da proteção de dados pessoais no Brasil em razão da regulamentação de bancos de dados de consumo, em seu artigo 43, e da presença de princípios aplicáveis nas relações de consumo que utilizam dados pessoais (MENDES, 2018).

Além disso, destacava-se a Lei nº12.965/2014, o Marco Civil da Internet, que foi elaborado com o objetivo de regulamentar o uso da Internet nas redes sociais e possui a privacidade e a proteção de dados pessoais como um dos pilares que estruturam o seu texto legislativo (DA SILVA SANTOS e PETRY, 2019).

Como havia disposições acerca da proteção de dados pessoais em diferentes diplomas legislativos, deveria realizar-se um diálogo dessas duas fontes para solucionar questões relacionadas a casos concretos e, dessa forma, compreender como o ordenamento jurídico brasileiro regulava esses assuntos (MENDES, 2018). Essas duas legislações continuam a ser aplicadas às operações de tratamento de dados de forma complementar à LGPD.

Destaque-se que a Lei Geral de Proteção de Dados não aboliu as normas anteriores que tratavam sobre a proteção de dados pessoais no Brasil e que deve haver uma aplicação conjunta de seus dispositivos normativos (MIRAGEM, 2019). Além disso, evidencia-se que a LGPD recebeu influências, principalmente do Código de Defesa do Consumidor, e por isso é relevante examinar se já havia algum indício de "risquificação" nas previsões que tratam sobre a proteção de dados.

Ressalte-se que essas leis não são o objeto principal de estudo do presente trabalho e, portanto, não se propôs realizar uma análise mais abrangente sobre seus dispositivos. As previsões examinadas foram aquelas diretamente relacionadas à proteção de dados e as que foram encontradas na pesquisa bibliográfica relevantes para o necessário diálogo das fontes.

1.2.1 Lei nº 8.078/1990 - Código de Defesa do Consumidor

O Código de Defesa do Consumidor, possui quatro relações diretas com a proteção dados pessoais e a presença do risco: a regulação dos bancos de dados e cadastros de consumidores; a responsabilidade civil preconizada nesse diploma legal; princípio da precaução e os riscos do desenvolvimento.

Primeiro, apresenta-se a relação mais notória, expressa dessa legislação com a proteção de dados pessoais: a regulamentação dos bancos de dados e cadastros de consumidores. As regras básicas, com direitos assegurados aos consumidores encontram-se no artigo 43 do CDC. O artigo 44 trata do registro dos "maus fornecedores", isto é, um cadastro atualizado de reclamações que deve ser publicado anualmente pelos órgãos públicos encarregados de proteger a relação de consumo (OLIVEIRA, 2015). Além disso, os artigos 72, 73 e 84 disciplinam o que deve ser feito em caso de registro irregular e correções, com destaque para o tratamento penal conferido a determinadas irregularidades de arquivos de consumo (BENJAMIN, 1992).

Os estudos e as pesquisas sobre o comportamento dos consumidores ganharam força a partir da década de 1960 nos Estados Unidos. Ao mesmo tempo em que mais informações sobre os cidadãos eram coletadas e eram utilizadas para averiguar os riscos e o nível de segurança dos consumidores para a decisão sobre concessão de crédito, com os chamados birôs de crédito, surgiram preocupações com essa catalogação de perfis de consumidores (ZANATTA, 2019).

Nesse contexto, no meio acadêmico, Zanatta destaca os posicionamentos de Nader, Miller e Westin sobre os riscos desses "dossiês". Esses debates influenciaram a elaboração do *Fair Credit Reporting Act*, o qual estabeleceu uma série de direitos básicos aos consumidores no que tange o tema em questão. Essa legislação foi resultado de uma proposta do Senador Proximore, que apresentou um conjunto de preocupações com os dossiês dos consumidores, como informações imprecisas, dificuldades em corrigir registros incorretos e informações relevantes (ZANATTA, 2019).

Essa referência à legislação estadunidense é necessária, pois uma das fontes de inspiração do artigo 43 do CDC foi o tratamento legal dos Estados Unidos sobre essa temática, tanto a legislação em vigor quanto propostas de instituições, com destaque para o *National Consumer Act* e o *Fair Credit Reporting Act (FCRA)*. Destarte, o legislador brasileiro, inspirado pelas discussões e pelo direito estadunidense, disciplinou os bancos de dados e os cadastros de consumidores, que já se encontravam em expansão no Brasil – primeiros Sistemas de Proteção ao Crédito (BENJAMIN, 2011).

Ressalte-se que os arquivos de consumo são essenciais em uma sociedade de consumo, dado que constituem uma manifestação e um condicionante desta. Reconhece-se uma função bastante positiva dos bancos de dados e cadastros de consumidores, vistos como meios de superar o anonimato, auxiliar a concessão de créditos e acelerar a celebração de negócios. Entretanto, é necessário controlá-los em razão das ameaças a direitos e garantias fundamentais. Por isso que um registro irregular de dados de consumidores constitui uma violação tanto ao Código de Defesa do Consumidor quanto à Constituição. Nesse sentido, destacam-se as ameaças ao direito da privacidade e da imagem, que justificam a imposição de limites formais e materiais sobre a coleta, manutenção e divulgação de dados (BENJAMIN, 2011).

A regulamentação dos arquivos de consumo possui quatro funções principais: a garantia de privacidade; a transparência na coleta, armazenamento e gerenciamento de informações; padrões temporais e de veracidade; e instituição do dever de reparar eventuais danos (BENJAMIN, 2011). Essas funções são encontradas no artigo 43, que define regras básicas – direitos e limitações - dos bancos de dados e cadastros de consumidores (ZANATTA, 2019).

O direito ao acesso – artigo 43, *caput* - ao dado cadastrado é fundamental para possibilitar o exercício de outros direitos. Relacionado a esse direito, há a disposição que obriga a comunicação prévia ao consumidor sobre a inscrição no arquivo de consumo – artigo 43, §2º. Evidencia-se que as informações fornecidas devem ser objetivas, claras, e verdadeiras, vedando-se quaisquer omissões ou inexatidões – artigo 43 §1º (MELO, 2019).

Outros direitos garantidos são a retificação ou correção dos dados – artigo 43 §3º- e o cancelamento da inscrição – artigo 43, §1º e §5º. Ademais, estabelece-se o caráter público dos arquivos de consumo, o que possibilita a interposição de *habeas data* contra estes (MELO, 2019; OLIVEIRA, 2015).

Em síntese, nessa regulação pioneira de dados pessoais no Brasil encontram-se alguns elementos da regulação do risco. Entre esses elementos, identificam-se: a regulamentação dos arquivos de consumo como uma forma de o Estado intervir para controlar riscos em uma área que apresenta elevados riscos a direitos dos indivíduos e a criação de regras e padrões, que estabelecem condições seguras para a utilização dos

arquivos de consumo. Além disso, apesar de não se direcionar especificamente à definição de perfis, são assegurados direitos básicos de acesso, informação e responsabilização e prestação de contas sobre os arquivos de consumo (ZANATTA, 2019).

Outrossim, o Código do Consumidor tutela a personalidade do consumidor contra o risco e assegura a este o direito à ampla informação acerca dos riscos a que está submetido – artigo 6º, incisos I e II (ZANATTA, 2017; MENDES, 2018). O artigo 8º *caput* também complementa e reforça o direito à informação sobre os riscos, as quais devem ser necessárias e adequadas. Cabe ressaltar que a falha no dever de prestar informações sobre o risco do produto e do serviço configuram hipóteses em que é devida a responsabilização, conforme os artigos 12 e 14 do diploma legal, que estabelecem a responsabilidade objetiva do fornecedor nas relações de consumo.

Não se ignora que a interpretação tradicional desses dispositivos legais entende o risco mencionado como ameaças à segurança física do consumidor. No entanto, não existem impedimentos para que haja uma ressignificação do conceito do risco a fim de compreendê-los como possíveis danos à segurança dos dados pessoais do consumidor (ZANATTA, 2017). Essa nova interpretação é necessária ao se considerar o volume crescente de transações feitas pela internet e como esse ambiente configura um novo espaço em que os direitos do consumidor podem ser violados. Destaque-se ainda a necessidade de diálogo das fontes (MENDES, 2018) e a complementaridade do Código de Defesa do Consumidor e da LGPD no que tange à privacidade e à proteção de dados pessoais (MIRAGEM, 2019).

Esse novo sentido atribuído ao conceito de risco expresso no CDC pode influenciar a responsabilidade civil objetiva, aplicada às relações de consumo segundo o artigo 14. Ressalte-se que o artigo dispõe que o fornecedor é responsável não só pela reparação dos danos, mas também por informações insuficientes ou inadequadas sobre a fruição e riscos do produto ou serviços. Esse regime encontra-se em consonância o artigo 927 do Código Civil, que em seu parágrafo único estabelece a obrigação de reparar o dano, independentemente de culpa, quando a atividade normalmente desenvolvida implicar em riscos a direitos (ZANATTA, 2017).

Essas referências legais ao risco revelam que o ordenamento jurídico brasileiro o considera de uma perspectiva predominantemente civil, uma vez que utiliza o risco na atribuição de responsabilidade civil, como um instrumento de controle *ex post*, ou seja, após a ocorrência do dano (ZANATTA, 2017). Desse modo, verificado o dano, recorre-se ao risco para estipular obrigações de reparar os prejuízos sofridos.

Apesar desse enfoque predominantemente civil, é possível encontrar mais instrumentos regulatórios da regulação do risco no CDC, uma vez que a interpretação dessa legislação não se exclui do contexto de sociedade do risco em que se encontra. Conforme já foi abordado na seção 1.1.1, as novas tecnologias favoreceram um ambiente em que se encontram diversos e novos riscos, o que faz surgir a necessidade de gerenciamento deles.

Nesse sentido, a socialização dos riscos é uma forma de reduzir os riscos – entendidos aqui com ameaças de danos. Como isso, se visa à redução dos riscos, mas não à sua eliminação, porquanto esta é impossível e sempre haverá um risco residual (BERGSTEIN e MARQUES, 2017). A teoria do risco criado, consagrada no Direito brasileiro no artigo 927, parágrafo único, do Código Civil, que atribui a obrigação de reparar os danos independentemente de culpa quando a atividade normalmente desenvolvida, por sua natureza, implicar riscos a direitos - a criação de riscos é suficiente para atribuir responsabilidade (BERGSTEIN e MARQUES, 2017).

Outra questão relevante diz respeito ao paradigma da segurança, ou seja, a busca pela segurança, presente em artigos do CDC já mencionados, os quais revelam a busca por diminuir os riscos no máximo possível como uma forma de manter a segurança do consumidor (BERGSTEIN e MARQUES, 2017). Assim, nessa seara também é possível notar uma relação com a regulação de risco, uma vez que esse é o seu objetivo primordial - gerenciar os riscos e alcançar um patamar de segurança que é construído a partir da redução de possíveis prejuízos na área regulada.

Ainda sobre essa temática, há a relação entre o princípio da precaução e o Código de Defesa do Consumidor. Primeiro, cabe ressaltar que em geral se discorre acerca da prevenção e reparação dos danos causados. Entretanto, há outros danos ou potenciais danos que exigem a perspectiva da precaução. Essa perspectiva ganha

notoriedade em contextos marcados pelo medo da incerteza, resultante dos riscos e perigos oriundos dos avanços tecnológicos e científicos (LOPEZ, 2010).

