**UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS**
**UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO**
**PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO**
**MESTRADO INTERINSTITUCIONAL – MINTER UNISINOS/UNIDAVI**
**NÍVEL MESTRADO**

**GUSTAVO FELIPE ANAMI SEGUNDO**

# A DEFESA DO CONSUMIDOR E O *PERSONAL DATA BREACH*: a adoção de uma norma no Mercosul à luz do Regulamento Geral de Proteção de Dados da União Europeia

**SÃO LEOPOLDO**
**2019**

GUSTAVO FELIPE ANAMI SEGUNDO

# **A DEFESA DO CONSUMIDOR E O *PERSONAL DATA BREACH*:**

a adoção de uma norma no Mercosul à luz do Regulamento Geral de Proteção de Dados da União Europeia

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre, pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos - UNISINOS

Orientadora: Prof.ª Dr.ª Luciane Klein Vieira.

São Leopoldo

2019

S456d Segundo, Gustavo Felipe Anami

A defesa do consumidor e o personal data breach: a adoção de uma norma no Mercosul à luz do regulamento geral de proteção de dados da União Europeia / Gustavo Felipe Anami Segundo -- 2019.

224 f. ; 30cm.

Dissertação (Mestrado em direito) -- Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, Mestrado Interinstitucional - Minter UNISINOS/UNIDAVI, 2019.

Orientadora: Profa. Dra. Luciane Klein Vieira.

1. Direito do consumidor. 2. Direito digital. 3. Proteção de dados pessoais. 4. Regulamento - Proteção de Dados - União Europeia. 5. MERCOSUL. I. Título. II. Vieira, Luciane Klein.

CDU 347.451.031

Catalogação na Publicação: Bibliotecário Eliete Mari Doncato Brasil - CRB 10/1184

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
NÍVEL MESTRADO

A dissertação intitulada: **"A DEFESA DO CONSUMIDOR E O PERSONAL DATA BREACH: a adoção de uma norma no Mercosul à luz do Regulamento Geral de Proteção de Dados da União Europeia"** elaborada pelo mestrando **Gustavo Felipe Anami Segundo,** foi julgada adequada e aprovada por todos os membros da Banca Examinadora para a obtenção do título de MESTRE EM DIREITO.

São Leopoldo, 17 de setembro de 2019.

Profa. Dra. **Fernanda Frizzo Bragato**
Coordenadora do Programa de Pós-Graduação em Direito.

Apresentada à Banca integrada pelos seguintes professores:

Presidente: Dra. Luciane Klein Vieira

Membro: Dr. Augusto Jaeger Junior

Membro: Dra. Têmis Limberger

## AGRADECIMENTOS

Gostaria de agradecer à minha mãe e conselheira, Katia Margareth Anami Segundo, por estar sempre presente, maternalmente, nos momentos de desilusão e, amistosamente, nos momentos de tensão acadêmica, jamais me deixando sem suporte qualquer, auxílio este sem igual e sem o qual talvez eu não estivesse onde estou agora. Você é uma força da natureza.

Gostaria de agradecer ao meu pai, motivador e financiador, Fulvio Cesar Segundo, por esta tríplice função que exerceu durante o cursar deste mestrado ao se certificar que eu viesse a encarar e superar todas as adversidades pessoais, profissionais e econômicas, fazendo da sua convivência, experiência e assistência alicerce indispensável à minha jornada acadêmica.

Gostaria de agradecer ao meu avô, Nilton Segundo, e à minha avó, Maria de Lourdes Segundo, por diretamente me incentivarem a encarar este desafio, obstáculo deveras custoso, e indiretamente me estimularem positivamente a manter meu desempenho acadêmico e profissional em níveis satisfatórios, cuidando sempre para que eu não me desprendesse do ambiente a que pertenço.

Gostaria de agradecer aos meus irmãos, primos e parentes pela compreensão da minha ausência nos recentes encontros e eventos familiares - ela não foi proposital, teve motivação e será compensada -, notadamente às primas Jéssica Mayumi Anami e Ana Beatriz Valim Suquisaqui que, também cursando mestrado, compartilharam comigo momentos de torcidas e desabafos.

Gostaria de agradecer aos meus amigos pelo suporte emocional, operacional e técnico nos últimos anos, especialmente ao Ruan Sccotti Mattos, pelos votos de confiança e pela manutenção dos projetos conexos em minha ausência; à Patricia Fagundes de Lacerda Flores, sempre na torcida pelo meu sucesso; e à Viviane Costanza Batalha, parceira para todos os momentos, situações e emoções.

Gostaria de agradecer à minha orientadora, Luciane Klein Vieira, exemplo de pessoa e de profissional, por me acolher em tempos de mudanças súbitas, por me apresentar à temática que hoje disserto, por sua disponibilidade, atenção e recomendações - sempre minuciosas e pertinentes - e, acima de tudo, por não desistir de mim apesar de todos os desencontros e percalços.

Dedico esta dissertação à Kamikasianami, quem custosamente soube respeitar minha privacidade, afastando-se nas horas precisas, para que o foco deste mestrado fosse mantido em evidência. Sua cooperação foi imprescindível, bem sabes disso, e seria egoístico não reconhecer este esforço, razão pela qual acredito que tu sejas merecedor desta dedicatória.

"Não devemos pedir aos nossos clientes que façam um equilíbrio entre privacidade e segurança. Precisamos oferecer-lhes o melhor de ambos. Em última análise, proteger os dados de outra pessoa é proteger a todos nós".[1]

**TIM COOK**

[1] COOK, Timothy Donald. "**Trecho do discurso recitado pelo CEO da Apple sobre privacidade e segurança, na conferência *Champions of Freedom".*** Evento organizado pelo EPIC e acontecido em 1º de junho de 2015, em Washington, D.C. (tradução nossa).

## RESUMO

A presente dissertação tem como objetivo analisar a viabilidade da adoção de uma norma, no âmbito do MERCOSUL, à luz do Regulamento Geral de Proteção de Dados da União Europeia (RGPD), que defenda os consumidores contra as violações de dados pessoais. O problema de pesquisa que guiará a dissertação se refere a: sob quais condições seria possível a adoção de uma norma, no âmbito do MERCOSUL, destinada a proteger o consumidor contra o *personal data breach*, aos moldes do RGPD? Trabalha-se com a hipótese de que referido espelhamento normativo seja possível no atual cenário do MERCOSUL. Acredita-se que as possíveis condições de êxito residam no fato de que existe (i) uma insuficiência legislativa, no âmbito do MERCOSUL, em matéria de proteção de dados pessoais, ao passo que existe uma forte tendência regional e internacional de normatização e padronização da temática; e (ii) uma compatibilidade relativa de critérios técnicos das leis protetivas de dados pessoais dos Estados Partes do MERCOSUL entre si e com o RGPD para que um processo de harmonização legislativo seja facilitado. O método de abordagem utilizado na dissertação foi a pesquisa qualitativa e aplicada; o método de procedimento foi a pesquisa normativa, descritiva e comparativa; e a técnica de pesquisa foi a bibliográfica e documental. Os resultados do trabalho se revelam satisfatórios ao demonstrar uma compatibilidade de critérios técnicos nas legislações de proteção de dados pessoais dos Estados Partes maior do que a esperada e, no caso da produção legislativa mercosurenha, ao evidenciar um promissor histórico de harmonizações legislativas nas áreas do direito do consumidor e do comércio eletrônico, conquanto iniciante no quesito proteção de dados pessoais. A somatória destas conclusões sinaliza positivamente no sentido de que é viável a adoção de uma norma protetiva, no âmbito do MERCOSUL, baseada no RGPD, que facilitará o tratamento e circulação de dados pessoais, diminuirá os casos de *personal data breaches* e reforçará a proteção do consumidor. Ao final, encontra-se uma proposta de tratado apresentada com este intuito.



**Palavras-chave**: proteção de dados pessoais; *personal data breach*; Regulamento Geral de Proteção de Dados da União Europeia; MERCOSUL; defesa do consumidor.

## ABSTRACT

The present dissertation aims to analyze the feasibility of adopting a legal rule within MERCOSUR, in the light of the General Data Protection Regulation of the European Union (GDPR), which defends consumers against breaches of personal data. The research problem that will guide the dissertation refers to: under what conditions would it be possible to adopt a MERCOSUR norm to protect the consumer against personal data breach, in the molds of the RGPD? It is worked with the hypothesis that such normative mirroring is possible in the current scenario of MERCOSUR. It is believed that the possible conditions to obtain success lie in the fact that there is (i) a lack of legislation within MERCOSUR regarding the protection of personal data, while there is a strong regional and international trend towards creation of legislations and standardization of this theme; and (ii) the relative compatibility of technical criteria of the personal data protection laws of the MERCOSUR States Parties with each other and with the RGPD to facilitate a process of legislative harmonization. The approach method used in the dissertation was qualitative and applied research; the method of procedure was normative, descriptive and comparative research; and the research technique was bibliographic and documentary. The results of the work are satisfactory in demonstrating greater than expected compatibility of technical criteria in Member States' personal data protection laws and, concerning MERCOSUR legislative production, by showing a promising record of legislative harmonization in the areas of consumer and e-commerce law, although beginner regarding to the protection of personal data. The sum of these findings positively signals that the adoption of, within MERCOSUR, a GDPR-based protective norm is viable, and shall facilitate the processing and circulation of personal data, reduce personal data breaches and strengthen consumer protection. At the end, there is a treaty proposal presented for this purpose.



**Keywords:** personal data protection; personal data breach; General Data Protection Regulation of the European Union; MERCOSUR; consumer protection.

## RESUMEN

La presente tesis de maestría tiene como objetivo analizar la viabilidad de la adopción de un reglamento dentro del MERCOSUR, a la luz del Reglamento General de Protección de Datos de la Unión Europea (RGPD), para defender a los consumidores contra las violaciones de datos personales. El problema de investigación que guiará el trabajo se refiere a: ¿bajo qué condiciones sería posible adoptar una norma, en el contexto del MERCOSUR, para proteger al consumidor contra la violación de datos personales, similar al RGPD? Trabajamos con las hipótesis de que tal reflejo normativo es posible en el escenario actual del MERCOSUR. Se cree que las posibles condiciones para el éxito radican en el hecho de que existe (i) una falta de legislación, dentro del MERCOSUR, con respecto a la protección de datos personales, mientras que existe una fuerte tendencia regional e internacional hacia la creación de una legislación y estandarización de esta temática; y (ii) la compatibilidad relativa de los criterios técnicos de las leyes de protección de datos personales de los Estados Partes del MERCOSUR entre sí y con el RGPD para facilitar un proceso de armonización legislativa. El método de enfoque utilizado en la tesis de maestría fue la investigación cualitativa y aplicada; el método de procedimiento fue la investigación normativa, descriptiva y comparativa; y la técnica de investigación fue bibliográfica y documental. Los resultados del trabajo son satisfactorios al demostrar una compatibilidad de criterios técnicos mayor a la esperada en las leyes de protección de datos personales de los Estados Partes y, en el caso de la producción legislativa del MERCOSUR, al demostrar un histórico de armonizaciones legislativas en las áreas del derecho del consumidor y del comercio electrónico, mientras que eso no se manifiesta en la protección de datos personales. La suma de estas conclusiones indica positivamente que es factible adoptar un reglamento de protección, en el contexto del MERCOSUR, basado en RGPD, que facilitará el tratamiento y la circulación de datos personales, reducirá los casos de violaciones de datos personales y fortalecerá la protección del consumidor. Al final, se presenta una propuesta de tratado para este propósito.



**Palabras clave:** protección de datos personales; violación de datos personales; Reglamento General de Protección de Datos de la Unión Europea; MERCOSUR; protección del consumidor.

## LISTA DE SIGLAS

| | |
|---|---|
| ADITAL | Agência de Informações Frei Tito para América Latina |
| AEPD | Autoridade Europeia para a Proteção de Dados |
| AGESIC | Agência para o Desenvolvimento do Governo de Gestão Eletrônica e da Sociedade da Informação e do Conhecimento |
| AIPD | Avaliação de Impacto sobre a Proteção de Dados |
| ALADI | Associação Latino-Americana de Integração |
| ANPD | Autoridade Nacional de Proteção de Dados |
| APD | Autoridades de Proteção de Dados |
| APEC | Asia-Pacific Economic Cooperation |
| Art. | Artigo |
| BD | Banco de Dados |
| BREXIT | Saída do Reino Unido da União Europeia |
| BSI | British Standards Institution |
| CAN | Comunidade Andina |
| CC | Codice Civile |
| CCM | Comissão de Comércio do Mercosul |
| CDH | Conselho e Direitos Humanos das Nações Unidas |
| CDFUE | Carta dos Direitos Fundamentais da União Europeia |
| CEDH | Convenção Europeia dos Direitos do Homem |
| CE | Comunidade Europeia |
| CEO | Diretor Executivo |
| CISO | Chefe de Segurança da Informação |
| CMC | Conselho do Mercado Comum |
| CNPD | Comissão Nacional de Protecção de Dados |
| COM | Comunicação |
| CMU | Carnegie Mellon University |
| CN | Constituição Nacional |
| CNIL | Commission Nationale de l'Informatique et des Libertés |
| CDC | Código de Defesa do Consumidor |
| CPI | Corte Penal Internacional |

| | |
|---|---|
| CRFB/1988 | Constituição da República Federativa Brasileira de 1988 |
| CSIRT | Computer Security Incident Response Teams |
| CSO | Chefe de Ciência |
| CT-7 | Comitê Técnico n.º 7 |
| DC | Directive |
| DNUPC | Diretrizes das Nações Unidas de Proteção do Consumidor |
| DOS | Denial of Service |
| DPDP | Dirección Nacional de Protección e Datos Personales |
| DNPDP | Direção Nacional de Proteção de Dados Pessoais |
| DUDH | Declaração Universal dos Direitos Humanos |
| ECOSOC | Conselho Econômico e Social |
| EPD | Encarregado de Proteção de Dados |
| ENISA | European Union Agency for Network and Information Security |
| EZLN | Exército Zapatista para Liberação Nacional |
| FCES | Foro Consultivo Econômico-Social |
| GDPR | General Data Protection Regulation |
| GMC | Grupo de Mercado Comum |
| GT29 | Grupo de Trabalho do Art. 29 |
| HEW | Secretary for Health, Education and Welfare |
| IDEC | Instituto de Defesa do Consumidor |
| IEC | Comissão Eletrotécnica Internacional |
| IETS | Internet Engineering Working Group |
| ISSO | International Organization for Standardization |
| JAI | Grupo de Justiça e Assuntos Internos |
| LGPD | Lei Geral de Proteção de Dados |
| LOPD | Lei Orgânica de Proteção de Dados de Caráter Pessoal |
| LORTAD | Lei Orgânica de Regulamentação de Tratamento Automatizado de Dados Pessoais |
| MERCOSUL | Mercado Comum do Sul |
| MST | Movimento dos Sem Terra |
| NIST | National Institute of Standards and Technology |

| | |
|---|---|
| OCDE | Organização para Cooperação e Desenvolvimento Econômico |
| ONU | Organização das Nações Unidas |
| PARLASUL | Parlamento do Mercosul |
| PPGDir | Programa de Pós-Graduação em Direito |
| RES | Resolução |
| RGPD / Regulamento | Regulamento Geral sobre Proteção de Dados |
| RFC | Request for Comments |
| RIPD | Rede Iberoamericana de Proteção de Dados |
| SAM | Secretaria Administrativa do Mercosul |
| SEI | Software Engineering Institute |
| SGBD | Sistema Gerenciador de Bancos de Dados |
| SGT-13 | Subgrupo de Trabalho sobre Comércio Eletrônico |
| SP | Special Publication |
| STIC | Setor de Tecnologia da Informação e Comunicação |
| TCE | Tratado da Comunidade Europeia |
| TIC | Tecnologia da Informação e Comunicação |
| TJCE | Tribunal de Justiça da Comunidade Europeia |
| TJUE | Tribunal de Justiça da União Europeia |
| TUE | Tratado da União Europeia |
| TFUE | Tratado sobre o Funcionamento da União Europeia |
| TPR | Tribunal Permanente de Revisão |
| URCDP | Unidad Regulaora y de Control de Datos Personales |
| US-CERT | United States Computer Emergency Readiness Team |
| UE | União Europeia |
| US | United States |
| UNISINOS | Universidade do Vale do Rio dos Sinos |

**SUMÁRIO**

## 1 INTRODUÇÃO

Parece indissociável a ideia de progresso, tecnologia e direito nos dias atuais. A arquitetura socioeconômica transformou-se. Vive-se hoje na chamada Sociedade da Informação. Prospera-se a dita Indústria 4.0, uma quarta Revolução Industrial que trouxe novos conceitos, técnicas e padrões, como os sistemas ciber-físicos, a Internet das Coisas, a computação em nuvem e a automação e transferência de dados.

Acontece que esta revolução digital também trouxe consigo inesperadas adversidades. A inovação, a praticidade e recursividade promovidas pelos bancos de dados e seus sistemas gerenciadores – e também pela readequação da infraestrutura virtual às demandas sociais - provocam a retenção de diversos dados dos seus usuários, inclusive dados pessoais.

Já enunciava Rodotà que "as velhas tecnologias tinham uma vantagem. Eram visíveis, volumosas, rumorosas. Impunham-se com tal materialidade que todos eram capazes de sentir seu peso, e quando pareciam intoleráveis, bastava pedir que alguém as suprimisse"[2]. Em definitivo, esta não é mais a realidade: os maquinários são silentes e diminutos; e os dados, impalpáveis e transmissíveis.

Se dados comuns, quando indevidamente manuseados, podem acarretar drásticos prejuízos aos seus titulares, imagine os danos irreversíveis que uma violação de dados pessoais (*personal data breache*s) pode causar aos seus donos. Maximize este número à casa dos milhões em episódios colossais de quebra de segurança de multinacionais, órgãos governamentais e redes sociais.

Não é espantoso que a preocupação com o tratamento destes dados pessoais esteja reconfigurando a forma como a tutela jurídica - poderes, direitos e obrigações – é utilizada para proteção das informações virtuais. Não apenas juridicamente, mas securitária, econômica, logística e politicamente. E, embora a inquietação transcenda fronteiras, os europeus tomaram a dianteira.

A altíssima incidência de casos na região levou a União Europeia a normatizar o vazamento de dados pessoais e reforçar a proteção destes dados através do *General Data Protection Regulation* (GDPR) ou, em português,

---

[2] RODOTÀ, Stefano. ***Um Codice per L'Europa? Diritti nazionali, diritto europeo, diritto globale***. In: *Codici. Uma reflessioni di fine millennio.* Paolo Cappellini Bernardo Sordi (orgs.). Milano: Giuffrè, 2002, p. 564.

Regulamento Geral de Proteção de Dados (RGPD), que dispõe acerca do tratamento, processamento, transferência, fiscalização e responsabilização quanto a dados pessoais.

Considerando este pioneiro Regulamento, a tendência internacional de normatização da proteção dos dados pessoais, o caráter transfronteiriço dos dados pessoais e a exigência de equiparação protetiva para circulação de informações pessoais com a União Europeia, os Estados com os quais o bloco mantém relações começaram a atualizar suas legislações; e com significativa urgência.

Com o desencadear desta inclinação mundial à normatização dos dados pessoais, tendo o RGPD europeu como inspiração, diversos países da América Latina resolveram promover esforços neste sentido. Eis que, sopesando a relevância da temática, ponderando as premissas levantadas e pensando em como implementá-las no contexto do Mercosul, chega-se na problematização e hipótese da dissertação.

Destarte, o problema de pesquisa que guiará a dissertação se refere a: sob quais condições seria possível a adoção de uma norma, no âmbito do Mercosul, destinada a proteger o consumidor contra o *personal data breach*, aos moldes do Regulamento Geral de Proteção de Dados da União Europeia?

A hipótese de trabalho, que responde ao problema em questão, aponta no sentido de que a viabilização do referido espelhamento normativo é possível no atual cenário do Mercosul diante da:

(i) insuficiência legislativa, no âmbito do Mercosul, em matéria de proteção de dados pessoais, ao passo que existe uma forte tendência regional e internacional de normatização e padronização da temática;
(ii) compatibilidade relativa de critérios técnicos das leis protetivas de dados pessoais dos Estados Partes do Mercosul entre si e com o RGPD.

A somatória destas condições leva à conclusão de que uma harmonização legislativa pelo Mercosul sobre proteção de dados pessoais é necessária e que um espelhamento no modelo europeu facilitará o tratamento e a circulação de dados pessoais, diminuirá os casos de *personal data breaches* e reforçará a proteção regional do consumidor.

Portanto, o objetivo geral da dissertação é verificar a viabilidade da adoção de uma norma, no âmbito do Mercosul, à luz do Regulamento Geral de Proteção de Dados da UE, que defenda os consumidores contra o *personal data breach*.

Assim, a dissertação está dividida em três capítulos, cada qual com seus respectivos objetivos específicos. O primeiro capítulo versará sobre a privacidade e a proteção de dados pessoais; o segundo abordará o RGPD e o *personal data breach;* e o terceiro analisará a possibilidade de adoção de norma mercosurenha baseada no RGPD, a partir da experiência legislativa interna dos Estados Partes.

No primeiro capítulo, buscar-se-á (i) contextualizar o direito à privacidade na sociedade da informação; (ii) esclarecer os conceitos, os aspectos humano e fundamental e a principiologia no tocante aos dados pessoais e dados sensíveis; e (iii) relacionar sua evolução jurídica protetiva com a moderna tecnologia, segurança, criminalidade e caráter transfronteiriço dos dados pessoais.

No segundo capítulo, buscar-se-á (iv) contextualizar a legislação global, regional europeia e regulações nacionais sobre privacidade e proteção de dados; (v) descrever a estrutura e funcionamento do RGPD; (vi) descrever os direitos dos titulares e as obrigações das autoridades de controle e de tratamento; (vii) explicar sobre os incidentes e violações de dados, incluindo o *personal data breach*; e (viii) descrever mecanismos de segurança de dados pessoais criados pelo RGPD.

No terceiro capítulo, buscar-se-á (ix) contextualizar a proteção de dados pessoais na América Latina; (x) investigar a produção legislativa mercosurenha sobre defesa do consumidor, comércio eletrônico e proteção de dados pessoais; (xi) investigar os direitos internos argentino, brasileiro, paraguaio, uruguaio e, como estudo paralelo, dos países falantes da língua portuguesa, sobre proteção de dados pessoais; e (xii) analisar, comparar e discutir a formulação de uma norma, no âmbito do MERCOSUL, seguindo os moldes do RGPD.

Ao final, como contribuição prática desta dissertação, e possivelmente como esboço inicial para eventual adoção de norma em matéria de proteção e circulação de dados pessoais a este cenário regional, será apresentada uma proposta de tratado baseada nas quatro legislações de proteção de dados pessoais dos Estados Partes do Mercosul e inspirada nas disposições do RGPD.

O método de abordagem utilizado na dissertação é a pesquisa qualitativa e aplicada. O fator qualitativo reside no fato de que a análise da viabilidade de criação de norma específica sobre dados pessoais, para proteção do consumidor contra o *personal data breach*, no MERCOSUL, requer maior interpretação do objeto e contexto investigados, além de possuir múltiplas fontes. Seu caráter aplicado consiste na busca de soluções para problemas e interesses regionais.

O método de procedimento usado é a pesquisa normativa-descritiva - por envolver análise de legislações nacionais e estrangeiras[3], notadamente no tocante ao tratamento e violações de dados pessoais, das nações mercosurenhas e da UE, bem como eventuais resoluções do MERCOSUL – e comparativa – uma vez que envolve o potencial espelhamento de modelos legislativos e a análise de compatibilidade (semelhanças e diferenças) entre direitos internos.

A técnica de pesquisa é a bibliográfica e a documental – mormente sobre diplomas legais de regulação e violação de dados pessoais; obras jurídicas de direito digital e consumerista; e textos especializados sobre direito internacional, transnacional, comparado e da integração.

Considerando a diversidade e especificidade das temáticas dos três capítulos envolvidos na dissertação, serão utilizadas três teorias de base em seu desenvolvimento. A primeira, conectará a proteção dos dados pessoas ao direito à privacidade. A segunda, trabalhará o *personal data breach* e as medidas protetivas do RGPD. A terceira, apresentará análises e critérios comparativos para verificação da viabilidade de criação de uma norma sobre proteção de dados pessoais, no MERCOSUL, baseada no RGPD.

A primeira teoria basilar compreenderá a "concepção protecionista dos dados pessoais como direito fundamental e suas relações com o direito à privacidade", desenvolvida por Danilo Doneda (2010[4], 2011[5]).

A segunda teoria de base compreenderá a conceituação, distinção e classificação de *security breach* (violação de segurança), *data breach* (violação de

[3] Tendo em vista que grande parte do referencial teórico da dissertação está em língua estrangeira, notadamente nos idiomas inglês e espanhol, e que muitas legislações internacionais foram utilizadas para fins descritivos e comparativos, para manter certa uniformidade de escrita e fluidez de leitura, no decorrer do trabalho, não constarão os textos nos idiomas originais. Constarão as traduções diretas do autor, com hyperlinks e/ou referências em rodapé para consulta dos originais. Serão mantidas, contudo, pequenas expressões estrangeiras com suas respetivas traduções no corpo do texto para rápida compreensão dos seus significados. Conceitos de maior complexidade constarão em rodapé, com suas respectivas significações, a título de glossário e com o objetivo de não saturar o texto e/ou desviar o foco da discussão. A justificativa reside no fato de que o Direito Digital e a Ciência da Computação utilizam muitos vocábulos técnicos e estrangeiros.

[4] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010.

[5] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 92.

dados) e *personal data breach* (violação de dados pessoais) da Direção Geral de Políticas Internas Europeia (2013)[6].

A terceira teoria de base compreenderá os "critérios de comparação legislativa de proteção de dados entre países pertencentes ao mesmo bloco econômico", usada por Felipe Stribe da Silva (2015)[7], bem como o estudo sobre a "compatibilidade de modelos normativos entre países falantes da língua portuguesa" de Manuel David Rodrigues Masseno (2018)[8].

A justificativa para escolha do tema da dissertação é multifatorial. São diversas as razões motivadoras, tendo em vista os atuais impactos nas dimensões jurídica, social, cultural, acadêmica, tecnológica, informacional e securitária que a discussão assume perante as civilizações modernas, em macroescala, e diante do MERCOSUL, em escala regional e nacional.

O trabalho é juridicamente relevante, pois consiste na tentativa de normatização padronizada e regional contra o *personal data breach*, questão insatisfatoriamente regulamentada e responsável por violações de direitos fundamentais, humanos e consumeristas que, em verdade, há tempo aguardam efetivação, o que esta idealizada harmonização legislativa poderia contribuir.

A importação ou cruzamento de modelos legislativos - neste caso, de protótipo europeu - fomenta a produção horizontal de conteúdo jurídico e o diálogo com o direito comparado, direito internacional, direito transnacional e com o direito da integração. Tais "experimentos", em que pese dificultados pela aculturação, têm se mostrado positivos e construtivos, o que valida juridicamente a discussão.

Complementarmente, o estudo das causas e efeitos das violações de dados pessoais – como alternativas preventivas - e a análise das violações de direitos humanos, fundamentais e consumeristas pela exposição de informações pessoais e apresentação de contramedidas legais – como alternativas protetivas, indenizatórias e penalizantes – igualmente tem mérito jurídico.

---

[6] EUROPEAN PARLIAMENT. Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy Industry, Research and Energy**. Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts**, 2013.

[7] DA SILVA, Felipe Stribe. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria, 2015. Dissertação. Universidade Federal de Santa Maria (UFSM).

[8] MASSENO, Manuel David Rodrigues. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa: uma cartografia das Fontes Legislativas. **Revista Direito & TI – Debates Contemporâneos**: Porto Alegre, 2018.

Também é perceptível a importância institucional dos programas de especialização *lato sensu* e *stricto sensu* jurídicos das universidades ao fomentar a discussão e produção de material crítico e analítico sobre temas controversos e modernos. Ademais, a inclusão de linhas de pesquisas multidisciplinares e transfronteiriças ambientam o direito regional e globalmente.

Nesta dissertação em particular, o direito digital e o direito da integração possuem grande relevo, porém estas áreas jurídicas não são numerosas nas linhas e projetos de pesquisa das universidades brasileiras. O surgimento de novos direitos, especialmente os de terceira e quarta dimensões, e o influxo da globalização são fatores que requerem maiores discussões acadêmicas.

Esta necessidade de aprofundamento está interligada às significativas transformações dos direitos e deveres provocados pelas novas tecnologias e pela influência transdisciplinar e internacional. Novos aportes teóricos contemporâneos teriam a missão de sofisticar estas discussões, modernizar estas relações e garantir à ciência jurídica a dinamicidade e atualidade que ela demanda.

Portanto, o estudo está inserto na Linha de Pesquisa 2 (“Sociedade, Novos Direitos e Transnacionalização”) do PPGDir (Programa de Pós-Graduação em Direito) da Unisinos (Universidade do Vale do Rio dos Sinos) e cria um diálogo aberto com o Projeto de Pesquisa desenvolvido pela Prof.ª Dra. Luciane Klein Vieira, intitulado “Coexistência, cooperação e solidariedade: o diálogo entre o Tribunal Permanente de Revisão e os tribunais constitucionais nacionais para a uniformização da interpretação e aplicação do Direito Ambiental e do Direito do Consumidor, no MERCOSUL”.

A temática se destaca, ainda, pela sua importância social e cultural. O *personal data breach* afeta direta e indiretamente consumidores empresas, órgãos e entidades cujos dados pessoais são vazados. Há um choque entre privacidade e segurança e isto repercute sobremaneira na forma como as pessoas físicas e jurídicas, nacional ou regionalmente, manuseiam as suas informações sensíveis.

Ademais, como as técnicas invasivas são complexas, criativas e mutáveis, o investimento na prevenção, proteção e responsabilização é necessário. Esta blindagem tecnológica, securitária e jurídica depende de uma mudança de postura cultural, uma vez que a adequação de todos aos parâmetros, protocolos e diretrizes - digitais, legais e burocráticas - é indispensável ao seu sucesso.

A atualidade da temática é indiscutível. O RGPD tornou-se aplicável em 25 de maio de 2018. Anúncios de atualização de políticas de privacidade de *softwares, desktops* e aplicativos *mobiles*, especialmente de redes sociais, de grandes e pequenas empresas, irromperam nos noticiários televisivos e navegadores digitais.

A repercussão é notável, mesmo porque é um feito legislativo histórico. Trata-se do mais completo regulamento - acredita-se que mundialmente - sobre o tratamento, o processamento, a transferência e a responsabilização no quesito de dados pessoais e dados sensíveis. Caracteriza uma empreitada sem precedentes contra as mazelas digitais.

# 2 DIREITO À PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS

Neste primeiro capítulo será contextualizado o direito à privacidade na Sociedade da Informação, esclarecidos os conceitos, aspectos humanos e fundamentais e a principiologia relativa aos dados pessoais e dados sensíveis. Também será relacionada a evolução jurídica protetiva com a moderna tecnologia, segurança, criminalidade e caráter transfronteiriço dos dados pessoais.

## 2.1 Histórico e conceito do direito à privacidade

A tríade progresso, direito e tecnologia delimita os contornos da indiscutível importância e do crescimento da preocupação atual dos cidadãos e governos com a tutela da privacidade. Trata-se de uma inquietação justificável, bastante característica desta era cibernética que vivenciamos, muito embora a noção de privacidade seja datada de outras épocas, com diferentes significados e, suas primordiais versões, localizadas em diversas sociedades.

A privacidade nem sempre foi considerada valorosa o suficiente para receber proteção jurídica, uma vez que não passaria de um sentimento subjetivo, de uma abstração pessoal. Igualmente não tinha vez em todas as sociedades, porquanto incompatível com aquelas detentoras de outros mecanismos regulatórios, como rígidas hierarquias sociais, arquiteturas dos espaços públicos e privados e ordenamentos jurídicos patrimonialistas ou corporativistas[9].

Investigando o passado, é possível encontrar vestígios de proteção à privacidade no instituto romano do *jus utendi* (direito de usar)*, fruendi* (direito de fruir) *et abutendi* (direito de dispor), direitos estes que asseguravam ao *dominus* (proprietário) amplas faculdades sobre as coisas que lhe pertenciam. Ainda que bastante relacionada com a noção de propriedade, o instituto trazia consigo a ideia de proteção à vida privada[10].

Percebe-se, avançando na crônica jurídica, que esta vinculação entre privacidade e propriedade romana influenciou o pensamento e o sistema britânico (*Common Law*). Os juízes ingleses também costumavam tratar a *privacy* (privacidade)

---

[9] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Monografia. Rio de Janeiro: Renovar, 2006. p. 4.

[10] FERNANDES, Milton. **Os direitos de personalidade:** estudos jurídicos em homenagem ao Professor Caio Mário da Silva Pereira. Rio de Janeiro: Forense, 1984. p. 12-13.

como *property* (propriedade), restringindo sua proteção no máximo à violação de atos ilícitos específicos como calúnia, difamação e quebras contratuais (aproximando-se dos direitos à honra)[11].