Nesse cenário, existem dúvidas quanto aos próprios novos riscos e ao seu potencial de provocar danos graves e irreversíveis. Esses fatores levam a uma preocupação maior em relação com o futuro e, por isso, destaca-se a precaução, que consiste em uma ação antecipada diante de um risco incerto (LOPEZ, 2010; HARTMANN, 2012). Por isso, o princípio da precaução assume um papel de destaque.

Antes de apresentar sua relação com o Código de Defesa do Consumidor, discorrer-se brevemente acerca de sua origem, definição e questões relacionadas a sua implementação para entender se há uma abertura no código para a sua implementação e como isso pode ser relacionado à "risquificação" da proteção de dados pessoais.

A origem do princípio da precaução encontra-se no direito ambiental, especificamente em decisões de cortes internacionais e previsões em tratados internacionais sobre o tema. Nesse contexto, o princípio da precaução surgiu para justificar a necessidade de regulação em casos em que não há certeza ou evidência clara dos danos que podem ser causados. Assim, foi se consolidando em documentos do direito internacional público, como na Declaração da Rio 92 (SUNSTEIN, 2005). No campo da regulação do risco, o princípio da precaução se destaca como uma de suas ferramentas, visto que busca gerenciar e reduzir riscos (GELLERT, 2015).

Em sua caracterização, é fundamental estabelecer a distinção entre prevenção e precaução. A principal diferença consiste no tipo de risco a qual cada uma dessas ações é endereçada. A prevenção se destina a riscos determinados e refere-se a uma visão mais mediata. Enquanto que a precaução se destina a riscos incertos, é uma ação antecipada em um universo em que predomina a incerteza quanto aos prejuízos a serem sofridos (HARTMANN, 2012).

Além disso, existem diferentes noções de precaução, pois esta pode se apresentar de forma mais forte ou mais fraca (SUNSTEIN, 2005). A noção mais forte é objeto de críticas em razão de seu caráter paralisante, porquanto não oferece direção e impossibilita qualquer curso de ação, inclusive a regulação. Assim, configura-se como um obstáculo para a regulação, a ausência de regulação e para qualquer outra coisa no meio desses dois extremos (SUNSTEIN, 2005).

A certeza científica desempenha importante papel na caracterização e implementação desse princípio, uma vez que sua definição mais divulgada se manifesta da seguinte forma: “a ausência de certeza científica quanto aos danos não justifica a falta de regulação”. Nesse sentido, ressalte-se que é impossível exigir certeza científica quanto à ausência de riscos, porém é possível trabalhar com provas científicas e riscos em diferentes níveis (HARTMANN, 2012).

É resumir o princípio da precaução nos seguintes pontos principais: I. a precaução não é uma obrigação de resultado, porque não é uma regra e nem sempre se verifica as mesmas consequências; II. há diversas formas de gerenciar os riscos; III. não é qualquer risco que deve ser evitado; IV. o princípio da precaução tem base legal e constitucional (HARTMANN, 2012).

A base para aplicar o princípio da precaução é a cognoscibilidade dos riscos que uma atividade implica para direitos dos indivíduos. Por isso, a pesquisa e o direito à informação são tão necessários para sua aplicação. É preciso conhecer os riscos para avaliá-los conforme critérios de razoabilidade e proporcionalidade e assim realizar as medidas adequadas para reduzi-los (HARTMANN, 2012).

Nesse ponto, situa-se a relação do princípio da precaução com o Código de Defesa do Consumidor, que coloca o direito à informação em posição de destaque. Assim, pode-se afirmar que os artigos 8º, 9º e 10 desse diploma legal abrangem o princípio da precaução de forma implícita (HARTMANN, 2012).

Por último, figura-se a questão dos riscos de desenvolvimento. Essa expressão se refere a defeitos que eram indetectáveis na época de entrada do produto no mercado em razão de limitações no conhecimento técnico e científico e cuja responsabilidade pode ser atribuída aos fornecedores (REINIG e CARNAÚBA, 2019). Embora não haja definição expressa no CDC, pode-se aplicar a responsabilidade do fornecedor pelos riscos de desenvolvimento, uma vez que não há incompatibilidade com a legislação consumerista.

Existiam dúvidas relacionadas à compatibilidade com a responsabilidade objetiva e se configuraria uma excludente de responsabilidade. Entretanto, entende-se que os riscos de desenvolvimento são defeitos e como tais são de responsabilidade do fornecedor sem que isso signifique uma violação ao regime da responsabilidade

objetiva (REINING; CARNAÚBA, 2019). Cabe ressaltar que isso gera percepções interessantes no campo da proteção de dados em razão do crescente e acelerado desenvolvimento, com o surgimento de tecnologias cujos efeitos não são inteiramente conhecidos.

Destarte, no Código de Defesa do Consumidor identificaram-se disposições sobre elementos da regulação do risco, criação de regras e padrões e reunião de informações e cognição de riscos, e instrumentos de *enforcement* – regime de responsabilidade. Ademais, encontram-se a valorização da transparência e acesso à informações, que são essenciais para processos de gerenciamento do risco, base legal para aplicação do princípio da precaução e compatibilidade com a responsabilidade por riscos de desenvolvimento.

Apesar disso, e das menções expressas ao risco no corpo da legislação, não é possível afirmar que há evidências suficientes de um processo de "risquificação" em razão de o papel desempenhado pelo risco ser mais civil, isto é, considerado como condição para que seja atribuída a responsabilidade em caso de dano (ZANATTA, 2017).

1.2.2 Lei nº 12.214/2014 - Marco Civil da Internet

A fim de analisar a presença do risco nessa legislação, delibera-se sobre seu contexto de elaboração para compreender sua relação com a regulação do risco e assim tecer considerações sobre a possibilidade de uma gradual "risquificação" na proteção de dados pessoais no ordenamento jurídico brasileiro, à semelhança do processo que ocorre na Europa.

A Lei nº 12.214/2014, conhecida como Marco Civil da Internet, representou um grande avanço na regulamentação da internet no Brasil. Reconhecem-se como principais inovações as disposições normativas sobre o exercício de direitos civis na internet e a ampla participação da população em se processo de elaboração. Nesse sentido, o Marco Civil da Internet se destaca como uma proposta da sociedade para disciplinar o uso da internet no Brasil e evitar a criminalização de condutas comuns praticadas no ambiente da internet (LEMOS, 2014).

Desse modo, seu enfoque era nos direitos e liberdades civis de modo a transpor para o ambiente da internet os princípios consagrados na Constituição Federal de 1988. Além disso, o processo de elaboração do Marco Civil da Internet foi bastante original, uma vez que, além de contar com a participação pública em uma plataforma colaborativa, mapeou comentários, propostas e opiniões nas redes sociais para definir princípios orientadores da normatização da internet e para produzir o texto legal destinado a concretizá-los (LEMOS, 2014).

Embora essa iniciativa e o texto resultante tenham sido elogiados, inclusive internacionalmente, e existirem boas expectativas em relação à qualidade da futura lei, a proposta do Marco Civil da Internet permaneceu dois anos no Congresso sem nenhuma movimentação. Os debates só foram retomados após o escândalo do caso Snowden, em que se divulgaram práticas de espionagem do governo dos Estados Unidos, inclusive sobre outros governantes, como a presidente do Brasil, Dilma Rousseff (LEMOS, 2014).

Nesse contexto, diante das opções presentes na época, a proposta do Marco Civil constituía a reação mais adequada e assim se consolidou como uma resposta política e técnica ao escândalo Snowden (LEMOS, 2014).

Ainda sobre a elaboração do MCI, na origem da ideia de existir uma proteção legal à rede e a seus usuários, encontram-se elementos conceituais da internet, os quais contribuíram para a elaboração do Marco Civil da Internet e na questão de como ele pode preservá-los. Nessa senda, situa-se o conceito “fim a fim”, ou seja, a caracterização da internet como uma rede “fim a fim”, em que deve ser possível a transferência de dados de uma ponta a outra sem interferências (GETSCHKO, 2014). Esse conceito auxilia na definição de neutralidade da rede, um dos princípios do MCI.

Ademais, a questão da privacidade, a qual também se encontra nos enfoques da lei, passa pela divisão da internet em camadas e outros aspectos técnicos da rede. Primeiro, deve estar claro que a privacidade se encontra relacionada a um contexto específico. Como a internet utiliza protocolos, tudo que ocorre na rede pode ser objeto de registro e acompanhamento – tudo pode ser monitorado (GETSCHKO, 2014). Nesse contexto, para que a privacidade seja preservada podem ser adotados procedimentos

técnicos, como criptografia, ou acordos éticos, morais e legais, como que se propõe o MCI (GETSCHKO, 2014).

Destarte, busca-se impedir que o atrativo que o armazenamento e o acúmulo de dados representam, considerando que vivemos em uma economia movida a dados em que estes representam poder e retorno financeiro, estimule um prestador de serviços a extrapolar sua função e obtenha e use dados sem relação com a transação executada. Portanto, apesar de a internet se caracterizar como uma rede de camadas sobrepostas, as interações específicas de uma camada devem resumir-se à camada em foco (GETSCHKO, 2014).

Nesse sentido, o MCI estabelece linhas gerais de privacidade ao definir limites da atuação de cada ator em cada contexto, vedar acúmulo de dados que não dizem respeito diretamente à transação, estabelecer que o usuário tem o direito de saber claramente que os dados serão armazenados caso se aceite os termos de serviço de um provedor de aplicações (GETSCHKO, 2014).

Essa breve apresentação do contexto de elaboração e da origem do Marco Civil da Internet se justifica para situar a regulamentação da internet no Brasil e a partir disso poder avançar sobre considerações acerca da sua relação com a regulação do risco. A existência de uma proposta sólida de regulação do uso da internet, mas cuja tramitação só se acelerou e concretizou-se em razão da deflagração do escândalo que chamou atenção para ameaças a direitos e garantias fundamentais, pode traçar-se um paralelo com os do surgimento de um regime de regulação do risco, dado que sua base é a interferência do Estado em um campo para enfrentar riscos e gerenciá-los – e este é um dos objetivos do MCI.

Além disso, encontram-se elementos componentes de um regime de regulação do risco ao longo do texto legal. Primeiro, os artigos 2º e 3º estabelecem fundamentos e princípios que devem disciplinar o uso da internet no Brasil, o que revela a presença do primeiro elemento componente: a criação de regras e padrões de conduta. Ressalte-se que os incisos II e III contêm referência expressa à proteção da privacidade e dos dados pessoais como princípios.

Dessa forma, já destaca a importância conferida a privacidade e a proteção de dados pessoais no MCI. Embora seja identificado nos princípios, essa lei não define o

que entende por dados pessoais, o que gerou dúvidas na interpretação dos dispositivos em que se encontra presente o termo (LIMA, 2014).

Em relação à privacidade e à proteção de dados cabe ressaltar que o Marco Civil da Internet nunca buscou suprir à lacuna legislativa, existente na época de sua elaboração, de uma lei específica para a proteção de dados e, portanto, não se pretendeu a exaurir o tema. Porém, isso não reduz a importância dada à privacidade no MCI, uma vez que os direitos à privacidade e à liberdade de expressão são os direitos humanos mais ameaçados no meio digital (BEATRIZ, 2014).