Nesta busca pela origem do "direito à privacidade", alguns estudiosos defendem que seu surgimento reside nas teses filosóficas dos britânicos John Locke e John Stuart Mill sobre liberdade, propriedade e responsabilização; com Locke sustentando a ideia de liberdade como autonomia para dispor da sua própria pessoa, atos e posses[12] e, Mill, argumentando que as condutas individuais não produzem deveres sociais se não afetarem outras pessoas[13].

Ainda em retrospecto histórico, encontram-se os episódios dos vazamentos não autorizados das cartas privadas dos literatos Alexander Pope e Jonathan Swift[14], cujo editor responsável pelas indevidas divulgações foi condenado, e da reprodução gráfica e venda de objetos de coleção privada do Príncipe Albert e da Rainha Vitória[15], cuja propriedade lhes restou ulteriormente assegurada pelo tribunal[16].

Indícios antigos de concessão de tutela jurídica do direito à privacidade também podem ser resgatados em julgados italianos. Tem-se o caso do filme biográfico do tenor Enrico Caruso onde expuseram aspectos íntimos da vida do cantor[17], cujo processo resultou no reconhecimento do *diritto alla riservatezza*; e do tratamento midiático acerca do relacionamento do ditador Benito Mussolini com sua amante[18] - o que lhes rendeu incidentes judiciais[19].

Ademais, Sampaio elenca dois antecedentes diferentes como marcos do direito à privacidade. O primeiro, indica como sendo o trabalho "*Grundzüge des naturrechts"*

---

[11] ALENCAR, Ianara de Souza; PACHECO, Ludgard Vinicius Andrade; FERREIRA, Rodrigo L. **A Evolução do conceito de privacidade diante das novas tecnologias utilizadas nos correios eletrônicos (E-mail).** Piauí: Revista de Direito UNINOVAFAPI. v. 1, n. 1., 2016. Disponível em: <https://revistainterdisciplinar.uninovafapi.edu.br/index.php/revinterdireito/article/view/1106/559 >. Acesso em: 15 jan. 2019.

[12] LOCKE, John. **Segundo tratado sobre o governo civil:** ensaio sobre a origem, os limites e os fins verdadeiros do governo. Petrópolis: Vozes, 1999.

[13] MILL, John Stuart. **A liberdade/utilitarismo.** 1. ed. Martins Fontes, 2000.

[14] POPE V. CURL, 26 Eng. Rep. 608 (1741); BLACKSTONE, William. ***Commentaries on the Laws of England.*** Oxford: Clarendon Press, 1765. p. 407.

[15] PRINCE ALBERT V. STANGE 64 ER 293 (1848).

[16] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Monografia. Rio de Janeiro: Renovar, 2006. p. 6.

[17] TRIBUNAL DE ROMA, sentença de 14 de setembro de 1953; DE CUPIS, Adriano. ***Il diritto all riservatezza existe***, in: Foro Italiano, IV. p. 90-97.

[18] AMADEO, Auletta Tommaso. ***Riservatezza e tutela della personalità.*** Milano: Giuffrè, 1978. p. 63-64.

[19] DONEDA, op. cit., p. 6.

(1846)[20], do advogado alemão Karl David August Röder, no qual o este definiu como condutas violadoras de privacidade os atos de incomodar outrem com perguntas indecentes ou adentrar recintos sem prévio anúncio, práticas estas mais relacionadas à etiqueta em tempos pretéritos[21].

O segundo precedente, sugere ser o estarrecedor caso *Affaire Rachelix c. O'Connell*[22], episódio acontecido com Elisa Rachel Félix, famosa atriz de teatro clássico francesa do século XIX, que solicitou que fosse fotografada em seu leito de morte. O problema residiu no fato de a referida imagem ter sido disponibilizada, sem autorização, à desenhista e, posteriormente, publicada em seminário. A família acionou a justiça e o tribunal decidiu em seu favor[23].

Imperioso registrar, todavia, que expressões como "intimidade", "privacidade" e "vida privada" não constavam no vocabulário da época, mas estes antecedentes "elitistas" trazidos pela doutrina - motivados pelo novo individualismo, pela nova relação entre Estado e cidadão, pela evolução tecnológica e pelo maior fluxo de informações - contribuíram sobremaneira para que os tribunais acolhessem aos poucos as teses sobre o direito à privacidade[24].

Não obstante a relevância dos incidentes mencionados, a doutrina majoritária considera como marco inicial e oficial do direito à privacidade o famigerado artigo *The right to privacy*[25], de autoria de Warren e Brandeis, publicado na *Harvard Law Review* (1980). O estudo foi uma tentativa de fixação dos limites relacionados à interferência na vida privada, inspirado na expressão "*right to be alone*" do juiz Cooley[26] e no escândalo conjugal da vida de Warren[27].

Em que pese a reverência e frequência com que o artigo é invocado, a crítica especializada - e a complexidade que o paradigma da privacidade alcançou não deixa

---

[20] RÖDER, Karl David August. ***Classic Reprint Series*****:** Grundzüge des Naturrechts oder der Rechtsfilosofie. Londres: Forgotten Books, 2018.
[21] SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família da comunicação e informações pessoais.** Belo Horizonte: Del Rey, 1998. p. 55.
[22] TRIBUNAL CIVIL DE LA SEINE (16 de junho de 1858, D>P., 1858.3.62); LINDON, Raymond. ***Une création pretorienne: Les droits de la personnalité*****.** Paris: Dalloz, 1974. p. 11.
[23] SAMPAIO, op. cit., p. 34.
[24] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Monografia. Rio de Janeiro: Renovar, 2006. p. 6-7.
[25] BRANDEIS, Louis; WARREN, Samuel. ***The right to privacy*****.** In: 4 Harvard Law Review 193, 1980.
[26] Expressão utilizada pelo juiz Thomas McIntyre Cooley no seu *Treatise of the law of torts* (1888), *v.* capítulo 3.2 e que poderia ser traduzida como "direito de ser deixado só".
[27] MACHADO, Joana de Moraes Souza. **A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados.** Revista da Ajuris: v. 41, n. 134, 2014. p. 6.

desmentir - concluiu que seus autores não foram capazes de definir os contornos do "direito à privacidade" a que se propuseram, mas apenas o limiar do "direito a ser deixado só". Neste contexto, a privacidade traduziria apenas uma prerrogativa individualista da classe burguesa[28].

Doneda entende haver uma continuidade temporal e não um obstáculo neste panorama. Argumenta que a privacidade surgiu com uma *zero-relationship*, uma carência de comunicação entre um ser humano e os demais, evidenciando um acentuado individualismo, entretanto, que esta concepção primeva foi otimizada com o passar do tempo em virtude da conscientização de que a privacidade é fundamental ao desenvolvimento da personalidade humana[29].

Considerando todo este histórico, como poderíamos conceituar apropriadamente o termo "privacidade"? Etimologicamente, a palavra possui raiz latina: *privare,* como verbo; *privatus*, como adjetivo. Muito embora a língua portuguesa derive sobremaneira do tronco linguístico latino, também reconhece as influências da língua inglesa – onde a privacidade fora bastante discutida -, razão pela qual sua derivação de *privacy* parece mais acertada[30].

Habermas denunciava a existência de múltiplos significados correntes, a variar conforme a época que estivesse associada, o que dificultaria ao direito, sociologia e política alcançar uma conceituação padrão[31]. Rodotà define sê-la "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular"[32], conferindo uma aparente maior relevância aos dados digitais.

Machado, revisando os estudos de Sampaio e a literatura de Kant, afirma que "[...] o direito à privacidade se mostra como uma nova forma de liberdade pessoal, que já não é mais a liberdade negativa de recusar ou proibir a utilização das informações

---

[28] MACHADO, Joana de Moraes Souza. **A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados.** Revista da Ajuris: v. 41, n. 134, 2014. p. 7.
[29] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Monografia. Rio de Janeiro: Renovar, 2006. p. 4-8.
[30] Ibid., p. 66.
[31] HABERMAS, Jürgen. ***Storia e critica della opinione pubblica.*** 5. ed. Editore Laterza, 2006. p. 11.
[32] RODOTÁ, Stefano. **A vida na sociedade de vigilância.** A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008. p. 15.

sobre a própria pessoa [...]". Avança defendendo que a privacidade se transformou na "[...] liberdade positiva de poder controlar os dados concernentes à própria pessoa."[33]

Imperioso observar que Warren, Brandeis e Cooley - autores do sistema do *common law* do final do século XIX - representam uma noção de privacidade relacionada à propriedade; já Rodotà, Sampaio e Machado - autores do *civil law* e da modernidade - defendem uma noção de privacidade com maior enfoque na questão informacional. Todos, contudo, parecem tentar, cada qual ao seu tempo, atualizar certos aspectos da privacidade.

Inclusive, lembra Doneda que Hubmann tentou conciliar as esferas de intimidade, privacidade e a vida pública[34]. A própria CRFB/1988, por exemplo, tratou do assunto e inseriu a proteção da "intimidade" e "da vida privada" (além da "honra" e "Imagem") entre as garantias e direitos fundamentais (art. 5º, inciso X), deixando ao intérprete sua aferição. Neste sentido, Doneda argumenta ser descabida a conceptualística linguística, uma vez que cada um dos vocábulos citados possui um campo semântico próprio, servindo, neste caso, não mais que um ardil retórico.

Explica que a literalidade de "vida privada" invoca a separação do que seja vida pública e vida privada, prezando por uma lógica de exclusão e enfatizando uma desunidade jurídica. Também esclarece que a literalidade de "intimidade" reflete uma sensação de particularidade e tranquilidade[35] e comporta uma carga emotiva que torna as noções de intimidade equívocas e ambíguas, dificultando a objetivação e mensuração do seu significado[36].

Acredita Doneda que a utilização da expressão "privacidade" seja a mais razoável por ser específica e atualizada o suficiente, por se distinguir de outros termos congêneres (imagem, honra ou identidade pessoal) e por compreender as noções de "vida privada" e "intimidade" que, a bem da verdade, servem mais como determinantes da amplitude da proteção à privacidade (uma vez que seus significados oscilam demais, conforme o contexto e momento histórico)[37].

---

[33] MACHADO, Joana de Moraes Souza. **A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados.** Revista da Ajuris: v. 41, n. 134, 2014. p. 10.
[34] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Monografia. Rio de Janeiro: Renovar, 2006. p. 67.
[35] Ibid., p. 68.
[36] LUÑO, Antonio-Henrique Pérez. ***Derechos humanos, estado de derecho y constituición***. Madrid: Tecnos, 1986. p. 327.
[37] DONEDA, op. cit., p. 87.

Outrossim, revela-se pertinente a transcrição da síntese do pensamento de Doneda acerca das inquietações que envolvem o direito à privacidade, direito este que, segundo o estudioso, vem passando por um acelerado processo de readequação temporal e reorientação espacial. Uma verdadeira transformação protetiva centrada no indivíduo e causada pela evolução tecnológica e informacional. Nas palavras do autor:

> A trajetória percorrida pelo direito à privacidade reflete uma mudança de perspectiva para a tutela da pessoa quanto a sua adequação às novas tecnologias de informação. Não basta pensar na privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma "predileção" individual, associada basicamente ao conforto e comodidade. A própria visão de privacidade como algo de que um cidadão respeitável poderia tranquilamente abrir mão (ou que ao menos se esperasse isto de um cidadão honesto e de bons costumes), a presumida "transparência de quem não tem nada a temer" [...] deixa de fazer sentido dada a crescente complexidade da matéria. Uma esfera privada, na qual a pessoa tenha condições de desenvolvimento da própria personalidade, livre de ingerências externas, ganha hoje ainda mais em importância; passa a ser pressuposto para que não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada (para tocar em conceito caro ao direito privado) e, em última análise, inviabilizariam o livre desenvolvimento de sua personalidade[38].

Refutando a predominância atual de um direito à privacidade subjetivista, individualista e patrimonialista, defende o autor que a complexidade do assunto ocasionou uma ressignificação do que seja a privacidade. Ressalta ainda ser mais valorosa a administração de um direito à privacidade que permita que seu direito personalíssimo seja respeitado e desenvolvido do que a reminiscência de um direito à privacidade atrelado a controles externos que lhe tolham autonomia.

Não dissonante destas ponderações, Iturraspe reconhece a pessoa humana como núcleo das preocupações do direito à privacidade e o seu caráter relacional, reforçando a ideia de se tratar de um direito de terceira ou quarta geração. Isto porque almejaria a completude e plenitude de uma proteção jurídica, seja na esfera pública ou particular, que garantisse também a liberdade, segurança, dignidade, respeito e identidade do ser humano[39].

---

[38] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Monografia. Rio de Janeiro: Renovar, 2006. p. 87.

[39] ITURRASPE, Jorge Mosset et. al. **Daños. Globalizacion – Estado – Economía.** Buenos Aires: Rubinzal-Culzoni, 2000. p.9.

Esta concepção moderna de maior amplitude da proteção à privacidade condiz com a definição proposta por Rodotà de sê-la "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada"[40]. Quer dizer com a assertiva que o novo eixo da privacidade agora é "pessoa-informação-circulação-controle" em substituição à estrutura antiga "pessoa-informação-segredo".

Foi seguindo esta tendência evolutiva que caiu em desuso nos tribunais alemães, tornando-se corrente minoritária, a referenciada *teoria das esferas concêntricas da vida privada* de Heinrich Hubmann. Segundo doutrina o autor, a personalidade humana possui diferentes níveis de manifestação e, portanto, pode ser dividida em: *Intimsphäre* (esfera da intimidade), *Privatsphäre* (esfera da privacidade) e *Geheimnisphäre* (esfera do segredo)[41].

Haveria, desta forma, uma tríplice dimensão da privacidade. Contudo, a outrora festejada esquematização sofreu variações quando atualizada por diferentes estudiosos. Heinrich Henkel foi um dos revisores da teoria, que também apresentou uma versão tripartida dos círculos concêntricos (um dentro do outro), porém utilizando uma diversa classificação, a qual acabou se tornando o entendimento majoritário alemão e foi melhor difundida no exterior[42].

Na variante de Henkel, dividiam-se os círculos da vida privada (em sentido amplo) em círculo da vida privada (em sentido estrito), círculo da intimidade e círculo do segredo. O círculo da privacidade seria a camada mais externa, onde aconteceriam as relações interpessoais superficiais, incluindo o convívio com indivíduos próximos e excluindo terceiros sem quaisquer conexões. Ter-se-ia aqui um interesse público, sem perda da condição de íntimo e de privado.

O círculo da intimidade seria a esfera intermediária, representando as relações mais reservadas, dispensando a divulgação ou conhecimento de outrem a quaisquer fatos da vida do indivíduo, a exemplo da inviolabilidade domiciliar, profissional e telefônica. Já o círculo do segredo seria a esfera mais interna, a camada mais

---

[40] RODOTÀ, Stefano. ***Tecnologie e diritti.*** Bolgna: Il Mulino, 1995. p 122.
[41] HUBMANN, Heinrich. ***Der zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion.*** 1957. p. 524, ID, *Das Persönlichkeitsrecht*. 2. ed., Köl/Graz, 1967, §34. p. 268-271.
[42] BOLESINA, Iuri; ROSSONI, Caroline. **A teoria dos círculos concêntricos e a proteção à vida privada:** análise ao caso Von Hannover Vs. Alemanha, julgado pela Corte Europeia de Direitos Humanos. In: XI Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea – VII Mostra de Trabalhos Jurídicos Científicos. 2014. p. 3.

profunda, simbolizando as informações mais sigilosas da pessoa como orientação sexual, religiosa, política, ideológica etc.

Não obstante a dificuldade de dissecar e interpretar as nuances da vida privada por envolverem aspectos subjetivos do ser humano, a teoria dos círculos concêntricos permite compreender a plenitude e a não limitação do direito à privacidade; sua elasticidade ou capacidade de flexibilização, quando enxergadas suas diversas profundidades de manifestação, capacitam melhores análises dos casos concretos e oportunizam melhores escolhas protetivas.

Acompanhando, ainda, o raciocínio de Bolesina e Rossoni, ao se considerar a potencialidade lesiva da interferência de terceiros na vida privada de alguém, percebe-se uma proporcionalidade entre o grau de profundidade da invasão e o grau de violação dos direitos personalíssimos: quanto maior a escala de quebra de privacidade (do mais interno círculo concêntrico), maior o prejuízo causado ao indivíduo e, portanto, maior o nível de proteção necessitado[43].

A classificação segundo esquematização em círculos concêntricos da vida privada proporciona um interessante critério avaliativo, pelo menos um pouco mais objetivo e com razoável maleabilidade, capaz de auxiliar no processo de identificação da intensidade danosa e da metodologia protetiva cabível. Acaba por ajudar no combate ao subjetivismo do julgador quando impregnado este com pré-conceitos moralistas.

O investigar dos introitos, constructos e desdobramentos histórico/culturais, etimológico/gramaticais e doutrinário/jurisprudenciais são fundamentais para a compreensão do surgimento, evolução e proteção dos dados pessoais e dados sensíveis. No entanto, é indispensável que algumas noções básicas da área computacional e informacional sejam revisitadas antes, com enfoque particular no tocante aos dados, informações e bancos de dados.

## 2.2 Dados, informações e bancos de dados

A compreensão do que sejam dados pessoais e da importância de protegê-los requer o entendimento anterior do que sejam dados, informações, metadados e banco

[43] BOLESINA, Iuri; ROSSONI, Caroline. **A teoria dos círculos concêntricos e a proteção à vida privada:** análise ao caso Von Hannover Vs. Alemanha, julgado pela Corte Europeia de Direitos Humanos. In: XI Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea – VII Mostra de Trabalhos Jurídicos Científicos. 2014. p. 3-5.

de dados. Para concatenar e diferenciar estes elementos e ferramentas indispensáveis ao processamento, armazenamento, gerenciamento, manipulação, apresentação, tratamento e proteção dos dados pessoais, na sequência serão apresentados conceitos-chaves recorrentes na área da Ciência de Dados[44].

Para começar, imagine o ambiente em que você vive, o mundo em que você habita. Todo esse espaço no qual você está inserto é composto por coisas e essas coisas possuem fatos sobre elas que valem a pena ser considerados. Pois bem, esses fatos brutos que caracterizam as coisas são chamados de *dados* - pode haver inclusive um fato único, caso no qual é chamado de *fragmento de dado*[45]. Em outras palavras, "dados são um conjunto de fatos primários dos quais conclusões podem ser extraídas"[46].

Este estado de bruteza dos fatos indica que eles não foram processados ainda para revelar seu significado. Aqui reside uma famosa confusão terminológica entre dados e *informações*[47], uma vez que o conteúdo de ambos aparece em situações similares, fazendo com que suas nomenclaturas sejam equivocadamente utilizadas como sinônimos. Certifica-se Doneda de descomplicá-los, esclarecendo a finalidade de ambos e o momento no estágio de cognição que os diferencia:

> Ambos os termos servem para representar um fato, determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular a ser considerado. Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada [...] o dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a

---

[44] *Ciência de dados:* "[...] é uma disciplina emergente que permite às empresas obterem valor de negócio a partir da big data. Ciência de dados representa a síntese de várias disciplinas existentes, tal como estatística, matemática, visualização de dados e ciência da computação, permitindo ao cientista de dados desenvolver algoritmos avançados com a finalidade de analisar uma grande quantidade de informações para criar novo valor e tomar mais decisões baseadas em dados [...]". (SOMASUNDARAM, G; SHRIVASTAVA, A.; **EMC Education Services. Armazenamento e Gerenciamento de Informações.** São Paulo: Bookman, 2012. p. 11).

[45] GILLENSON, Mark. L. **Fundamentos da gerência de banco de dados** tradução Acauan Fernandes, Elvira Maria Antunes Uchôa. – Rio de Janeiro: LTC, 2006. p. 15.

[46] SOMASUNDARAM et al., op. cit., p. 11.

[47] *Informação:* "Significado dos dados tal como se pretende que as pessoas os interpretem. Os dados consistem em factos, que se tornam informações quando examinados no devido contexto, transmitindo um significado às pessoas. Os computadores processam dados sem qualquer entendimento daquilo que eles representam". (MICROSOFT, Corporation. **Dicionário Prático de Informática.** – 22. ed. Portugal: McGraaw-Hill, 2000. p. 172).

> informação carrega também um sentido instrumental, no sentido da redução de um estado de incerteza [...][48].

Depreende-se da explicação acima que os dados são anteriores e, portanto, é válido dizer que "os dados são o fundamento das informações"[49] e é justamente a ocorrência de um *processamento*[50] que demarca o ponto de transição daqueles para estas. Este processamento dos dados pode ser simples (organização em padrões) ou complexo (previsões estatísticas), mas é através deles que é descoberto o contexto dos dados e revelado ao interessado seus significados (informações).

O processamento também auxilia na formatação adequada dos dados para viabilizar e facilitar o *armazenamento*[51], *gerenciamento*[52] e *apresentação*[53] das informações posteriormente[54]. São estas engenhosas e invisíveis ações, dentre outras cujo destaque não é agora oportuno, que movimentam, em microescala, o mundo dos *bits*[55] *e bytes*[56] e, em macroescala, toda a infraestrutura de dados virtuais privada e pública globalmente.

---

[48] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 94.

[49] PETER, Rob; CORONEL, Carlos. **Sistemas de banco de dados: projeto de implementação e gerenciamento.** revisão técnica Ana Paula Appel; [tradução All Tasks]. 8. ed. – São Paulo: Cengage Learninh, 2011. p. 4-6.

[50] *Processamento de dados:* "Manipulação de dados num sistema de computador. O processamento representa o passo essencial entre a recepção dos dados (entrada) e a produção de resultados (saída)". (MICROSOFT, Corporation. **Dicionário Prático de Informática**. – 22. ed. Portugal: McGraaw-Hill, 2000. p. 269).

[51] *Armazenamento de dados:* Em informática, "[...] designa qualquer dispositivo no qual se pode guardar informação. Os microcomputadores têm dois tipos principais de armazenamento: a memória de acesso aleatório e as unidades de disco e outros meios de armazenamento externo. Outros tipos de armazenamento incluem a memória só de leitura e as memórias temporárias". (Ibid., p. 316).

[52] *Gerenciamento de dados:* Em informática, significa "[...] Controlo dos dados, desde a obtenção e introdução até ao processamento, saída e armazenamento. Por exemplo, as aplicações gerem dados quando recebem e processam entradas e quando enviam os resultados para um dispositivo de saída ou para o armazenamento em disco. O utilizador também gere dados, quando arquiva ficheiros e quando remove material desnecessário. " (Ibid., p. 92).

[53] *Apresentação de dados:* Em informática, significa "[...] A sexta das sete camadas do modelo ISO/OSI para a normalização da comunicação entre computadores. A camada de apresentação é responsável pela formação da informação, de modo que esta possa ser apresentada ou impressa. Esta tarefa costuma incluir códigos de interpretação (como tabulações) relacionados com a apresentação, mas também pode incluir código de conversão de encriptação e outros, além de tradução de diferentes conjuntos de caracteres [...]". (Ibid., p. 264).

[54] PETER et al, op. cit., p. 5-6.

[55] *Bit:* "*s.m.* Abreviatura de binary digit (algarismo binário). A mais pequena unidade de informação gerida por um computador [...]". (MICROSOFT, op. cit., p. 36).

[56] *Byte:* "*s.m.* Abreviatura de binary term (termo binário). Unidade de dados, composta, a maior parte das vezes, por 8 bits. Um byte pode representar um único carácter, como seja uma letra, um algarismo ou um sinal de pontuação [...]". (MICROSOFT, Corporation. **Dicionário Prático de Informática.** – 22. ed. Portugal: McGraaw-Hill, 2000. p. 47).

Destarte, em nível planetário, não é difícil conceber que a presente era tecnológica precisou de novas ferramentas para suportar a produção maciça e o tráfego acelerado de dados sem que houvesse desperdícios com *manutenção de dados*[57] e precisão das informações, mesmo porque a sobrevivência virtual do mundo dependia desta otimização. Eis que então as funções de armazenar e acessar dados com celeridade e praticidade ganharam a notoriedade devida, já que outrora eram vistas como simples funcionalidades[58].

A solução adequada de gerenciamento encontrada pelos especialistas foi o investimento nos *data bases* (bases de dados[59] ou banco de dados[60]), estruturas computacionais integradas[61] ou compartilhadas[62] que armazenam blocos de dados finais (dados relativos aos usuários) e *metadados*[63] (dados relativos aos dados). Enquanto as bases de dados servem como arquivos eletrônicos organizados, os metadados registram as características dos dados, tudo através de um *sistema de gerenciamento de banco de dados (SGDB)*[64].

O SGDB é o responsável por intermediar a comunicação de usuários e/ou *aplicações*[65] com o banco de dados. Estas e aqueles fazem solicitações e o SGBD traduz os comandos, retornando os resultados desejados e dispensando os

---

[57] *Manipulação de dados:* Em informática, corresponde "[...] Processamento de dados através de programas que aceitam comandos do utilizador, que proporcionam formas de gerir dados e que informam o hardware sobre o que fazer com eles". (Ibid., p. 92).

[58] PETER, Rob. CORONEL, Carlos. **Sistemas de banco de dados: projeto de implementação e gerenciamento**; revisão técnica Ana Paula Appel; [tradução All Tasks]. 8. ed. – São Paulo: Cengage Learninh, 2011. p. 5-6.

[59] *Base de dados:* Em informática, significa "[...] Ficheiro composto por registros cada um com campos e um conjunto de operações para pesquisa, ordenação, combinação e outras funções [...]". (MICROSOFT, op. cit., p. 89).

[60] *Bancos de dados:* "[...] são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações [...]". (DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 92).

[61] *Integração de dados:* "[...] se refere à habilidade de juntar partes de dados relacionados dentro um sistema de informações [...]". (GILLENSON, Mark. L. **Fundamentos da gerência de banco de dados;** tradução Acauan Fernandes, Elvira Maria Antunes Uchôa. – Rio de Janeiro: LTC, 2006. p. 54).

[62] *Redundância de dados:* "[...] se refere ao mesmo fato de o ambiente do negócio estar armazenado mais de uma vez dentro de um sistema de informações [...]". (GILLENSON et al, op. cit., p. 54).

[63] *Metadados:* Em informática, significam "[...] Dados sobre ados. Por exemplo, o título, assunto, autor e tamanho de um ficheiro constituem metadados do ficheiro [...]". (MICROSOFT, op. cit., p. 215).

[64] *Sistema de gerenciamento de banco de dados:* "[...] é um conjunto de programas que gerenciam a estrutura de banco de dados e controlam o acesso aos dados armazenados. Até certo ponto, o banco de dados se assemelha a um arquivo eletrônico com conteúdo muito bem organizado com a ajuda de um software poderoso [...]". (PETER et al., op. cit., p. 6).

[65] *Aplicação:* Em informática, significa "[...] Programa concebido como ferramenta auxiliar para o desempenho de uma determinada tarefa, como o processamento de texto, a contabilidade ou a gestão de inventários [...]". (MICROSOFT, Corporation. **Dicionário Prático de Informática.** – 22. ed. Portugal: McGraaw-Hill, 2000. p. 17-18).

solicitantes de lidar com a complexidade técnica dos bancos de dados. O SGBD elevou a um novo patamar a forma como os dados são manuseados em termos de praticidade, acessibilidade, celeridade e segurança aos usuários. Um inquestionável ganho em eficiência e eficácia.

Especificamente, os BD e os SGBD trouxeram vantagens como o aprimoramento do compartilhamento de dados (quantitativa e qualitativamente), aprimoramento da segurança de dados (menores riscos de falhas securitárias, inconsistência dos dados e melhores políticas de privacidade), aprimoramento da integração e acesso de dados (melhores perspectivas das informações e velocidade no retorno das consultas), bem como produtividade e decisibilidade aos usuários (otimização do processo de tomada de decisão)[66].

Com este potencial tecnológico para sistematizar, armazenar e manipular quantidades colossais de informações houve um crescimento imensurável de aplicabilidades e funcionalidades a elas relacionadas, expandindo seus horizontes para campos técnicos, profissionais e educacionais, além de áreas desportivas, recreativas, pessoais etc. Ato contínuo, deflagrou-se um processo de conquista por cada vez mais espaço no cotidiano das pessoas, notadamente com o barateamento e proliferação de dispositivos portáteis.

Acontece que esta nova revolução digital também trouxe consigo inesperados desafios. A inovação e a recursividade promovidas pelos bancos de dados ocasionam a retenção de diversos dados dos usuários finais, inclusive os que dizem respeito aos seus dados pessoais. Estes últimos, em particular, são os responsáveis por reconfigurar toda a forma como a tutela jurídica - poderes, direitos e obrigações – é utilizada para proteção das informações virtuais. Não apenas juridicamente, mas securitária, econômica, logística e politicamente[67].

Considerando o nível de precisão e minúcia que os dados pessoais fornecem aos terceiros interessados na sua manipulação, compreende-se o porquê de serem cada vez mais visados como *commodities* e aproveitados para desenvolvimento e movimentação de novos mercados, negócios e tendências. Uma vez que estes dados pessoais representam a própria pessoa, sua disponibilização e regulamentação

---

[66] PETER, Rob. CORONEL, Carlos. **Sistemas de banco de dados:** projeto de implementação e gerenciamento; revisão técnica Ana Paula Appel; [tradução All Tasks]. 8. ed. – São Paulo: Cengage Learninh, 2011. p. 7-8.

[67] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 93.

determinarão "a própria autonomia, identidade e liberdade do cidadão contemporâneo"[68].

## 2.3 Segurança de dados

A segurança dos dados está diretamente associada com o conceito de segurança de computadores, tendo em vista que as disposições normativas relativas ao tratamento automatizado e ao resguardo dos direitos e liberdades dos seus titulares são de natureza técnica, as quais se remetem, por conseguinte, aos parâmetros protetivos computacionais.

Seguindo o raciocínio, o Manual de Segurança da Computadores da NIST elucida que a segurança de computadores é a proteção fornecida a um "sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confiabilidade dos recursos do sistema de informação (incluindo *hardware*[69], *software*[70], *firmware*[71], informações/dados e telecomunicações)"[72].

A proteção da integridade, da disponibilidade e da confidencialidade[73] constituem então a tríade dos objetivos fundamentais da segurança de dados e dos serviços de informação e computação que, acompanhados dos propósitos acessórios

---

[68] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 94.

[69] *Hardware:* "*s.m* Componentes físicos de um sistema de computador, incluindo qualquer equipamento periférico, tais como impressoras, modems e ratos [...]". (MICROSOFT, Corporation. **Dicionário Prático de Informática.** – 22. ed. Portugal: McGraaw-Hill, 2000, p. 157).

[70] *Software:* "*s.m* Programas de computador; instruções que dão origem ao funcionamento do hardware [...]". (Ibid., p. 310).

[71] *Firmware:* "*s.m.* Rotinas de software armazenadas na memória só de leitura (ROM). Ao contrário da RAM, a ROM permanece intacta, mesmo na ausência de energia elétrica. As rotinas de iniciação e as instruções de entrada/saída de baixo nível são armazenadas no firmware. Em termos de facilidade de modificação, a classificação do firmware situa-se entre o software e o hardware [...]". (Ibid., p. 138).

[72] SINGHAL, Anoop; WINOGRAD, Theodore; SCARFONE, Karen. NIST – National Institute of Standards and Technology. **Guide to Secure Web Services - SP 800-95.** Computer Security Resource Center (CSRC), 2007. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf>. Acesso: 18 jul. 2019.

[73] *Integridade:* "[...] prevenir-se contra a modificação ou destruição imprópria de informação, incluindo a irretratabilidade e autenticidade dela. Uma perda de integridade seria a modificação ou destruição não autorizada de informação". **Disponibilidade:** "[...] assegurar acesso e uso rápido e confiável da informação. Uma perda de disponibilidade é a perda de acesso ou de uso da informação ou sistema de informação". **Confidencialidade:** "[...] preservar restrições autorizadas sobre acesso e divulgação de informação, incluindo meios para proteger a privacidade de indivíduos e informações privadas. Uma perda de confidencialidade seria a divulgação não autorizada de informação (STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas; tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi, Messer Barreto, Rafael Misoczki. – 6. ed. São Paulo: Pearson Education do Brasil, 2015, p. 7).

de autenticidade e responsabilização[74], defendem organizações, empresas e indivíduos contra quebras de segurança.

Quando estes princípios são desrespeitados (por negligência, imprudência, imperícia, tecnologia desatualizada, maquinário defasado etc.) ou são violados (por ameaças/ataques externos, como *ciberativismo*, *ciberterrorismo* etc.) ocorrem problemas de segurança que costumam ser classificados conforme seus níveis de impacto sobre referidos sujeitos: baixo[75], moderado[76] ou alto[77].

Este nivelamento de impacto diz respeito à potencialidade danosa causada às operações das organizações, aos recursos destas e, especialmente, aos titulares de dados (públicos, pessoais, sensíveis etc.), podendo impedir empresas de executarem suas atividades primárias, reduzir sua eficiência significativa ou drasticamente e lesionar financeira, fisiológica e psicologicamente indivíduos.