As violações desses direitos podem ocorrer tanto por parte de excessos cometidos pelo Estado quanto por ameaças de empresas, as quais possuem o dever não são de respeitá-los, mas também de se preocupar com sua proteção e reparação em caso de violações. As decisões de remoção de conteúdo, o bloqueio de contas em redes sociais e o armazenamento indevido de dados figuram como exemplos concretos de ameaças à liberdade de expressão e à privacidade (BEATRIZ, 2014).

Em razão disso, o Marco Civil da Internet se atenta a essa problemática e contém outros dispositivos que tratam sobre a privacidade e a proteção de dados pessoais: artigo 7º, I, II, III, VI, VII, VIII, IX e X; artigo 8º; artigo 10º; artigo 11; e artigos 13 a 17. Nessas disposições, é possível delimitar três grandes assuntos: princípios, direito dos usuários e proteção de dados pessoais, e proteção e guarda de registros.

Além disso, os incisos I a III, VII a XI são identificados como um manto de proteção da vida em rede. Inclusive, as disposições do artigo 7º solucionam uma questão que dividia interpretações da jurisprudência em relação ao sigilo dos dados armazenados. Antes do MCI, alguns tribunais entendiam que o sigilo das comunicações, aplicados na internet, restringia-se apenas aos dados em curso e que os armazenados por serviços de cloud computing, por exemplo não se inseriam nessa proteção. Outros tribunais, no entanto, não procediam a essa diferenciação e defendiam o sigilo dos dados armazenados também. O MCI solucionou essa dúvida ao determinar que os dados armazenados também estão amparados sobre o sigilo (GUERRA, 2014).

No Marco Civil os seguintes artigos contêm previsões acerca da privacidade e da proteção de dados: artigo 10, §1º, em que há a previsão da regra de proteção dos registros eletrônicos e dos dados, que encontra sua exceção no §3º do mesmo artigo,

segundo o qual as autoridades administrativas competentes podem ter acesso aos dados cadastrais do usuário; artigo 11, que estabelece o respeito à privacidade e à proteção de dados em todas as atividades de coleta, armazenamento, guarda e tratamento de dados eletrônicos. Destaque-se que essas atividades necessitam do consentimento livre, expresso e informado do usuário/titular de dados para que sejam realizadas de forma legal. Além disso, deve ser resguarda a possibilidade de exclusão de seus dados (LIMA, 2014).

Percebe-se que os dispositivos do Marco Civil da Internet estabelecem condições em que o tratamento de dados é considerado seguro, ou pelo menos, critérios que, caso observados, arrefecem os riscos a violações a direitos dos titulares de dados. Essa é uma característica dos regimes de regulação do risco – traduzida pelo elemento componente "estabelecimento de padrões". Entretanto, o paradigma do consentimento ainda direciona e é a base da proteção de dados encontrada nessa legislação.

Entre os direitos dos usuários, evidenciam-se garantias de inviolabilidade da intimidade e da vida privada (art.7º, I), inviolabilidade e sigilo tanto do fluxo das comunicações quanto das comunicações armazenadas (art. 7º, II e III). Ademais, verifica-se a presença do direito de acesso a informações sobre o tratamento de dados (art. 7º, VIII), o que aponta para a garantia da transparência, que é essencial para um regime de regulação do risco: a reunião de informações e cognição de riscos. O inciso VIII do artigo 7º também dispõe sobre as finalidades que possibilitam o tratamento de dados, o que também se insere na definição de regras e padrões de conduta.

Desse modo, o Marco Civil da Internet apresenta indicativos de um regime de regulação do risco por: ser uma forma do Estado intervir em área que ameace direitos dos cidadãos; apresentar elementos componente de um regime de regulação do risco e meios de assegurar a transparência.

Nesse sentido, as disposições dos artigos 10º e 11 sobre a proteção de registros, dados pessoais e comunicações privadas também se inserem como exemplos de previsões relativas à criação de regras e padrões de conduta. Enquanto que os artigos 8º e 13 a 17 podem ser identificados como exemplos do terceiro elemento – *enforcement* e monitoramento da modificação de comportamento social-, uma vez que contêm vedações e determinam obrigações a serem cumpridas pelos agentes relacionados ao

uso e tratamento de dados, como o prazo de 1 ano para guarda do registro de conexão (art. 13) e a vedação de guarda do registro de acesso a aplicações de internet (art. 15)[12].

Embora considere-se a elevada importância da Lei nº 12.965/2014 no campo da regulação da privacidade e da proteção de dados no Brasil, existem muitas críticas relacionadas à sua efetividade e ao resultado final do seu processo de elaboração. Em relação à proteção da privacidade, destaca-se a insuficiência do MCI diante das novas tecnologias e ameaças a direitos fundamentais na internet. A exemplo disso há a questão de que os metadados, - como endereços de IP e cookies, que são objeto de procedimentos de coleta, armazenamento, análise e tratamento para identificar o usuário e fazer inferências - não estão abrangidos da proteção destinada às "comunicações pessoais armazenadas" (MORAES e NETO, 2014).

Ademais, o artigo 7º introduz direitos e garantias aos usuários, mas os restringe à privacidade, desconsiderando que existem outros direitos fundamentais que podem ser violados, e também trata a privacidade de forma bastante reducionista, ao igualá-la à vida privada. Outra forte crítica realizada é que o MCI depende da territorialidade, o que não resolve problemas decorrentes da modernidade líquida (MORAES e NETO, 2014).

Em seguida, há o artigo 7º, que estabelece uma série de direitos aos titulares de dados. Entre eles, destaca-se o inciso IX, o qual assegura ao usuário da internet o direito de ser informado e exige o consentimento expresso e destacado deste em relação as atividades de coleta, tratamento e transferência de dados. Essa previsão visa garantir que o usuário compreenda como suas informações de natureza pessoal poderão ser utilizadas pelo provedor da internet e assim constitui uma densificação legal de direitos estabelecidos na Constituição Federal: intimidade, vida privada, honra e imagem.

[12] As definições de registro de conexão, aplicações de internet e registro de acesso a aplicações da internet encontram-se do artigo 5º da Lei 12.965/2014: "VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados; VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (BRASIL, 2014).

Portanto, cabe falar em um direito fundamental ao consentimento expresso e informado (LIMA, 2014).

Apesar disso, não é incorreto afirma que o Marco Civil da Internet contém previsões que apontam para um novo rumo regulatório, baseado no risco. Portanto, é possível identificar essa lei como um ponto de partida, ainda que em escala menor do que a experimentada na legislação europeia, para um novo rumo regulatório na proteção de dados, agora baseada no risco.

Em síntese é possível encontrar indícios que corroboram com a tese de que a proteção de dados é um regime de regulação de risco em sua origem no Marco Civil da Internet, primeira disposição a conter disposições sobre a proteção de dados de modo mais ou menos geral no Brasil, o que torna possível traçar um paralelo com a Diretiva Europeia e assim apontar para o início de um processo gradual de "risquificação" da proteção de dados pessoais no Brasil, mesmo que em menor grau do que na Europa.

CAPÍTULO 2 - RELAÇÃO ENTRE A LEI GERAL DE PROTEÇÃO DE DADOS E O MODELO TEÓRICO DA REGULAÇÃO DO RISCO, COM O USO DO MODELO TLICS

Neste capítulo, identificam-se as variáveis jurídicas que demonstram o fenômeno de "risquificação" da proteção de dados pessoais. Conforme as teorias trazidas no capítulo, relacionam-se as variáveis jurídicas do Modelo TLICS aplicado à proteção de dados pessoais ao regime de regulação do risco e à regulação baseada no risco.

Assim, utilizam-se esses indicadores para investigar se a Lei Geral de Proteção de Dados segue a tendência de "risquificação" da proteção de dados pessoais, como verificado na legislação europeia. Por fim, realiza-se uma comparação entre a identificação dessas variáveis na na LGPD e no RGPD. Com isso, é possível investigar a relação entre a LGPD e o modelo teórico da regulação do risco, respondendo à pergunta de pesquisa que orienta o presente trabalho.

2.1 MODELO TLICS

Usa-se o Modelo TLICS (*Telecommunications Law Indicators for Comparative Studies*) em caráter instrumental para identificar variáveis relacionadas ao modelo

teórico da regulação do risco na Lei Geral de Proteção de Dados e, desse modo, buscar respondera pergunta orientadora do presente trabalho. Em razão disso, explicitam-se os fundamentos teóricos dessa metodologia para compreender as bases para identificar as variáveis jurídicas relacionadas ao regime de regulação do risco e a regulação baseada no risco, apresentadas nas seções seguintes.

O Modelo TLICS fundamenta-se na coordenação entre a hermenêutica prescritiva e concreta, nas garantias institucionais e na presunção de finitude da gramática legal. Essa metodologia possibilita: revelar conceitos legais comensuráveis, cobrir diversos cenários na perspectiva comparativa e construir sequências de variáveis inter-relacionadas aderentes à cultura jurídica dos países por meio da diferenciação entre garantias institucionais e garantias do instituto (MENDES, BIONI, *et al.*, 2019).

Para a estruturação do modelo, Márcio Iorio Aranha utilizou a hermenêutica prescritiva, segundo a estruturação de Dilthey e Betti, e concreta, conforme estruturada por Hesse. Além disso, recorreu-se à teoria institucional do direito, de Romano, e a teoria das garantias institucionais. Por fim, recorre-se a diferença entre garantia institucionais e garantias do instituto como ferramenta operacional da correlação legal (ARANHA, 2011). O resumo do método, teorias de suporte e ferramentas operacionais encontra-se no diagrama abaixo:

Figura 2 – Diagrama com a metodologia, teorias de suporte e ferramentas operacionais do Modelo TLICS

Figura retirada de: ARANHA, M. I. Telecommunications Law Indicators for Comparative Studies (TLICS) Model: A Hermeneutical Approach. Acorn-Redecom Conference. Cidade do México: Americas Information and Communications Research Network. 2011. p. 28.

O Modelo TLICS supre uma lacuna de metodológica verificada nos estudos comparativos de TIC: a ausência de uma abordagem jurídica consistente. O problema principal gerado pela não utilização de um método jurídico nessa análise é o uso de conceitos muito abrangentes e frequentemente ambíguos como formas ideais na interpretação de variáveis institucionais (ARANHA, 2011).

A interpretação realizada segundo o Modelo TLICS permite a compreensão de uma variável jurídica por blocos e, desse modo, evita-se que uma previsão seja interpretada da mesma forma em países com tradições jurídicas distintas (ARANHA, 2011). Por isso, esse modelo pode ser usado para enfrentar dificuldades da comparação de institutos legais de países diferentes e, assim, possibilitar a identificação de características legais semelhantes na regulação de proteção de dados (MENDES, BIONI, *et al.*, 2019).

Entre suas aplicações anteriores destacam-se: análises empíricas de variáveis das TIC relacionadas ao Federalismo (ARANHA, ARRUDA, *et al.*, 2018), índices das TIC na Região das Américas (ARANHA e OLIVEIRA, 2016) e a análise de proteção de dados pessoais em perspectiva comparada (MENDES, BIONI, *et al.*, 2019).

Assim, esse último estudo empregou o Modelo TLICS como metodologia para análise comparativa das legislações brasileira e europeia de proteção de dados pessoais de modo a mensurar a comensurabilidades desses dois regimes de proteção de dados. Nessa análise, utilizaram-se 7 instituições jurídicas do Modelo TLICS (pessoa jurídica, qualidade jurídica, objeto jurídico, status jurídico, relação jurídica entre sujeitos, configuração jurídica, relação jurídica entre sujeito e objeto) e os princípios aplicados à proteção de dados pessoais, divididas em 29 instituições jurídicas (autoridade de proteção de dados, conselho de proteção de dados, titulares de dados, operador, controlador, órgão de pesquisa, encarregado, dados pessoais, dados pessoais sensíveis, âmbito de aplicação territorial, âmbito de aplicação material, banco de dados, avaliação de impacto, bases legais para o tratamento de dados, bases legais para o tratamento de dados sensíveis, dados anonimizadados, bloqueados ou deletados, tratamento transnacional, uso compartilhado de dados, responsabilidade e compensação de prejuízos, sanções administrativas, tratamento de dados, tratamento de dados sensíveis, tratamento de dados de crianças e adolescents, tratamento de dados por autoridades públicas, anonimização, obrigações do controlador, governança e

mecanismos de *accountability*, princípios do tratamento de dados) e 51 subtipos de instituições jurídicas[13].

2.2 VARIÁVEIS JURÍDICAS RELACIONADAS AO MODELO TEÓRICO DA REGULAÇÃO DO RISCO NA LGPD

No Capítulo 1, investigou-se a "risquificação" da proteção de dados em dois níveis: regime de regulação de risco e regulação baseada no risco. Portanto, as variáveis jurídicas relacionadas ao risco também foram analisadas segundo essas perspectivas. Primeiro, apresentam-se as variáveis jurídicas do Modelo TLICS que se associam ao regime de regulação do risco e depois aquelas que se correlacionam com a regulação baseada no risco.

2.2.1 Variáveis relacionadas ao regime de regulação do risco

O referencial teórico utilizado (GELLERT, 2015) identifica os elementos componentes de um regime de regulação de risco Diretiva de Proteção de Dados Pessoais (95/46/CE). Entretanto, como a análise do autor apresenta aspectos gerais sobre a relação entre a regulação de risco e a proteção de dados pessoais e da privacidade, recorre-se a esses fundamentos para identificar variáveis jurídicas do Modelo TLICS que possam ser reconhecidas como pertencentes ao regime de regulação de risco.

A identificação desses elementos componentes nas variáveis jurídicas utilizadas no Modelo TLICS, de forma abstrata, e posteriormente, de forma concreta na Lei Geral de Proteção de Dados, corroboram para a tese que afirma que a regulação de proteção de dados pessoais é uma regulação do risco (GELLERT, 2015).

As variáveis associadas ao regime de regulação do risco na Lei Geral de Proteção de Dados foram encontradas considerando os componentes desse regime - criação de regras e padrões de conduta; reunião de informações e cognição de riscos;

[13] Para ter acesso à tabela completa, com todas as variáveis jurídicas analisadas no Modelo TLICS aplicado à comparação de legislações de proteção de dados, ver: <https://sites.google.com/ndsr.unb.br/getel/research/tlics-model-data-protection>

enforcement e monitoramento do comportamento social. Por isso, estruturam-se as variáveis jurídicas em três grupos, de acordo com os elementos componentes.

O primeiro grupo abrange as variáveis jurídicas dos princípios e das bases legais. Os artigos da legislação de proteção de dados que preveem essas variáveis expressam a criação de regras e padrões de conduta. Os princípios e as bases legais são responsáveis por definir condições em que o tratamento de dados é seguro, por isso é possível identificá-los como expressões da criação de regras e padrões de conduta (GELLERT, 2015).

Esse grupo foi formado com base na definição de que o elemento componente criação de regras e padrões de conduta se refere à definição de condições em que determinada atividade deve ser realizada de modo a reduzir os riscos inerentes ao seu exercício – conforme se encontra mais detalhado no item 1.1. Estabelecido esse critério, é necessário explicar com cada uma dessas variáveis se relaciona com esse componente.

Os princípios da proteção de dados pessoais constituem um conjunto de regras de caráter procedimental e que se encontram presentes em diversas normas de proteção de dados ao redor do mundo (DONEDA, 2020). Desse modo, é possível identificar princípios comuns em ordenamentos jurídicos diferentes, o que indica uma convergência de soluções legislativas. Assim, mesmo que esses princípios sejam adaptados, eles podem ser identificados em diversas normas, pois representam um núcleo de questões que precisam ser enfrentadas por todo ordenamento que busca soluções para desafios relativos à privacidade e à proteção de dados pessoais (DONEDA, 2020).

Um "núcleo comum" de princípios da proteção de dados pessoais começou a se delinear na década de 1980, com a Convenção 108 do Conselho da Europa e as Orientações da OCDE sobre proteção da privacidade e transferência internacional de dados (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*) (DONEDA, 2020).

Esses princípios podem ser sintetizados em cinco. Primeiro, há ***o princípio da publicidade ou transparência***, o qual estabelece que a existência de um banco de dados pessoais deve ser de conhecimento público. Entre os meios para garantir sua aplicação estão a autorização prévia para funcionamento, a notificação a uma autoridade sobre as

atividades desenvolvidas e a divulgação de relatórios periódicos das operações realizadas. Segundo o ***princípio da exatidão***, os dados utilizados no tratamento devem corresponder à realidade, assim, é necessário assegurar que a coleta e o tratamento sejam feitos com cuidado e correção, também deve realizar-se atualizações periódicas para manter os dados fiéis à realidade (DONEDA, 2020).

O ***princípio da finalidade*** determina que os dados devem ser utilizados para finalidade previamente conhecida (ou informado). Esse princípio fundamenta restrições de transferência de dados a terceiros e também consistem em o critério para valorar a razoabilidade do uso dos dados, isto é, caso os dados estejam utilizados fora da finalidade, corresponde a um abuso em seu tratamento (DONEDA, 2020).

O ***princípio do livre acesso*** prevê que os indivíduos, os titulares dos dados, devem ter pleno acesso ao banco de dados. Esse princípio, aliado com o princípio da exatidão, garantem o direito à correção, pois possibilita que o indivíduo tenha acesso aos seus dados armazenados e corrija os dados incorretos. Por último, ***o princípio as segurança física e lógica*** estabelece o dever de proteção dos dados contra riscos de extravio, destruição, modificação, transmissão ou acesso não autorizado (DONEDA, 2020).

Em vista disso, os princípios para o tratamento de dados representam o elemento *criação de regras e padrões de conduta* por determinar diretrizes que devem ser observadas pelos controladores e processadores nas atividades de processamento de dados. Com isso, estabelecem-se condições para se diminuir riscos e, portanto, aumentar a segurança do titular de dados.

No Modelo TLICS, são identificadas e classificadas instituições jurídicas e foi adicionada a análise dos princípios aplicados à proteção legal de dados pessoais (MENDES, BIONI, *et al.*, 2019). Elencam-se dez princípios: finalidade (*purpose*); adequação (*adequacy*); necessidade (*necessity*); livre acesso (*free access*); exatidão ou qualidade dos dados (*data quality*); transparência (*transparency*); segurança (*security*); prevenção (*prevention*) não-discriminação (*non-discrimination*); e responsabilização e prestação de contas (*accountability*). Na Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), identificaram-se todos esses dez princípios no artigo 6º, incisos I a X, conforme é a apresentado na tabela abaixo:

Tabela 4: Princípios identificados na LGPD

Princípios aplicados à proteção legal de dados pessoais	Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)
Finalidade	Art. 6º, I: "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;"
Adequação	Art. 6º, II: " compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;"
Necessidade	Art. 6º, II: " compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;"
Livre Acesso	Art. 6º, IV: "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;"
Qualidade de dados	Art. 6º, V: "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;"
Transparência	Art. 6º, VI: "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;"
Segurança	Art. 6º, VII: "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;"
Prevenção	Art. 6º, VIII: "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;"
Não discriminação	Art. 6º, IX: " impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;"
Responsabilização e prestação de contas	Art. 6º, X: "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."

Fonte: MENDES, L. S. et al. Methodology for Comparative Law Analysis on Personal Data Legal Protection. Communication Policy Research, 2019. 141-162.

As bases legais correspondem às situações em que o tratamento de dados pessoais é autorizado pela lei. Elas definem e delimitam condições em que as operações podem ser realizadas dentro de parâmetros de segurança. Por isso, expressam o *elemento criação de regras e padrões de conduta*. Além de bases legais para o tratamento de dados pessoais no geral, existem as bases específicas para o processamento de dados sensíveis. Na Lei Geral de Proteção de dados, como regra geral, o tratamento de dados pessoais exige a identificação de uma base legal. Assim, permite-se o tratamento de dados quando se encontra em uma das bases legais previstas de forma taxativa nos artigos 7º e 11 (VIOLA e TEFFÉ, 2021).

Ressalte-se que inexiste hierarquia entre as bases legais e que basta estar em conformidade com uma delas para o tratamento ser considerado lícito e legítimo. Dito isso, embora não seja superior às demais, o consentimento ocupa uma posição de destaque, o que demonstra a preocupação do legislador com a participação do indivíduo no fluxo de suas informações e, assim, indica uma manifestação do modelo centrado na autodeterminação (VIOLA e TEFFÉ, 2021).

Apesar dessa tutela destacada, atualmente verifica-se insuficiências do paradigma do consentimento e a necessidade de sua revisão (MENDES e FONSECA, 2021). O paradigma do consentimento significa que o consentimento é utilizado como vetor dominante no objetivo de materialização da autonomia do titular de dados. Embora tenha norteado o modelo centrado na autodeterminação, esse paradigma se mostra insuficiente no cenário atual de desenvolvimento tecnológico em razão de limitações cognitivas, assimetria de poderes e desafios das novas tecnologias e o potencial de agregação da informação (MENDES e FONSECA, 2021).

As limitações cognitivas compreendem a falta de compreensão adequada sobre riscos e prejuízos advindos do consentimento para processamento de dados, isso principalmente por duas razões: o titular não costuma ler a Política de Privacidade e as informações de difícil compreensão. Por isso, afirma-se que o consentimento não traduz a vontade real do titular de dados (MENDES e FONSECA, 2021).

A assimetria de poderes – entre o titular de dados e os agentes envolvidos no tratamento de dados – também corrobora para questionar sobre a real autonomia decisória da escolha de consentir. Como muitos serviços ainda funcionam na ótica do

take it ou leave it, em que o não consentimento significa que o indivíduo não poderá usufruir do serviço, parece que a autonomia e a liberdade de escolha do titular não se concretizam (MENDES e FONSECA, 2021).

Por último, os avanços tecnológicos construíram um cenário em que existe uma cadeia muito mais ampla do que a coleta de informações. Isso impossibilita que o titular gerencie de modo pleno a forma como seus dados e informações serão utilizados, uma vez que isso ocorrerá no futuro e envolve várias incertezas. Assim, torna-se cada vez mais difícil a manutenção da integridade contextual e isso exige que sejam considerados outros parâmetros para legitimar o tratamento, além do consentimento (MENDES e FONSECA, 2021).