A intensidade do impacto, conforme sugestivas nomenclaturas, indica a gravidade dos efeitos adversos decorrentes destes problemas de segurança, a escalar gradativamente, desde uma simples desfiguração do *layout* de um *website*[78]*,*

---

[74] *Autenticidade:* "[...] a propriedade de ser genuíno e capaz de ser verificado e confiável; a confiança na validação de uma transmissão, em uma mensagem ou na origem de uma mensagem. Isso significa verificar que os usuários são quem dizem ser e, além disso, que cada entrada no sistema vem de uma fonte confiável". **Responsabilização:** "[...] a meta de segurança que gera o requisito para que ações de uma entidade sejam atribuídas exclusivamente a ela. Isso provê irretratabilidade, dissuasão, isolamento de falhas, detecção e prevenção de intrusão, além de recuperação pós-ação e ações leais [...]". (STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas; tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi, Messer Barreto, Rafael Misoczki. – 6. ed. São Paulo: Pearson Education do Brasil, 2015, p. 7).

[75] *Baixo impacto:* "[...] é esperado que a perda represente um efeito adverso limitado nas operações da organização, em seus recursos ou nos indivíduos. Um efeito adverso limitado implica que, por exemplo, a perda da confidencialidade, integridade ou disponibilidade (i) causa uma degradação na capacidade de cumprir sua missão em uma extensão e por um tempo nos quais a organização consiga realizar suas funções primárias, mas com a eficiência delas notadamente reduzida; (ii) resulte em um dano limitado nos recursos da organização; (iii) apresente uma perda financeira limitada; ou (iv) origine um menor prejuízo aos indivíduos". (Ibid., p. 8)

[76] *Moderado impacto:* "[...] é esperado que a perda represente graves efeitos adversos nas operações da organização, em seus recursos ou nos indivíduos. Um efeito adverso grave implica que, por exemplo, a perda (i) cause uma degradação significativa na capacidade de cumprir sua missão em uma extensão e por um tempo nos quais a organização consiga realizar suas funções primárias, mas com a eficiência delas reduzida de forma significativa; (ii) resulte em danos expressivos nos recursos da organização; (iii) mostre significativas perdas financeiras; ou (iv) aponte prejuízos relevantes para indivíduos que não signifiquem perda da vida ou lesões graves, com risco de morte". (Ibid., p. 8).

[77] *Alto impacto:* "[...] a perda esperada possui efeitos adversos muito graves ou catastróficos nas operações da organização, em seus recursos ou nos indivíduos. Um efeito adverso muito grave ou catastrófico implica que, por exemplo, a perda (i) cause uma grave degradação ou perda da capacidade de cumprir sua missão por uma extensão e um período nos quais a organização não consiga desempenhar uma ou mais de suas funções primárias; (ii) resulte em grande dano aos recursos da organização; (iii) origine grandes perdas financeiras; ou (iv) desencadeie danos grandes ou catastrófico aos indivíduos envolvendo perda da vida ou lesões graves, com risco de morte". (Ibid., p. 8).

[78] *Website:* "[...] *s.m.* Grupo de documentos HTML relacionados entre si, além de ficheiros, scripts e bases de dados associados, que são representados por um servidor HTTP na World Wide Web. [...] A

a um lucro indevido com propagandas ou desvirtuação de finalidade de tratamento ou ainda a uma falsificação de credencial e um vazamento de dados pessoais.

Aqui reside a importância da arquitetura de segurança, uma vez que necessária a definição dos requisitos de segurança e caracterização das técnicas para satisfazê-los. Algumas das noções mais relevantes são as de ataque à segurança[79], mecanismos de segurança[80] e serviços de segurança[81] e a distinção entre ameaça[82] e ataque[83] para fins de combate às quebras de segurança.

Os serviços de segurança funcionam como um sistema de proteção contra ataques à segurança, utilizando um ou mais mecanismos de segurança para detectá-los, impedi-los e, eventualmente, deles se recuperar, tornando o processamento de dados e a transferência de informações menos vulneráveis, e, contribuindo para que novas ameaças não se convertam em porventura ataques.

Os mecanismos de segurança podem ser específicos ou difusos. Os específicos, que são os incorporáveis aos protocolos das camadas próprias de serviços de segurança, se exemplificam nos casos de codificação, da assinatura digital, do controle de acesso, da integridade de dados, da troca de autenticação, do preenchimento de tráfego, do controle de roteamento e da notarização[84].

Já os mecanismos de segurança difusos não são incorporáveis a quaisquer camadas de protocolos de serviços de segurança. Alguns exemplos citáveis são a funcionalidade confiada, o rótulo de segurança, a detecção de evento, a trilha de

---

maioria dos websites tem uma homepage como ponto de partida, que muitas vezes funciona como índice do conteúdo do site [...]". (MICROSOFT, Corporation. **Dicionário Prático de Informática.** – 22. ed. Portugal: McGraaw-Hill, 2000. p. 360).

[79] *Ataque à segurança:* "[...] qualquer ação que comprometa a segurança da informação pertencida a uma organização". (STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas; tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi, Messer Barreto, Rafael Misoczki. – 6. ed. São Paulo: Pearson Education do Brasil, 2015, p. 10).

[80] *Mecanismos de segurança*: "[...] um processo (ou um dispositivo incorporando tal processo) que é projetado para detectar, impedir ou recuperar-se de um ataque à segurança)". (Ibid., p. 10).

[81] *Serviços de segurança:* "[...] um serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento de dados e das transferências de informação de uma organização. Os serviços servem para frustrar ataques à segurança, e utilizam um ou mais mecanismos para isso". (Ibid., p. 10).

[82] *Ameaça:* "[...] uma chance de violação de segurança que existe quando há uma circunstância, ação ou evento que poderia quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo a explorar uma vulnerabilidade". (Ibid., p. 10).

[83] *Ataque:* "[...] Um ataque à segurança do sistema, derivado de uma ameaça inteligente; ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de fugir dos serviços de segurança e violar a política de segurança de um sistema". (Ibid., p. 10).

[84] Ibid., p. 15.

auditoria de segurança e a recuperação de segurança. Não há razão, contudo, para adentrar nas nuances operacionais de cada um destes mecanismos[85].

Os serviços de segurança são divididos em de (i) autenticação (de entidade pareada ou origem de dados); (ii) controle de acesso (para uso autorizado); (iii) confidencialidade (da conexão, sem conexão, com campo de tráfego ou do fluxo do tráfego); (iv) integridade (conexão, com ou sem recuperação ou com campo; sem conexão, com ou sem campo); e (v) irretratabilidade (origem ou destino)[86].

Os ataques à segurança podem ser ativos ou passivos. Os ativos são aqueles que tentam modificar recursos do sistema ou afetar sua operação; buscam alterar ou criar fluxos de dados. Os passivos, por sua vez, são os que tentam descobrir ou utilizar informações do sistema, mas não afetam os seus recursos; buscam bisbilhotar e monitorar transmissões e expor informações[87].

São exemplos de ataques à segurança ativos, como macro categorias, os disfarces, os repasses, as modificações de mensagens e as negações de serviço, bastante comuns estas últimas em ataques a *websites* governamentais. São exemplos de ataques à segurança passivos a análise de tráfego de dados e o vazamento de conteúdo de mensagens[88].

E não é pouca a variedade de técnicas digitais invasivas, não são poucos os interesses motivadores destas condutas, não são poucas as consequências e não são poucos os praticantes destas violações; nossa realidade atual escancara notícias de casos massivos de quebra de segurança, investigações e julgamentos de cibercriminosos e de novos métodos intrusivos e tecnologias disruptivas.

Seja por meio de prejuízos de ordem financeira, criminal ou pessoal, as principais vítimas destas violações, destes malfeitores do ciberespaço, destas tecnologias invasivas são os ciberconsumidores, aqueles usuários que consomem serviços e produtos digitais e são os mais vulneráveis na relação consumerista, com agravante da sua hipossuficiência técnica.

A expertise para lidar com problemas de segurança de dados não está inclusa no pacote de contratação eletrônica de um produto ou serviço. Imagine, se a grande

---

[85] STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas; tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi, Messer Barreto, Rafael Misoczki. – 6. ed. São Paulo: Pearson Education do Brasil, 2015, p. 15.
[86] Ibid., p. 13.
[87] Ibid., p. 11-12.
[88] Ibid., p. 11-12.

maioria destes ciberconsumidores não está preparada para resolver operações informáticas medianas, imagine para solucionar problemas complexos que, muitas vezes, nem profissionais de segurança capacitados obtém êxito.

A motivação e o *animus* doloso podem ser destes cibercriminosos, a responsabilidade dos provedores e/ou fornecedores, mas quem sofre uma superexposição de informações pessoais vazadas, quem arca com uma reputação manchada, com compras indevidas por terceiros, decorrentes de uma clonagem de credencial ou de senhas, por exemplo, são os ciberconsumidores.

E, no ambiente do mercado eletrônico ou do ciberespaço, os mecanismos de proteção do consumidor de outrora não são suficientes. Neste sentido, Marques esclarece que "[...] a distância física, a imaterialidade do meio eletrônico, a atemporalidade e a internacionalidade eventual da contratação, dificultam a eficácia do uso dos instrumentos tradicionais de proteção dos consumidores"[89].

Mitnick, um dos mais conhecidos *hackers* e especialistas em falhas de segurança de dados do mundo, vai além ao afirmar que mesmo que sejam realizadas as mais avançadas medidas de segurança, que sejam aplicados todos os produtos de segurança, os indivíduos que interagem com o ciberespaço continuarão totalmente vulneráveis em razão da fragilidade do fator humano envolvido:

> Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. [...] Por quê? Porque o fator humano é o elo mais fraco da segurança.[90]

Quando se pensa nesta interação indesejada entre ciberconsumidores e cibercriminosos não há como também não se relacionar à questão da segurança de dados com a criminalidade de dados. O tópico seguinte abordará sobre estes sujeitos que habitam o *underground* do ciberespaço, os movimentos que os caracterizam e diferenciam e relevantes eventos em que "marcaram presença".

---

[89] MARQUES. Cláudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor:** um estudo dos negócios jurídicos de consumo no comércio eletrônico. São Paulo: Revista dos Tribunais, 2004. p. 72.

[90] MITNICK, Kevin David; SIMON, William L. **A Arte de Enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Ed. Pearson, 2003. p. 3

## 2.4 Criminalidade dos dados

Da mesma forma que são proferidos decisões e acórdãos ativistas ou judicializantes, existem grupos cujas práticas cibernéticas seguem ideais éticos, fundamentais e humanos, assumindo uma postura ativista positiva (*hackers* - *white hats*); em contrapartida, há grupos que as executam almejando benefícios pessoais (*crakers* – *black hats*), adotando uma postura ativista negativa[91].

Neste diapasão, Lemos define o *cyberativism*[92] (ciberativismo ou ativismo digital, em português) como um conjunto de práticas sociais que utilizam a *Internet* e as novas tecnologias do ciberespaço para realização de movimentos de natureza política para alcançar suas metas[93]. Este fenômeno costuma ser representado pelos *hacktivistas,* apesar de que um cidadão sem tal *expertise* nele pode se enquadrar.

É, neste sentido, que complementa Silveira, ao estender a manifestação do ciberativismo também às causas socioambientais, sociotecnológicas e socioculturais e declarar que ele chega, muitas vezes, a confundir-se com a própria noção de ciberespaço e *Internet*, influenciando e contribuindo para com a otimização dos protocolos de comunicação e conformação do universo digital[94].

A temática ciberativista é pouco trabalhada ante a ausência de muitos estudiosos na área, além do fato de sua conceituação ser complexa, uma vez que em constante processo de transformação. Ademais, o movimento começou a ganhar notoriedade em meados dos anos 80 e atualmente é compreendido como um gênero para qualquer ativismo digital, do qual o *hacktivismo*, por exemplo, é espécie.

---

[91] SKOUDIS, Ed. **Counter hack:** a step-by-step guide to computer attacks and effective defenses. In: Prentice Hall series in computer networking and distributed systems. Upper Saddle River: PH PTR: 2002. p. 10.

[92] *Ciberativismo:* Trata-se da junção dos termos “cyber” e “ativismo”. “O termo ‘cyber’ surge, pela primeira vez nos trabalhos de um dos fundadores da Cibernética, o pesquisador Norbert Wiener, em 1939. [...] Também há outra definição, tratando-se de universos virtuais, gerenciado por máquinas. Segundo o dicionário Michaelis, ativismo possui dois significados: ‘1. Acentuação da atuação consequente da vontade, na formação da cultura e da sociedade; toda criação espiritual, bem como a arte e a teoria científica devem servir à atividade dirigida a uma meta’. ‘2. Doutrina ou prática de dar ênfase à ação vigorosa, por exemplo, ao uso da força para fins políticos’” (RODRIGUES, Luciana Ribeiro; PIMENTA, Francisco José Paoliello. **Discussões sobre o conceito de ciberativismo e suas práticas atuais através de uma abordagem pragmaticista.** Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. XXXVIII Congresso Brasileiro de Ciências a Comunicação – Rio de Janeiro, RJ – 2015. p. 4).

[93] LEMOS, André. **Cidade Ciborgue:** As cidades na Cibercultura, vol. 8. - São Paulo: 2004. p. 129-148.

[94] SILVEIRA DA, Sérgio Amadeus. **Ciberativismo, cultura *hacker* e o individualismo colaborativo.** Revista USP, São Paulo, n.º 86, 2010, p. 31.

São alguns exemplos de ciberativismos: o MST (Movimento dos Sem Terra)[95], o EZLN (Exército Zapatista para Liberação Nacional)[96] e a ADITAL (Agência de Informações Frei Tito para América Latina)[97]; todos se caracterizando pela construção de uma plataforma de comunicação e divulgação no ciberespaço, através da *Internet*, com o intuito de ajudar seus idealizadores e adeptos a alcançarem metas humanistas.

Tendo em vista o breve esclarecimento sobre o ciberativismo, possível a explicação do que vem a ser o *hacktivism*[98] ("hacktivismo", em adaptação ao português). Segundo Samuel, este fenômeno consiste no "uso não violento, legal ou ilegal, de ferramentas digitais para perseguir finalidades políticas"[99]. Para Denning, o hacktivismo combina a política da desobediência civil com as inovadoras técnicas e tecnologias *hackers* de computadores, objetivando alterar o normal funcionamento de *sites* e não causar danos graves[100].

---

[95] *MST:* "No contexto de busca por espaço das lutas sociais nos media, destaca-se, no Brasil, o maior movimento social latino-americano: o Movimento dos Trabalhadores Rurais Sem Terra, mundialmente conhecido por sua sigla MST. Ciente da campanha de marginalização sofrida pelo movimento através dos grandes media, o MST inclui a comunicação em suas bandeiras de luta e constrói espaços de atuação nos meios de comunicação a fim de quebrar a hegemonia da informação. Em seu sítio na internet, o MST define, além da reforma agrária, mais oito bandeiras de luta: saúde pública, desenvolvimento, diversidade étnica, sistema político, soberania nacional popular, cultura, o combate à violência sexista e a luta pela democratização da comunicação" (CAVALCANTE, Rebeca Freitas. **Ciberativismo:** como as novas formas de comunicação estão a contribuir para a democratização da comunicação. Universidade Nova de Lisboa, 2010. p. 47-48).

[96] *EZLN:* Sigla Exército Zapatista para Liberação Nacional, movimento mexicano no qual indígenas invadiram delegacias e gabinetes da região de Chiapas reivindicando autonomia, liberdade e igualdade aos indígenas. "O movimento zapatista em Chiapas arrebatou a imaginação popular pelo mundo todo ao congregar apoio para sua causa através de redes eletrônicas de faxes e da Internet, em conexão com o mundo da mídia e uma estrutura descentralizada de grupos de solidariedade (CASTELLS, Manuel. **A galáxia da Internet:** reflexões sobre a internet, os negócios e a sociedade. – Rio de Janeiro: Zahar, 2003. p. 115).

[97] *ADITAL:* "Campanha em defesa do Rio Madeira, no Norte do Brasil. A Agência de Informações Frei Tito para América Latina veiculou, no dia 11 de Dezembro de 2007, uma notícia na qual chamava a população a enviar e-mails para barrar o projeto do Governo Federal de construção do Complexo Madeira, que prevê a instalação de quatro hidroelétricas, de eclusas, hidrovias e uma grande transmissão de energia que vai de Porto Velho (em Rondônia) até São Paulo [...] A estrutura da Adital é toda baseada na Internet" (CAVALCANTE, op. cit., p. 55).

[98] *Hacktivismo:* "Notadamente na sua análise morfológica, a palavra *hacktivismo* refere-se a um amálgama das palavras *hacker* e ativismo, sendo, importante, para a definição deste último termo (ativismo), o uso da força para fins políticos [...] Já a definição de *hack* pode ser explicada como 'uma tentativa de usar a tecnologia de uma maneira original, não ortodoxa e inventiva". (BARRETO JUNIOR, I. F.; AULER, H.; BARBOSA, M. A. **Hacktivismo e ativismo digital na sociedade da informação.** In: Redes: R. Eletr. Dir. Soc., Canoas, v. 4, 2016, p. 126-146. Disponível em: <https://revistas.unilasalle.edu.br/index.php/redes/article/view/2318-8081.16.28/pdf>. Acesso em: 18 jul. 2019. p. 131).

[99] SAMUEL, Alexandra Whitney. **Hacktivism and the Future of Political Participation.** Cambridge, Harvard university, 2004. Disponível em: <http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-frontmatter.pdf>. Acesso em: 18 jul. 2019. p. 4. Tradução adaptada de "the non-violent use of illegal or legally ambiguous digital tools in pursuit of political ends".

[100] DENNING, Dorothy E. **Activism, hacktivism, and cyberterrorism:** The internet as a tool for influencing foreign policy. Chapter Eight. In: Networks and Netwars: The Future of Terror, Crime, and Militancy. 2002. p. 241.

Acredita-se que o termo *hacktivismo* foi mencionado pela primeira em 1996 por um *hacker*, apenas conhecido como "*Omega*", sujeito este responsável por vincular o *hacking* (ação de *hackear,* feita pelos *hackers*) com o viés político da ação. Contudo, especula-se que a popularização da expressão se deve ao grupo *hacker* intitulado "*Cult of the Dead Cow* (CDC)" e que a vinculação da ideologia *hacktivista* com os direitos fundamentais seja mérito do *hacker* "*Reid Fleming*"[101].

Houve nos últimos anos o surgimento de diversos grupos *hacktivistas* e a ocorrência de variados casos de *hacktivismo* que repercutiram internacionalmente. Alguns grupos hacktivistas conhecidos, a título de curiosidade, são: "Worldmach1n3", "LulzSec", "Sud0H4k3rs", "AntiSecPT", "Team Whit3 Portugal", "Hackers Street", "SideKingdom12", "OutsideTheLaw", "TeaMp0isoN", "th3j35t3r, "A-Team" e o grupo "Anonymous"[102].

Algumas operações hacktivistas recentes foram: a "Operação Valquíria" (protestava-se contra a não votação nas eleições legislativas portuguesas de 2015); a "Operação Stop Corruption Part 1" (protestava-se contra a corrupção governamental); a "Operação System Failed" (protestava-se contra entidades bancárias e políticas); a "Operação RiosAoCarmo" (protestava-se contra partidos políticos); além das publicações da "Wikileaks" e dos "Panama Papers"[103].

Evitando adentrar em demais pormenores históricos, ideológicos, característicos e tradicionais da cultura *hacker*[104] - porquanto extravasaria o espaço delimitado para essa dissertação, sem conseguir contemplar sua integralidade, traçar-se-á algumas linhas divisórias entre o *ciberativismo* (ativismo digital), o *hacking,* o *hacktivismo*, o *ciberterrorismo*.

Samuel diferencia *hacktivismo*, *ciberativismo* e *ciberterrorismo* através de critério estratégico, principiológico e cultural. Taticamente, os *hacktivistas* preferem ferramentas mais diretas (ostensivas) e transgressivas (ilegais) do que os

---

[101] Ibid., p. 275.
[102] DOMINGUES, Elisabeth Júlio. **Os Ciberataques como um Novo Desafio para a Segurança:** o *Hacktivismo*. Instituto Superior de Ciências Policiais e Segurança Interna. Monografia. Lisboa, 2015. p. 53-54.
[103] Ibid., p. 57.
[104] *Cultura Hacker:* "diz respeito ao conjunto de valores e crenças que emergiu das redes de programadores de computadores que interagiam on-line em torno de sua colaboração em projetos autonomamente definidos de programação criativa" (CASTELLS, Manuel. **A galáxia da Internet:** reflexões sobre a internet, os negócios e a sociedade. – Rio de Janeiro: Zahar, 2003. p. 38).

*ciberativistas* - que priorizam artifícios indiretos (não ostensivos) e não violadores (legais) - pois as consideram mais eficazes que as técnicas convencionais[105].

E, principiologicamente, afastam-se os *hacktivistas* dos *ciberterroristas*, pois estes pretendem o mal-estar social enquanto aqueles almejam o bem-estar social; culturalmente, distinguem-se os *hacktivistas* dos *hackers e crackers* por disporem aqueles de suas habilidades para fins sociais e por utilizarem estes de suas expertises para ganhos pessoais[106].

Domingues, outrossim, faz comentário acerca das distinções existentes entre *ciberativismo, hacktivismo* e *ciberterrorismo*[107]*;* acresce ainda a diferenciação havida do *hacktivismo* (campo de atuação no ciberespaço) para com a desobediência civil (campo de atuação na realidade tangível); e a diferenciação entre *hacktivismo* (propósito social, construtivo) e *hacking* não ativista (propósito pessoal, destrutivo). Segue abaixo inteiro teor do excerto mencionado:

> O hacktivismo caracteriza-se por recorrer a atividade legais, mas também ilegais, o que o faz diferir do ativismo online (por exemplo sites pelos direitos dos animais ou antiglobalização), que não compreende a existência de ações ilegais, ou seja, não transgride a Lei. Quanto à tradicional desobediência civil, distingue-se do hacktivismo na medida em que apresenta como campo de ação o mundo real e não o ciberespaço. O hacking relaciona-se com o hacktivismo, existindo, porém, um afastamento entre ambos, uma vez que os hacktivistas julgam que as suas capacidades podem ser utilizadas a favor do bem social comum, ao contrário do que acontece com o hacking, que apresenta um propósito meramente destrutivo. O hacktivismo tem um caráter não violento e assenta a sua ação no respeito pelos direitos humanos, distinguindo-se do ciberterrorismo, que é causador de danos provocados em seres humanos.[108]

---

[105] SAMUEL, Alexandra Whitney. **Hacktivism and the Future of Political Participation.** Cambridge, Harvard university, 2004. Disponível em: <http://www.alexandrasamuel.com/dissertation/pdfs/>. Acesso em: 18 jul. 2019. p. 13.

[106] Ibid., p. 13.

[107] *Ciberterrorismo:* "é a forma de terrorismo realizada no ciberespaço. [...] o terrorismo tem acompanhado a evolução tecnológica, por conta disso é grande a necessidade de tipificação de tais atos e punição dos mesmos, visando sempre coibir toda forma de propagação do terror. [...] A legislação brasileira buscou definir o ciberterrorismo, trazendo à baila punição para a prática de terrorismo nesses meios, conforme se vê no artigo 2o, inciso IV da lei 13.260/2016". (PEREIRA, J.; DAL MAGRO, E. C.; CARRES, A. F. N. **Terrorismo e ciberterrorismo:** uma análise frente a nova legislação brasileira de combate ao terror. Paraná: Unioeste, 2017. p. 5).

[108] DOMINGUES, Elisabeth Júlio. **Os Ciberataques como um Novo Desafio para a Segurança: o *Hacktivismo***. Lisboa, 2015. p. 40. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/15403/1/Disserta%C3%A7%C3%A3o%20de%20mestrado%20Final%20Elisabete%20Domingues.pdf>. Acesso em: 18 jul. 2019.

A autoria destas “façanhas” ou “deméritos” - a depender da carga ideológica imbuída nas condutas - ou destes “crimes” ou “desacatos” - a variar segundo a tipologia criminal ou civilista aplicável – geralmente é atribuída aos *hackers*[109] e aos *crackers*[110]*;* e aqui cabe rápido aparte técnico distintivo entre eles, relevante para compreensão de seus ideais, artifícios e modo de operação.

Barreto Júnior, Auler e Barbosa designam como *crackers* “aqueles que utilizam seu conhecimento para detectar vulnerabilidades no sistema e as utilizam para ganho pessoal. O termo foi criado por Richard Stallman [...] como forma de diferenciar estes indivíduos dos demais *hackers* da comunidade”[111]. Percebe-se, portanto, o fator cultural diferenciador e a tendência classificatória das comunidades.

Domingues complementa que os *crackers* recorrem a ataques (*political cracking*) no estilo *site defacements* (modificação de conteúdo e *layout* de páginas *web)*, *redirects* (redirecionamento de páginas *web)*, *denial of servive* – DoS (ataques de negação de serviço)*,* roubo de informação e sabotagem, além de geralmente escolherem o anonimato, trabalharem sozinhos ou em grupos reduzidos[112].

Observam-se ainda outros termos utilizados na área da segurança da informação para diferenciar os tipos de *hackers* e *crackers*, a saber: (i) *white hats* (“chapéus brancos”, em tradução literal), enquadrados como *hackers* do “bem”, sendo especializados na descoberta de falhas em sistemas de segurança com objetivo de solucioná-los, remunerada ou gratuitamente[113].

Conquanto bastante engajados, tem-se os menos benevolentes (ii) *black hats* (“chapéus pretos”, em tradução literal), reconhecidos como *hackers* do “mal” - os *crackers*; e os (iii) *gray hats* (“chapéus cinzas”, em tradução literal), misto de *hackers*

---

[109] *Hackers:* “[...] *pirata s. m.* ***1.*** Adepto de computadores; pessoa que está totalmente envolvida na tecnologia e programação de computadores ou que gosta de examinar o código dos sistemas operativos e outros programas para ver como funcionam. **2.** *pirata s. m.* Pessoa que utiliza os seus conhecimentos informáticos para fins ilícitos, como a obtenção não autorizada de acesso a sistemas de computadores e a alteração de programas e dados”. (MICROSOFT, Corporation. **Dicionário Prático de Informática.** – 22. ed. Portugal: McGraaw-Hill, 2000. p. 155).

[110] *Cracker:* “[...] *pirata s.m.* Pessoa que quebra as medidas de segurança de um sistema de computador e obtém um acesso não autorizado. O objectivo de alguns piratas consiste em obter informações de um computador ou em utilizar recursos informáticos ilegalmente. No entanto, o objetivo da maioria é meramente conseguir entrar no sistema [...]”. (Id., p. 85).

[111] BARRETO JUNIOR, I. F.; AULER, H.; BARBOSA, M. A. **Hacktivismo e ativismo digital na sociedade da informação.** In: Redes: R. Eletr. Dir. Soc., Canoas, v. 4, 2016, p. 126-146. Disponível em: <https://revistas.unilasalle.edu.br/index.php/redes/article/view/2318-8081.16.28/pdf>. Acesso em: 18 jul. 2019. p. 134.

[112] DOMINGUES, op. cit., não paginado.

[113] MARQUES FILHO, Glenio Leitão. **Hackers e Crackers na Internet**: as duas faces da moeda. Revista eletrônica – Temática. – Ano VI, n.º 01, 2010. p. 20-22.

*e crackers,* sendo difícil discernir qual sua verdadeira intenção por alternarem seu *modus operandi* e não declarem abertamente seus ideais[114].

Não bastasse a complexidade terminológica, existem grupos com condutas especializadas, tais quais: (iv) *phreakers* ("malucos", em tradução literal), são especializados em questões de telefonia móvel e fixa; (v) script kiddies ("script-de-crianças", em adaptação aportuguesada), são *crackers* inexperientes que costumam dispor de programas viróticos; (vi) *lammers* ("otários", em tradução literal), são aqueles que se autopromovem para tentar alcançar o *status* de *hacker*[115].

E ainda os (vii) *newbies* ("novatos", em tradução literal), são os aprendizes do mundo *hacking*; (viii) *defacers* ("deformadores", em tradução aproximada), são *crackers* que alteram os *websites* da *Internet*; (ix) *carders* ("cardadores", em tradução aproximada), focados em fraudes de cartões de crédito e boletos; e (x) *warez* ("piratas", em tradução adaptada), são aqueles que usam o comércio ilegal de produtos com direitos autorais, para hospedá-los e compartilhar na *internet*[116].

Independentemente de serem *hackers* ou *crackers* (*white hats*, *black hats* ou *gray hats*), ou quais sejam suas especialidades de ataques ou suas motivações subjetivas, assustadora é a capacidade de burlarem os mecanismos de segurança de dados, mesmo os mais avançados e vigiados, sorrateira e remotamente, e deixarem órgãos governamentais, grandes companhias e, principalmente, cibernautas e ciberconsumidores à sua mercê.

Geralmente estes cibercriminosos se aproveitam da prosperidade do comércio eletrônico e da inocência dos ciberconsumidores para sequestrar seus dados financeiros e/ou dados pessoais para obtenção de vantagens. Segundo Skoudis, "[...] quando eles assumem o controle de um sistema, os mais experientes tendem a silenciosamente se espreitar em segundo plano, cuidadosamente cobrindo seus rastros e reunindo informação sensível para uso futuro"[117].

E nesta "pessoalidade" e "sensibilidade" dos dados e informações é que reside o maior perigo, pois suas violações são as mais intrusivas, seus danos são os mais irreversíveis e suas compensações as mais insatisfatórias. E cada vez mais os

---

[114] Ibid., p. 22-23.
[115] Ibid., p. 25-27.
[116] Ibid., p. 27-30.
[117] SKOUDIS, Ed. **Counter hack:** a step-by-step guide to computer attacks and effective defenses. In: Prentice Hall series in computer networking and distributed systems. Upper Saddle River: PH PTR: 2002. p. 10. (tradução nossa).

mecanismos de segurança não são capazes de prevenir estas violações e cada vez mais os instrumentos tradicionais de defesa do consumidor não são capazes de remediar estas situações, contribuindo para a evolução da criminalidade de dados.

## 2.5 Dados pessoais e dados sensíveis

Tomando, a *grosso modo,* como princípio que os dados pessoais são potenciais informações personalíssimas e que sua tutela jurídica costuma ser reconhecida como uma evolução do direito à privacidade, cumpre tecer previamente alguns conceitos sobre dados pessoais, para depois apresentar as definições legislativas aplicáveis, oportunidade na qual será feito um breve retrospecto histórico sobre esta proteção privatista.

Estudos de cinquenta anos atrás já consideravam o conceito informático de dados, outros inclusive já utilizavam a terminologia "dados privados". Kaku descrevia os dados, amplamente, como quaisquer informações armazenadas trafegáveis na *internet*[118]. Hoeschl, por sua vez, os concebia como sendo informações sistematizadas e codificadas eletronicamente[119]. Apostaram ambos na virtualização das informações em plena virada do século.

Explorando o aspecto "pessoal" dos dados, enquanto Tucci tratava os dados pessoais como informações particulares e intimistas dos indivíduos, não passíveis de publicação[120], Cretella Junior, restritivamente, os abordava como informações personalíssimas inerentes às pessoas[121]. Em interpretação similar, Lacombe enxergava uma personalização do conceito de dados, sendo assim um "conjunto de registros sobre fatos" sistematizáveis e privatísticos[122].

Sobre o tema, cabe destacar que o Conselho Europeu, através da Convenção de Estrasburgo (1981), apresentou versão conceitual para informação pessoal como

---

118 KAKU, William Smith. **Internet e comércio eletrônico: pequena abordagem sobre a regulação da privacidade.** In: ROVER, Aires José (Org.) Direito, Sociedade e Informática: limites e perspectivas da vida digital. Florianópolis: Boiteaux, 2000. p. 89-90.

119 HOESCHL, Hugo César. **Alguns aspectos constitucionais da Lei n.9296/1996.** In: ROVER, Aires José (Org). Direito, Sociedade e Informática: limites e perspectivas da vida digital. Florianópolis: Boiteux, 2000. p. 89-90.

120 TUCCI, Rogério Lauria. **Direitos e garantias individuais no Processo Penal Brasileiro.** São Paulo: Saraiva, 1993, p. 428.

121 CRETELLA JÚNIOR, José. **Comentários à Constituição Brasileira de 1988.** Rio de Janeiro: Forense Universitária. 1988, p. 269.

122 LACOMBE, Francisco José Masset et. al. **Administração Princípios e Tendências**. São Paulo: Saraiva, 2003. p. 490.

sendo “qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação”[123], acepção esta bastante próxima das encontradas nos próprios enunciados legais europeus futuros. Isto demonstra evolução na discussão ao aceitar que sejam dados pessoais referentes a indivíduos identificáveis.

Uma das mais completas definições para “dados pessoais” foi a do art. 2º, “a”, da Diretiva 95/46/CE[124]: “qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa)”, onde identificável seria “todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social”[125].

Percebe-se da redação deste documento europeu: (i) uma possível equiparação semântica entre dados e informações, contrariando a diferenciação técnica outrora mencionada; (ii) uma não pluralidade de sujeitos, evidenciada pela menção à “pessoa singular”; (iii) um requisito de identificação ou ao menos sua viabilidade; e (iv) exemplos de dados que são, direta ou indiretamente, capazes de identificar ou determinar quem seja referido indivíduo.

Duas décadas depois houve uma atualização legislativa europeia do significado de dados pessoais. A nova conceituação, prevista no art. 4º, “1”, do Regulamento (UE) 2016/679, entende dados pessoais como: “informação relativa a uma pessoa singular identificada ou identificável (titular dos dados)”, considerando como identificável “uma pessoa que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador”[126].