Nesse contexto, surgem tendências de materialização da proteção de dados, como a proteção de dados por meio da tecnologia, a análise de risco e *accountability* e limites materiais em torno do consentimento (MENDES e FONSECA, 2021). A presença da análise e gerenciamento de risco como uma alternativa para adequar a proteção de dados ao cenário atual de desenvolvimento tecnológico reforça a tese de que se verifica uma tendência à "risquificação" dessa regulação.

No Modelo TLICS, as bases legais para tratamento de dados pessoais e para dados sensíveis se encontram no bloco referente ao status jurídico – apresentação válida de propriedades de um objeto (MENDES, BIONI, *et al.*, 2019). Como subtipos de instituições jurídica, elencam-se 13 bases legais para o tratamento de dados pessoais: consentimento (*consent*), execução de um contrato (*performance of a contrac*t), obrigação legal (*legal obligation*), proteção de interesses vitais do titular de dados ou do terceiro (*protection of the vital interests of the data subject or of another natural person*), interesse público (*public interest*), interesse legítimo (*legitimate interest*), propósitos de pesquisa (*research purpose*), exercício regular de direito em processo judicial (*regular exercise of rights in judicial process*), tutela da saúde (*health protection*), proteção do crédito (*credit protection*), acesso público (*public access*), anonimização (*anonymization*) e registro civil (*civil register*).

Da mesma forma, apresentam-se oito bases legais para o tratamento de dados sensíveis: consentimento específico (*specific consent*), obrigação legal (*legal obligation*), interesse público (*public interest*), estudos (*studies*), exercício regular de

direitos em processo judicial (*regular exercise of rights in judicial process*), proteção da vida ou segurança física do titular de dados (*protecting life or physical safety of the data subject*), tutela da saúde (*protect health*) e prevenção à fraude (*prevention of fraud*).

Na LGPD, identificam-se doze bases legais para o tratamento de dados e oito bases legais para o tratamento de dados sensíveis, como mostram as tabelas abaixo:

Tabela 5: Bases legais identificadas na LGPD

Bases legais para tratamento de dados	Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)
Consentimento	Art. 7º, I: "mediante o fornecimento de consentimento pelo titular;"
Execução de um contrato	Art. 7º, V: "quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;"
Obrigação legal	Art. 7º, II: "para o cumprimento de obrigação legal ou regulatória pelo controlador;"
Proteção de interesses vitais do titular de dados ou do terceiro	Art. 7º, VII: "para a proteção da vida ou da incolumidade física do titular ou de terceiro;"
Interesse público	Art. 7º, III: "pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;"
Interesse legítimo	Art. 7º, IX: "quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;"
Propósitos de pesquisa	Art. 7º, IV: "para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;"
Exercício regular de direito em processo judicial	Art. 7º, VI: "para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);"
Tutela da saúde	Art. 7º, VIII: "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;"

Proteção do crédito	Art. 7º, X: "para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."
Acesso público	Art. 7º, §4º: "É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei."
Anonimização	Art. 12: "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido."
Registro civil	-

Fonte: MENDES, L. S. et al. Methodology for Comparative Law Analysis on Personal Data Legal Protection. Communication Policy Research, 2019. 141-162.

Tabela 6: Bases legais para tratamento de dados sensíveis identificadas na LGPD

Bases legais para tratamento de dados sensíveis	Lei nº 13.709/2018 - Lei Geral de Proteção de dados Pessoais (LGPD)
Consentimento específico	Art. 11, I: "quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;"
Obrigação legal	Art. 11, II, alínea "a": "cumprimento de obrigação legal ou regulatória pelo controlador;"
Interesse público	Art. 11, II, alínea "b": "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;"
Estudos	Art. 11, II, alínea "c": "realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;"
Exercício regular de direitos em processo judicial	Art. 11, II, alínea "d": "exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem;"
Proteção da vida ou segurança física do titular de dados	Art. 11, II, alínea "e": "proteção da vida ou da incolumidade física do titular ou de terceiro;"
Tutela da saúde	Art. 11, II, alínea "f": "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;"
Prevenção à fraude	Art. 11, II, alínea "g": "garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos

	mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.”

Fonte: MENDES, L. S. et al. Methodology for Comparative Law Analysis on Personal Data Legal Protection. Communication Policy Research, 2019. 141-162.

Os princípios e bases legais – presentes nos artigos 6º, 7º e 11 da LGPD – estabelecem as condições em que um tratamento de dados é adequado e seguro. Assim, formam um padrão de segurança, característico da regulação de risco, conforme a interpretação de Gellert para identificar a proteção de dados como um regime de regulação do risco (GELLERT, 2015).

Segundo esse autor, a criação desse padrão ocorre por meio da realização de um teste de proporcionalidade *sui generis* que se opera de acordo com as restrições estabelecidas nas normas, previsões e parâmetros da proteção de dados pessoais (GELLERT, 2015). Nessa perspectiva, as bases legais fornecem critérios objetivos para realizar teste de proporcionalidade, sendo que a ponderação é realizada a partir das restrições estabelecidas. Esse teste é uma forma legal de realizar avaliação de riscos a direitos fundamentais dos titulares de dados (GELLERT, 2015).

Expostas as instituições jurídicas relacionadas à *criação de regras e padrões de conduta*, passa-se ao segundo elemento componente do regime de regulação do risco – *a reunião de informações e cognição de riscos*. Cabe ressaltar a intrínseca relação entre o gerenciamento de riscos e a coleta de informações. Para gerir e reduzir os riscos, é necessário que se conheça detalhadamente aspectos da atividade desenvolvida. Na verdade, a reunião de informações é fundamental para todo tipo de regulação, porém ganha mais centralidade e importância na regulação do risco por ser fundamental para definir probabilidades e consequências (HOOD, HOTHSTEIN e BALDWIN, 2001).

Foi encontrada somente uma variável jurídica relacionada a esse elemento: governança e mecanismos de responsabilização e prestação de contas – registro das operações de tratamento. O elemento *reunião de informações e cognição de riscos*, aplicado à proteção de dados pessoais, refere-se a dispositivos que determinam notificar a autoridades antes mesmo da realização do tratamento para oferecer informações sobre ele e também a publicação de registro de atividades de processamento de dados (GELLERT, 2015).

Portanto, identificam-se principalmente uma abordagem interativa/participativa, da reunião de informações (HOOD, HOTHSTEIN e BALDWIN, 2001), uma vez que os regulados – controladores - fornecem ao regulador – autoridade de dados – informações, que servirão para identificar e averiguar os riscos da operação de tratamento de dados.

Na LGPD, verifica-se a presença dessa variável no art. 50[14], que apesar de não tratar sobre registro de atividades, estabelece várias formas de responsabilização e prestação de contas sobre as operações desenvolvidas. No inciso I, são apresentados os conteúdos ou requisitos mínimos de um programa de governança de privacidade e o inciso II abre a possibilidade de o controlador evidenciar como esse programa e as boas práticas estão sendo cumpridas efetivamente. Ademais, é importante trazer aqui o §3º do art. 50: "As regras de boas práticas e de governança **deverão ser publicadas** e atualizadas periodicamente e **poderão ser reconhecidas e divulgadas pela autoridade nacional**".

Observa-se que os subtipos de instituições jurídicas direito ao acesso e direito à informação não são identificados como expressões do elemento reunião de informações e cognição de riscos. Esses direitos são essenciais para o conhecimento acerca das condições de tratamento de dados e de seus riscos.

O direito ao acesso, por exemplo, ocupa posição central na sistemática de exercício de direitos dos titulares de dados, desempenhando um duplo papel na proteção de dados pessoais: I. possibilita o exercício de muitos outros direitos dos titulares, como o direito de retificação; II. atua como uma ferramenta estratégia para avaliar o cumprimento da legislação de proteção de dados (AUSLOOS e DEWITTE, 2018).

Apesar dessa relevância, o elemento *reunião de informações e cognição de riscos* diz respeito a atitudes de fiscalização e fornecimento de informações entre os

[14] Artigo 50 da Lei 13.709/2018: "Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais"(BRASIL, 2018).

regulados e o regulador, no caso entre os agentes envolvidos no processamento de dados – operadores e controladores – e o regulador – autoridade nacional de proteção de dados. Como esses direitos estão relacionados à relação entre os controladores e os titulares de dados, não podem ser identificados como pertencentes a esse elemento.

O Gellert afirma que existe uma linha tênue entre o elemento anterior e o *enforcement e monitoramento da modificação do comportamento social*, o que gera dúvidas, como a qual deles pertence a obrigação de notificar a autoridade de controle (GELLERT, 2015). A partir da caracterização de Gellert desse elemento, as variáveis jurídicas relacionadas a ele devem conter previsões acerca de meios de mitigação dos riscos e meios de cuidar preocupação com os danos concretos (GELLERT, 2015).

Existem diversas formas de *enforcement e monitoramento de modificação do comportamento social*: I. restrições, que constituem a forma mais extrema de prevenção; II. consulta prévia; III. previsão geral de medidas de segurança, as quais devem ser proporcionais ao risco; IV. regime de responsabilidade do controlador (GELLERT, 2015).

Nessa senda, identificam-se duas variáveis jurídicas do Modelo TLICS como expressões desse elemento: responsabilidade e indenização, que pertence à instituição "relação jurídica entre sujeitos" – que representam um conjunto de expectativas de pessoas sobre o comportamento recíproco (MENDES, BIONI, *et al.*, 2019); e obrigações do controlador, pertencente à instituição "relação jurídica entre sujeito e objeto" (MENDES, BIONI, *et al.*, 2019).

Na LGPD, ambas as variáveis são identificadas. Os artigos 52, 53 e 54 definem o regime de responsabilidade da lei de proteção de dados brasileira. É a perspectiva do elemento que se preocupa com os danos resultantes do risco. Nesse caso, o risco já se materializou e se busca uma reparação. Além disso, encontram-se os seguintes subtipos do tipo obrigações do controlador: segurança de dados (artigo 41), comunicação de violação de dados (artigo 46) e encarregado (artigo 48).

No modelo TLICS aplicado à proteção de dados pessoais, não há variáveis relacionadas à consulta prévia nem a restrições. No entanto, é possível encontrar proibições ao longo do texto da LGPD, como a proibição geral de tratamento de dados sensíveis, o qual só é permitido dentro das hipóteses legais previstas.

Tabela 7: Variáveis jurídicas relacionadas aos elementos componentes de um regime de regulação de risco identificadas na LGPD

ELEMENTOS COMPONENTES	VARIÁVEIS JURÍDICAS RELACIONADAS	LEI Nº13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)	NÚMERO DE VARIÁVEIS ENCONTRADAS
Criação de regras e padrões de conduta	Bases legais para tratamento de dados pessoais	Art. 7º Art. 12	12
	Bases legais para tratamento de dados sensíveis	Art. 11	8
	Princípios aplicados ao tratamento de dados pessoais	Art. 6º	10
Reunião de informações e cognição de risco	Governança e mecanismos de responsabilização e prestação de contas	Art. 50.	1
***Enforcement* e modificação de comportamento**	Responsabilidade e indenização;	Art. 42;	1
	Obrigações do controlador	Art. 41 Art. 46 Art. 48	3

Além desses elementos componentes, a LGPD possui disposições relativas à constituição de uma autoridade administrativa para supervisionar e implementação a aplicação da lei, no inciso XIX, e garante direitos aos titulares de dados para assegurar a transparência – direito à informação, acesso e retificação, presentes no artigo 6º, inciso IV e VI, e no artigo 18. Gellert destaca à existência de autoridades administrativas e a transparência como essenciais ao regime de regulação de risco (GELLERT, 2015).