Exemplifica ainda, no mesmo item do artigo, quais são estes identificadores: “um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos de identidade física, fisiológica,

---

[123] CONSELHO DA EUROPA. **Convenção n.º 108, de 28 de janeiro de 1981**, relativa à Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Disponível: <http://www.ministeriopublico.pt/instrumento/convencao-para-proteccao-das-pessoas-relativamente-ao-tratamento-automatizado-de-dados-2>. Acesso em: 15 fev. 2019.

[124] UNIÃO EUROPEIA. **Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 15 fev. 2019.

[125] Foi utilizada a versão consolidada, em português, da Diretiva, com adequações ortográficas ao português brasileiro, sem quaisquer alterações do conteúdo original. Ademais, a diretiva não está mais vigente desde 24/05/2018 ante sua revogação pelo Regulamento (UE) 2016/679.

[126] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

genética, mental, econômica, cultural ou social dessa pessoa singular"[127], acrescentando novo fator identificador e alterando a nomenclatura de elemento.

As alterações são moderadamente significativas. A legislação posterior (i) passou a nomear o portador da informação como "titular dos dados" em substituição à expressão anterior "pessoa em causa"; (ii) resolveu chamar o elemento "psíquico" como "mental"; e (iii) decidiu acrescentar o nome, dados de localização, indicadores eletrônicos e o elemento genético como fatores capazes de identificar uma pessoa.

A preferência pela escolha das definições legais europeias de dados pessoais, especialmente neste trabalho, é justificável na sua grande aceitação mundial, na sua aplicação em vastíssimo território e no seu altíssimo reflexo do cenário tecnológico atual, mesmo porque o RGPD é referência para os demais países. Não seria demasiado pretensioso considerar seu pioneirismo e sua inspiração para a criação de novas legislações estrangeiras.

Dentre estes variados identificadores dos dados pessoais, encontra-se uma categoria especial: os *dados sensíveis*. Diferenciam-se de dados pessoais em decorrência do seu maior potencial danoso caso utilizados discriminatória e indevidamente. Podendo ocasionar prejuízos irreversíveis à indivíduos e afetar até mesmo uma coletividade, os dados sensíveis são geralmente tratados de maneira específica e expressamente relacionados[128].

Eles são reconhecidos e disciplinados pelo Regulamento Geral de Proteção de Dados (RGPD) em alguns de seus considerandos[129] e artigos seguintes[130], pois a peculiaridade que circunda os dados sensíveis faz com que o consentimento dos seus titulares seja exigível. Portanto, tratamentos arbitrários são vedados e a sujeição às condições distintas é imprescindível para evitar quaisquer violações de direitos humanos e liberdades fundamentais.

São exemplos de dados sensíveis aqueles capazes de revelar: origem racial ou étnica; fatos tocantes à vida sexual ou orientação sexual; dados genéticos[131] ou

---

[127] Utilizada novamente a versão consolidada, em português, do Regulamento, com adequações ortográficas ao português brasileiro, sem quaisquer alterações do conteúdo original.

[128] PEZZI, Ana Paula Jacobus**. A necessidade de proteção dos dados pessoais nos arquivos de consumo:** em busca da concretização do direito à privacidade. Monografia. Universidade do Vale dos Rios do Sino - UNISINOS: São Leopoldo, 2007. p. 91. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf>. Acesso em: 11 mar. 2019.

[129] Vide considerandos nos 10 e 51 a 56 do Regulamento n.º 679/2016.

[130] Vide arts. 4º, nos 13, 14, 15 e art. 9º do Regulamento n.º 679/2016.

[131] *Dados genéticos:* "os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente

dados relativos à saúde[132]; dados biométricos[133] inequívocos; opiniões políticas, convicções filosóficas ou religiosas; e filiação sindical (art. 9º, "1", do RGPD)[134]. Percebe-se apenas pela menção destes dados identificadores a periculosidade que podem desencadear quando indevidamente utilizados.

Doneda esclarece que estes dados sensíveis, quando processados, comportam uma carga maior de intensidade e, consequentemente, representam maior periculosidade em caso de tratamento inadequado[135]. A potencialidade lesiva aos titulares - mormente nos casos de exposição e circulação indevidas - justificam esta subdivisão, exortando os fundamentos clássicos relacionados à privacidade e validando o princípio da igualdade material[136].

Ademais, é de bom alvitre a relativização de quaisquer "tratamentos extremistas" de dados pessoais (e também sensíveis), ou seja, a proibição arbitrária de manuseio ou a autorização da utilização discriminatória destes dados, conforme alerta: "O tratamento de dados sensíveis é, portanto, possível e mesmo necessário em uma série de circunstâncias, porém deve ser sempre uma exceção justificada pela relevância dos valores em questão [...]"[137].

Interessante destacar o 10º considerando do RGPD acerca da legislação horizontal dos dados sensíveis que confere - em virtude da estrutura do megabloco, do sistema de supranacionalidade da UE e da existência de leis setoriais dos Estados Membros – certa maleabilidade e permissibilidade para regulamentação do tratamento de dados sensíveis em cada país[138].

---

da pessoa singular em causa" **(Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Art. 4º, item "13". Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 07 out. 2018).

[132] *Dados relativos à saúde:* "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde" (Ibid., art. 4º, "15").

[133] *Dados biométricos:* "dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos" (Ibid., art. 4º, "14").

[134] Ibid., art. 9º, "1".

[135] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. p. 27.

[136] RODOTÁ, Stefano. ***Tecnologie e diritti***. Bologna: Il Mulino, 1995. p. 85.

[137] BRASIL, op. cit., p. 27.

[138] Vide *10º Considerando do RGPD:* "Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa

Contudo, há uma semelhança nas legislações, seja como dados pessoais coletados ou como informações pessoais processadas: a adjetivação “pessoal” é recorrente e não é gratuita, pois determinados requisitos para sua caracterização devem ser obedecidos. Quando dados ou informações possuem vínculos diretos com alguma pessoa, quer dizer que eles retratam algo sobre ela, dizem respeito “às características ou ações desta pessoa”[139].

Uma vez que seguem padrões característicos, as informações pessoais podem ser classificadas em subcategorias. A importância desta setorização reside, não exclusivamente, na otimização do processo de criação e aplicação de leis específicas, tanto como uma forma de fragmentação da tutela em contextos setoriais ou como a constituição de uma tutela integrada em contextos pessoais, a exemplo dos já mencionados dados sensíveis[140].

Visando compactar a matéria, mas não olvidando a existência de questões tocantes à proibição genérica de coleta e tratamento e à antecipação dos efeitos do tratamento dos dados pessoais, à adoção de regimes por contextos setoriais de dados sensíveis e às técnicas e qualitativos da tutela de dados pessoais - as quais serão explorados conjuntamente à outras temáticas *a posteriori*, segue breve contextualização a respeito.

## 2.6 Proteção dos dados pessoais como direito humano e fundamental

Com a sofisticação das técnicas de armazenamento e o refinamento do cruzamento de dados, inumeráveis tarefas e serviços cotidianos que envolvem a coleta, a guarda, o processo, a gestão, o trato e a difusão de dados pessoais ganharam novas dinâmicas e funcionalidades. São facilmente perceptíveis os ganhos com praticidade, operabilidade e velocidade obtidos, contudo, por vezes, relativizados, ignorados ou mesmo ocultados os malefícios trazidos.

---

medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais”. (UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 15 fev. 2019).

[139] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 93.

[140] BRASIL. Escola Nacional de Defesa do Consumidor**. A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. p. 25.

Despontam duas correntes sobre esta problemática. A primeira, negativista, defende a inexistência de conexão entre violações dos bancos de dados com a vida privada, visto que aqueles não são criação da informática[141], pois historicamente a sociedade sempre manipulou fichários e arquivos policiais[142] e administrativos. Esta vertente denega a relação de causalidade entre a tecnologia de dados e o desrespeito aos direitos de personalidade.

A segunda, positivista, reconhece esta parcela de culpa do avanço da tecnologia informacional pelas mudanças quantitativas e alterações qualitativas na segurança da vida privada, das liberdades individuais e, inclusive, no equilíbrio dos poderes políticos e harmonia dos grupos sociais. Esta corrente é a majoritária, referendada pelas maiores mentes jurídicas no assunto e comprovada pelo atual desgaste das fronteiras da privacidade[143].

Nos dizeres quase proféticos de Santa Maria "Retumbam, por todos os quadrantes das Nações Cultas, um vigoroso alerta, denunciando a invasão devastadora e inconsiderada do direito à privacidade pela tecnologia avançada das últimas décadas, no uso abusivo do direito à informação [...]"[144]. Esta é a outrora velada realidade envolvendo o tratamento de dados pessoais e o agora escancarado problema mundial quanto ao seu tratamento.

Observa Costa Júnior outra nefasta faceta da tecnologia: a nulificação da individualidade. Trata-se de um fenômeno moderno, de um sentimento de resignação, de normalização quanto à exposição da privacidade, motivadas pela capacidade de ocultamento, facilitação e banalização da intimidade e pela estimulação e compulsão da sua renúncia para fins de autossatisfação, autopromoção ou para evitar desvalorização ou marginalização:

> É que a civilização da técnica, identificando o homem com a sua função social, transformando-o em insignificante peça da complexa engrenagem industrial, nele inculca sentimentos de desvalorização. Ele se sente esmagado pelo anonimato, pela diluição de sua individualidade nas grandes concentrações urbanas da era industrial-tecnológica, de sorte que a exposição de sua vida à curiosidade e controle alheios resulta, paradoxalmente, na superação de sua

---

141 MAIA, Luciano Soares. **A privacidade e os princípios de proteção do indivíduo.** In: XVI Congresso Nacional do CONPEDI, 2008, Belo Horizonte. Pensar Globalmente: Agir localmente. Florianópolis: Fundação Boiteux, 2008. v. 1. p. 459

142 FERNANDES, Milton. **Proteção civil da intimidade.** São Paulo: Saraiva, 1977. p. 225.

143 MAIA, op. cit., p. 459.

144 SANTA MARIA, José Serpa de. **Direitos da personalidade e a sistemática civil geral.** Campinas: Julex, 1987. p. 57.

> mediocridade: ser espionado é, de algum modo, ser importante. Este sentimento a tal ponto foi difundido e prestigiado pela filosofia tecnológica que, nos tempos vertentes, a vida privada, a solidão, é interpretada como um prazer vicioso, índice de excentricidade, sintoma de marginalização e mediocridade. Aceita-se hoje, com surpreendente passividade, que o nosso passado e nosso presente, os aspectos personalíssimos de nossa vida, até mesmo sejam objeto de investigação – todas as informações arquivadas e livremente comercializadas. O conceito de vida privada, como algo preciosos, parece estar sofrendo uma deformação progressiva em muitas camadas da população. Realmente, na moderna sociedade de massas, a existência da intimidade, privatividade, contemplação e interiorização vem sendo posta em xeque, numa escala de assédio crescente, sem que reações proporcionais possam ser notadas[145].

Em virtude desta sempre potencial violação dos dados pessoais, consentida, desautorizada ou despercebida, os defensores da necessidade de criação de instrumentos legislativos para controle destas "informações" começaram a ganhar maior espaço midiático, acadêmico e governamental nos países desenvolvidos. O interesse em conciliar o progresso tecnológico e a proteção da privacidade dos cidadãos movimentou o *lobby* internacional.

Cientes de que estes dados pessoais (e sensíveis) são capazes de caracterizar e identificar seus titulares – representando assim suas próprias personalidades - e buscando remediar as mazelas modernas que a ausência de uma diretriz e alicerce maior apropriado para proteger as "informações pessoais virtualizadas", começaram aos poucos a incorporar a titulação de direito humano e de direito fundamental.

Estas classes de direitos basilares, os direitos humanos e os direitos fundamentais, envolvem situações jurídicas sobremaneira complexas e costumam serem confundidas. Pode-se dizer, segundo Gomes, Oliveira e Santos, que os direitos humanos consistem nos "direitos e liberdades que as pessoas detêm pelo simples facto de serem dotadas de caráter humano, possuindo uma natureza essencial para garantir a existência do indivíduo"[146].

Já os direitos fundamentais são entendidos, de acordo com Miranda, como *"*os direitos ou as posições jurídicas subjectivas das pessoas enquanto tais, individual ou institucionalmente consideradas, assentes na Constituição"[147]. Ou, nas palavras de

---

[145] COSTA JÚNIOR, Paulo José da. **O direito de estar só:** tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995. p. 25.
[146] GOMES, Carla de Marcelino; OLIVEIRA, Bárbara Nazareth; SANTOS, Rita Páscoa dos. **Os direitos fundamentais em Timor-Leste:** teoria e prática. Portugal: Coimbra Editora, 2015. p. 30.
[147] MIRANDA, Jorge Manuel Moura Loureiro de. **Direitos Fundamentais:** Introdução Geral. Lisboa: Diversos, 1999. p. 11.

Canotilho, como “a incorporação de direitos subjetivos do homem em normas formalmente básicas, subtraindo-se o seu reconhecimento e garantia à disponibilidade do legislador originário”[148].

A conclusão, descomplicando a terminologia, é de que os direitos humanos exaltam a humanidade característica das pessoas como justificativa para resguardar direitos e liberdades existenciais, demonstrando uma vertente mais jusnaturalista. Já os direitos fundamentais objetivam a proteção destes direitos e liberdades individuais em níveis constitucionais, como resultado de um processo de *constitucionalização*, evidenciando um viés mais juspositivista.

Tomando como válida esta desambiguação – visto que a similitude existente entre as duas definições reside no fato de ambas estarem interligadas com as noções de igualdade e de liberdade dos indivíduos (mesmos valores éticos)[149] -, tem-se uma importante premissa: os direitos humanos pertencem a todas as pessoas ou coletividade de pessoas e os direitos fundamentais pertencem àquelas sob a jurisdição do ordenamento jurídico que os positivou.

Constata-se, desta forma, pairar sobre os direitos humanos um *status* de universalidade, de independência de positivação jurídica em ordenamento jurídico específico e de ausência de uma limitação espacial. Em contrapartida, os direitos fundamentais estão positivados nos direitos internos dos países, estão restritos temporalmente e vinculam apenas os cidadãos que estão sob a égide do seu próprio ordenamento jurídico.

A compreensão destas singularidades dos direitos humanos e direitos fundamentais encontra validade para esta dissertação não apenas para corroborar a relação dos direitos personalíssimos com o direito à privacidade e destes com a proteção dos dados pessoais e dados sensíveis, como também possui valia para melhor contextualização, localização e exportação/importação de documentos internacionais e legislações nacionais acerca da temática.

Neste sentido, Doneda comenta sobre a amplitude internacional alcançada: “[...] a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito

---

[148] CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. 7. ed. Coimbra: Almedina, 2003. p. 378.
[149] GOMES et all., op. cit., p. 32.

fundamental”[150]. Este processo de consolidação aparenta ter seguido uma produção legislativa ora vertical ora horizontal, conforme seu histórico jurídico comprova.

O introito desta proteção digital privatista foi tímido, começando sua escalada internacional com o art. 12 da Declaração Universal dos Direitos Humanos (DUDH - 1948): “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação [...]”[151]. Todas as pessoas têm direito a amparo legal na ocorrência destas intromissões ou ataques.

Neste diploma humanitário já era perceptível uma preocupação com a existência de intervenções discricionárias na vida privada e familiar das pessoas, muito embora dissesse respeito apenas às interferências físicas e psíquicas; ou seja, não abordava em sua redação ressalvas e advertências acerca do tratamento dos dados pessoais e sensíveis, o que não é motivo para estranheza, visto que o estopim da revolução tecnológica chegaria décadas mais tarde.

Contudo, sempre atualizando e contextualizando os conceitos e elementos da privacidade, a doutrina costuma sistematizar temporalmente estas legislações em gerações. Apostando em uma abordagem progressiva, na sequência, serão apresentadas as três gerações usualmente conhecidas para logo investigar em alguns documentos jurídicos nacionais, regionais e internacionais seus registros como direitos humanos e fundamentais.

A primeira geração, composta por iniciativas legislativas do curso da década de 70, seguia os ditames da difusão midiática e dos serviços públicos e a da contagiosa revolução informática. Caracterizava-se como garantista de direito; com conteúdo normativo genérico, aplicação uniforme para todas as situações; destinada somente às pessoas físicas; e com enfoque na autorização de funcionamento prévia e controle de tratamento póstumo[152].

Destacam-se como legislações pioneiras desta geração: a Lei do *Land* alemão de *Hesse* (1970) e a Lei *Data Legen* sueca (1973). Seguiram-se: o *Fair Credit*

---

[150] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 2.

[151] ASSEMBLEIA GERAL DA ONU. **Resolução n.º 217-A, inciso III, de 10 de dezembro de 1948.** Declaração Universal dos Direitos Humanos. Disponível em:<http://www.un.org/en/universal-declaration-human-rights/>. Acesso em: 21 fev. 2019).

[152] SAMPAIO, José Adércio Leite **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998**.** p. 490.

*Reporting Act* (1974) americano; o Estatuto de Proteção de Dados do *Land* alemão de *Rheinland-Pfalz* (1974); a Lei Federal de Proteção de Dados alemã (1977) e as Leis n.º 243/244 de Proteção de Dados dinamarquesas (1978), responsáveis por introduzir a proteção às pessoas jurídicas também[153].

A segunda geração, constituída por legislações produzidas no final da década de 80, ainda predominantemente europeias, evidenciam-se pela mudança de perspectiva das suas estruturas: o foco da proteção de dados não está centrado na inovação informática e sim no controle da privacidade pelos próprios cidadãos/usuários - a chamada liberdade negativa. Deslocou-se a atenção das questões de *hardware* para as questões qualitativas de dados[154].

São exemplares dessa geração: o *Privacy Act* americano (1974); a redação do art. 35 da constitucional portuguesa (1977); as leis francesas de proteção de dados pessoais, nomeadas *Informatique et Libertées* (1978); a previsão constitucional espanhola do art. 18, §1º, sobre proteção da privacidade contra invasões de atividade informática (1978); e das leis norueguesa (1978), luxemburguesa (1979), suíça (1981) e islandesa (1981)[155].

A terceira geração, formada por legislações surgidas no final da década de 80, demonstrou uma preferência pela proteção dos cidadãos através da efetivação dos seus direitos e liberdades. As normatizações buscaram atender as novas exigências da sociedade informatizada e aproveitaram os mecanismos de identificação e controle de informações pessoais da geração passada, fomentando assim a participação social dos titulares dos dados[156].

Um dos documentos jurídicos citáveis que abraçaram os preceitos desta geração foi a Convenção de Estrasburgo (1981)[157], responsável pela uniformização do direito europeu relativa à proteção dos direitos e liberdades fundamentais face ao

---

153 LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p. 79.
154 PEZZI, Ana Paula Jacobus. **A necessidade de proteção dos dados pessoais nos arquivos de consumo:** em busca da concretização do direito à privacidade. Monografia. UNISINOS: São Leopoldo, 2007. p. 95.
155 LIMBERGER, op. cit., p. 79.
156 PEZZI, Ana Paula Jacobus. **A necessidade de proteção dos dados pessoais nos arquivos de consumo:** em busca da concretização do direito à privacidade. Monografia. UNISINOS: São Leopoldo, 2007. p. 95.
157 CONSELHO DA EUROPA. **Convenção n.º 108, de 28 de janeiro de 1981**, relativa à Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal Disponível em:<http://www.ministeriopublico.pt/instrumento/convencao-para-proteccao-das-pessoas-relativamente-ao-tratamento-automatizado-de-dados-2>. Acesso em: 14 mar. 2019.

tratamento automatizado de dados pessoais, a qual influenciou no desenvolvimento das vindouras leis nacionais britânica (1984), alemã (1990), italiana (1996), portuguesa (1998) e espanhola (1999)[158].

Na sequência da Convenção de Estrasburgo, o Conselho da Organização para Cooperação e Desenvolvimento Econômico (OCDE) adotou uma Recomendação (1980) com normas protetivas à privacidade e controle do fluxo de dados públicos e privados transfronteiriços. O documento versava sobre questões terminológicas, alcance de diretrizes, princípios básicos de aplicação nacional e cooperação internacional[159].

Recorda Sampaio, que infelizmente nenhum dos citados diplomas internacionais alcançou os efeitos desejados, pois seus signatários não seguiram suas diretivas e o que predominou foi uma desarmonia legislativa[160]. Entretanto, a principiologia inserta nos documentos revelou um esboço das preocupações com a situação dos dados pessoais e serviu de base para a confecção das normatizações europeias seguintes.

A Diretiva n.º 46/1995/CE do Parlamento Europeu e do Conselho sobre proteção das pessoas singulares relativas ao tratamento de dados pessoais e à livre circulação destes dados (1995) foi o novo marco regulatório que esteve operante na UE até 24/05/2018 - quando foi revogado pela exigência dos efeitos do Regulamento (UE) n.º 679/2016 (RGPD) – e incorporava em seus 33 artigos a essência dos documentos nacionais e internacionais anteriores.

Na Diretiva referida, a proteção dos dados pessoais como direito fundamental já é reconhecida preambularmente (1º Considerando). A confluência dos direitos e liberdades fundamentais com os princípios de proteção de dados pessoais igualmente recebe imediata previsão (2º Considerando). Em suas disposições gerais, inclusive, é considerado objetivo máximo da diretiva a proteção dos direitos e liberdades fundamentais (arts. 1º e 2º)[161].

---

158 LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p. 79.

159 OCDE ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais, de 1º de outubro de 1980.** Disponível em: < http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf>. Acesso em: 14 mar. 2019.

160 SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998**.** p. 92-93.

161 UNIÃO EUROPEIA. **Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995**, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de

A produção legislativa europeia a respeito da proteção de dados pessoais continuou próspera nas décadas seguintes. A discussão se manteve sob os holofotes das nações integrantes do megabloco e dos fóruns internacionais, sempre na tentativa de acompanhar a imparável tecnologia de dados. Eis que em 2000 foi publicada a Carta dos Direitos Fundamentais da União Europeia (CDFUE), trazendo em seu bojo disposições de natureza "humanista".

A relevância desta Carta jaz não apenas na previsão do respeito pela vida privada, familiar e pelo seu domicílio e comunicações (art. 7º), uma formalização de conjunto de direitos outrora reconhecidos, mas também da inclusão da proteção aos dados pessoais, regrada por um tratamento legítimo, finalístico e confiável, provido de consentimento do titular, quem ainda teria direito de os acessar e retificar quando lhes dissesse respeito (art. 8º, "1" e "2")[162].

Os princípios dos diplomas internacionais anteriores foram coligados na CDFUE, as normas receberam o *status* de direitos fundamentais e de aplicabilidade para todos os membros da UE. Complementarmente, o Tratado sobre o Funcionamento da União Europeia (TFUE) reafirmou o direito à proteção aos dados pessoais (art. 16, "1") e conferiu ao Parlamento Europeu e ao Conselho a competência legislativa sobre a matéria (art. 16, "2")[163].

Condicionando o exercício do tratamento e circulação de dados pessoais, as atividades relativas à sua aplicação pelas instituições, órgãos, organizações e Estados Membros da UE - em que pese destinando seu controle às autoridades independentes e não prejudicando normas específicas (art. 39) do Tratado da União Europeia (TUE)[164] -, o TFUE buscou harmonizar normativa e verticalmente a temática em toda a região.

Novos reforços jurídicos surgem da Assembleia Geral do Conselho de Direitos Humanos das Nações Unidas (CDH) com o objetivo de reafirmar propósitos e princípios da CDFUE, de reafirmar direitos e liberdades fundamentais da DUDH, bem

---

dados pessoais e à livre circulação desses dados. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 15 mar. 2019.

[162] PARLAMENTO EUROPEU E CONSELHO, 2000/C/364, de 18 de dezembro de 2000. **Carta dos Direitos Fundamentais da União Europeia.** Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 21 fev. 2019.

[163] Id. 22/47, de 13 de dezembro de 2007. **Tratado sobre o Funcionamento da União Europeia.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12012E%2FTXT>. Acesso em: 21 fev. 2019.

[164] UNIÃO EUROPEIA. **Tratado da União Europeia (Tratado de Maastricht),** 29 de julho de 1992. Disponível em: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF>. Acesso em: 14 mar. 2019.

como de reconhecer e regulamentar direitos à privacidade na presente e complexa sociedade digital através da publicação das Resoluções n.º 68/167/2013 e n.º 69/166/2014.

A resolutiva de 2013 demonstra a preocupação do CDH com as implicações do estado de vigilância e das comunicações com os direitos de privacidade, liberdade de opinião e liberdade de expressão, com a interceptação de comunicações, coleta arbitrária de dados pessoais, violações intrusivas de informações sensíveis, preocupação pública com segurança digital, governamental com o *ciberterrorismo*[165] e negativo impacto extraterritorial[166].

A resolutiva de 2014, considerando sua antecessora e avaliando tecnicistas relatório especial e comentário geral encomendados, reconhece a necessidade de maiores discussões e análises do direito internacional, problemas relacionados à proteção e promoção de dados pessoais, procedimentos securitários, diagnósticos e impactos domésticos, benefícios e malefícios das ferramentas disponíveis etc. e recomenda providências[167].

Com enfoque na defesa dos consumidores, a Assembleia Geral recentemente adotou e revisou a Resolução n.º 70/186/2015 - intitulada de Diretrizes das Nações Unidas de Proteção do Consumidor (DNUPC) -, que se trata de um conjunto de orientações primeiramente adotadas na Resolução n. 39/248/1985 e depois expandidas pelo Conselho Econômico e Social (ECOSOC, em inglês) na Resolução n. E/1999/2/Add.2.

As Diretrizes, em sua versão de 2015, consistem em compêndio de princípios e orientações - com regras de conduta - que determina as principais características

---

165 *Ciberterrorismo:* entende-se pelo "[...] uso do ciberespaço com o objetivo de aterrorizar através de ataques que possam causar a destruição, ou distorção deliberada de dados digitais e fluxos de informação, por motivos religiosos, políticos ou ideológicos [...] consiste em um ataque à um fator tecnológico usando outro fator tecnológico, sendo o feitor do ciberterrorismo um ciberterrorista. Isso é diferente de um terrorista utilizando a tecnologia para cometer um ato tradicional do terrorismo, e também é diferente de um terrorista usando meios não tecnológicos para cometer um ato de terrorismo contra uma rede de sistema de computador [...]". (CHAGAS, Morgana Santos das. **Ciberterrorismo:** as possibilidades da expansão do terror nas relações internacionais. Monografia. João Pessoa: UEPB, 2012. p. 29-31).

166 NAÇÕES UNIDAS. Assembleia Geral. **Resolução 68/167, de 18 de dezembro de 2013 [on the report of the Third Committee (A/68/456/Add.2)].** O Direito à privacidade na era digital. Disponível em:< http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>. Acesso em: 21 fev. 2019.

167 NAÇÕES UNIDAS. Assembleia Geral. **Resolução 69/166, de 18 de dezembro de 2014 [on the report of the Third Committee (A/69/488/Add.2 and Corr. 1)].** O Direito à privacidade na era digital. Disponível em:< http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166>. Acesso em: 21 fev. 2019.

legislativas de proteção do consumidor, a criação de autoridades de controle da ONU (Seção V-A, "14" e "15"), o fornecimento de assistência para adequação de sistemas e, em específico ao tema discutido, novos princípios gerais (Seção III) e princípios para boas práticas comerciais, incluindo tratamento equitativo, transparência e privacidade (Seção IV, "11").

Ademais, o documento reserva espaço para recomendações protetivas sobre o comércio eletrônico, como a melhora da confiança neste nicho do mercado, com políticas transparentes, eficazes e equivalentes aos demais comércios (Seção V-I, "63"), garantia da clareza dos direitos e obrigações no mercado digital aos consumidores (Seção V-I, "64") e observação e conformação às diretrizes e padronizações internacionais (Seção V-I, "65")[168].

Trazendo diretrizes de prevenção e resolução de problemas de privacidade, propriedade intelectual e concorrência dos consumidores, carrega o título de mais importante documento internacional em termos de proteção ao consumidor. E, diante da sua relação com a proteção de dados pessoais do consumidor e com o mercado digital, esperado é que qualquer legislação nacional ou regional vindoura atentasse para seu conteúdo.

Eis que então, com a vigência dos seus efeitos (25/05/2018), o recente RGPD (2016) ganha aplicabilidade, consolidando as últimas discussões modernas, normatizações internacionais, particularidades regionais europeias e características supranacionais do megabloco; trata-se da mais completa regulação relativa à proteção de dados pessoais mundialmente, uma necessária evolução jurídica da Diretiva europeia n.º 95/46/CE.

Percebe-se ao longo da sua quase centena de artigos e dos 173 considerandos a influência e os desdobramentos dos direitos e liberdades fundamentais, todavia o caráter de direito fundamental da proteção dos dados pessoais, sua circulação em nível territorial e extraterritorial, bem como seu amoldamento aos regramentos da CDFUE e do TFUE, constam expressamente no corpo do Regulamento (Considerandos n.os 1 a 5 e art. 1, "1" a "3")[169].

---

[168] Id. Assembleia Geral. **Resolução 70/186, de 22 de dezembro de 2015 [on the report of the Second Committee (A/70/470/Add.1)]**. Diretrizes das Nações Unidas para proteção do consumidor. Disponível: <https://unctad.org/meetings/en/SessionalDocuments/ares70d186_en.pdf>. Acesso em: 14 mar. 2019.

[169] UNIÃO EUROPEIA. Parlamento Europeu e Conselho. **Regulamento n.º 679, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a

Em contrapartida, na América Latina, engatinhava-se no quesito proteção de dados pessoais. Dispunha-se mais de resquícios de defesa civilista e consumerista em tempos pretéritos. Posteriormente à produção legislativa europeia de terceira geração é que maiores avanços nesta seara são encontrados, destacando uma predominância do tratamento constitucional sobre o infraconstitucional em um primeiro momento de regulamentação.

Trilhando semelhante rastro, guardadas as peculiaridades de cada tutela jurídica implementada, tem-se registrado os tratamentos constitucionais e infraconstitucionais de Argentina (2000), Brasil (1988, 1990, 2002, 2018 e 2019), Colômbia (1991), Paraguai (1992 e 2001), Peru (1993, 2001 e 2004), Guatemala (1993), Nicarágua (1995), Equador (1997), Venezuela (1999), Chile (1999), Bolívia (2004), México (2002) e Uruguai (2004 e 2008)[170].

Não obstante a sensação de atraso normativo latente, que seja lembrado também o pioneirismo latino legislativo sobre a matéria. Houve um elogiável empreendimento jurídico-institucional: a criação da Rede Iberoamericana de Proteção de Dados (RIPD - 2003), ocorrida na XIII Reunião de Cúpula, em Santa Cruz de la Sierra – Bolívia, encontro que possui natureza de fórum de discussão direta e de aprovação de decisões e documentos sobre proteção de dados[171].

A propósito, no 15º Encontro Ibero-Americano de Proteção de Dados (2017), organizado pela RIPB e pelo Conselho de Transparência do Chile, restaram aprovados os “Padrões Proteção de Dados Pessoais para os Estados Ibero-Americanos”, concretizando-se a meta necessária ao cumprimento do acordo relacionado à criação de proposta cooperativa de proteção de dados pessoais adotado na XXV Cúpula Ibero-Americana na Colômbia (2016).

Este conjunto de diretrizes orientadoras objetiva a emissão de iniciativas regulatórias de proteção de dados pessoais aos países integrantes que não contenham legislações sobre a temática, validando premissa estratégica convencionada pela RIPD (2016), plasmada no documento “RIPD 2020”, em

---

Proteção de Dados). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj >. Acesso em: 14 mar. 2019.

[170] PEZZI, Ana Paula Jacobus. **A necessidade de proteção dos dados pessoais nos arquivos de consumo:** em busca da concretização do direito à privacidade. Monografia. UNISINOS: São Leopoldo, 2007. p. 104-107.

[171] A discussão sobre autoridades de proteção de dados pessoais será melhor trabalhada no 2º capítulo enquanto a análise da produção legislativa Ibero-americana, conjuntamente à mercosurenha, será melhor abordada no 3º capítulo, tendo em vista a maior afinidade de temáticas e o pareamento com a proposta da dissertação.

Montevidéu, que incentiva o fortalecimento e adequação dos processos regulatórios na região mediante parametrizações.

Atribuiu-se no documento padronizador o *status* de direito fundamental à proteção de dados pessoais (1º Considerando), assegurando a integridade dos direitos e liberdades fundamentais à vida privada, familiar e intimidade (2º Considerando), em caráter altamente prioritário (11º Considerando), com ressalvas ao interesse público e de terceiros, quando não incorrerem em arbitrariedades, e com respeito aos ideais democráticos (12º Considerando)[172].

Neste contexto latino-americano é possível ainda encontrar a realidade jurídica do MERCOSUL que, como bloco de integração, também debate e regulamenta a proteção de dados pessoais em suas reuniões ordinárias e resoluções; inserto no mesmo cenário estão os direitos internos argentino, brasileiro, paraguaio e uruguaio, legislando sobre a matéria, inclusive com provável maior especificidade, conforme será explorado no terceiro capítulo.