2.2.2 Variáveis relacionadas à regulação baseada no risco

Como foi visto no Capítulo 1, o risco já se encontrava presente na legislação europeia antes do novo regulamento. Entretanto, na normativa atual sua presença se expandiu no texto legislativo e também ganhou novos papéis. Neste trabalho, analisou-

se se a legislação brasileira, que recebeu muitas influências do RGPD, também acompanhou essa tendência. Já foram identificadas variáveis jurídicas relacionadas ao regime da regulação do risco e agora busca-se a apresentar as variáveis jurídicas relacionadas à regulação baseada no risco.

Utilizando-se as variáveis do Modelo TLICS para análise comparativa de legislações de proteção de dados, identificaram-se os seguintes indicadores que possuem relação com a regulação baseada no risco: dados pessoais sensíveis ou categorias especiais de dados pessoais, tratamento de dados sensíveis, comunicação de violação de dados, proteção de dados desde a concepção e por defeito (*privacy by design* e *privacy by* default), relatório de impacto ou relatório de avaliação. Com exceção da variável *privacy by default*, todas estão presentes na Lei Geral de Proteção de Dados.

"Dados pessoais sensíveis ou outras categorias especiais de dados" compõem o bloco da instituição objeto jurídico (MENDES, BIONI, *et al.*, 2019). Os dados sensíveis são uma categoria específica de dados que se referem a um tipo de informações com maior potencial de uso discriminatório ou lesivo para o titular de dados pessoais, logo, são dados que apresentam maiores riscos potenciais de provocarem lesões a direitos e liberdades, principalmente no que diz respeito à igualdade material. A elaboração dessa categoria advém de uma observação da diferença dos efeitos do tratamento. Exemplos de dados sensíveis são: informações referentes a raça, religião, opinião política, orientação sexual, histórico médico ou dados genéticos (DONEDA, 2020). A LGPD apresenta a definição de dados sensíveis em seu artigo 5º, inciso II.

Destaca-se que classificar determinados dados como sensíveis não significa que somente eles podem ser usados para fins discriminatórios. Ademais, deve-se notar que os dados sensíveis não são sempre usados de modo lesivo e há fins lícitos e legítimos para o seu tratamento (DONEDA, 2020).

A instituição jurídica "tratamento de dados sensíveis" se encontra no bloco referente à instituição "relação jurídica entre sujeito e objeto" e cuida das disposições sobre como se deve processar os dados sensíveis. Na LGPD, o artigo 11 estabelece as situações em que o tratamento de dados pessoais sensíveis é permitido e considerado

legítimo, sendo que seus incisos correspondem às bases legais que autorizam seu tratamento.

O regime de tratamento de dados sensíveis varia conforme as interpretações sobre o tema em cada ordenamento jurídico (DONEDA, 2020). Apesar disso, pode-se afirmar uma tendência a adotar-se uma maior rigidez – no sentido de se buscar uma tutela mais significativa - ao disciplinar o tratamento de dados pessoais sensíveis em razão de sua natureza. Assim, percebe-se que o risco se encontra implícito na caracterização de dados sensíveis e dados comuns (MACENAITE, 2017).

Isso se explica porque ao inserir a categoria de dados sensíveis se considera que eles possuem um maior risco de potencial de danos aos titulares de dados, risco esse que demanda um maior cuidado e uma normatização mais rígida por parte do legislador no que tange disposições sobre o seu tratamento. Por isso, as variáveis jurídicas "dados pessoais sensíveis ou outras categorias especiais de dados" e "tratamento de dados sensíveis" indicam que o risco desempenha um papel de delimitar o objeto regulatório na regulação da proteção de dados, o que encontra paralelo na análise de Macenaite abordada anteriormente (MACENAITE, 2017).

Embora essas variáveis sejam importantes para demonstrar a presença e o papel do risco na legislação brasileira, não é uma novidade em termos de regulação de dados pessoais. A caracterização de dados pessoais sensíveis e uma disciplina mais rígida quanto ao seu tratamento já estavam presentes na Diretiva 45/96/CE (MACENAITE, 2017). Essa é uma situação distinta da próxima variável analisada, que é considerada expoente da regulação baseada no risco na legislação de proteção de dados.

A instituição jurídica "Relatório de Impacto ou Avaliação de Impacto" pertence ao bloco da instituição "objeto jurídico" – que representa entidades que possam a ser objeto de determinado atos (MENDES, BIONI, *et al.*, 2019). Conquanto se encontrem como uma única variável, existem diferenças entre os termos relatório e avaliação. A avaliação de impacto consiste em uma metodologia para avaliar impactos da privacidade de um produto ou operação de tratamento de dados, de modo a fornecer medidas para evitar ou diminuir danos (WRIGHT e HERT, 2012). Assim, a avaliação de impacto se refere à metodologia empregada e, portanto, precede a elaboração do relatório, que é o resultado (GOMES, 2019).

Na Lei Geral de Proteção de Dados Pessoais, no artigo 5º, inciso XVII, encontra-se a previsão dessa ferramenta tão importante, com o nome e a definição de relatório de impacto à proteção de dados pessoais. A lei também contém previsão de processo de avaliação sistemática de impactos e riscos à privacidade, no artigo 50, §2º, alínea "d", entendida como a avaliação de impacto que é anterior ao relatório (GOMES, 2019).

A avaliação de impacto sobre a proteção de dados (AIPD) constitui uma forma de desregulação ou meta regulação no sentido de que são os próprios regulados – os controladores – que avaliam os riscos das operações com dados pessoais realizados por eles (QUELLE, 2018). Dessa forma, consiste em uma importante ferramenta para efetivar a "*Compliance 2.0*" e para o controlador exercer suas responsabilidades e implementar a legislação de modo a considerar os riscos envolvidos na atividade.

À primeira vista, isso pode parecer um pouco dissonante da regulação baseada no risco, porque não são os reguladores que avaliam o risco. Porém, como essas avaliações são apresentados às autoridades de proteção de dados, percebe-se que o regulador continua a exercer seu papel de direcionar as cobranças paras as áreas que geram mais problemas (QUELLE, 2018).

Além disto, a regulação baseada no risco acha-se no centro da definição da obrigatoriedade de se realizar uma AIPD, uma vez que o risco da operação de tratamento fundamenta a necessidade do controlador proceder a ela. Nos casos em que os riscos são elevados, é obrigatória a realização de AIPD, tanto para analisar efeitos sobre a privacidade e a proteção de dados dos titulares quanto para buscar formas de mitigar esses riscos (MACENAITE, 2017).

Por isso, o relatório e a avaliação de impacto relacionam-se com a perspectiva de risco e sua presença na LGPD evidencia um gradual processo de "risquificação". Entretanto, não basta a previsão legal, mas também como essas ferramentas serão colocadas em prática (GOMES, 2019). No Capítulo 1, foram estudas as Orientações do Grupo de Trabalho do Artigo 29.º sobre a AIPD e esse documento tornou ainda mais explícita a relação com a abordagem baseada no risco ao apresentar critérios para realização e o objeto da avaliação de risco.

No Brasil, entende-se que a Autoridade Nacional de Proteção de Dados deverá exercer uma função fundamental na aplicação prática do relatório e da avaliação de

impacto. Nesse sentido, caberá a ela fornecer modelos de relatório para os controladores, como geralmente é feito por autoridades de proteção de dados em outros países. Porém, ressalva-se que a avaliação de impacto é um processo contínuo e por isso deve-se entender o relatório como uma ferramenta dinâmica, sempre disposto a ser alterado para se adaptar a novas demandas, situações e riscos (GOMES, 2019).

Por fim, dentro da instituição "relação jurídica entre sujeito" existem três subtipos de obrigações dos controladores relacionadas à regulação baseada no risco: comunicação de violação de dados, privacidade desde a concepção (*privacy by design*) e privacidade por padrão (*privacy by default*). Na LGPD, identifica-se apenas uma dessas variáveis jurídicas – a comunicação de violação de dados, prevista no artigo 48.

A comunicação de violações de dados se encontra relacionada à regulação baseada no risco porque só é obrigatória caso tenha causado danos ou represente elevados riscos aos titulares. Nesse caso, o risco exerce o papel de determinar novas obrigações (MACENAITE, 2017). As outras duas variáveis se associam diretamente à abordagem baseada no risco, visto que, em conjunto com a AIPD, são formas de efetivar a responsabilidade do controlador baseada no risco (QUELLE, 2018).

Tabela 8: Variáveis jurídicas relacionadas a regulação baseada no risco identificadas na LGPD

VARIÁVEIS JURÍDICAS RELACIONADAS À REGULAÇÃO BASEADA NO RISCO	LEI Nº13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)	NÚMERO DE VARIÁVEIS ENCONTRADAS
Dados pessoais sensíveis ou outras categorias especiais de dados	Art. 5º, II: "dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;"	1
Tratamento de dados sensíveis	Art. 11: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses (..)"	1

Relatório de Impacto ou Avaliação de Impacto	Art. 5º, XVII: "relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;" Art. 50, §2º, alínea "d": "estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade"	1
Comunicação de violação de dados	Art. 48: "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares."	1
Privacidade desde a concepção (*privacy by design*)	-	-
Privacidade por padrão (*privacy by default*)	-	-

2.3 COMPARAÇÃO ENTRE LGPD E RGPD QUANTO ÀS VARIÁVEIS DO RISCO

Após identificar as variáveis relacionadas ao regime de regulação do risco e regulação baseada no risco, comparam-se a LGPD e o RGPD. Desse modo, buscou-se avaliar se LGPD passa por um processo de "risquificação" da proteção de dados pessoais, semelhante ao estudado no RGPD, uma vez que a legislação brasileira recebeu muitas influências da europeia. Existem tantas convergências entre essas duas legislações que é possível estudá-las para analisar critérios de uma decisão de adequação e desse modo alcançar um nível de equivalência (MENDES e BIONI, 2019).

Primeiro, em relação às variáveis jurídicas relacionadas ao regime de regulação do risco, todas as instituições jurídicas que foram identificadas como expressões dos três elementos componentes se encontram presentes nas duas legislações. Isso

corrobora a tese de Gellert de que a proteção de dados é um regime de regulação de risco desde sua origem (GELLERT, 2015).

A LGPD e o RGPD apresentam os mesmos princípios e bases legais, o que é justificado pelo fenômeno da convergência regulatória na proteção de dados pessoais observado desde a década de 1970. Como buscavam-se soluções para problemas semelhantes quanto ao fluxo de dados, modelaram-se princípios e diretrizes gerais que influenciaram legislações de diversos países (MENDES e FONSECA, 2021).

Em relação ao segundo elemento componente, *a reunião de informações e a cognição de riscos*, ambas as legislações possuem disposições relativas a única variável identificada– "governança e mecanismos de responsabilização e prestação de contas". Ademais, a LGPD e o RGPD possuem previsões quanto ao registro das atividades de tratamento de dados por controladores e processadores, em seus artigos 37 e 30, respectivamente.