## 2.7 Princípios da proteção dos dados pessoais

É consabido que a tecnologia trouxe um colossal avanço à vida moderna, no entanto, a facilidade, praticidade e acessibilidade obtidas com os bancos de dados, sistemas gerenciadores de bancos de dados e com o tratamento de dados pessoais trouxe consigo um dos maiores problemas cibernéticos deste século: vazamentos de dados pessoais[173].

Custosa parece a constatação de que estas fortalezas digitais, que transmitiam outrora uma renovadora impressão de segurança, são agora os principais alvos de *ciberataques*. Semanalmente brotam notícias comunicando que milhões de dados pessoais “vazaram” e não é espantoso que esta diáspora digital esteja preocupando os usuários e autoridades públicas e privadas.

A temerária gestão do tratamento de dados pessoais, especialmente sensíveis, pelas multinacionais e conglomerados midiáticos, a dissimulada transparência, o insuficiente controle, a ausência de consentimento e a mantença *ad aeternum* das

---

[172] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Padrões de Proteção de Dados Pessoais para os Estados Ibero-Americanos,** de 20 de junho de 2017**.** Disponível em: < http://www.redipd.es/documentacion/common/Estandares_PORTUGUES.pdf>. Acesso em: 15 mar. 2019.

[173] A questão do vazamento de dados pessoais será apropriadamente trabalhada no 2º capítulo da dissertação conjuntamente às medidas adotadas pelo RGPD para combatê-lo.

bases de dados são outros problemas sintomáticos que minam a privacidade dos seus próprios titulares.

Neste sentido, a proteção de dados pessoais é a ferramenta de combate contra esta mazela aplicável no momento. Guiada por diversos princípios informáticos e securitários e pautada em direitos humanos e fundamentais - notadamente a dignidade da pessoa humana e os direitos à privacidade e à intimidade - imperioso registrar algumas notas sobre esta principiologia.

Segundo Mendes, estes princípios "*t*êm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder ao indivíduo para que esse possa controlar o fluxo de seus dados"[174]. Teriam assim uma dúplice intenção: a de condicionar o tratamento de dados pessoais à elementos limitadores e a de restituir aos seus titulares a autonomia sobre o que lhes dizem respeito.

Doneda entende que "mesmo com a mudança de perfil das leis de proteção de dados com a sua maturação, é possível reagrupar seus objetivos e linhas de atuação principais em torno de alguns princípios comuns, presentes em vários ordenamentos"[175]. A linha evolutiva jurídica da proteção de dados anteriormente traçada comprova este pensamento.

Registros indicam que o núcleo básico dos princípios de proteção de dados reproduzido até hoje teve origem na década de 1960, mas que foi com a publicação de estudo em 1973 sobre a relação direta entre privacidade e tratamento de dados pessoais, por uma comissão especializada da *Secretary for Health, Education and Welfare* (HEW), que as diretrizes ganharam contornos[176].

Este conjunto de medidas acabou sendo importado por diversas normativas de proteção de dados pessoais e ficou conhecida como *Fair Information Principles*. Sua influência foi tão acentuada que serviu de base inclusive à elaboração da Convenção n.º 108 do Conselho da Europa e das *guidelines da* OCDE de 1980, já retratadas no tópico anterior[177].

---

[174] MENDES, Laura Schertel. **Transparência e Privacidade:** violação e proteção de informação pessoal na sociedade de consumo. Universidade de Brasilia - UNB. Dissertação (Mestrado em Direito). 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em: 29 jul. 2019. p. 56.

[175] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. p. 43.

[176] UNITED STATES OF AMERICA. Records, computers and the rights of citizens. **Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973**. Disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm>. Acesso em: 15 mar. 2019.

[177] BRASIL, op. cit., p. 44-45.

Seus princípios costumam variar de uma normatização para outra, sendo identificados de maneira fracionada, condensada ou adaptada[178], contudo, de acordo com Rodotà e Sampaio, é possível sintetizá-los em cinco principais: princípio da transparência, princípio da qualidade, princípio da finalidade, princípio do livre acesso e princípio da segurança física e lógica[179].

Todavia serão trabalhados aqui apenas os princípios elencados no art. 5º, "1" e "2" do RGPD, tendo em vista o enfoque da proposta da dissertação, a vinculação destes princípios com o capítulo seguinte e a amplitude e a atualidade da sua aceitação no universo jurídico. Frise-se novamente que, em nível internacional, estes princípios não compõem um rol taxativo.

Destarte, serão explorados na sequência, sem o objetivo de esgotar a matéria, os princípios da licitude, lealdade e transparência; o princípio da limitação das finalidades; o princípio da minimização; o princípio da exatidão; o princípio da limitação da conservação; os princípios da integridade e confiabilidade; e o princípio da responsabilidade.

### 2.7.1 Princípios da licitude, lealdade e transparência

Severas vezes encontrados em suas versões inglesas, *lawfullness, fairness* e *transparency*, tratam-se de três princípios correlacionados que norteiam diversas diretrizes, normativas e regulamentos e, em especial no caso em apreço, a proteção de dados pessoais. Estão previstos no art. 5º, "1", "a", do RGPD, como características de um correto tratamento de dados pessoais.

O princípio da licitude está bastante interligado com a obediência estrita de um comando legal ou com a inobservância autorizada por um dispositivo legal. Para que um tratamento de dados pessoais seja considerado lícito, ele deverá comportar ao menos uma das seis hipóteses legais estabelecidas no art. 6º, "1", "a" a "f", do Regulamento europeu.

São exemplos de tratamentos lícitos os necessários para: (i) uma ou mais finalidades específicas, se consentidos pelo titular; (ii) execução contratual ou

---

[178] PEZZI, Ana Paula Jacobus. **A necessidade de proteção dos dados pessoais nos arquivos de consumo:** em busca da concretização do direito à privacidade. Monografia. UNISINOS: São Leopoldo, 2007. p. 84.

[179] RODOTÀ, Stefano. ***Repertorio difine secolo***. Bari: Laterza, 1999. p. 62. SAMPAIO, José Adércio L. **Direito à intimidade e à vida privada.** Belo Horizonte: Del Rey, 1999, p. 509.

diligência pré-contratual referente ou solicitada ao/pelo titular; (iii) cumprimento de obrigação jurídica; (iv) defesa de interesses vitais do titular ou terceiro singular; (v) exercício de função ou autoridade pública; e (vi) efetivação dos interesses do responsável, salvo casos especiais de proteção.

O princípio da lealdade ou princípio da boa-fé consiste na premissa de que o sujeito responsável pela coleta dos dados pessoais deve obtê-los com o consentimento do respectivo titular e não através de subterfúgios proibidos, bem como estar comprometido em fazer com que o processo de coleta e manuseio dos dados pessoais seja conduzido com a devida ética[180].

O princípio da transparência ou princípio da publicidade zela pelo conhecimento aberto da existência e da motivação dos bancos de dados pessoais, seja pela exigência de autorização anterior para funcionamento, notificação à autoridade da sua existência ou pela emissão rotineira de relatórios[181]. Há previsão deste princípio no art. 12, “1” a “8”, do RGPD.

Mendes, fazendo paralelo entre legislação de dados pessoais e legislação consumerista brasileira, comenta que a essência do princípio é que o tratamento dos dados pessoais “[...] seja realizado de forma transparente e que o consumidor seja informado de forma clara e precisa, especialmente, sobre os tipos de dados coletados, quais as finalidades da coleta e do uso de dados pessoais [...]”[182].

Acrescenta que o titular dos dados, o consumidor, deve ser informado “[...] se há acesso de terceiros a esses dados e quais as medidas de segurança adotadas [...]”[183]. Quer dizer a autora que não basta que se tenha conhecimento da existência de um banco de dados, a finalidade do tratamento, a tipagem dos dados e o controle e segurança de acesso devem estar claros e às claras.

Argumenta ser a transparência obrigatória e independer do meio de divulgação escolhido pelo mantedor dos dados, “[...] seja por meio de políticas de privacidade, seja pelos contratos de prestação de serviço publicados nos sites dos provedores ou

---

[180] CALHEIROS, Tânia da Costa; TAKADA, Thalles Alexandre. **Reflexões sobre a privacidade na sociedade da informação.** Londrina, v. 4, n. 1, p. 120 – 134, jan./jun. 2015. p. 6.
[181] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 10.
[182] MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor.** São Paulo, v. 25, n. 106, jul./ago., 2016. p. 45.
[183] Ibid., p. 45.

mesmo por meio de informações específicas fornecidas ao consumidor antes da obtenção do consentimento [...]"[184].

Este princípio reafirma o preceito democrático ao contribuir para o combate a abusos como existência de bancos de dados sigilosos ou mercantilização de dados clandestinamente. Sua aplicação também é relativizada, suas exceções previstas legalmente, como nos casos de defesa nacional, segurança púbica, cobrança tributária, programas sociais etc.[185]

Ademais, não se deve confundir o princípio da publicidade dos dados pessoais com a publicidade comportamental, sobretudo com a ideológica. Mesmo que a publicidade tenha superado a dimensão do estritamente informacional, surtindo efeitos sobre o psicológico dos indivíduos[186], o princípio aqui discutido está relacionado com o tratamento de dados pessoais.

### 2.7.2 Princípios da especificação e limitação da finalidade

Os princípios prelecionam que as finalidades destinadas aos dados pessoais sempre devem ser legítimas, específicas e prévias às suas coletas, sendo irregular qualquer tratamento posterior com diferentes desígnios. Noutras palavras, o princípio prega a utilização dos dados pessoais seja condizente com seus propósitos originais. É o que dispõe o art. 5º, "1", "b", parte inicial, do RGPD.

Verifica-se uma grande relevância prática na aplicação deste princípio. Não apenas por fundamentar a restrição da transferência dos dados pessoais a terceiros (o que constitui nova finalidade), mas também por auxiliar no dimensionamento da razoabilidade na utilização de referidos dados em relação à sua finalidade, combatendo eventuais abusos[187].

Imperioso destacar que o tratamento de dados pessoais para finalidades escusas, desconhecidas ou indeterminadas descumpre a legislação, assim como esta resta descumprida quando finalidades ulteriores são incompatíveis com as iniciais.

---

[184] Ibid., p. 45.
[185] SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998. p. 513.
[186] MACHADO, Fernando Inglez de Souza; RUARO, Regina Linden. **Publicidade comportamental, proteção de dados pessoais e o direito do consumidor.** In: CONPEDI Law Review. Braga, vol. 14, n. 43, abr./jun., 2017. p. 422.
[187] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 10.

Uma nova finalidade exige nova base legal[188]. Havendo finalidade incompatível, o tratamento é ilegítimo e ilícito (art. 5º, "b", da Convenção 108)[189].

### 2.7.3 Princípio da minimização

Reconhecido no art. 5º, "1", "c", do RGPD, preceitua que deve haver uma adequação, pertinência e limitação dos dados pessoais para com suas finalidades. Somente as categorias de dados pessoais sujeitas à coleta são necessárias à concretização das operações de tratamento. Havendo dissonância ou excessos de finalidade, o tratamento de dados deve ser restrito.

Estes tríplices fatores constituem a essência do princípio de minimização dos dados pessoais, cuja significância parece pouco influenciar quando há consentimento do titular dos dados pessoais para tratamento, muito embora por intermédio de tecnologias especiais seja possível evitar manuseio de quaisquer dados ou dados pseudonimizados, ganhos estes em questão de privacidade[190].

### 2.7.4 Princípios da exatidão e da atualização

Os princípios estão insculpidos no art. 5º, "1", "d", do RGPD e transmitem as ideias de que (i) os dados pessoais devem ser armazenados e atualizados, visando garantir a exatidão do conteúdo presente nos bancos de dados, primando pela qualidade e veracidade dos mesmos e (ii) que os dados inexatos sejam apagados ou retificados sem demora[191].

A legislação europeia possui uma grande preocupação para que os dados pessoais não estejam desatualizados ou equivocados, razão pela qual alinha suas diretrizes com a Convenção n.º 108, objetivando manter a fidedignidade destes dados

---

[188] CONSELHO DA EUROPA. **Manual da legislação europeia sobre proteção de dados.** Agência dos Direitos Fundamentais da União Europeia, 2014. p. 72.

[189] Id. **Convenção n.º 108, de 28 de janeiro de 1981,** relativa à Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Disponível: <http://www.ministeriopublico.pt/instrumento/convencao-para-proteccao-das-pessoas-relativamente-ao-tratamento-automatizado-de-dados-2>. Acesso em: 20 fev. 2019.

[190] CONSELHO DA EUROPA. **Manual da legislação europeia sobre proteção de dados.** Agência dos Direitos Fundamentais da União Europeia, 2014. p. 75.

[191] CALHEIROS, Tânia da Costa; TAKADA, Thalles Alexandre. **Reflexões sobre a privacidade na sociedade da informação.** Londrina, v. 4, n. 1, p. 120 – 134, jan./jun. 2015. p. 7.

à realidade, demandando procedimentos cuidadosos, periódicos e, se necessários, correcionais[192].

Não ignorando as hipóteses nas quais dados pessoais suspeitos (suficientes e justificáveis) sejam legalmente admissíveis e atualizações de acontecimentos passíveis de documentação sejam normativamente proibidas, o princípio quer assegurar a precisão e atualidade dos dados pessoais, conforme finalidade dos seus tratamentos e tomada das razoáveis providências[193].

### 2.7.5 Princípio da limitação da conservação

Também intitulado de princípio da caducidade ou *storage limitation*, este indispensável princípio de proteção privatística está cravado no art. 5º, "1", "e", do RGPD e traduz a noção de que o armazenamento dos dados pessoais capazes de identificar seus titulares é dispensável quando alcançadas as finalidades que motivaram seus recolhimentos ou tratamentos[194].

Haverá sempre um prazo para conservação destes dados pessoais, segundo a redação do princípio e esta data-limite está vinculada ao "período necessário para prossecução das finalidades", notadamente no setor policial, momento no qual seu armazenamento deverá ser apagado dos bancos de dados[195]. Cumpre registrar, todavia, algumas ressalvas legais ao princípio.

A limitação temporal é aplicável somente aos dados pessoais capazes de identificar seus titulares, sendo legal o armazenamento de outras categorias de dados mediante sua anonimização ou pseudonimização (art. 4º, "5", do RGPD)[196/197]. Desta forma, resta dificultado o acesso de terceiros aos dados personalíssimos através de consultas genéricas sem identificadores específicos.

---

[192] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 10.
[193] CONSELHO DA EUROPA, op. cit., p. 76-77.
[194] CALHEIROS, op. cit., p. 7.
[195] CONSELHO DA EUROPA. **Manual da legislação europeia sobre proteção de dados.** Agência dos Direitos Fundamentais da União Europeia, 2014. p. 78.
[196] Ibid., p. 78.
[197] **Anonimização ou pseudonimização:** "o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável". (UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016,** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 21 fev. 2019).

Ademais, dados pessoais valiosos para investigações científicas, históricas e estatísticas podem ser mantidos por períodos maiores, desde que sejam tratados exclusivamente como “arquivo de interesse público” e a continuidade do seu armazenamento e utilização estejam acompanhadas por “garantias especiais”, preconizadas no art. 5º, “e”, parte final, do RGPD[198].

### 2.7.6 Princípios da integridade e confidencialidade

O princípio da integridade ou princípio da segurança física e lógica consiste na proteção dos dados pessoais contra eventuais “riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado”[199]. O preceito determina que o responsável pelo armazenamento dos dados pessoais deve adotar as medidas técnicas e administrativas securitárias aplicáveis.

Complementarmente, o princípio da confidencialidade atribui aos dados pessoais caráter de sigilosidade, visando a garantir que estejam acessíveis unicamente aos seus titulares e terceiros autorizados e evitar ilicitudes nos seus tratamentos[200]. São estes dois princípios imprescindíveis à integridade e à privacidade, motivo pelo qual constam expressamente no art. 5º, “f”, do RGPD.

### 2.7.7 Princípio da responsabilidade objetiva

Trata-se de princípio que objetiva penalizar os responsáveis pelos bancos de dados pessoais, em virtude de eventuais danos provocados pela inobservância proposital (dolo) ou casual (culpa) de quaisquer dos princípios anteriormente expostos. Independente da gradação de seu envolvimento no incidente, o risco objetivo do serviço desempenhado recairá sobre o agente[201].

Devidamente prescritos no art. 5º, “2”, do RGPD, os responsáveis pela mantença dos bancos de dados devem implementar as medidas suficientes para salvaguardar os dados pessoais. Conjuntamente a esta incumbência, os responsáveis

---

[198] CONSELHO DA EUROPA, op. cit., p. 78.
[199] DONEDA, Danilo. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011. p. 11.
[200] CALHEIROS, Tânia da Costa; TAKADA, Thalles Alexandre. **Reflexões sobre a privacidade na sociedade da informação.** Londrina, v. 4, n. 1, p. 120 – 134, jan./jun. 2015. p. 7.
[201] Ibid., p. 8.

pelo tratamento devem possuir condições de demonstrar sua conformidade à legislação aos respectivos titulares e autoridades de controle[202].

## 2.8 Proteção transfronteiriça dos dados pessoais

A proteção de dados pessoais transfronteiriça é um obstáculo deveras complexo à eficácia de qualquer legislação a respeito. Os fluxos pessoais de informações e de conteúdo não processados que trespassam fronteiras geográficas e jurisdicionais, ininterruptamente, são massivos e requerem avançadas técnicas de gerenciamento e tratamento. Esta dinâmica evolução das Tecnologias da Informação e Comunicação (TICs) está desencadeando profundas mudanças na vida econômica, social e jurídica do ser humano.

Sublinha Araújo que "[...] As leis domésticas de proteção de dados perdem grande parte da sua eficácia com uma simples transferência desses dados para uma país que não os proteja adequadamente"[203] e isso descreve a realista constatação de que este compartilhamento informativo muitas vezes acontece desprovido de uma estrutura legal que devidamente proveja a segurança, integridade e privacidade que os direitos e liberdades fundamentais e humanitárias prescrevem às pessoas singulares.

Mas o que seriam estas transferências? De acordo com a leitura do art. 2º, "1", do Protocolo Adicional à Convenção 108/1981, podemos conceituar transferência transfronteiriça de dados pessoais como "uma transferência de dados pessoais para um destinatário que está sujeito a uma jurisdição estrangeira"[204]. Em verdade, não parece existir uma definição uniforme no direito europeu e internacional sobre transferência transfronteiriça de dados pessoais, mas algumas aferições legais e excertos jurisprudenciais servem de auxílio.

A Diretiva 95/46/CE, quando vigente na UE, em seu Capítulo IV, disciplinava a "Transferência de Dados Pessoais para Países Terceiros" (arts. 25 e 26), sem

---

[202] CONSELHO DA EUROPA. **Manual da legislação europeia sobre proteção de dados.** Agência dos Direitos Fundamentais da União Europeia, 2014. p. 81.
[203] ARAÚJO, Alexandra Maria Rodrigues. **As transferências transatlânticas de dados pessoais:** o nível de proteção adequado depois de *Schrems*. Revista de Direitos Humanos e Democracia. Editora Unijuí, ano 5. n. 9. jan./jun, 2017. p. 203.
[204] CONSELHO DA EUROPA. **Manual da legislação europeia sobre proteção de dados.** Agência dos Direitos Fundamentais da União Europeia, 2014. p. 138.

qualquer definição sobre sua terminologia. A legislação europeia seguinte[205] trabalhou melhor essa questão. Pela redação do art. 45, "1", do RGPD, consiste no método mais prático para exportação de dados pessoais para uma jurisdição terceira estrangeira com nível de proteção tido como suficientemente adequado. No art. 4º, "23", "a" e "b", o conceito é destrinchado:

> Tratamento transfronteiriço: a) O tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro; ou b) O tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro[206].

Araújo explica que a interpretação do seu significado depende da leitura atenta do acórdão de *Schrems*, no qual o Tribunal de Justiça da União Europeia (TJUE) esclareceu que "a transferência de dados pessoais de um Estado-Membro para um país terceiro constitui, enquanto tal, um tratamento de dados pessoais"[207]. Trata-se o julgado de grande referência para compreensão do sentido do princípio do nível de proteção adequado do art. 45 do RGPD.

Recorda Araújo que o acórdão *Bodil Lindqvist,* igualmente objeto de apreço pelo TJUE, abordou a hipótese de inexistência de transferência de dados pessoais transfronteiriços. No excerto é feita suposição onde dados pessoais, e não quaisquer dados, são inseridos em página de fornecedor de serviços situado dentro da circunscrição territorial do país ou do megabloco originário de modo que todos que a conectem tenham acesso. Segue abaixo transcrição do trecho que desconsidera a estudada transferência:

> [...] quando uma pessoa que se encontra num Estado-Membro insere numa página Internet, armazenada num fornecedor de serviços de anfitrião que está estabelecido no mesmo Estado ou noutro Estado-

[205] Tendo em vista as complexidades e fragmentações jurídicas decorrentes da criação de 28 leis nacionais, restava dificultosa a comunicação de dados pessoais entre os Estados Membros. A transição de instrumento normativo, de uma diretiva para um regulamento, era precisa para que houvesse aplicabilidade sobre a matéria em toda UE (art. 288 do TFUE).
[206] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.
[207] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão de 6 de outubro de 2015**, **processo C-362/14.** Maximilian Schrems c. Data Protection Commissioner. par. 45.

> Membro, dados de caráter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros [...][208].

A conclusão do julgado foi de que a transferência transfronteiriça de dados só restará caracterizada quando houver comunicações privativas enviadas a destinatários específicos de país terceiro, descaracterizando, portanto, casos em que os dados pessoais estejam em servidores anfitriões ou situações de "mero trânsito dos dados" em território estrangeiro[209]. Observa-se que nuances fáticas como localização, tipagem dos dados e entidades envoltas nas transferências podem modificar juridicamente o contexto das operações.

O RGPD também trouxe consigo um pacote de regras acerca desta transferência transfronteiriça privatística. Demonstra, desde as justificativas, suas preocupações e expectativas como a necessidade da circulação de dados pessoais para o desenvolvimento do comércio e cooperação internacionais (101º Considerando), da mantença de razoável autonomia para tratativas bilaterais entre UE e países e organizações estrangeiras (102º Considerando) e da nivelação adequada de proteção de dados pessoais (103º Considerando).

No Capítulo V da norma referida constam as regras específicas sobre estas transferências, como princípio geral (art. 44º), decisão de adequação para transferências (art. 45º), transferências com garantias adequadas (art. 46), regras vinculativas aplicáveis às empresas (art. 47), casos de divulgações não autorizadas (art. 48), derrogações (art. 49) e cooperação internacional (art. 50)[210].

No tocante ao "nível adequado de proteção de dados pessoais", forçoso o registro de alguns comentários. Inicialmente, não existe uma definição expressa na legislação europeia que o defina, porém existem alguns critérios legais, não taxativos, capazes de elucidar sua significação, funcionamento e importância nestas transferências transfronteiriças.

Deve ser considerado para tanto o máximo de circunstâncias que envolvem as transferências transfronteiriças de dados pessoais: a natureza dos dados; a finalidade

---

[208] Id. **Acórdão de 6 de novembro de 2003, processo C-101/01**. Göta hovrat c. Bodil Lindqvist. par. 71.

[209] ARAÚJO, Alexandra Maria Rodrigues. **As transferências transatlânticas de dados pessoais:** o nível de proteção adequado depois de *Schrems*. Revista de Direitos Humanos e Democracia. Editora Unijuí, ano 5. n. 9. jan./jun, 2017. p. 210-211.

[210] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

e a duração do tratamento; os países, órgãos ou organizações internacionais transmissoras ou receptoras; e as legislações domésticas, setoriais e internacionais[211].

Para avaliar estes fatores, uma Comissão será designada para analisar a compatibilidade ou nível de adequação protetiva oferecida pela legislação interna do país ou mediante verificação dos "compromissos internacionais" dos quais este país é signatário, obviamente com foco na proteção à privacidade e direitos e liberdades fundamentais das pessoas.

O Grupo de Trabalho do Artigo 29 (GT), da Diretiva 95/46/CE, relativo ao tratamento de dados pessoais, funcionava como órgão consultivo proferindo pareceres de conformação ou desajustamento do nível protetivo dos envoltos na transferência transfronteiriça, tendo sido sua praxe consultiva bastante valiosa para interpretação desta "adequação".

O GT utilizava como parâmetro de medição o conteúdo do direito interno vigente, os meios usados à sua concretização, pautando-a em seis princípios basilares: (i) limitação da finalidade do tratamento; (ii) proporcionalidade e qualidade dos dados; (iii) transparência; (iv) segurança; (v) direitos de acesso, retificação e oposição e (vi) restrições a transferências subsequentes[212].

Estes cinco primeiros princípios do tratamento transfronteiriço não divergem da essência dos correspondentes princípios de proteção dos dados pessoais explorados no tópico anterior. Os seguintes ganharam ênfase do Grupo para confecção dos seus pareceres. O princípio do direito de acesso é importante para garantir aos seus titulares obtenção de cópia de dados a seu respeito.

Para maior controle dos dados pessoais, o direito de retificação garante aos portadores autorização para os corrigir em caso de eventuais inexatidões; o direito de oposição, lhes garante o direito de se contrapor ao tratamento dos dados e, o direito à restrição de transferências posteriores, proíbe transmissões aqueles destinatários com nível de proteção inadequado[213].

---

[211] ARAÚJO, Alexandra Maria Rodrigues. **As transferências transatlânticas de dados pessoais:** o nível de proteção adequado depois de *Schrems*. Revista de Direitos Humanos e Democracia. Editora Unijuí, ano 5. n. 9. jan./jun., 2017. p. 214-215.

[212] ARAÚJO, Alexandra Maria Rodrigues. **As transferências transatlânticas de dados pessoais:** o nível de proteção adequado depois de *Schrems*. Revista de Direitos Humanos e Democracia. Editora Unijuí, ano 5. n. 9. jan./jun, 2017. p. 215-217.

[213] CONSELHO DA EUROPA. **Manual da legislação europeia sobre proteção de dados.** Agência dos Direitos Fundamentais da União Europeia, 2014. p. 112-222.

Interessante registrar que as autorizações concedidas por Estado-Membro ou autoridade controladora quanto às garantias das transferências transfronteiriças do art. 26º, "2", da Diretiva 95/46/CE, permanecem em vigor até que sejam alteradas, substituídas ou revogadas, caso seja necessário, segundo determinação do RGPD (art. 46º, "5")[214].

A importância deste estudo da normatização e do funcionamento do fluxo transfronteiriço de dados pessoais e das decisões de níveis de adequação protetiva privativa[215], sobretudo das constantes no novíssimo modelo europeu, reside na compreensão deste novo alinhamento jurídico, informacional, tecnológico e securitário mundialmente crescente.

Grande parte da preocupação institucional e repercussão midiática dos governos, entidades internacionais e das empresas multinacionais com transferências de dados pessoais com a UE é devida à adoção do RGPD e da sua exigência de qualidade protetiva. Apreensivos com a vigência dos seus efeitos, uma discussão e produção legislativa teve início.

A relevância deste "novo fenômeno legislativo" é imprescindível à proposta da dissertação que se apresenta, a qual objetiva verificar a possibilidade de uma normatização baseada no RGPD, mas contextualizada na realidade do MERCOSUL, cujos Estados Partes são exemplos das nações interessadas em atualizar suas legislações de tratamento de dados pessoais, como medida destinada a proteger o consumidor transfronteiriço.

Como a problemática da dissertação envolve também a questão do *personal data breach*, o capítulo seguinte vai se dedicar a investigar os pormenores da estrutura e arcabouço jurídico do RGPD e suas medidas de combate aos vazamentos de dados pessoais para garantia dos direitos humanos e direito e liberdades fundamentais neste capítulo abordados.

---

[214] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[215] Sobre o assunto, ver os livros de Luciane Klein Vieira: "*Protección internacional del consumidor. Procesos de escasa cuantía en los litigios transfronterizos*" (2013) e "*La hipervulnerabilidad del consumidor transfronterizo y la función material del derecho internacional privado*" (2017).

# 3 REGULAMENTO GERAL EUROPEU DE PROTEÇÃO DE DADOS

Neste Segundo Capítulo será feita uma breve contextualização sobre o panorama legislativo global, regional europeu e nacional da proteção de dados pessoais e serão trabalhadas questões gerais e técnicas diretamente relacionadas com o RGPD, notadamente as tocantes ao *personal data breach*, aos mecanismos de segurança de dados pessoais e às suas relações com o direito do consumidor.

A abordagem iniciará versando sobre documentos internacionais, normas da UE e regulações nacionais sobre o tema para ambientar e introduzir o RGPD; seguirá com a sistemática, objetivos, âmbitos de aplicação, direitos dos titulares de dados do RGPD para então adentrar nas suas questões técnicas sobre tratamentos, incidentes, violações e mecanismos de segurança de dados pessoais.

## 3.1 Contexto normativo global, regional europeu e nacional

Com a finalidade de localizar a produção legislativa global, regional europeia e nacional tocante à proteção de dados pessoais, como semelhante se pretende fazer com as nações mercosurenhas no próximo capítulo, os tópicos seguintes versarão a respeito das normas internacionais globais, das normas da UE e das regulações nacionais mais relevantes para com a temática.

### 3.1.1 Normas internacionais no âmbito global

Os tratados[216] constituem a principal fonte normativa do Direito Internacional por representarem as vontades das entidades envolvidas na regulação de uma ou mais relações jurídicas comuns entre si. Desta forma, não havendo obrigatoriedade no ato da subscrição do documento, fica evidenciada a noção de consentimento, o viés democrático dos tratados e a preservação da soberania dos signatários[217].

---

[216] *Tratado:* "[...] significa um acordo internacional concluído por escrito entre Estados e regido pelo Direito Internacional, quer conste de um instrumento único, quer de dois ou mais instrumentos conexos, qualquer que seja sua denominação específica". (BRASIL. **Decreto n.º 7.030, de 14 de dezembro de 2009.** Promulga a Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos Artigos 25 e 66. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Decreto/D7030.htm>. Acesso em: 28 jul. 2019. Art. 2º, n.º 1, "a").

[217] VARELLA, Marcelo D. **Direito internacional público**. – 6. ed. – São Paulo: Saraiva, 2016. p. 37.

É possível depreender, a partir destas características traçadas, duas dimensões dos tratados: uma prática e uma jurídica. A dimensão prática enseja o acatamento dos compromissos dos signatários, de um lado, com a comunidade internacional e, de outro, com os poderes públicos e cidadãos; e a dimensão jurídica abrange os aspectos internacionais dos tratados e as disposições constitucionais[218].

Considerando estes fatores básicos dos tratados, a produção legislativa internacional e a compreensão da importância de algumas destas convenções à proteção de dados pessoais restam facilitadas. Cita-se como exemplos a Convenção Europeia dos Direitos do Homem (CEDH) e a Convenção n.º 108/1981 de Estrasburgo, acerca das quais serão tecidos alguns comentários.

A CEDH consistiu em tratado realizado em Roma, adotado pelo Conselho da Europa (1950), que teve sua vigência três anos depois (1953), recebeu protocolos posteriores e objetivou a proteção de direitos humanos e liberdades fundamentais, como o direito ao respeito à vida privada e à vida familiar (art. 8º), bem como o direito à liberdade de expressão (art. 10º)[219].

A propósito, em termos de conceituação, considera-se o artigo 10º da CEDH a pedra angular da liberdade de informação em todo continente europeu[220], uma vez que nele restou traduzido em singular enunciado os diversos posicionamentos das nações europeias envolvidas na tratativa, servindo então de baluarte à confecção de vindouros documentos legislativos sobre a temática.

A Convenção para Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, consistiu em tratado adotado pelo Conselho da Europa em Estrasburgo (1981) e simbolizou o primeiro documento

---

[218] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 63.
[219] CONSELHO DA EUROPA. Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 4 de novembro de 1950. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 3 jul. 2019.
[220] RIPOL CARULLA, Santiago**.** ***Las libertades de información y de comunicación em europa.*** Madrid: Tecnos, 1995. p. 43.

jurídico unificado sobre o tema - já que as diretrizes de intimidade e fluxo de dados transfronteiriços da OCDE (1980) eram de *soft law*[221], não eram obrigatórias[222].

Referido tratado conferiu juridicidade ao campo de aplicação (art. 3º); aos deveres das partes (art. 4º); à qualidade dos dados (art. 5º); aos dados especiais (art. 6º); à segurança dos dados (art. 7º); aos direitos dos titulares (art. 8º); à circulação transfronteiriça de dados pessoais (art. 12º); à cooperação internacional (arts. 13º e 14º); regras também atualizadas em póstumas legislações[223].

### 3.1.2 Normas da União Europeia

Com o estrondoso avanço tecnológico e comunicacional, o crescimento do tratamento de dados pessoais informatizados trouxe consigo riscos inerentes ao seu indevido manuseio e ao desnivelamento protetivo dos dados pessoais em transferências entre países e continentes. Nasceu desta conclusão um interesse em conciliar a livre circulação e proteção de dados dos cidadãos e consumidores.