As variáveis jurídicas relacionadas ao terceiro elemento – *enforcement e modificação de comportamento* – são a "responsabilidade e indenização" e "obrigações do controlador". Nesse caso, também se verificam, em ambas as legislações, artigos correspondentes a essas variáveis. Em relação ao regime de responsabilidade, notam-se diferenças entre os adotados pela União Europeia e pelo Brasil. Entretanto, para fins desse trabalho, o interesse maior é a sua existência como componente do regime de regulação do risco.

A variável jurídica "obrigações do controlador" aparece nos dois grupos de variáveis relacionadas ao risco identificadas, pois três de seus subtipos foram considerados como evidências da presença da regulação baseada no risco – comunicação de violação de dados, privacidade desde a concepção (*privacy by design*) e privacidade por padrão (*privacy by default*).

Esses subtipos são mais discutidos ao se abordar a regulação baseada no risco, mas a variável jurídica "obrigações dos controladores" pertence ao grupo de variáveis relacionadas ao regime regulação do risco por refletir o elemento de *enforcement e monitoramento da modificação de comportamento social*, uma vez que busca

implementar as previsões da lei de proteção de dados por meio de ações a serem tomadas pelos controladores. Como essas obrigações são adequadas e calibradas pelos riscos envolvidos nas atividades, esta é uma discussão da regulação baseada no risco.

Uma última comparação entre o regime de regulação de risco notado em ambas as regulações se refere ao tratamento conferido à autoridade de proteção de dados e a transparência, que não são elementos componentes, mas se encontram presentes em todo regime de regulação do risco (GELLERT, 2015). Tanto o RGPD (artigo 51) quanto a LGPD (artigo 5º, XIX) preveem a constituição de uma autoridade de proteção de dados. A diferença é que enquanto segundo a legislação europeia essa autoridade é autônoma ou independente, inclusive contando com um artigo que se dedica assegurar e tratar sobre essa independência (artigo 52), na legislação brasileira ela não é autônoma ou independente (MENDES, BIONI, *et al.*, 2019). Outrossim, em ambas as legislações são assegurados direitos aos titulares de dados como forma de se efetivar a transparência – direito à informação, direito ao acesso, retificação e ao apagamento de dados.

Quanto às variáveis relacionadas à regulação baseada no risco, a maior diferença entre as duas legislações é que o RGPD contém artigos sobre a privacidade desde a concepção e a privacidade por padrão, que são variáveis ausentes na LGPD e o RGPD.

As variáveis "dados sensíveis ou categorias especiais de tratamento de dados" e "tratamento de dados sensíveis" são encontradas na LGPD e no RGPD e não geram mais discussões dos que a já mencionadas na seção anterior. A próxima variável – "relatório de impacto ou avaliação de impacto" – também se encontra nas duas legislações. Na Europa, tanto as disposições legais quanto outras normas e instruções normativas – como as orientações analisadas no capítulo 1– conferem um tratamento legal mais completo e específico sobre a avaliação e o relatório de impacto do que o presente no ordenamento jurídico brasileiro.

Em relação aos subtipos da variável "obrigações dos controladores", é necessário ressaltar que mesmos em casos que haja o preenchimento da variável na análise da LGPD, percebe-se que há diferenças na extensão do papel do risco conferido por cada legislação. Por exemplo, ambas as legislações preenchem os subtipos

"segurança de dados" e "encarregado", mas somente na legislação europeia contém referências expressas ao risco nos artigos em que se identificam essas variáveis.

No artigo 32 (1) do RGPD, os riscos são mencionados como um dos parâmetros para as medidas de segurança a serem adotadas pelos controladores. Além disto, no artigo 37 explicita-se que a indicação de um encarregado só é obrigatória em determinadas situações, que denotam um risco maior. Assim, percebe-se a abordagem baseada no risco mesmo em dispositivos legais que se referem quanto aos subtipos de obrigações de controladores que não foram identificados como variáveis relacionadas à regulação baseada no risco. Isso revela uma limitação na utilização do Modelo TLICS para analisar a "risquificação", pois o simples preenchimento de uma variável não significa que o risco esteja presente na mesma intensidade.

O tratamento legal da "comunicação de violação de dados" é bastante semelhante nas duas legislações, no que tange à relação com a regulação baseada no risco. Em ambas, tal obrigação é modulada com base no risco, isto é, com base no potencial de que a violação de dados provoque danos aos titulares, como se percebe no artigo 38 da LGPD e no artigo 33 do RGPD.

Por fim, quanto às variáveis "privacidade desde a concepção" (*privacy by design*) e "privacidade por padrão" (*privacy by default*) ", a legislação brasileira, como já foi apresentado, não apresenta disposições sobre nenhuma dessas duas variáveis, enquanto que a RGPD possui as duas. Essa ausência é importante porque a privacidade desde a concepção (*privacy by design*) e privacidade por padrão (*privacy by default*) são consideradas, por Claudia Quelle, componentes do "triângulo do risco" presente no RGPD (QUELLE, 2018). Deste modo, essa ausência influencia a perspectiva de que "risquificação" da proteção de dados pessoais aparece de forma mais incipente na legislação brasileira.

Nessa lógica, Rafael Zanatta observou, ainda no projeto da LGPD, que era possível notar algumas disposições que evidenciavam da "risquificação", como o relatório de impacto, mas que lhes faltavam a especificação que se encontra no RGPD (ZANATTA, 2017). Por isso, é possível concluir que a legislação brasileira

experimenta um processo gradual de “risquificação” da proteção de dados pessoais, porém em menor grau do que aquele observado na legislação europeia.

Ademais, há outras evidências de que a “risquificação” é mais forte no RGPD do que na LGPD. O risco adquiriu um papel maior no regulamento europeu, como elemento central princípio da responsabilização e prestação de contas e como desencadeador de novas obrigações e também fortalecendo sua função como calibrador de obrigações dos controladores. Com base nisso, Milda Macenaite questiona se há alguma disposição do RGPD que esteja completamente imune à regulação baseada no risco (MACENAITE, 2017).

Em resumo, é possível avaliar que a proteção de dados no Brasil se adequa à caracterização de um regime de regulação de risco. Também são identificadas quase todas as variáveis relacionadas à regulação baseada no risco. Entretanto, isso não é suficiente para se considerar que o fenômeno da “risquificação” da proteção de dados pessoais é presente na mesma intensidade que na legislação europeia.

CONCLUSÃO

O presente trabalho buscou entender a relação entre o modelo teórico da regulação do risco e a lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais. Para isso, recorreu-se à estruturação de regime de regulação de risco, conforme Hood, Hothstein e Baldwin, e à definição de regulação baseada no risco segundo Baldwin, Lodge e Cave. Esses referenciais teóricos foram adotados nos estudos de Gellert, Macenaite e Quelle, os quais investigam a “risquificação” da proteção de dados na Europa. Ainda foi utilizado o Modelo TLICS de forma instrumental, para se identificar variáveis jurídicas relacionadas ao regime de regulação do risco e à regulação baseada no risco na LGPD.

Diante de tecnologias como Big Data, definição de perfis, decisões automatizadas, algoritmos, entre outras, o paradigma do consentimento e o modelo da autodeterminação se revelam insuficientes para assegurar a proteção de dados pessoais. A crescente utilização do risco na legislação europeia – processo de “risquificação”da proteção de dados pessoais - origina o questionamento acerca da relação entre um modelo centrado no risco e a legislação brasileira.

Nesse sentido, analisou-se primeiro as evidências da "risquificação" na legislação europeia. Para tanto, considerou-se a perspectiva de Macenaite, segundo a qual esse giro rumo à "risquificação" ocorreu em dois níveis: regulação do risco e regulação baseada no risco.

No que tange à regulação de risco, fez-se paralelo com a tese de Gellert de que a proteção de dados pessoais constitui um regime de regulação de risco. Como o autor identificou seus três elementos componentes e outros dois aspectos fundamentais – autoridades independentes e transparência - na Diretiva 95/46/CE, foi necessário atualizar esse referencial em conformidade com o Regulamento Geral sobre Proteção de Dados. Ademais, analisou-se a presença desses elementos nas Orientações do Grupo de Trabalho do Artigo 29.º sobre a definição de perfis e decisões automatizadas. Essa fonte normativa reforçou as evidências de regulação do risco na proteção de dados pessoais na Europa.

Quanto à regulação baseada no risco, recorreu-se aos elementos centrais desse quadro regulatório para se avaliar a presença da abordagem baseada no risco no RGPD. Aqui foi trazida a perspectiva de Macenaite quanto aos novos papéis assumidos pelo risco no RGPD, em comparação com a presença do risco na Diretiva. Além disto, adotou-se a teoria de Quelle quanto ao "triângulo do risco" na legislação europeia, composto pela responsabilidade baseada no risco, proteção de dados desde a concepção e por defeito e a avaliação de impacto sobre a proteção de dados pessoais. Outra questão estudada foi o risco como elemento central do princípio da responsabilização e prestação de contas, como forma de se buscar um cumprimento prático e efetivo das disposições legais sobre privacidade e proteção de dados.

Nesse âmbito, abordou-se as Orientações do Grupo de Trabalho do Artigo 29.º sobre a AIPD para compreender essa ferramenta, que se encontra intrinsicamente relacionada à avaliação e gerenciamento de riscos para se buscar sua efetivação. Aqui também foi possível traçar paralelos com a regulação baseada no risco e essa fonte normativa acabou por corroborar com a tese de crescente "risquificação" da proteção de dados na Europa.

Um passo importante neste trabalho foi o estudo de evidências da "risquificação" no Brasil em legislações anteriores que tratavam da proteção de dados

antes da LGPD – Código de Defesa do Consumidor e Marco Civil da Internet. No Código de Defesa do Consumidor foi possível identificar alguns dos elementos componentes de um regime de regulação do risco e também referências à transparência e ao risco, contando inclusive com abertura para o princípio da precaução. Porém, o risco é utilizado em uma perspectiva eminentemente civil, para definir a atribuição de responsabilidade civil. No Marco Civil da Internet também se reconheceram alguns elementos de um regime de regulação do risco, porém faltam disposições relativas a abordagem baseada no risco.

Assim, procedeu-se a busca pela resposta da pergunta orientadora por meio da identificação variáveis jurídicas relacionadas ao risco – ao regime de regulação do risco e à regulação baseada no risco. Para tanto, o Modelo TLICS foi utilizado de forma instrumental de modo a se identificar em abstrato as variáveis jurídicas pertencentes a cada grupo e que foram, imediatamente, aplicadas à análise de LGPD de modo a constituir sua relação com o modelo teórico do risco.

Os três elementos componentes de um regime de regulação de risco foram associados a variáveis jurídicas, a partir das instituições jurídicas usada no Modelo TLICS, bem como a autoridade e a transparência, que são essenciais a qualquer estrutura de regulação de risco. Desse modo, concluiu-se que é possível caracterizar a proteção de dados pessoais asseguradas pela LGPD como um regime de regulação do risco.

Outrossim, foram identificadas as variáveis jurídicas associadas à regulação baseada no risco e, em resumo, foram encontradas variáveis suficientes para afirmar que a LGPD adota a abordagem baseada no risco em alguns de seus dispositivos. Porém, existem muitos fatores a se considerar, como a ausência de disposições sobre a privacidade desde a concepção e a privacidade por padrão na lei brasileira.