No desafio de harmonizar estes dois direitos fundamentais, potencialmente conflituosos, valeu-se o Conselho da Europa de disposições materiais, especiais e funcionais para desenhar um corpo normativo-protetivo. Os direitos materiais foram

---

[221] *Soft law:* "[...] na sua moderna acepção ela compreende todas as regras cujo valor normativo é menos constringente que o das normas jurídicas tradicionais, seja porque os instrumentos que as abrigam não detêm o status de 'norma jurídica', seja porque os seus dispositivos, ainda que insertos no quadro dos instrumentos vinculantes, não criam obrigações de direito positivo aos Estados, ou não criam senão obrigações pouco constringentes". (MAZZUOLI, Valério de Oliveira. **Curso de direito internacional público.** 5 ed., Editora RT, 2011. p. 992)

[222] Há discussão doutrinária a respeito da anterioridade ou do diálogo entre *soft law* e *hard law.* Neste sentido, Vieira esclarece que "[...] alguns tem defendido que primeiro se deve adotar o *soft law*, por exemplo, manifestado por meio da criação de princípios sobre contratos internacionais com consumidores, para depois transformá-los em *hard law*, tendo em conta as dificuldades de elaboração de um direito duro, inicialmente. Outra vertente doutrinária aduz que o *soft law* e o *hard law* se comunicam e dialogam entre si e que por este motivo o *soft law*, que deve estar baseado em padrões internacionais (neste caso, de proteção do consumidor), inspira e influencia o comportamento dos Estados para a adoção do *hard law*, ainda que esteja desvinculado da ideia de poder e não seja juridicamente vinculante. Desta forma, é incontestável o papel dos instrumentos de *soft law*, como mecanismos de persuasão e fontes de direito, na formulação dos valores que poderão ser no futuro referendados por convenções internacionais, na medida em que ervem para preencher lacunas e estimular a criação do direito duro". (VIEIRA, Luciane Klein. **La hipervulnerabilidad del consumidor transfronterizo y la función del Derecho Internacional Privado.** – 1 ed. Ciudad Autónoma de Buenos Aires: La Ley, 2017. p. 164. p. 444-445 [tradução nossa]).

[223] CONSELHO DA EUROPA. **Convenção n.º 108, de 28 de janeiro de 1981, relativa à Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal**. Disponível em: <https://www.coe.int/en/web/data-protection/legal-instruments>. Acesso em: 3 jul. 2019.

insertos sob a forma de princípios com o objetivo de condicionarem o tratamento dos dados pessoais aos ditames legais[224].

Quanto às normas especiais, optou-se por trabalhar com recomendações[225] aos governos europeus ante a existência de setores cuja proteção dos dados pessoais demonstrava maior complexidade. As vantagens destas recomendações e resoluções[226] às normas tradicionais são de que a confecção, adaptação e aplicação delas são facilitadas por dispensarem assinatura e ratificação.

Enquanto estas recomendações versavam sobre o fluxo transfronteiriço de dados pessoais, especialmente os de natureza médica, securitária, bancária e policial, as normas funcionais/instrumentais, pautadas pelos anseios dos cidadãos e consumidores, focavam nos recursos de entrada e consulta de dados pelos seus respectivos titulares, concedendo-lhes maior autonomia, gerência e transparência[227].

Esta influência é percebida, por exemplo, na adoção das Resoluções n.º 22/1973 e n.º 29/1974 do Conselho da Europa que esboçaram os princípios da proteção de dados pessoais no tratamento automatizado nos setores públicos e privados europeus com o intuito de nortear e incentivar a criação de legislações nacionais, mormente pela chegada dos bancos de dados virtuais a partir de 1960.

A Resolução n.º 22/1973[228], adotada em Copenhague, versava sobre a proteção da privacidade nos bancos de dados eletrônicos do setor privado. Já a Resolução n.º 29/1974[229], adotada em Paris, dispunha acerca de princípios aplicáveis

---

[224] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 67-68.

[225] *Recomendação:* "[...] é um acto unilateral, emitido pelo Conselho de Ministros da UE, pela Comissão Europeia ou em conjunto pelo Conselho e pelo Parlamento Europeu, ao abrigo das suas competências, visando produzir efeitos jurídicos não vinculativos. A sua natureza não vinculativa decorre do prescrito no §5 do artigo 288º TFUE." (SILVA, José Luís Moreira. **Novo Dicionário de Termos Europeus:** Disponível em: <http://euroogle.com/dicionario.asp?definition=835>. Acesso em: 29 jul. 2019, não paginado).

[226] *Resoluções:* "[...] são atos unilaterais, emitidos por órgãos comunitários, ao abrigo das suas competências, visando produzir efeitos políticos, aprovando um programa de ação ou uma política comunitária. As resoluções mais comuns são emitidas pelo Conselho e pelo Parlamento Europeu. As resoluções não estão previstas no artigo 288º TFUE, pelo que são considerados atos atípicos. Até por este facto as resoluções não poderiam produzir efeitos jurídicos, pois apenas os atos típicos, ou seja, os atos expressamente previstos no Tratado como produzindo efeitos jurídicos, o podem fazer, ao abrigo do princípio da legalidade [...]". (Ibid., não paginado).

[227] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 67-68.

[228] CONSELHO DA EUROPA. ***Resolution 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector***, de 26 de setembro de 1973. Disponível em: <https://www.coe.int/en/web/data-protection/legal-instruments>. Acesso em: 3 jul. 2019.

[229] Id. ***Resolution 29 on the protection of individuals vis-à-vis electronic data banks in the public sector***, de 20 de setembro de 1974. Disponível em: <https://www.coe.int/en/web/data-protection/legal-instruments>. Acesso em: 3 jul. 2019.

às informações pessoais armazenadas em bancos de dados públicos. E, mesmo assim, sentiu-se uma necessidade de reforçá-las com normas da UE.

Adiante na cronologia legislativa, inobstante havidas outras recomendações e resoluções neste interregno[230], destaca-se a adoção da Diretiva n.º 95/46/CE, sobre a proteção das pessoas físicas quanto ao tratamento de dados pessoais e livre circulação de dados na UE, com prazo de 3 (três) anos[231] (art. 32, n.º 1)[232] para adaptação dos direitos internos ao texto da diretiva[233].

Seus desígnios principais – que também eram compatíveis com objetivos da própria integração europeia – consistiam na proteção dos direitos fundamentais dos cidadãos/consumidores (proteção dos dados pessoais) e na consolidação de um mercado interno (circulação de dados pessoais). Apesar de baseada nas disposições

---

[230] São exemplos de relevantes recomendações expedidas sobre proteção de dados pessoais: ***Recommendation R(85) 20*** *on the protection of personal data used for the purposes of direct marketing (25 October 1985).* ***Recommendation R(86) 1*** *on the protection of personal data for social security purposes (23 January 1986).* **Recommendation R(87) 15** *regulating the use of personal data in the police sector (17 September 1987) and evaluation reports (1994, 1998, 2002 e 2013);* ***Recommendation R(90) 19*** *on the protection of personal data used for payment and other related operations (13 September 1990).* ***Recommendation R(91) 10*** *on the communication to third parties of personal data held by public bodies (9 September 1991).* ***Recommendation R(95) 4*** *on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995).* ***Recommendation R(97) 5*** *on the protection of medical data (13 February 1997);* ***Recommendation R(97) 18*** *on the protection of personal data collected and processed for statistical purposes (30 September 1997).* ***Recommendation R(99) 5*** *for the protection of privacy on the Internet (23 February 1999).* ***Recommendation R(2002) 9*** *on the protection of personal data collected and processed for insurance purposes (18 September 2002).* ***Recommendation CM/Rec(2010)13*** *of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010).* ***Recommendation CM/Rec(2012) 3*** *of the Committee of Ministers to member states on the protection of human rights with regard to search engine.* ***Recommendation CM/Rec(2012) 4*** *of the Committee of Ministers to member states on the protection of human rights with regard to social networking services.* ***Recommendation CM/Rec(2014) 6*** *of the Committee of Ministers to member States on a Guide to human rights for Internet users (16 April 2014).* ***Recommendation CM/Rec(2015) 5*** *of the Committee of Ministers to member States on the processing of personal data in the context of employment.* ***Recommendation CM/Rec(2016) 8*** *of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests.* ***Recommendation CM/Rec(2018) 2*** *of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries.* ***Recommendation CM/Rec(2019) 2*** *of the Committee of Ministers to member States on the protection of health-related data.* Todas estas recomendações estão disponíveis em: <https://www.coe.int/en/web/data-protection/legal-instruments>. Acesso em: 7 jul. 2019.

[231] A regra geral de fixação de prazo para transposição da diretiva na UE é de 02 (dois) anos.

[232] UNIÃO EUROPEIA. **Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho**, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 7 jul. 2019.

[233] *Diretiva:* "[...] é um ato unilateral, emitido por um órgão comunitário, ao abrigo das suas competências, tendo como destinatários os Estados-Membros, visando produzir efeitos jurídicos vinculativos de resultado. A sua natureza decorre do prescrito no §3 do artigo 288º TFUE [...]" (SILVA, José Luís Moreira. **Novo Dicionário de Termos Europeus:** Disponível em: <http://euroogle.com/dicionario.asp?definition=467>. Acesso em: 29 jul. 2019).

da Convenção, não se pretendia apenas replicá-las, mas também otimizá-las e efetivá-las.

Foi preciso para tanto que a Comunidade Europeia tivesse competência para adoção de princípios e normativas da Convenção n.º 108/1981, o que veio a acontecer em 01/01/1999, conforme previsto no antigo art. 286 do TUE (atual art. 16.º, n.º 2, do TFUE)[234]. Legitimados, o Parlamento Europeu e o Conselho, tornaram obrigatória a observância das disposições pelos demais Estados Membros.

Embora tenha alcançado lugar junto às legislações de dados pessoais mais robustas da época, a Diretiva n.º 46/1995/CE não conseguiu concretizar todos os seus objetivos, mesmo com a adoção da Diretiva n.º 66/1997/CE[235] - destinada à proteção da intimidade no setor das telecomunicações; a complexidade da matéria, o progresso tecnológico e outros fatores minaram seu êxito.

Apontam-se como tais fatores: a incompleta aplicação das regras, motivada pelo descompasso entre o texto legislativo e sua efetividade; as disparidades entre as legislações das nações europeias, cujos problemas e soluções distavam entre si, obstando a configuração de uma política europeia integrada protetiva; conformidade dos produtos tecnológicos com as normas protetivas de dados.

Ademais, a preferência das nações europeias por estreitar a cooperação com as autoridades controladoras ao invés de reduzir a autonomia dos legisladores nacionais evidenciava outros impasses: a insuficiência da coerção das autoridades de controle; a não adequação dos responsáveis pelo tratamento de dados à diretiva; e o baixo conhecimento dos titulares sobre seus direitos[236].

Alguns acórdãos do TJUE sobre o tratamento de dados pessoais da Diretiva n.º 46/1995/CE merecem destaque. Acerca do tratamento excluído do âmbito de aplicação da diretiva, cita-se o Acórdão que discutia questão de segurança pública em

---

[234] "O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.o do Tratado da União Europeia". (UNIÃO EUROPEIA. C 202/47, de 7 de junho de 2016. **Tratado sobre o Funcionamento da União Europeia (TFUE).** Versão Consolidada. Disponível em: <https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-overview.html>. Acesso em: 3 jul. 2019).

[235] Id. **Diretiva 97/66/CE do Parlamento Europeu e do Conselho**, de 15 de dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações. Disponível em: <http://data.europa.eu/eli/dir/1997/66/oj>. Acesso em: 7 jul. 2019.

[236] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 72-73.

acordo internacional da CE com os EUA[237] e a Decisão Prejudicial que envolvia atividades exclusivamente domésticas[238].

Interessante, outrossim, os julgados sobre a conceituação do tratamento de dados pessoais, a exemplo da Decisão Prejudicial que envolvia tratamento de dados sensíveis para exercício de atividades religiosas[239] e da Decisão Prejudicial que envolvia pedido de tratamento de supressão ou alteração de dados pessoais em pesquisa *online* a seu respeito[240].

Ainda na esteira das normas da UE, pertinente mencionar a Carta dos Direitos Fundamentais da União Europeia (CDFUE), proclamada em Nice (2000), pelo Parlamento Europeu, Conselho e Comissão, anunciada novamente anos depois (2007), em face de alterações, mas cuja vigência ocorreu somente com a adoção do Tratado de Lisboa (2009, art. 6.º, n.º 1)[241].

Concluído este trâmite quase decenal, a Carta passou a funcionar como fonte vinculante de direito primário e como mecanismo de controle interno, judicial, prévio e autônomo, a nível de UE. Ela está estruturada em três distintas classes de direitos: (i) os direitos individuais e de participação; (ii) os direitos sociais; e (iii) os novos direitos (como meio-ambiente, bioética e proteção de dados pessoais).

Tendo a dignidade da pessoa humana como princípio nuclear, a Carta disciplina o respeito à vida privada (art. 7º), dispositivo considerado deveras genérico, e a proteção de dados pessoais (art. 8º), inclusas aqui prerrogativas funcionais, como consulta aos dados e eventual retificação, e limitadoras, como a restrição do tratamento aos parâmetros consentidos e aos objetivos destinados[242].

---

[237] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão de 30 de maio de 2006 (Grande Secção)**, Parlamento/Conselho (C-317/04 e C-318/04, EU:C:2006:346). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/SUM/?qid=1564976182834&uri=CELEX:62004CJ0317_SUM>. Acesso em: 29 jul. 2019.

[238] Id**. Acórdão de 11 de dezembro de 2014**, František Ryneš contra Úřad (C-212/13, EU:C:2014:2428). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564976362204&uri=CELEX:62013CJ0212>. Acesso em: 29 jul. 2019.

[239] Id. **Acórdão de 6 de novembro de 2003 (Assembleia Plenária),** Bodil Lindqvist (C-101/01, EU:C:2003:596). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564992216541&uri=CELEX:62001CJ0101>. Acesso em: 29 jul. 2019.

[240] Id. **Acórdão de 13 de maio de 2014 (Grande Secção),** Google Spain e Google (C-131/12, EU:C:2014:317). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>. Acesso em: 29 jul. 2019.

[241] Id. **Tratado de Lisboa (2007/C 306/01)**, que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, de 13 de dezembro de 2007. Disponível em: < http://data.europa.eu/eli/treaty/lis/sign>. Acesso em: 3 jul. 2019.

[242] Id. **Carta dos Direitos Fundamentais da União Europeia (2010/C 83/02)**, do Parlamento Europeu, do Conselho e da Comissão. Disponível em: < http://data.europa.eu/eli/treaty/char_2010/oj>. Acesso em: 3 jul. 2019.

Em matéria jurisprudencial, sobre o direito à proteção de dados pessoais reconhecido pela CDFUE, no específico à conformidade do direito derivado da União com o direito à proteção dos dados pessoais, cabe citar, no âmbito do TJUE, a Decisão Prejudicial sobre aplicabilidade do direito da União[243]; a Decisão Prejudicial sobre processo de adoção normativa e proporcionalidade[244] e da Decisão Prejudicial sobre competência, serviço de comunicação eletrônica e conservação de dados[245].

Ainda sobre o direito à proteção de dados pessoais reconhecido pela CDFUE, mas específico ao respeito do direito à proteção dos dados pessoais na aplicação do direito da União, é possível colacionar a Decisão Prejudicial que permitiu a conservação seletiva de dados de comunicações eletrônicas com base em diretiva invalidada, a título preventivo e com vista à luta contra criminalidade[246].

Posteriormente, a Diretiva n.º 58/2002/CE veio completar a Diretiva n.º 46/1995/CE[247], procedendo à harmonização da legislação dos Estados Membros relacionadas à proteção de dados pessoais nas comunicações eletrônicas, mas foi alterada pela Diretiva n.º 24/2006/CE[248] que, por sua vez, foi declarada inválida pelo TJCE no já lembrada Decisão Prejudicial (*Digital Rights Ireland e Seitlinger)*[249]*.*

---

[243] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão de 9 de novembro de 2010 (Grande Secção),** Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564948498369&uri=CELEX:62009CJ0092>. Acesso em: 29 jul. 2019.

[244] Id. **Acórdão de 17 de outubro de 2013,** Michael Schwarz (C-291/12, EU:C:2013:670). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564948616770&uri=CELEX:62012CA0291>. Acesso em: 29 jul. 2019.

[245] Id. **Acórdão de 8 de abril de 2014 (Grande Secção),** Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564946739627&uri=CELEX:62012CA0293>. Acesso em: 29 jul. 2019.

[246] Id. **Acórdão de 21 de dezembro de 2016 (Grande Secção),** Tele2 Sverige (processos apensos C-203/15 e C-698/15, EU:C:2016:970. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564950891168&uri=CELEX:62015CJ0203>. Acesso em: 29 jul. 2019.

[247] UNIÃO EUROPEIA. **Diretiva 58/2002/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002**, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). Disponível em: <http://data.europa.eu/eli/dir/2002/58/oj>. Acesso em: 29 jul. 2019.

[248] Id. **Diretiva 24/2006/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006**, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. Disponível em: <http://data.europa.eu/eli/dir/2006/24/oj>. Acesso em: 29 jul. 2019.

[249] Id. **Acórdão de 8 de abril de 2014 (Grande Secção),** Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564946739627&uri=CELEX:62012CA0293>. Acesso em: 29 jul. 2019.

No campo da liberdade, segurança e justiça (ex-arts. 30 e 31 do TUE), a Decisão-Quadro n.º 977/2008/JAI[250] veio para regulamentar a proteção dos dados pessoais no âmbito da cooperação judiciária em matéria penal e policial. Contudo, este panorama jurídico foi atualizado com adoção do Regulamento (UE) n.º 679/2016[251] - que revogou a Diretiva n.º 46/1995/CE - e da Diretiva (UE) n.º 680/2016[252] - que revogou a Decisão-Quadro n.º 977/2008.

Finalmente, na seara do tratamento de dados pessoais pelas instituições e órgãos da União, outrora disciplinada pelo Regulamento n.º 45/2001/CE[253] - responsável pela criação da Autoridade Europeia para Proteção de Dados (2004) -, está vigente o Regulamento (UE) n.º 1.725/2018[254] que modernizou a legislação e a alinhou com o Regulamento (UE) n.º 679/2016.

### 3.1.3 Regulações nacionais

O arcabouço legislativo europeu tocante à proteção de dados pessoais nem sempre foi unificado. Antes da Convenção de Estrasburgo n.º 108/1981 e da Diretiva n.º 46/1995/CE, questões referentes à privacidade, proteção e circulação de dados recebiam respaldo constitucional, regimes jurídicos específicos, interpretações doutrinárias e construções jurisprudenciais pelas próprias nações europeias.

---

[250] CONSELHO DA UNIÃO EUROPEIA. **Decisão-Quadro n.º 977/2008/JAI do Conselho, de 27 de novembro de 2008**, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60), revogada a partir de 6 de maio de 2018. Disponível em: <https://www.consilium.europa.eu/pt/documents-publications/ >. Acesso em: 29 jul. 2019.

[251] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho,** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 29 jul. 2019.

[252] Id. **Diretiva (UE) 680/2016 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível em: <http://data.europa.eu/eli/dir/2016/680/oj>. Acesso em: 29 jul. 2019.

[253] Id. **Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000**, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Disponível em: < http://data.europa.eu/eli/reg/2001/45/oj >. Acesso em: 29 jul. 2019.

[254] Id. **Regulamento (UE) n.º 1.725/2018 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018,** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE (Texto relevante para efeitos do EEE.). Disponível em: <https://eur-lex.europa.eu/eli/reg/2018/1725/oj>. Acesso em: 29 jul. 2019.

Como já explorado em linhas anteriores[255], três momentos histórico-jurídicos distintos caracterizam a regulação de proteção de dados europeias: a primeira fase, marcada por normas rigorosas para criação de cadastros; a segunda fase, preocupada com os direitos fundamentais e normas cadastrais menos austeras; e a terceira fase, buscando um equilíbrio entre proteção e avanço informático[256].

Durante esta linha evolutiva geracional cada país europeu foi desenvolvendo suas próprias experiências baseadas nos supervenientes desafios que a tecnologia, que proteção de dados pessoais e que a defesa do consumidor lhes proporcionava. Essas contribuições, algumas episódicas, outras significativas, serviram para moldar os costumes e os direitos das vindouras legislações.

Neste sentido, serve de exemplo o projeto francês SAFARI (*Système Automatisé pour lês Fichiers Administratifs et lê Répertoire de Individus*), revelado pelo Instituto Nacional de Estatística em 1970, que objetivava a identificação dos franceses conforme uma numeração. Teve uma péssima repercussão, foi criticado por violação de privacidade, descartado e motivou a nova lei protetiva de dados[257].

E também o grande repúdio pela sociedade civil e pela imprensa sueca contra o censo governamental realizado, também em 1970, em decorrência da especificidade dos questionários aplicados e da potencial comercialização de informações sobre origem étnica e qualificação profissional para empresas de *marketing*[258], uma violação dúplice, de direito fundamental e consumerista.

De forma semelhante, mas na esfera judicial, houve a declaração de inconstitucionalidade da lei censitária alemã, em 1983, pelo Tribunal Constitucional Alemão, tendo em vista que ela obrigava os cidadãos a fornecerem inúmeros dados pessoais sem garantia de proteção adequada, oportunidade na qual se reconheceu o direito à autodeterminação informativa, reforçando o poder do consentimento[259].

E, com o reconhecimento da necessidade do consentimento, com o aumento da preocupação com os dados pessoais, com o aprimoramento das tecnologias, as legislações protetivas europeias precisaram se otimizar, mormente pelo crescimento

---

255 Vide-se tópico 2.6 do 1º capítulo desta dissertação para mais informações.
256 LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 79.
257 MENDES, Laura Schertel. **Transparência e Privacidade:** violação e proteção de informação pessoal na sociedade de consumo. Universidade de Brasilia - UNB. Dissertação (Mestrado em Direito). 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em: 29 jul. 2019. p. 30.
258 Ibid., p. 31.
259 Ibid., p. 37.

dos ciberconsumidores e do comércio eletrônico que elevou o nível de vulnerabilidade. Neste sentido, traça Mendes uma relação de causa-consequência:

> São inúmeras as situações em que o consumidor pode ter sua privacidade violada na sociedade atual, principalmente por meio das formações de arquivos pessoais. Diante da grande massa de consumidores anônimos, as empresas buscam diversas fontes de informação sobre eles para segmentar produtos e serviços, aumentar a eficiência do seu processo produtivo, reduzir as operações de riscos e ampliar a eficácia de marketing[260]

Destaca ainda que cada vez mais "[...] é provável que todas as legislações na Europa se tornem mais homogêneas, sempre com um alto nível de proteção individual, principalmente em razão do intenso fluxo transfronteiriço de informações e das exigências econômicas globais"[261], tendência esta que se confirmou depois com a adoção de diversas diretivas pela UE.

E finaliza afirmando que "[...] é provável que diante do fluxo de informações pessoais entre países, as normas nacionais de proteção de dados pessoais sejam enfraquecidas, ampliando a forca de regulamentações regionais"[262], o que também se demonstrou uma assertiva correta dados os mais recentes regulamentos de proteção de dados pessoais pela UE.

Diante da importância destas experiências nacionais ao processo de unificação do direito europeu sobre proteção de dados pessoais e para encontro de paralelos com a produção legislativa dos Estados Partes do MERCOSUL, levantam-se a seguir algumas contribuições relevantes trazidas à temática pelo Reino Unido, Alemanha, França, Itália, Alemanha, Espanha e Portugal[263].

A construção jurídica da proteção de dados britânica, localmente conhecida como *privacy*, despontou no início da década de 1960 como resposta ao preocupante crescimento dos programas radiofônicos e televisivos. Um destes projetos, a Lei de

---

[260] MENDES, Laura Schertel. **Transparência e Privacidade:** violação e proteção de informação pessoal na sociedade de consumo. Universidade de Brasilia - UNB. Dissertação (Mestrado em Direito). 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em: 29 jul. 2019. p. 10.

[261] Ibid., p. 40.

[262] Ibid., p. 40.

[263] A escolha destes países para análise das regulações nacionais é motivada nas suas maiores produções legislativas sobre a proteção de dados pessoais e contribuições diretas para com o processo de unificação do direito europeu na matéria. Ademais, especula-se que a grande influência destes países sobre suas outrora colônias, dados seus históricos como colonizadores europeus, possibilite encontrar paralelos ou padrões normativos, o que também interessa a este estudo e, portanto, encontra justificação.

Walden (1969), buscava regulamentar o armazenamento de dados pessoais em computadores, fomentando a discussão da temática[264].

Inovou depois o *Data Protection Act* (1984), atualmente revogado (2000), ao condicionar a captação de dados aos princípios da lealdade e legalidade e ao restringi-la, bem como a sua utilização, às finalidades originais (*Part I, Preliminary*). Tratou ainda da adequação, exatidão e atualização da conservação dos dados e direitos de acesso, informação e retificação (*Part III - Rights of Data Subjects*)[265].

Com provável inspiração nos princípios da Convenção de Estrasburgo, referida legislação britânica determinou ainda a criação de medidas de segurança para impedir, ou ao menos minorar, a incidência de acessos, alterações, revelações e destruições acidentais de dados pessoais, práticas estas ilegais bastante relacionadas com o *personal data breach* e os cibercrimes.

A conclusão alcançável é que esta legislação apresentava um perfil de maior generalidade, interpretatividade e flexibilidade na aplicação das suas normas, um caráter mais principiológico, compatível com o sistema do *Common Law* seguido no país. Acreditava-se que este dinamismo poderia facilitar a adaptação às novas tecnologias e não obstaculizar a circulação de dados pessoais[266].

Na Seção 16 da Constituição do Reino Unido (*Constitution of the United Kingdom*), recorda Drummond, encontram-se os direitos referentes à privacidade, que declaram que ninguém sofrerá interferência arbitrária em sua privacidade pessoal e familiar, correspondência ou residência, tampouco será atacado em sua reputação e honra, garantias estas estendidas a todos dentro do Reino Unido.

Ressalva hipótese para interceptação de comunicações (correspondências e serviços telefônicos) mediante autorização judicial, criminalizando demais interpretações invasivas (Seção 16, n.º 6); e, com base na *Data Protection Act* (1984), prevê que responsáveis pelo tratamento criem registros de dados, forneçam acesso e gestão deles aos cidadãos e lhes indenizem se devido (Seção 16, n.º 7)[267].

---

[264] MENDES, Laura Schertel. Transparência e Privacidade: violação e proteção de informação pessoal na sociedade de consumo. Universidade de Brasilia - UNB. Dissertação (Mestrado em Direito). 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em: 29 jul. 2019. p. 80-81.

[265] UNITED KINGDOM. Public General Acts. **Data Protection Act 1998 c.35.** Disponível em: <http://www.legislation.gov.uk/ukpga/1984/35/contents>. Acesso em: 4 jul. 2019.

[266] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 80-81.

[267] DRUMMOND, Victor Gameiro. **Internet, privacidade e dados pessoais.** – Rio de Janeiro: Editora Lumen Juris, 2003. p. 156.

No ano seguinte, foi publicado regulamento dispondo sobre as funções do Tribunal de Proteção de Dados (1987)[268], uma das autoridades de controle (*Data Protection Authority*), responsável por receber e analisar os recursos de apelação contra as resoluções tomadas pelo Registrador (outra das autoridades). O órgão também fiscaliza atividades, interpreta normas e representa a comunidade[269].

Não se pode olvidar, outrossim, da britânica Lei de Abusos Informáticos (*Computer Misuse Act*, 1990)[270] que, segundo Lima, tinha como objetivo penalizar a conduta ilícita de alterar dados informáticos – desde o impedimento de utilização do dispositivo e dificultação ao seu acesso até a manipulação de dados eletrônicos – com detenção, prisão e multas a depender da gravidade e danosidade dos atos[271].

Com a vigência da longeva diretiva (Diretiva n.º 46/1995/UE), o Reino Unido precisou aderir aos seus padrões comunitários protetivos. Promulgou-se ainda nova legislação com objetivo de proteger bancos de dados armazenados em computadores (*Data Protection Act, 1998*)[272], seguida pela adoção do RGPD e pela lei complementar (*Data Protection Act, 2018*)[273].

Questão importante de ser mencionada é o anúncio da saída do Reino Unido da União Europeia (Brexit)[274] e interessante de ser investigada é a situação da transferência de dados pessoais entre os Estados Membros da UE com o Reino Unido com esta ruptura. Uma possível resposta à indagação consta em cartilha expedida pela Comissão Europeia recentemente (07/2018):

> Atualmente, os dados pessoais podem circular livremente entre os Estados-Membros da UE. Depois do Brexit, a transferência de dados pessoais da UE para o Reino Unido continuará a ser possível, mas ficará sujeita a condições específicas estabelecidas no direito da União. As empresas que atualmente transferem dados pessoais para o Reino Unido devem estar cientes de que se tratará de uma «transferência» de dados pessoais para um país terceiro. Se o nível

---

[268] UNITED KINGDOM. *Statutory Instruments.* ***Data Protection Act 1987 n. 2028.*** Disponível em: < http://www.legislation.gov.uk/uksi/1987/2028/contents/made>. Acesso em: 5 jul. 2019.
[269] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 80-81.
[270] UNITED KINGDOM. *Public General Acts.* ***Data Protection Act 1990 c.18.*** Disponível em: <http://www.legislation.gov.uk/ukpga/1990/18/contents>. Acesso em: 5 jul. 2019.
[271] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005. p. 92-93.
[272] UNITED KINGDOM. *Public General Acts.* ***Data Protection Act 1998 c.29.*** Disponível em: <http://www.legislation.gov.uk/ukpga/1998/29/contents>. Acesso em: 5 jul. 2019.
[273] Id. *Public General Acts.* ***Data Protection Act 2018 c.12.*** Disponível em: <http://www.legislation.gov.uk/ukpga/2018/12/contents>. Acesso em: 5 jul. 2019.
[274] CONSELHO EUROPEU. **O Brexit**. Disponível em: <https://www.consilium.europa.eu/pt/policies/eu-uk-after-referendum/>. Acesso em: 5 jul. 2019.

> de proteção dos dados pessoais no Reino Unido for essencialmente equivalente ao da UE, e se estiverem reunidas determinadas condições, a Comissão Europeia poderá adotar uma decisão de adequação que autorize a transferência de dados pessoais para o Reino Unido sem restrições. Na ausência de uma decisão de adequação, as empresas devem avaliar se são necessárias medidas para poder garantir a continuação de tais transferências[275].

A solução para o impasse, de acordo com o documento, consiste na mantença da transferência de dados pessoais do Reino Unido com os Estados Membros, desde que cumpridas as exigências jurídicas padrões e obtida a decisão de adequação de nível protetivo para fim de autorização. O Reino Unido passaria, contudo, a ser reconhecido como país terceiro nas transferências de dados pessoais, se efetivamente for confirmada a sua saída do bloco em 31/10/2019.

No tocante à experiência dos franceses, em que pese não sejam os maiores produtores de legislações informáticas ou tenham se preocupado normativamente com diversas questões técnicas inerentes à proteção de dados pessoais, a eles cabe a autoria da publicação da primeira lei relativa à informática, aos arquivos de dados e liberdades individuais dentre todas as nações latinas[276].

A primeva lei francesa de tratamento de dados informatizados foi substituída pela Lei n.º 17/1978 (Lei de Informática e Liberdades)[277], que dispõe sobre informação tecnológica, arquivos de dados e liberdades civis, pois inexiste previsão constitucional da matéria. O fundamento destes direitos reside nas liberdades públicas e no constructo doutrinário-jurisprudencial *vie privée* (vida privada).

Tutelando valores e interesses derivados da proteção à pessoa humana ao invés de trabalhar uma noção de privacidade informática, esta carência foi suprida por doutrinas e sentenças, a exemplo da Decisão n.º 92-316/1993 (proteção da liberdade

---

[275] COMISSÃO EUROPEIA. **Sete coisas que as empresas da UE27 precisam de saber para se preparar para o Brexit.** Disponível em: <https://ec.europa.eu/info/sites/info/files/factsheet-preparing-withdrawal-brexit-preparedness-web_pt.pdf>. Acesso em: 5 jul. 2019.

[276] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005. p. 87.

[277] FRANCIE. ***Loi n° 78-17, du 6 janier 1978, relative à l'informatique, aux fichiers et aux libertés*.** Disponível em: <https://bit.ly/2NpkgtB>. Acesso em: 7 jul. 2019.

individual perante à legislação)[278] e da Decisão n.º 94-352/1995 (proteção contra videovigilância)[279], recebendo *status* de direito fundamental[280].

Regulamentava ainda princípios e definições (arts. 1º ao 5º), informações nominativas e tratamentos automatizados (arts. 6º ao 10º), direito de acesso (art. 35), direito de retificação (art. 36), direito de oposição ao tratamento de dados em cadastros privados (art. 26), bem como demais direitos das pessoas singulares em relação ao tratamento de dados pessoais (arts. 38 ao 43)[281].

São ainda os responsáveis pela criação da Comissão Nacional para a Proteção de Dados (*Commission Nationale de l'Informatique et des Libertés)*[282]*,* contribuição revolucionária no âmbito jurídico informacional. Com viés notadamente garantista, a comissão objetivava priorizar a segurança e proteção das informações pessoais em caso de aquisição e circulação pelas instituições públicas[283].

Com a introdução da Lei n.º 19/1988, sobre fraude informática, dispuseram em matéria criminal em seu *Code Pénal* sobre: (i) o acesso fraudulento a um sistema de elaboração de dados (art. 462-2); (ii) a sabotagem informática (art. 462-3); (iii) a destruição de dados (art. 462-4); a falsificação de documentos informatizados (art. 762-5); e sobre o uso de documentos informatizados falsos (art. 462-6)[284].

Cita-se ainda, como legislação secundária, o Decreto n.º 1.309/2005, regulamentando a aplicação da Lei sobre Processamento de Dados, Arquivos e Liberdades Individuais[285] e isto demonstra que os franceses conseguiram "cercar bem as condutas criminosas praticadas por meio de computadores"[286], como também buscaram dar efetividade às suas normativas.

---

[278] Id. **Decisão n. 92-316 de 20/1/93**, Rec. p. 14, citado por *Combrexelle, Jean-Denis. Les Limites du controle de la Commission natiolanes de l'informatique et des libertés dans le régime de la declaration*. *RFDA*, v. 13, n. 3, *mai/juin*, p. 555.

[279] Id. **Decisão n. 94-352 de 18/1/95**, Rec. p. 179.

[280] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 89.

[281] FRANCIE. ***Loi n° 78-17, du 6 janier 1978, relative à l'informatique, aux fichiers et aux libertés*.** Disponível em: <https://bit.ly/2NpkgtB>. Acesso em: 7 jul. 2019.

[282] Id. **Commission Nationale de l'Informatique et des Libertés - CNIL.** Disponível em: <https://www.cnil.fr/en/home>. Acesso em: 6 jul. 2019.

[283] LIMBERGER, op. cit., p. 89-91.

[284] FRANCIE. ***Code pénal,*** *as last amended by Loi* n°2012-410 du 27 mars 2012. Disponível em: <http://www.legislationline.org/documents/action/popup/id/18094>. Acesso em: 7 jul. 2019.

[285] Id. ***Décret n°2005-1309 du 20 octobre 2005****, pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. Disponível em: <https://bit.ly/2ovIzhd>. Acesso em: 7 jul. 2019.

[286] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005. p. 87.

A legislação italiana de proteção de dados se destaca pela unificação do direito da UE e pela livre circulação de dados, resultado direto da ratificação do país à Convenção de Estrasburgo e da adoção à Diretiva n.º 46/1995/CE, motivos pelos quais é possível sua classificação como uma lei de terceira geração. Sobressai-se, também, contudo, na doutrina de direitos fundamentais e no campo da informática.

A privacidade no direito italiano seguiu três fases. Sua primeira concepção se firmou na máxima de respeito pela vida privada e familiar (art. 8º da CEDH)[287]; desenvolveu-se depois com respaldo no direito de imagem (art. 10 do CC)[288] e evoluiu adiante para um direito de personalidade (art. 2º da Constituição)[289] antes de, finalmente, ser reconhecida como uma tutela protetiva comunitária da pessoa[290].

Drummond ressalta a existência de dispositivo constitucional sobre privacidade nas comunicações, garantindo aos cidadãos italianos liberdade de correspondência (sua inviolabilidade e seu segredo) e limitação deste direito de privacidade mediante decisão judicial nos casos legalmente permitidos (art. 15, n.º "1" e "2")[291]. Porém, nada constitucional acerca da proteção de dados pessoais.

Em nível infraconstitucional há antecedentes legislativos e projetos relacionados à privacidade e banco de dados, tais quais a Lei de Segurança Pública (1926), o Estatuto Laboral (1927) e os projetos Accame (1981), Picano (1982) e Mirabelli (1983)[292] e a Lei n.º 241/1990 para regulamentar o sistema informático pessoal, mormente no tocante ao acesso dos documentos públicos (arts. 22 a 31)[293].

Registra Lima que o ordenamento jurídico italiano sofreu mudanças bruscas na década de 90 no quesito crimes informáticos, a exemplo da publicação do Decreto n.º 518/1992 – que introduziu a tutela do direito do autor e tipificação dos crimes de

---

[287] CONSELHO DA EUROPA. **Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais**, de 4 de novembro de 1950. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 3 jul. 2019.

[288] ITALIA. ***Codice Civile**, R.D. 16 marzo 1942*, n. 262. Disponível em: <https://www.brocardi.it/codice-civile/libro-primo/>. Acesso em: 7 jul. 2019.

[289] Id. ***Costituzione dela Repubblica Italiana (2012).*** Disponível em: <https://www.senato.it/documenti/repository/istituzione/costituzione.pdf >. Acesso em: 7 jul. 2019.

[290] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 92-93.

[291] DRUMMOND, Victor Gameiro. **Internet, privacidade e dados pessoais.** – Rio de Janeiro: Editora Lumen Juris, 2003. p. 159.

[292] LIMBERGER, op. cit., p. 95.

[293] ITALIA. ***Legge 7 agostos 1990, n. 241**, nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.* Disponível em: <http://www.legislationline.org/documents/action/popup/id/7245>. Acesso 7 jul. 2019.

duplicação ilícita e manipulação abusiva de *softwares*) – e das alterações do Código Penal e do Código de Processo Penal italianos (1993)[294].

O autor elenca algumas dessas inovações legais trazidas: sabotagem informática (art. 635 bis do CP); crimes contra a inviolabilidade de domicílio (art. 615 do CPI); crimes contra a inviolabilidade dos segredos (arts. 616, 617 e 621 do CPI); crimes contra o patrimônio (art. 635 do CPI); fraude informática (art. 640 do CPI); e até mesmo a criação de definição própria para *documentos informáticos*[295].

Notabilizaram-se ainda pela criação de autoridade administrativa italiana responsável pela proteção de dados pessoais pela Lei n.º 675/1996[296], regulamentada pelo Decreto n.º 196/2003 (Código de Proteção de Dados Pessoais)[297], e pela publicação da Resolução n.º 217/2001[298], como legislação secundária, contendo disposições sobre procedimento e direito de acesso à documentos administrativos.

E, sistematicamente, no seu Código de Proteção de Dados Pessoais, constaram princípios gerais (Título I), direitos dos titulares de dados (Título II), regras gerais e específicas de processamento de dados em corpos públicos e privados (Título III), autoridades de proteção de dados (Título IV), segurança de dados e sistemas (Título V) e regras de fluxo transfronteiriço de dados (Título VII)[299].

A respeito da experiência normativa alemã, surgida no *Land de Hasse* (1970) e considerada precursora, a primeira legislação de proteção de dados alemã abrangia apenas os bancos de dados públicos, com exigência de inscrição constitutiva para obtenção de autorização cadastral, rigoroso modelo de criação de cadastros este característico da primeira geração de leis protetivas de dados[300].

---

294 LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005. p. 87.
295 LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005. p. 87-90.
296 ITALIA. ***Garante per la protezione dei dati personali.*** Disponível em: <https://www.garanteprivacy.it/web/guest/home/autorita>. Acesso em: 7 jul. 2019.
297 Id. ***Legislative Decree n. º 196 of 30 June 2003, Personal Data Protection Code***. Disponível em: <https://www.legislationline.org/legislation/section/legislation/topic/3/country/22>. Acesso em: 7 jul. 2019.
298 Id. ***Resolution n.º 217/01/CONS.*** *Regulation concerning the access to documents*. Disponível em: <https://www.legislationline.org/legislation/section/legislation/topic/3/country/22>. Acesso em: 7 jul. 2019.
299 Id. ***Legislative Decree n. º 196 of 30 June 2003.*** *Personal Data Protection Code*. Disponível em: <https://www.legislationline.org/legislation/section/legislation/topic/3/country/22>. Acesso em: 7 jul. 2019.
300 LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 86.

Os bancos de dados públicos, e também os cadastros privados, foram regulamentados pela Lei Federal de Proteção de Dados (1977)[301] – lembrando que ao Governo Central competia a coordenação de políticas protetivas de dados e aos Estados a regulamentação localizada – e foram desenvolvidos órgãos de proteção de dados[302], a exemplo do Comissariado Federal de Proteção de Dados[303].

Ao contrário dos franceses, existe base constitucional para proteção da intimidade dos alemães em ambiente informático. A interpretação é, contudo, jurisprudencial e está pautada no direito à personalidade (art. 2.1), no direito à dignidade da pessoa humana (art. 1.1) e na privacidade das comunicações (art. 10), insculpidas na Lei Fundamental da República Federal da Alemanha (1949)[304].

Outra contribuição histórica alemã ao contexto europeu de proteção de dados foi a anulação parcial da Lei do Censo (1982), por força de polêmica sentença (15/12/1983)[305] que a considerou atentatória aos direitos fundamentais, mormente à liberdade de opinião e expressão e inviolabilidade de domicílio. A decisão deflagrou estudos temáticos, resultando na nova Lei de Proteção de Dados (1990).

Referida legislação, apesar de ser de terceira geração, não mudou a essência da anterior (1977); serviu ao propósito de suprir brechas legais, definindo o bem jurídico a ser tutelado, estabelecendo princípios e proteção contra coleta, tratamento e processamento de dados abusivos, mas não desenvolveu um sistema normativo protetivo completo, além de possuir diversos conceitos jurídicos indeterminados[306].

Destaca Lima que, em matéria penal, houve a criação da Lei contra Criminalidade Econômica (1986), nela sendo tipificados diversos delitos, como a espionagem de dados (art. 202-a), extorsão informática (art. 263-a), falsificação de elementos probatórios (art. 269), alteração de dados (art. 303-b) e sabotagem informática (art. 303-b). Não criminalizou, contudo, a simples intrusão informática[307].

---

[301] DEUTSCHLAND. ***Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG*).** Disponível em: <https://germanlawarchive.iuscomp.org/?p=712>. Acesso em: 8 jul. 2019.
[302] LIMBERGER, op. cit., p. 86.
[303] DEUTSCHLAND. ***Federal Commissioner for Data Protection and Freedom of Information.*** Disponível em: <https://www.bfdi.bund.de/EN/Home/home_node.html>. Acesso em: 8 jul. 2019.
[304] Id. ***Deutscher Bundestag, 23 mai. 1949.*** Disponível em: <https://www.btg-bestellservice.de/pdf/10080000.pdf>. Acesso em: 8 jul. 2019.
[305] Id. TRIBUNAL CONSTITUCIONAL ALEMÃO. **Sentença de 15/12/1983**, BJC n.º 33, jan. 1984, p. 137.
[306] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 86-89.
[307] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005. p. 82.

Pode-se citar ainda como legislações primárias relacionadas com a proteção de dados, a título de complemento, a Lei de Informação Ambiental (1994), o Código Criminal (1998), a Lei de Registros e Segurança Interna (1991), Lei Federal de Proteção de Dados (2003) e a Lei de Liberdade de Informação (2006), muito embora algumas tenham sido revogadas e outras tenham sofrido emendas[308].

A legislação espanhola de proteção de dados é classificada como de terceira geração por manifestar traços de direito unificado e por garantir constitucionalmente[309] proteção à intimidade em face ao tratamento de dados pessoais[310]. Ela se preocupou com a limitação no uso da informação para proteção da honra pessoal (art. 18, n.º 4), com a privacidade nas comunicações (art. 18, n.º 3) e coleta de informações (art. 20, n.º 5)[311].

Os espanhóis seguiam as orientações da Convenção de Estrasburgo n.º 108/1981 até a promulgação da Lei n.º 05/1992 (Lei Orgânica de Regulamentação de Tratamento Automatizado de Dados Pessoais - LORTAD), substituída anos depois pela Lei n.º 15/1999 (Lei Orgânica de Proteção de Dados de Caráter Pessoal - LOPD), que ampliou os direitos fundamentais e liberdades públicas constitucionais.

Esta última atualização legislativa teve como motivo combater a potencial ameaça à privacidade trazida pelos bancos de dados, haja vista os receios de desvirtuação dos seus propósitos, de má utilização ou mesmo de comercialização dos dados pessoais e sensíveis. Dentre seus méritos, a exigência de consentimento do titular e outros mecanismos de controle preventivo dos dados[312].

Houve grande evolução no âmbito criminal também. A antiga Lei n.º 6/1987 (antigo Código Penal) tipificava apenas a cópia ilícita de *softwares.* Com a chegada da Lei n.º 107/1995 (novo Código Penal), alcançaram o patamar de legislação mais atualizada do continente, criminalizando “condutas de *hacking*, acessos ilegítimos a sistemas informáticos e distribuição de vírus e bombas lógicas”.[313]

---

[308] As leis mencionadas estão disponíveis para consulta e *download* em idioma inglês e alemão em: < https://www.legislationline.org/legislation/section/legislation/topic/3/country/28>.
[309] ESPANÃ. ***Constitución Española, de 29 de diciembre de 1978***. Disponível em: < https://www.boe.es/eli/es/c/1978/12/27/(1)>. Acesso em: 9 jul. 2019.
[310] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. – Porto Alegre: Livraria do Advogado Editora, 2007. p. 98.
[311] DRUMMOND, Victor Gameiro. **Internet, privacidade e dados pessoais.** – Rio de Janeiro: Editora Lumen Juris, 2003. p. 159.
[312] LIMBERGER, op. cit., p. 99.
[313] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005. p. 84-85.

Ela dispôs sobre equiparação de mensagens eletrônicas aos documentos privados (art. 197); apropriação, utilização ou modificação de dados pessoais em plataformas informáticas (art. 197); ameaças, calúnias e injúrias difundidas por quaisquer meios de comunicação (art. 169 e 211); fraudes informáticas (art. 248); proteção de *softwares* e suportes informáticos (art. 264) etc.[314].

Ademais, são dignas de menção: a Lei n.º 34/2002 (Lei de Serviços da Sociedade da Informação e Comércio Eletrônico); a Lei n. 32/2003 (Lei de Telecomunicações Estatais); a Lei n.º 62/2003 (Lei de Medidas Fiscais, Medidas Administrativas e Medidas de Natureza Social); e Decreto Real n.º 1.720/2007 (Regulamento da Lei Orgânica de Proteção de Dados Pessoais n.º 15/1999)[315].

Registre-se ainda a criação da Agência Espanhola de Proteção de Dados (AEPD)[316] - com o Decreto Real n.º 428/1993 e posterior emenda da Lei Orgânica n.º 15/1999 -, atuante na proteção de dados em sua fase de captação e conservação. E, mais recentemente, entrou em vigor a Lei n.º 19/2013 (Lei de Transparência, Acesso à Informação Pública e Boa Governança)[317], seguindo a tendência moderna.

A legislação portuguesa de proteção de dados também se aproxima da terceira geração. Não distando muito do modelo protetivo espanhol, reconheceram constitucionalmente[318] questões afetas à privacidade. Sob o título de "outros direitos pessoais", garantiram os direitos à identidade pessoal, personalidade, capacidade civil, cidadania, reserva da intimidade da vida privada e familiar (art. 26, n.º 1).

Dispuseram ainda, em texto constitucional, sobre a inviolabilidade do domicílio e das correspondências (art. 34, n.º 1) e da ingerência arbitrária das autoridades públicas na privacidade das comunicações e das telecomunicações (art. 34, n.º 4) como reforço de privacidade como direito fundamental já consolidado como direito humano nos documentos internacionais.

---

314 ESPANÃ. ***Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.*** Disponível em: <>. Acesso em: 9 jul. 2019.

315 As leis mencionadas estão disponíveis para consulta e *download* em idioma inglês e espanhol em: <https://www.legislationline.org/legislation/section/legislation/country/2/topic/3>.

316 ESPANÃ. ***Agencia Española de Portección de Datos – AEPD.*** Disponível em: <https://www.aepd.es/index.html>. Acesso em: 9 jul. 2019.

317 Ib. ***Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.*** Disponível em: <https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887>. Acesso em: 9 jul. 2019.

318 PORTUGAL. **Constituição da República Portuguesa.** Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 9 jul. 2019.

No que diz respeito à utilização da informática, no específico à proteção de dados pessoais, trouxeram na sua constituição o direito de acesso aos próprios dados informatizados, bem como direito de retificação, atualização e conhecimento das finalidades (art. 35, n.º 1), definições técnicas aplicáveis (art. 35, n.º 2), proteção extra aos dados sensíveis (art. 35, n.º 3), dentre outras garantias acessórias[319].

Aprovaram, mais de uma década depois, a Lei n.º 10/1991 (Lei de Proteção de Dados Pessoais Face à Informática)[320] conferindo executividade aos ditames constitucionais supramencionados. Tiveram ainda a Diretiva n.º 46/1995/CE que, por sua vez, foi substituída pela Lei n.º 67/1998 (Lei de Proteção de Dados Pessoais)[321], protetora dos dados pessoais e da livre circulação desses dados[322].

Primando por tecnicismos, publicaram a Lei n.º 2/1994 (Lei de criação de mecanismos de controle e fiscalização do Sistema de Informação Schengen), a Lei n.º 43/2004 (Lei de Organização e Funcionamento da CNPD) - acrônimo da Comissão Nacional de Proteção de Dados portuguesa[323]- e a Lei n.º 103/2015 (Lei de Inserção de dados falsos) sobre a temática.

Na área das comunicações eletrônicas, tem-se a Lei n.º 5/2004 (Lei de criação de base de dados de devedores de serviços de comunicações eletrônicas), Lei n.º 41/2004 (Regulação da proteção de dados pessoais nas comunicações eletrônicas), Lei n.º 32/2008 (transposição da Diretiva n.º 46/1995/CE) e do Regulamento (UE) n.º 611/2013 (notificação de violação de dados pessoais)[324].

Publicaram, na área da saúde, a Lei n.º 12/2005 (Lei de Informação Genética Pessoal de Saúde)[325]; e, no âmbito criminal, a Lei n.º 109/2009 (Lei do Cibercrime)[326] e os tipos penais da Lei n.º 109/1991: falsidade informática (art. 4º); dano a dados ou

---

[319] DRUMMOND, Victor Gameiro. **Internet, privacidade e dados pessoais.** – Rio de Janeiro: Editora Lumen Juris, 2003. p. 155.

[320] PORTUGAL. ***Lei n.º 10/91 - Lei da Protecção de Dados Pessoais face à Informática.*** Disponível em: <https://www.cnpd.pt/bin/legis/nacional/lei_1091.htm>. Acesso em: 9 jul. 2019.

[321] Id. ***Lei n.º 67/98 - Lei da Protecção de Dados Pessoais.*** Disponível em: <https://www.cnpd.pt/bin/legis/nacional/LPD.pdf>. Acesso em: 9 jul. 2019.

[322] MASSENO, Manuel David Rodrigues. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa: uma cartografia das Fontes Legislativas. **Revista Direito & TI – Debates Contemporâneos**: Porto Alegre, 2018, p. 2.

[323] PORTUGAL. ***Comissão Nacional de Protecção de Dados – CNPD***. Disponível em: <https://www.cnpd.pt/index.asp>. Acesso em: 9 jul. 2019.

[324] As leis mencionadas neste parágrafo e no anterior estão disponíveis para consulta e *download* em idioma português em <https://www.cnpd.pt/bin/legis/leis_nacional.htm#Historico>.

[325] Id. ***Lei n.º 12/2005 – Lei de Informação Genética Pessoal e Informação de Saúde.*** Disponível em: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1660&tabela=leis>. Acesso em: 9 jul. 2019.

[326] Id. ***Lei n.º 109/2009 – Lei do Cibercrime.*** Disponível em: <https://www.cnpd.pt/bin/legis/nacional/LEI109_2009_CIBERCRIME.pdf>. Acesso em: 9 jul. 2019.

*softwares* informáticos (art. 5º); sabotagem informática (art. 6º); acesso ilegítimo (art. 7º); interceptação ilegítima (art. 8º); e reprodução ilegítima de *software* (art. 9º)[327].

### 3.2 Regulamento Geral de Proteção de Dados Europeu

A UE reformou, em 06/04/2016, sua legislação que tratava sobre a proteção de dados e, neste intento, adotou novos instrumentos jurídicos sobre o tema: o Regulamento (UE) n.º 679/2016 (Regulamento Geral de Proteção de Dados - RGPD) e a Diretiva (UE) n.º 680/2016 (Diretiva de Cooperação Policial), os quais, juntamente com o Regulamento (UE) n.º 1.725/2018 (Regulamento de Proteção de Dados Pessoais pelas Instituições, Órgãos e Organismos da União), compõem o atualizado pacote normativo protetivo europeu[328].

O RGPD, como já antecipado em linhas anteriores, estabelece novos regramentos no que diz respeito à proteção de dados pessoais das pessoas singulares e à livre circulação de dados e revoga a Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho[329], que tinha por finalidade a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

O Regulamento foi assinado em 27/04/2016, com entrada em vigor 20 dias após sua publicação no Jornal Oficial da União Europeia (art. 99, n.º 1). No entanto, tendo-se em vista o grande impacto e a complexidade da legislação, estabeleceu-se um período de transição de 02 (dois) anos para que os Estados Membros e demais interessados se adaptassem às novas disposições, quando então seus efeitos seriam aplicáveis. A data restou marcada para 25/05/2018 (art. 99, n.º 2)[330].

---

[327] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005. p. 93-94.

[328] Em que pese sejam complementares os três instrumentos normativos, apenas o primeiro, o Regulamento (UE) n.º 679/2016 (RGPD), será objeto direto de estudo na dissertação, que não pretende adentrar em pormenores do tratamento de dados pessoais pelas instituições, órgãos e organizações públicos, tampouco em questões afetas à cooperação policial inerente, por se distanciarem mais do espectro privado e consumerista delimitado como escopo e temática.

[329] UNIÃO EUROPEIA. **Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,** relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 10 jul. 2019.

[330] Id. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho,** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 10 jul. 2019.

É pertinente ressaltar que a elaboração do Regulamento foi baseada em 20 anos de atividade doutrinária, legislativa e jurisprudencial europeia, experiência esta revelada tanto através dos documentos internacionais quanto das regulações nacionais. Neste contexto, ele incorpora o espírito e aperfeiçoa a abordagem da Diretiva n.º 95/46/CE, clarificando-a, modernizando-a e reforçando a proteção dos direitos fundamentais e liberdades individuais de outrora[331].

Este conjunto uniforme de atualizadas regras, primando por sua completude e amplitude, pretende beneficiar significativamente indivíduos, empresas, administração pública e outras organizações europeias, contribuindo assim para que a UE se torne líder global no quesito segurança de dados e proteção da privacidade. Inclusive, nações e blocos regionais externos à UE estão interessados em otimizar suas próprias legislações e enxergam nele um modelo a ser espelhado[332].

O RGPD está estruturado em 173 considerandos e 11 capítulos, totalizando 99 artigos sobre a matéria. Suas inúmeras disposições introdutórias registram as finalidades e justificativas, os princípios e características, os direitos e deveres, as definições e operações, os trâmites e sanções constantes na quase centena de artigos que os seguem. Funcionam praticamente como exposição de motivos e cartilha descritivo-explicativa que fundamenta e norteia seu corpo normativo.

No Capítulo I traz disposições gerais (arts. 1º ao 4º); no Capítulo II trata dos princípios (arts. 5º ao 11º); no Capítulo III aborda os direitos e limitações dos titulares dos dados (art. 12º ao 23º); no Capítulo IV versa sobre os responsáveis e subcontratantes do tratamento de dados pessoais (arts. 24º ao 43º); no Capítulo V trabalha a transferência transfronteiriça de dados pessoais (arts. 44º ao 50º); no Capítulo VI envolve as autoridades de controle independentes (arts. 51º ao 59º).

No Capítulo VII trata da cooperação e coerência (arts. 60º ao 76º); no Capítulo VIII prescreve sobre vias de recurso, responsabilidade e sanções (arts. 77º ao 84º); no Capítulo IX apresenta disposições relativas a situações específicas de tratamento (arts. 85º ao 91º); no Capítulo X aborda os atos delegados e os atos de execução (art.

---

331 COMISSÃO EUROPEIA. **COM/2018/043 final – Comunicação da Comissão ao Parlamento Europeu e ao Conselho, de 24 de janeiro de 2018.** Maior proteção, novas oportunidades — Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0043>. Acesso em: 11 jul. 2019. p. 2-3.

332 COM/2018/043 final, op. cit., p. 2-7.

arts. 92º ao 93º); e finalmente, no Capítulo XI, traz suas disposições finais (art. 94º ao 99º), inclusa a previsão do prazo para exigência de seus efeitos[333].

Agora que explorados os fundamentos e princípios da proteção dos dados pessoais, as tecnologias informáticas e comunicacionais dos bancos de dados, e uma vez contextualizadas as influências europeias nacionais e internacionais sobre a temática, bem como introduzidos o panorama e estrutura do RGPD, passemos à análise de algumas das suas tecnicidades jurídicas, como objetivos, âmbitos de aplicação e direitos dos titulares de dados.

### 3.2.1 Objetivos do RGPD

O Regulamento, conforme o seu segundo considerando, objetiva "[...] contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares"[334]. Depreende-se dessa ponderação diversos objetivos.

Na Comunicação n.º 43/2018 da Comissão ao Parlamento Europeu e do Conselho há síntese destas finalidades. No documento consta que ele objetiva: (i) formar um quadro jurídico harmonizado que vise uma aplicação uniforme das regras em prol do mercado único digital da UE; (ii) a fornecer condições de concorrência equânimes para todas as empresas que estejam operantes no mercado da UE.

Prossegue resumindo servir a norma para (iii) incentivar a criação de soluções inovadoras às questões de proteção de dados desde a concepção[335] e por defeito[336];

---

[333] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho,** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 10 jul. 2019.

[334] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho,** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 11 jul. 2019.

[335] **Privacidade desde a concepção (*Privacy by design*):** "Abordagem pró-ativa que assenta na necessidade de garantir a privacidade durante todo o processo de desenvolvimento de um novo produto/processo. Quando da concepção de um novo produto ou serviço, deve-se considerar o risco que tal representa para a privacidade, em vez de considerar questões de privacidade apenas posteriormente". (MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. **Regulamento Geral de Proteção de Dados:** manual prático. Vida Económica: Porto, 2017. Glossário. p. 3).

[336] **Privacidade por defeito (*Privacy by default*):** "Obrigação de assegurar que são colocados em prática os mecanismos necessários para garantir que, por defeito, apenas será recolhida, utilizada e conserva para cada tratamento a quantidade necessária de dados pessoais. Esta obrigação aplica-se à extensão do seu tratamento, ao prazo da conservação e à sua acessibilidade". (Ibid., p. 3).

(iv) reforçar os direitos individuais; (v) prover maior controle em relação aos dados pessoais dos indivíduos; (vi) propiciar maior proteção contra violações de dados; (vii) habilitar as autoridades a aplicar multas aos responsáveis pelos seus tratamentos.

Assinalam pretender ainda (viii) trazer maior flexibilidade e clareza aos responsáveis e subcontratados para tratamento de dados ao esclarecer suas obrigações; (ix) construir um sistema de governança moderno cujas normas são cumpridas com firmeza e coerência; e (x) garantir elevado nível de proteção de dados pessoais fora do território da UE[337].

Comenta Guidi que as alterações mais relevantes trazidas pelo RGPD condizem com suas finalidades principais. São elas o fortalecimento dos direitos dos titulares, o alargamento das competências das Autoridades de Proteção de Dados, bem como a introdução e o incentivo de certos comportamentos pelos responsáveis (e subcontratantes) pelos tratamentos de dados pessoais[338].

### 3.2.2 Âmbito de aplicação do RGPD

No que diz respeito ao âmbito material de aplicação do RGPD, existe artigo expresso validando o tratamento de dados pessoais por meios total ou parcialmente automatizados, assim como por meios não automatizados de dados pessoais contidos em ficheiros (bancos de dados) ou a eles destinados (art. 2, n.º 1)[339]. Há discriminação ainda das hipóteses de inaplicabilidade do Regulamento.

Assim, não é aplicável ao tratamento de dados (i) de atividades não sujeitas ao direito da UE; (ii) de atividades de competência exclusiva do TUE (Título V, capítulo II)[340]; (iii) de atividades domésticas praticadas por pessoas físicas; e (iv) de atividades

---

[337] COMISSÃO EUROPEIA. **COM/2018/043 final – Comunicação da Comissão ao Parlamento Europeu e ao Conselho, de 24 de janeiro de 2018.** Maior proteção, novas oportunidades — Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0043>. Acesso em: 11 jul. 2019, p. 3-6.

[338] GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 11 jul. 2019. p. 7-8.

[339] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: < http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 6 jul. 2019.

[340] Id. **Tratado da União Europeia (Tratado de Maastricht), 29 de julho de 1992.** Disponível em: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF>. Acesso em: 6 jul. 2019.

efetuadas por autoridades competentes para prevenção, investigação, detecção, repressão e execução de infrações e sanções (art. 2, n.º 1, “a” a “d”)[341].

Ademais, o Regulamento n.º 45/2001/CE, aplicável ao tratamento de dados pessoais por instituições, órgãos, organismos ou agências da UE e demais atos jurídicos do bloco afetos à matéria de tratamento de dados pessoais, também estão obrigados a adaptar-se aos regramentos e princípios do RGPD (art. 98)[342]. Percebe-se aqui a influência do RGPD sobre importantes documentos anteriores.

Entretanto, mesmo para documentos pretéritos, a área de aplicação do RGPD não é absoluta. A aplicação da Diretiva n.º 31/2000/CE, por exemplo, no que diz respeito às disposições sobre responsabilidade dos prestadores intermediários de serviços (art. 12 a art. 15)[343], independe dos ditames do RGPD (art. 2º, n.º 4)[344]. É preciso analisar cada caso concreto para conferir a legislação aplicável.

Observa-se do teor dos dispositivos relativos à territorialidade e extraterritorialidade do âmbito de aplicação do RGPD que estas normas se destinam à proteção de dados pessoais realizada no contexto das atividades de um responsável pelo tratamento dos dados ou de um subcontratante situado no território da UE, independe de o tratamento ocorrer dentro ou fora da UE (art. 3º, n.º 1)[345].

Trata-se de questão de grande relevância do Regulamento, uma vez que define sua abrangência nacional, regional e internacional; ele é, portanto, aplicável a todo tratamento de dados pessoais dos residentes europeus das nações signatárias (28 Estados Membros, desde 8 de julho de 2013), contudo, válido aos responsáveis pelo tratamento, ou subcontratantes, “estrangeiros” em certos casos (art. 3º, n.º 2)[346].

Estas condições estariam restritas aos casos nos quais as atividades de tratamento estão relacionadas (i) com oferta de bens e serviços aos titulares de dados na UE, não importando a exigência de qualquer pagamento; ou com (ii) o controle do

---

341 Regulamento n.º 679/216, op. cit., não paginado.
342 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: < http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 6 jul. 2019.
343 Id. **Posição Comum (CE) n.º 31/2000, de 25 de Maio de 2000, adoptada pelo Conselho** deliberando nos termos do procedimento previsto no artigo 251.o do Tratado que institui a Comunidade Europeia, tendo em vista a adopção de um regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CEE) n.º 2.913/92 do Conselho, que estabelece o Código Aduaneiro Comunitário. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1562447137990&uri=CELEX:52000AG0031>. Acesso em: 6 jul. 2019.
344 Regulamento n.º 679/216, op. cit. não paginado.
345 Regulamento n.º 679/216, op. cit. não paginado.
346 Regulamento n.º 679/216, op. cit. não paginado.

seu comportamento, desde que este comportamento tenha lugar na UE (art. 3º, n.º 2, alíneas “a” e “b”)[347].

Vale lembrar que - embora o Regulamento seja aplicável quanto ao tratamento de dados pessoais aos responsáveis pelo tratamento fora do território da UE - é preciso que a localidade onde será aplicado reconheça o direito de um Estado Membro da UE em decorrência do Direito Internacional Público ou Privado. A aplicação restará prejudicada se não houver este reconhecimento (art. 3, n.º 3)[348].

Tendo em vista que o RGPD não se restringe à normatização da circulação de dados pessoais intrabloco, mas também legisla sobre sua transmissão transfronteiriça extrabloco, qualquer intercâmbio de dados pessoais da UE com o MERCOSUL, ou mesmo com seus Estados Partes individualmente, requer a observância de condições jurídicas e de critérios técnicos de adequação.

Outra conclusão atingível, ainda sobre a aplicabilidade territorial do RGPD, é que ele consegue ser mais amplo que a Diretiva (CE) 46/1995 e a razão para isto é que aquela engloba a questão dos subcontratantes e apresenta condições de tratamento extraterritoriais. Esta compreensão também é alcançável através da leitura de Moniz sobre coerência de aplicabilidade e enigma linguístico do RGPD[349].

Reforça-se ainda que questões tocantes à aplicabilidade territorial podem facilmente perder sua confiabilidade quando buscadas em outras áreas transfronteiriças. Neste sentido comenta Araújo que: “[...] As leis domésticas de proteção de dados perdem grande parte da sua eficácia com uma simples transferência desses dados para um país que não os proteja adequadamente”[350].

---

[347] Regulamento n.º 679/216, op. cit. não paginado.

[348] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: < http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 6 jul. 2019.

[349] MONIZ, Graça Canto. **Finalmente:** coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD. UNIO - EU Law Journal, Braga, Vol. 4, No. 2, julho 2018, pp 119-131. Disponível em: <https://bit.ly/2Nswu4E>. Acesso em: 6 jul. 2017.