Esses fatores se destacam quando é feita a comparação com as variáveis relacionadas ao risco identificadas no RGPD. Esse passo é importante porque mostra que o risco possui uma maior centralização e presença na legislação europeia. Assim, é inegável que o processo de "risquificação" da proteção de dados se encontra mais consolidado na Europa do que no Brasil.

Portanto, verificou-se a possibilidade de se classificar a proteção de dados como um regime de regulação de risco no Brasil, com base na Lei Geral de Proteção de Dados Pessoais. Esse diploma legal também contém disposições importantes relativas à regulação baseada no risco e que permitem a afirmação de que existem evidências do processo de "risquificação" no Brasil. Entretanto, elas possuem menos especificidades em comparação às encontradas na legislação europeia, o que permite concluir que a "risquificação" está presente, mas em menor grau e com menos intensidade do que a observada na Europa.

REFERÊNCIAS BIBLIOGRÁFICAS

ARANHA, M. I. Diálogo político-jurídico na comparação de modelos regulatórios de comunicação. **Revista Brasileira de Políticas de Comunicação**, v. 1, p. 1-20, 2011.

ARANHA, M. I. **Telecommunications Law Indicators for Comparative Studies (TLICS) Model:** A Hermeneutical Approach. Acorn-Redecom Conference. Cidade do México: Americas Information and Communications Research Network. 2011. p. 283-329.

ARANHA, M. I. et al. Federalism, ICT and Development in the Global South. **Communication Policy Research Latina America**, 2018. 297-318.

ARANHA, O. M. I.; OLIVEIRA, F. M. **ICT Institucional Frameyork:** Americas Region ICT Federal Index. London: Laccademia Publishing, 2016.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. [S.l.]: [s.n.]. 2018. p. 1-37.

AUSLOOS, J.; DEWITTE, P. Shattering one-way mirrors – data subject access rights in practice. **International Data Privacy Law**, v. 8, p. 4-28, january 2018. ISSN 1.

BACHRACH, Y. et al. **Personality and patterns of Facebook usage**. Proceedings of the 4th annual ACM web science conference. [S.l.]: [s.n.]. 2012. p. 24-32.

BALDWIN, R. . L. M. . &. C. M. **Understanding Regulation**. Oxford: Oxford University Press, 2012.

BEATRIZ, C. Os direitos humanos e o exercício da cidadania em meios digitais. In: SALOMÃO, G. L.; LEMOS, R. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 66-78.

BECK, U. **Risk Society:** Towards a New Modernity. London: Sage, 1992.

BENJAMIN, A. H. Crimes de Consumo no Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, n. 88, p. 248, 1992.

BENJAMIN, A. H. D. V. E. Das práticas comerciais. In: GRINOVER, A. P.; BENJAMIN, A. H. D. V. E.; FINK, D. R. **Código brasileiro de defesa do consumidor:** comentado pelos autores do anteprojeto. 10ª. ed. Rio de Janeiro: Forense, 2011. Cap. 5, p. 414-431.

BERGSTEIN, L.; MARQUES, C. L. Socialização de Riscos e Reparação Integral do Dano no Direito Civil e do Consumidor no Brasil. **Conpedi Law Review**, v. 3, n. 1, p. 250-278, Janeiro - Junho 2017. ISSN ISSN.

BEZERRA DE MENEZES, J. O direito dos danos na sociedade das incertezas : a problemática do risco de desenvolvimento no Brasil. **Civilística**, 2013. 1-19.

BIONI, B. R.; LUCIANO, M. O Princípio da Precaução na Regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada. Inteligência artificial e direito: ética, regulação e responsabilidade. **Thomson**, São Paulo, 2019.

BLACK, J.; BALDWIN, R. Really Responsive Risk-Based Regulation. **Law & Policy**, v. 32, n. 2, p. 181-213, April 2010.

CLAPTON, W. Risk in International Relations. **International Relations**, n. 25, p. 280-295, september 2011.

CORRY, O. Securitisation and 'Riskification': Second-order Security and the Politics of Climate Change. **Millennium**, 40, janeiro 2012. 235-258.

DA SILVA SANTOS, L.; PETRY, A. T. Direito à privacidade e proteção de dados pessoais frente à lei nº 12965/14 (denonimada Marco Cvil da Internet). **Justiça e Sociedade**, v. 4, n. 1, p. 315-352, 2019.

DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**. 2ª. ed. São Paulo: Thomson Reuters Brasil, 2020.

DOSHI-VELEZ, F.; KORTZ, M. Accountability of AI Under the Law: The Role of Explanation, 2017.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. **Handbook on European data protection law - 2018 edition**. Luxembourg: Publications Office of the European Union, 2018.

FEDERAL TRADE COMMISSION. **Internet of Things: Privacy & Security in a Connected World**. Federal Trade Commission. Washington, DC. 2015.

GELLERT, R. Data protection: A risk regulation? Between the risk management of everything and the precautionary alternative. **International Data Privacy Law**, Oxford, v. 5, p. 3-19, 2015. ISSN 1.

GELLERT, R. Understanding the notion of risk in the General Data Protection Regulation. **Computer Law & Security Review**, v. 34, n. 2, p. 279-288, 2018.

GETSCHKO, D. As origens do Marco Civil da Internet. In: LEITE, G. S.; LEMOS, R. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 12-17.

GILLESPIE, T. The relevance of algorithms. In: _____ **Media Technologies:** Essays on Communication, Materiality, and Society. Cambridge: The MIT Press, 2014.

GOMES, M. C. O. Relatório de impacto à proteção de dados. **Revista do Advogado**, São Paulo, n. 133, p. 6-15, 2019.

GRUPO DE TRABALHO DO ARTIGO 29.º. **Parecer sobre o papel da abordagem baseada no risco em estruturas legais de proteção de dados**. [S.l.]. 2014.

GRUPO DE TRABALHO DO ARTIGO 29.º. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679**. Grupo de Trabalho do Artigo 29.º. [S.l.], p. 1-27. 2017.

GUERRA, G. R. Direito à inviolabilidade e ao sigilo de comunicações privadas armazenadas: um grande salto rumo à proteção judicial da privacidade na rede. In: SALOMÃO, G. L.; LEMOS, R. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 392-416.

HARTMANN, I. A. M. O princípio da precaução e sua aplicação no direito do consumidor: dever de informação. **Direito & Justiça**, v. 38, n. 2, p. 156-182, Jul./Dez. 2012.

HOOD, C.; HOTHSTEIN, H.; BALDWIN, R. **Government of Risk**. Oxford: Oxford University Press, 2001.

KUNER, C. The European Comission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. **Bloomberg BNA Privacy and Security Law Report**, 6, 2012. 1-15.

KUNER, C. The European Comission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. **Bloomberg BNA Privacy and Security Law Report**, 6, 2012. 1-15.

LEMOS, R. O Marco Civil como símbolo do desejo por inovação no Brasil. In: LEITE, G. S.; LEMOS, R. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 3-11.

LIMA REINIG, G. H.; CARNAÚBA, D. A. Riscos Do Desenvolvimento No Código De Defesa Do Consumidor: a Responsabilidade Do Fornecedor Por Defeitos Não Detectáveis Pelo Estado Dos Conhecimentos Científicos E Técnicos. **Revista do Direito do Consumidor**, 2019. 1-36.

LIMA, C. C. C. Garantia de Privacidade e dados pessoais à luz do Marco Civil da Internet. In: LEITE, G. S.; LEMOS, R. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 148-164.

LOPEZ, T. A. Responsabilidade civil na sociedade de risco. **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 105, p. 1223-1234, Janeiro 2010.

MACENAITE, M. The "Riskification" of European data protection law through a two-fold shift, Cambridge, 8, 2017. 506-540.

MAYER-SCHÖNBERGER, V. Generational development of data protection in Europe. In: AGRE, P.; ROTENBERG, M. **Technology and privacy:** The new landscape. Cambridge: Mit Press, 1998. p. p. 219-241.

MELO, T. D. D. Bancos de dados e cadastro de consumidores tasso. **Cadernos Jurídicos**, São Paulo, n. 49, p. 185-195, Maio - Junho 2019.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, L. S. O diálogo entre o Marco Civil da Internet e o Código de Defesa. **Revista de Direito do Consumidor**, v. 106, p. 37-69, julho-agosto 2018.

MENDES, L. S. et al. Methodology for Comparative Law Analysis on Personal Data Legal Protection. **Communication Policy Research**, 2019. 141-162.

MENDES, L. S.; BIONI, B. R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, n. 124, p. 157-180, Jul.-Ago. 2019.

MENDES, L. S.; FONSECA, G. C. S. D. Proteção de dados para além do consentimento: tendências de materialização. In: BIONI, B., et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. Cap. 4, p. 90-112.

MIRAGEM, B. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, 2019. 1-35.

MONTEIRO, R. L. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Artigo Estratégico 39, Instituto Igarapé**, 2018.

MORAES, J. L. B. D.; NETO, E. J. D. M. A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. In: LEITE, G. S.; LEMOS, R. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 417-439.

OLIVEIRA, J. M. Banco de dados, cadastro de consumidores, a lei do cadastro positivo e o novo sistema de scoring de crédito. **Revista Brasileira de Direito Comercial**, São Paulo, v. 4, p. 46-60, Abril 2015.

PASQUALE, F. **The Black Box Society:** the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

QUELLE, C. Enhancing compliance under the general data protection regulation: The risky upshot of the accountability and risk-based approach. **European Journal of Risk Regulation**, v. 9, n. 3, p. 502-526, 2018.

REINIG, G. H. L.; CARNAÚBA, D. A. Riscos do desenvolvimento no Código de Defesa do Consumidor: a responsabilidade do fornecedor por. **Revista de Direito do Consumidor**, v. 124, p. 343 - 392 , Jul. - Ago. 2019.

SPADACCINI DE TEFFÉ, C.; BODIN DE MORAES, M. C. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar - Revista de Ciências Jurídicas**, 2017. 108-146.

SPINA, A. Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law. **European Journal of Risk Regulation**, 5, 2014. 248 - 252.

SPINA, A. A regulatory mariage de Figaro: Risk regulation, data protection, and data ethics. **European Journal of Risk Regulation**, Cambridge, 8, 2017. 88 -94.

SUNSTEIN, C. R. **Laws of Fear:** beyond the Precautionary Principle. Cambridge: Cambridge University Press, 2005.

UNITED STATES SENATE. **A Review of the Data Broker Industry: Collection, Use,and Sale of Consumer Data for Marketing Purposes**. Committee on Commerce, Science, and Transportation. Washington, DC, p. 1-35. 2013.

VIOLA, M.; TEFFÉ, C. S. D. Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos arts. 7ºe 11. In: (COORDENADORES), D. D. E. A. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. Cap. 6, p. 131-162.

WESTIN, A. F. New tools for invading privacy. In: WESTIN, A. F. **Privacy and Freedom**. New York: Ig Publishing, 1967. Cap. 4 - 7, p. 66-131.

WILSON, E. J. **The Information Revolution and Developing Countries**. Cambridge: The MIT Press, 2006.

WRIGHT, D. . &. D. H. P. **Privacy Impact Assessment**. Amsterdam: Springer Netherlands, 2012.

ZANATTA, R. A. F. **Proteção de dados pessoais como regulação de risco:** uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet. [S.l.]: [s.n.]. 2017. p. p. 175-193.

ZANATTA, R. A. F. Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais, fevereiro 2019.