[350] ARAÚJO, Alexandra Maria Rodrigues. **As transferências transatlânticas de dados pessoais:** o nível de proteção adequado depois de Schrems. Revista de Direitos Humanos e Democracia. Editora Unijuí, ano 5. n. 9. jan./jun, 2017. p. 203.

### 3.3 Direitos do titular de dados

Não há grande mistério quanto aos sujeitos de dados pessoais. O Regulamento considera como titular de dados a pessoa singular identificada ou identificável com a qual os dados estão relacionados. Se já está identificada, dispensa-se qualquer processo de especificação e, provada sua relação com os dados, sua titularidade restará garantida.

Se for pessoa singular desconhecida, porém identificável, direta ou indiretamente, através de simples processo de especificação - este feito pela análise de um critério identificado - a titularidade também lhe será atribuída. O Regulamento se remete aos identificadores nominais, numéricos, geoespaciais, eletrônicos ou mesmo físicos, genéticos, mentais, econômicos, culturais e sociais (art. 4, n.º 1).

Embora variadas as opções para identificação de um titular, não se confundem as noções de titularidade e responsabilidade. A primeira diz respeito aos direitos que os proprietários (pessoas naturais) têm sobre seus dados. A segunda diz respeito aos sujeitos tomadores de decisões sobre o tratamento de dados de outrem (pessoas naturais ou jurídicas, de direito público ou privado) (art. 4, n.º 7).

Na dinâmica do fluxo de dados, diferem-se também as noções de destinatário e de terceiro. Enquanto aquela é usada para falar de quem recebe comunicações de dados pessoais, esta é utilizada para denominar quem está autorizado a tratar deles. Em ambos os casos, podem ser pessoas singulares ou coletivas e até autoridades públicas, agências ou órgãos (art. 4º, n.º 9 e n.º 10)[351].

A importância da titularidade dos dados pessoais reside nos direitos à disposição de seus titulares que, conforme sua autonomia e preferência, podem consentir, rejeitar ou manejar seus dados personalíssimos, acessando-os, retificando-os, apagando-os, limitando-os, opondo-se e portando-os, salvo exceções, protegendo assim sua privacidade e a credibilidade das suas informações pessoais.

---

[351] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: < http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 6 jul. 2019.

### 3.3.1 Direito à transparência e direito de acesso

Os titulares dos dados têm o direito de saber como serão tratados os seus dados pessoais e, consequentemente, os responsáveis pelos respectivos tratamentos têm a obrigação de informá-los. Portanto, segundo os princípios e dispositivos do RGPD, alguns elementos de transparência devem ser observados e informações específicas lhes devem ser prestadas.

Antes de apontá-los, imperioso esclarecer o que é "transparência", princípio cuja definição não está expressa no Regulamento. Trata-se, a grosso modo, "[...] de uma expressão do princípio da lealdade em relação ao tratamento de dados [...]", trata-se "[...] de criar confiança nos processos que afetam os cidadãos fazendo com que estes compreendam e, se necessário, se oponham a esses processos [...]"[352].

Segundo Mendes, o princípio da transparência ou da publicidade também é um dos princípios de proteção de dados pessoais e está relacionado com a cientificação pública da existência de uma base de dados e que muitas vezes sua efetivação requer uma autorização judicial para que seja criada ou esteja vinculada à uma obrigação legal de monitoração periódica:

> O primeiro princípio que todas as atividades de processamento de dados devem seguir é o princípio da publicidade. Também chamado de princípio da transparência, ele exige que a existência de um banco de dados pessoais seja de conhecimento público. Este princípio pode ser atendido por meio da exigência de autorização estatal prévia para a criação de um banco de dados pessoais ou pela necessidade de divulgação periódica de relatórios sobre o seu funcionamento[353].

Limberger aponta a relação do princípio da transparência com os princípios da Administração Pública, demonstrando estar ele integrado aos princípios da publicidade, ao direito de informação e ao princípio democrático[354]. A lógica é que os

---

[352] GT29. **Orientações relativas à transparência na acepção do Regulamento 2016/679, adotadas em 29 de novembro de 2017; revistas e adotadas pela última vez em 11 de abril de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp260rev01_pt.pdf>. Acesso em: 11 jul. 2019. p. 6.

[353] MENDES, Laura Schertel. **Transparência e Privacidade:** violação e proteção de informação pessoal na sociedade de consumo. Universidade de Brasilia - UNB. Dissertação (Mestrado em Direito). 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em: 29 jul. 2019. p. 56.

[354] LIMBERGER, Têmis. Transparência Administrativa e Novas Tecnologias: o Dever de Publicidade, o Direito a ser informado e o Princípio Democrático. In: **Revista do Direito Administrativo.** v. 244. FGV: 2007, p. 248-263. Disponível em: <bibliotecariodigital.fgv.br>. Acesso em: 29 ago. 2019. p. 262.

administrados têm o direito de saber sobre os tratamentos dos seus dados e os administradores o dever de os informar para que deles possam dispor se preciso.

Portanto, como alicerce da publicidade, lealdade e legalidade, a transparência garante aos titulares de dados o exercício dos seus direitos. E, para que haja lisura nesta prestação de informações, deve sê-la feita: (i) de maneira concisa, inteligível e acessível; (ii) com linguajar claro, simples e adequado (em especial no caso de crianças, para que a mensagem seja alcançada).

E, ainda mais, elas devem ser (iii) fornecidas por meio escrito ou outros meios, como o eletrônico; ou (iv) oralmente, se assim preferir o titular dos dados pessoais; e (v) a título gratuito, ou seja, os responsáveis pelo tratamento não podem, via de regra, exigir de quem tenha titularidade pagamento pelas informações[355]. A principiologia aqui aplicável descende dos diplomas internacionais humanitários.

Há uma série de informações a serem prestadas à garantia da transparência: (i) identidade e contato dos responsáveis pelo tratamento; (ii) contato do encarregado da proteção de dados; (iii) finalidades e fundamentos do tratamento; (iv) categorias de dados envoltas; (v) destinatários em questão; (vi) se houve fluxo transfronteiriço e (vii)0 o nível de adequação protetivo (art. 14, n.º 1, “a” a “f”)[356].

Para transparência máxima, podem ser solicitados ainda (i) o prazo de conservação dos dados pessoais ou os critérios para sua fixação; (ii) os interesses legítimos dos responsáveis ou terceiros; (iii) a origem dos dados e se acessíveis de fontes públicas; (iv) a existência de decisões automatizadas; e, com posse de tais dados, exercidos seus demais direitos (art. 14, n.º 2, “a” a “g”)[357].

Já o direito de acesso é aquele que possibilita ao seu titular obter os dados pessoais, automatizados ou não, que lhe dizem respeito[358], e “compreende o conhecimento sobre os dados armazenados, incluindo informações acerca da sua

---

[355] GT29. **Orientações relativas à transparência na acepção do Regulamento 2016/679, adotadas em 29 de novembro de 2017; revistas e adotadas pela última vez em 11 de abril de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp260rev01_pt.pdf>. Acesso em: 11 jul. 2019. p. 7.
[356] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 11 jul. 2019.
[357] Id., Regulamento n.º 679/2016.
[358] DRUMMOND, Victor Gameiro. **Internet, privacidade e dados pessoais.** – Rio de Janeiro: Editora Lumen Juris, 2003. p. 54.

origem; sobre os organismos receptores das informações transmitidas ou a sua categoria; e sobre o objetivo do armazenamento"[359].

A frequência desse acesso varia conforme as diversas legislações, bem como a sua gratuidade ou onerosidade. Associado com a transparência, esse direito serve então para conhecimento dos seus dados pessoais e verificação da licitude do tratamento deles. Poderá, contudo, ser limitado por medidas legislativas, parcial ou totalmente, adotadas pelos Estados Membros em certas hipóteses.

O RGPD lista situações que autorizam a restrição do direito de acesso, a exemplo dos casos para (i) não prejudicar inquéritos, investigações e procedimentos oficiais e judiciais; (ii) não prejudicar prevenção, detecção, investigação, repressão ou execução de penas; (iii) proteger a segurança jurídica e/ou segurança nacional; e (iv) proteger direitos e liberdades de terceiros (art. 15, n.º 1, "a" a "e")[360].

Em matéria jurisprudencial, sobre o direito de acesso dos cidadãos aos documentos das instituições da UE e a proteção dos dados pessoais, tem-se o Recurso de Decisão do TJUE na qual restou confirmado, através de consulta, o uso indevido de dados pessoais e foi garantido ao titular seu direito de oposição[361].

### 3.3.2 Direito de retificação e direito de apagamento

É prerrogativa do titular que seus dados pessoais não sejam maculados com inexatidões ou incompletudes. Estas circunstâncias estão relacionadas com o direito de retificação, cujo exercício pelo respectivo detentor obriga que os responsáveis pelo tratamento dos dados, sem demora infundada, procedam à correção das imprecisões ou ao preenchimento das omissões/lacunas (art. 16)[362].

Uma retificação pode inclusive acontecer mediante declaração adicional e servir para ocasionais desatualizações dos dados, sejam causadas pelos usuários ou

---

[359] MENDES, Laura Schertel. **Transparência e Privacidade:** violação e proteção de informação pessoal na sociedade de consumo. Universidade de Brasilia - UNB. Dissertação (Mestrado em Direito). 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em: 29 jul. 2019. p. 54.

[360] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 11 jul. 2019.

[361] Id. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão de 29 de junho de 2010 (Grande Secção), Comissão/Bavarian Lager (C-28/08 P, EU:C:2010:378).** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62008CJ0028>. Acesso em: 29 jul. 2019.

[362] Regulamento n.º 679/2016, op. cit., não paginado.

pelos provedores; todavia, se a responsabilidade pelo tratamento for de uma entidade da Administração Pública, o administrado/titular terá não apenas o direito de retificação, como também o dever de os manter atualizados[363].

O direito à retificação, por conseguinte, permite ao titular dos dados pessoais, especialmente aos ciberconsumidores, exigir a exatidão de seus dados. Destaca-se, inclusive, que a retificação não precisa, necessariamente, da iniciativa do titular dos dados pessoais, uma vez que o próprio responsável pelo tratamento dos dados tem essa obrigação[364].

O direito ao apagamento de seus dados pessoais, muitas vezes chamado de "direito a ser esquecido" ou "direito ao esquecimento", é outra faculdade à disposição de quem possua titularidade sobre eles. O Regulamento autoriza a exclusão dos respectivos dados pessoais, sem injustificada demora, nas hipóteses legais ou para cumprimento de dever do responsável pelo tratamento dos dados.

Cumpre registrar que embora seja entendido que o direito ao apagamento e o direito ao esquecimento sejam termos semelhantes, Marques e Silveira explicam que possuem âmbitos de proteção distintos. Segundo os autores, o direito ao apagamento estava previsto na Diretiva n.º 46/1995 (arts. 12º e 14º) e o direito ao esquecimento está previsto no RGPD:

> De qualquer forma, são dois direitos com âmbitos de proteção distintos. Por meio do direito ao esquecimento o afetado reclama proteção contra a difusão de dados pessoais que são processados/propagados e se tornam acessíveis por intermédio de motores de busca – ou seja, um direito originariamente concebido para ser exercido *online*. Nessa medida, o direito ao esquecimento se distingue do direito ao apagamento originariamente previsto na Diretiva 95/46 para ser exercido *offline*, pois o último implica que os dados pessoais sejam conservados apenas por um certo período de tempo, exigindo-se o seu apagamento a partir de um prazo adequado às finalidades do tratamento[365].

---

[363] MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. **Regulamento Geral de Proteção de Dados:** manual prático. Vida Económica: Porto, 2017. p. 12.

[364] DRUMMOND, Victor Gameiro. **Internet, privacidade e dados pessoais.** – Rio de Janeiro: Editora Lumen Juris, 2003. p. 56.

[365] MARQUES, João; SILVEIRA, Alessandra. Do direito a estar só ao Direito ao esquecimento. Considerações sobre a proteção de dados pessoais informatizadas no Direito da União Europeia: sentido, evolução e reforma legislativa. In: **Revista da Faculdade de Direito UFPR.** v. 61, n. 3, 2016. p. 91-118. Disponível em: <https://revistas.ufpr.br/direito/article/view/48085/29828>. Acesso em: 30 jul. 2019. p. 111.

Os casos permissivos guardam relação com os princípios de tratamento de dados pessoais (licitude, lealdade, finalidade, adequação, exatidão, atualização, mínima conservação etc.); a retirada do consentimento, o tratamento ilícito, a atuação de autoridade, o cumprimento de decisão judicial e a coleta de dados pessoais para oferta de serviços são casos autorizadores (art. 17, n.º 1, "a" a "f")[366].

Tendo em vista a tecnologia disponível, os custos da operação e questões técnicas inerentes, o responsável pelo tratamento dos dados a serem deletados pode apenas limitá-los em determinadas situações, "nomeadamente as que se prendem com os prazos de conservação dos dados por razões de interesse público, segurança nacional, de faturação, comerciais, fiscais ou outros"[367].

### 3.3.3 Direito à limitação de tratamento e obrigação de notificação

Seguindo um modelo normativo centrado nos cidadãos e pautado em maior transparência dos dados e maior autonomia dos titulares, o RGPD garante a estes o direito à limitação do tratamento de seus dados pessoais em quatro situações. Ato contínuo, se contemplada uma das hipóteses aplicáveis e realizada a limitação, o titular deverá ser cientificado pelos responsáveis.

Ademais, a legislação prevê os casos de (i) contestação da exatidão dos dados pessoais, durante período razoável para apuração; (ii) preferência do titular pela limitação do tratamento (ilícito) ao invés de apagamento; (iii) requisição do titular para fins de declaração, exercício ou defesa em processo judicial, quando já desnecessários; e (iv) oposição do titular ao tratamento (art. 18, n.º 1)[368].

Nas considerações iniciais são elencados alguns métodos de restrição de tratamento. Um deles é a transferência temporária de certos dados para outro sistema de tratamento; outro método é a não disponibilização do acesso de dados específicos

---

366 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 11 jul. 2019.

367 MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. **Regulamento Geral de Proteção de Dados:** manual prático. Vida Económica: Porto, 2017. p. 13.

368 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 12 jul. 2019.

por alguns utilizadores; um terceiro é a retirada temporária de um endereço eletrônico dos dados publicados (considerando n.º 67)[369].

Por outro lado, uma vez limitado o tratamento, os dados pessoais só poderão ser objeto de novo tratamento pelo responsável se houver consentimento do respectivo titular ou se necessário para fins declarativos, potestativos ou defensivos judiciais, ou ainda se houver interesse público da União ou Estado-Membro. Excepciona-se a esta regra a conservação dos dados pessoais (art. 18, n.º 2 e 3)[370].

Determinou-se também que compete ao responsável pelo tratamento de dados pessoais a obrigação de notificação ao respectivo titular de dados sempre que houver quaisquer retificações ou apagamentos de dados pessoais ou limitações de tratamento, desde que referida comunicação não seja impossível ou requeira demasiado esforço (art. 19)[371].

### 3.3.4 Direito à portabilidade dos dados

O direito à portabilidade, no tocante ao tratamento de dados pessoais, pode ser definido como a transferência de determinada informação personalíssima de uma fonte para outra fonte. Com este direito, os titulares estão autorizados a receber os dados pessoais outrora fornecidos aos responsáveis pelo tratamento e de os retransmitir a outrem, adquirindo, desta forma, maior controle sobre eles.

Este recebimento deve acontecer sob formato estruturado, de utilização costumeira e de leitura automática e esta transmissão não poderá ser obstada pelo responsável. Duas são as condições ao seu exercício: (i) que o tratamento seja baseado no consentimento ou execução de contrato; e (ii) que o tratamento seja efetuado por meios automatizados (Considerando n.º 68 e art. 20, n.º 1, “a” e “b”)[372].

O RGPD apresenta ressalvas quanto ao exercício deste direito. A transmissibilidade direta entre os responsáveis pelo tratamento fica à mercê da viabilidade técnica. Será inaplicável o direito se o tratamento envolver funções de

---

369 Ibid., não paginado.
370 Ibid., não paginado.
371 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 12 jul. 2019.
372 Ibid., não paginado.

interesse público ou atuação de autoridade pública e se prejudicar direitos e/ou liberdades de terceiros (art. 20, n.º 2, 3 e 4)[373].

Semelhante, à primeira vista, com o direito de acesso, com ele não deve ser confundido. O direito à portabilidade de dados pessoais "possibilita a transmissão direta de dados pessoais entre dois responsáveis pelo tratamento", apoiando a livre circulação de dados pessoais na UE, estimulando concorrência entre os responsáveis pelo tratamento e fomentando o mercado de serviços digitais[374].

Impende esclarecer que, de acordo com Janal, o direito à portabilidade possui uma dupla conceituação. No contexto do RGPD (art. 20) e da Proposta de Diretiva sobre Contratos de Fornecimento de Conteúdo Digital (COM n.º 0634/2015, art. 13, n.º 2, "c"; art. 16, n.º 4, "b")[375], "o termo portabilidade descreve o direito de recuperar dados relativos à uma pessoa singular"[376].

Em contrapartida, no contexto da Proposta de Regulamentação em matéria de Portabilidade Transfronteiriça de Serviços *Online* (COM n.º 627/2015)[377], a portabilidade "busca assegurar que o conteúdo digital adquirido por um consumidor no Estado Membro possa ser acedido sem qualquer taxa por qualquer outro Estado-Membro"[378], primando assim por uma isenção tributária dentro do megabloco.

O que se percebe aqui é uma efetivação multidimensional dos direitos dos consumidores em relação à portabilidade transfronteiriça dos seus dados pessoais. Enquanto o RGPD e o *DCD-Proposal* fortalecem este direito do titular de dados pessoais, a COM n.º 627/2015 segue um viés mais econômico e logístico, que se revertem em benefícios ao ciberconsumidor.

Seguindo este raciocínio, Cravo destaca que "deve-se reconhecer que os dados figuram atualmente como um insumo indispensável para a maior parte dos

---

[373] Ibid., não paginado.
[374] GT29. **Orientações sobre o direito à portabilidade dos dados, adotadas em 13 de dezembro de 2016; com a última redação revista e adotada em 5 de abril de 2017.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf>. Acesso em: 12 jul. 2019. p. 3.
[375] COMISSÃO EUROPEIA. **COM n.º 0634/Final/2015/0287, de 9 de dezembro de 2015.** Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015PC0634>. Acesso em: 30 jul. 2019.
[376] JANAL, Ruth. **Data Portability:** a tale of two concepts. In: Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC). v. 8. Issue 1, ISSN 2190-3387, 2017. 29-69. Disponível em: <https://bit.ly/2q5Ut1u>. Acesso em: 30 jul. 2019. p. 59-60. (tradução nossa).
[377] COMISSÃO EUROPEIA. **COM n.º 0627/Final/2015/0284, de 9 de dezembro de 2015.** Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A0627%3AFIN>. Acesso em: 30 jul. 2019.
[378] JANAL, op. cit., p. 59-60. (tradução nossa).

serviços disponibilizados no mercado digital"[379]. Quer dizer a autora que simplesmente regular a privacidade, desconsiderando a aspecto mercadológico da portabilidade dos dados pessoais, resultará em parcial proteção do consumidor.

### 3.3.5 Direito de oposição e não sujeição às decisões automatizadas

O direito à oposição é prerrogativa que o titular dos dados pessoais faz jus. Como seu nome indica, este direito permite ao seu portador, percebida a ilicitude no tratamento dos seus dados, demandar, a qualquer momento, sua cessação pelo responsável. Contudo, o tratamento não cessará se expostas razões legítimas que sobrepujem direitos do titular ou envolvam questões judiciais (art. 21, n.º 1)[380].

É igualmente oponível pelo seu titular o tratamento de dados pessoais para efeito de comercialização direta, incluindo a definição de perfis feita com este objetivo; com a oposição, que pode ser realizada por meios automatizados, o responsável pela negociação cessará o tratamento mercantil dos dados e deverá comunicar de forma clara e distinta ao titular sobre a situação (art. 21, n.º 2 ao 5)[381].

Considera-se definição de perfil como qualquer tratamento informatizado de dados pessoais com intuito de avaliar características individuais do seu titular, especialmente relacionados "com seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (art. 4º, n.º 4)[382].

Estudos comprovaram que a definição de perfil, o chamado *profiling*, perpetua o cultivo de estereótipos e a segregação social, restringindo a liberdade de escolha dos titulares dos dados pessoais ao lhes enquadrar em categorias específicas. Com isso, aumenta a margem de suscetibilidade de haverem previsões imprecisas e discriminações injustificadas de negações de serviços e bens[383].

---

[379] CRAVO, Daniela Copetti. **Direito à portabilidade de dados:** necessidade de regulação *ex ante* e *ex post*. Tese (Doutorado em Direito). UFRS: Porto Alegre, 2018. p. 172.
[380] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.
[381] Ibid., não paginado.
[382] Ibid., não paginado.
[383] GT29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017; com a última redação revista e adotada em 6 de fevereiro de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf>. Acesso em: 13 jul. 2019. p. 6.

O Regulamento garante ainda ao titular de dados pessoais sua oposição ao tratamento deles para finalidades de investigação científicas, históricas ou artísticas se justificadas por motivos particulares. Este regramento estará excepcionado nos casos em que o tratamento for indispensável ao prosseguimento de obrigações de interesse público (art. 21, n.º 6)[384].

Conquanto predomine o interesse público, este tratamento ficará sujeito à preservação dos direitos e liberdades do titular, a exemplo da utilização de métodos organizacionais para garantir os princípios da minimização de dados, da proporcionalidade e da necessidade, ou mesmo a pseudonimização. Os Estados Membros ditarão as metodologias e condições específicas (considerando n.º 156 )[385].

Ao titular de dados também está previsto o direito de não sujeição a decisões exclusivamente automatizadas com seus dados pessoais, inclusive definição de perfis, e que tenham repercussão no âmbito jurídico ou lhe afetem significativamente. Isto quer dizer que o titular pode solicitar que tratamentos informatizados a seu respeito tenham intervenção humana (art. 22, n.º 1)[386].

Trata-se de prática cada vez mais recorrente e automática. Os sistemas informacionais, prezando cada vez mais pela celeridade do recolhimento, processamento e gerenciamento de dados pessoais costumam excluir a atuação humana da equação, fazendo com que recrutamentos eletrônicos ou recusas instantâneas de crédito, por exemplo, afetem os titulares com frequência.

Estas decisões automatizadas podem ser baseadas em qualquer tipagem de dados, tais quais os fornecidos pelos próprios titulares (através de respostas a questionários), os observados/recolhidos dos titulares (como dados de localização obtidos via aplicações) ou os deduzidos através de perfis pré-existentes deles (como as pontuações de créditos). Neste sentido, comenta Bioni[387]:

> Cada vez mais, os dados dos cidadãos, dispersos na rede, dizem mais sobre eles e quem os manipula sabe até mais sobre eles mesmos.

---

384 Regulamento n.º 679/2016, op. cit., não paginado.
385 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.
386 Ibid., não paginado.
387 GT29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017; com a última redação revista e adotada em 6 de fevereiro de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf>. Acesso em: 13 jul. 2019. p. 8.

> Essa capacidade de identificar os mais diversos padrões de comportamentos e prever a sua recorrência no futuro é uma verdadeira "mina de ouro" para a abordagem publicitária[388].

Percebe-se aqui a veracidade da máxima popular, a de que "a corda sempre arrebenta do lado mais fraco"; e, neste contexto, o lado é o do ciberconsumidor, que trespassa por situações, muitas vezes sem perceber, nas quais seus dados pessoais são violados, seja pelo tratamento instantâneo e automatizado dos dados, seja pelo seu desconhecimento normativo e vulnerabilidade técnica ou financeira.

Esta hipossuficiência nem sempre quer traduzir a ideia de que os consumidores não saibam lidar com tecnologia, mesmo porque, se assim o fosse, o avanço do comércio eletrônico não seria tão significativo. Logo, constata Bioni que "cada vez mais os usuários da Internet subvertem-se em consumidores, sendo uma clara amostra de tal afirmação o crescimento exponencial do comércio eletrônico"[389].

E a este crescimento dos ciberconsumidores acompanha um massivo aumento de pessoas vulneráveis, cuja hipossuficiência acontece longe das vistas comuns, com a coleta de dados pessoais e informações de consumo, com a formação de bancos de dados e cadastros de consumo, no microverso dos *bits e bytes e* dos algoritmos de preferência.

Vejam-se os *websites* de redes sociais e de compras *online* que recolhem, compilam, codificam e transformam em indicadores as preferências pessoais e de consumo dos titulares de dados; vejam-se os aplicativos de monetização de pesquisas que barganham com os ciberconsumidores dados pessoais e sensíveis por centavos; ou mesmo as políticas de privacidade com cláusulas nebulosas.

Neste sentido, alertam Zuin e Assis sobre a utilização dos meios eletrônicos como instrumento de massa, sobre os riscos das relações consumeristas virtuais decorrentes de um ambiente promissor e envolvedor e, ao mesmo tempo, inóspito e desregrado, destacando ainda o dever dos responsáveis pelo tratamento dos dados e as políticas que minimizem o desconforto/insegurança do ciberconsumidor:

> A internet revolucionou a sociedade na capacidade de prover meios para satisfação das suas volições, através do consumo por meio eletrônico, podendo, num futuro não muito longínquo, ser considerado

---

388 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. – Rio de Janeiro: Forense, 2019. p. 61.
389 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. – Rio de Janeiro: Forense, 2019. p. 43.

> um instrumento da massa, pautado na perspectiva da conhecida globalização e da sociedade da informação consumidora. Os riscos e perigos inerentes as relações de consumo via internet trazem receios sobre as possibilidades de agressão ao direito do consumidor, em razão de sua reconhecida vulnerabilidade, em especial na subtração da sua capacidade de compreensão das implicações das ações no mundo cibernético no atendimento de sua vontade, motivo pelo qual, em muitos pontos, a atual sistemática aponta a necessidade da adoção de mecanismos integrativos do ordenamento jurídico para se alcançar uma solução capaz de minorar o desconforto e a insegurança do consumidor. Com efeito, a vulnerabilidade e a informação são os princípios-guia que relembram a posição desfavorável do consumidor, bem como a possibilidade deste também ser afetado pela conformação ambiental inadequada, o que torna ainda mais latente a necessidade da responsabilidade do fornecedor após o consumo, como instrumento indutor das relações consumistas sob uma perspectiva ambiental ótima[390].

Não obstante haja situações expressamente autorizadas pela UE ou pelos Estados Membros para tratamento automatizado irrestrito pelos responsáveis - como para prevenir fraudes e evasões fiscais, garantir segurança, confiança ou execução de contrato feito ou serviço prestado, ou ainda direitos e liberdades dos próprios titulares (se consentidos) -, há limites a serem respeitados (art. 21, n.º 2, "a" a "c")[391].

Mesmo nestes casos, o titular dos dados pessoais pode manifestar seu ponto de vista, opor-se à decisão automatizada e solicitar intervenção humana para obtenção de explicação da decisão tomada (art. 21, n.º 3). Ademais, decisões automatizadas que envolvam crianças (considerando n.º 71) ou dados sensíveis, sem as devidas precauções e autorizações cabíveis, são ilegais (art. 21, n.º 4)[392].

A conclusão alcançável é de que as definições de perfis e as decisões automatizadas podem ser vantajosas para pessoas e organizações nos quesitos eficiência e economia de recursos, mas que também são suscetíveis de ocasionar riscos aos direitos e liberdades dos titulares de dados pessoais[393] e que, portanto, as medidas protetivas trazidas pelo RGPD são pertinentes e necessárias.

---

[390] ASSIS, Ana Cláudia Mrando Lopes; ASSIS, Vinicius de; ZUIN, Aparecida Luzia Alzira. **A dinâmica tecnológica e os desafios na regulação do direito do consumo no Brasil.** p. 20-35. In: Desafios socioambientais das sociedades de consumo, informacional e tecnológica [recurso eletrônico] / Aidee Moser Torquato Luiz... [et al.]; organizadores, Pedro Abib Hectheuer, Bruna Borges Moreira Lourenço, Marcia Abib Hecktheuer. – Itajaí: UNIVALI, 2018. p. 33.

[391] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.

[392] Ibid., não paginado.

[393] GT29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017; com a última redação**

## 3.4 Autoridades de proteção de dados pessoais

Tendo em vista o espírito, a ambição e o propósito da UE com a adoção do RGPD, a criação e a regulação das autoridades protetoras de dados pessoais serão fundamentais para cumprimento deste quadro normativo moderno, contribuindo para fiscalização e proteção de direitos e liberdades fundamentais dos cidadãos, ainda mais pela quantidade de organizações e de informações em larga escala.

Seguindo a legislação, registra-se a existência da: (i) a Autoridade Europeia para a Proteção de Dados (AEPD); (ii) as Autoridades Públicas Independentes de Proteção de Dados (APD), também conhecidas como Autoridades de Controle; (iii) os Responsáveis pelo Tratamento de Dados; e (iv) os Encarregados de Proteção de Dados (EPD); cada qual com suas próprias atribuições e finalidades.

Diante da importância das atividades exercidas por essas instituições para proteção dos dados pessoais, imperioso que sejam feitos alguns comentários a respeito das criações, atribuições e poderes das referidas autoridades para que então sejam tratadas as medidas de segurança promovidas pelo RGPD para combater o *personal data breach* e minimizar seus efeitos.

### 3.4.1 Autoridade Europeia para a Proteção de Dados

A Autoridade Europeia para a Proteção de Dados (AEPD), doravante chamada pelo seu acrônimo, consiste em órgão de controle independente criado pelo Regulamento (CE) n.º 45/2001[394] - revogado pelo Regulamento (UE) n.º 1.725/2018[395] – com o objetivo de controlar todas as operações de tratamento de dados pessoais efetuadas pelas instituições e pelos órgãos da União (art. 1º, n.º 3).

---

**revista e adotada em 6 de fevereiro de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf>. Acesso em: 13 jul. 2019. p. 5.

[394] UNIÃO EUROPEIA. **Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000**, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001R0045>. Acesso em: 14 jul. 2019.

[395] Id. **Regulamento (UE) 1.725/2018 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE (Texto relevante para efeitos do EEE.). Disponível em: <https://eur-lex.europa.eu/eli/reg/2018/1725/oj>. Acesso em: 14 jul. 2019.

A AEPD foi habilitada a desempenhar suas funções e poderes de forma totalmente autônoma. Não sofrendo influências externas, sejam elas diretas ou indiretas, tampouco precisando solicitar ou receber instruções de terceiros, o órgão precisa funcionar com integridade, discrição e sigilo profissional, não podendo exercer quaisquer outras atividades profissionais durante seu mandato (art. 55 e 56).

Referida autoridade, sediada em Bruxelas (art. 54, n.º 6), é nomeada por um período de 05 (cinco) anos (art. 53, n.º 1), com mandato renovável uma única vez (art. 53, n.º 3) e conta com várias atribuições expressas (art. 57, n.º 1, "a" a "q"), além de poderes de investigação (art. 58, n.º 1), correção (art. 58, n.º 2), autorização e consulta (art. 58, n.º 3) e submissão de pleitos à apreciação do TJ (art. 58, n.º 4)[396].

No tocante às suas atribuições, a AEPD (i) controla e aplica normas protetivas de dados dos órgãos e instituições da União (salvo as do TJ); (ii) promove a conscientização do público acerca de riscos, direitos e garantias inerentes à temática; (iii) promove a conscientização dos responsáveis pelo tratamento de suas obrigações; (iv) presta informações e coopera com autoridades quando preciso.

Outrossim, (v) trata e investiga reclamações recebidas e informa aos envolvidos sobre seu andamento e resultado; (vi) presta aconselhamento sobre medidas legislativas e administrativas; (vii) acompanha a evolução e nível da tecnologia da informação e comunicação; (viii) adota cláusulas contratuais; (ix) conserva lista de critérios de avaliação de impacto; (x) participa do Comitê Europeu.

Ela ainda (xi) assegura o secretariado do Comitê Europeu[397]; (xii) presta conselhos sobre tratamento de consulta prévia; (xiii) autoriza cláusulas contratuais de transferência de garantias adequadas; (xiv) conserva registros internos de violações; (xv) executa tarefas de proteção de dados pessoais; e (xvi) elabora seu próprio regulamento interno (art. 57, n.º 1, "a" a "q")[398].

Enquanto o Regulamento (UE) n.º 1.725/2018 dispõe sobre os Responsáveis pelo Tratamento de Dados (art. 26 e seguintes) e Encarregados de Proteção de Dados

---

[396] UNIÃO EUROPEIA. **Regulamento (UE) 1.725/2018 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE (Texto relevante para efeitos do EEE.). Disponível em: <https://eur-lex.europa.eu/eli/reg/2018/1725/oj>. Acesso em: 14 jul. 2019.

[397] A Autoridade Europeia de Proteção de Dados redige e publica os critérios de acreditação de um organismo para monitorizar códigos de conduta para auxiliar a Secretaria do Comitê Europeu no cumprimento de suas obrigações (arts. 41 e 43 do RGPD).

[398] Regulamento (UE) n.º 1.725/2018, op. cit., não paginado.

(art. 23 e seguintes), o Regulamento (UE) n.º 679/2016 dispõe acerca da Autoridade de Controle (art. 51 e seguintes). Ambos os regulamentos estão vigentes e são complementares no quesito tratamento de dados pessoais.

### 3.4.2 Autoridades de Controle

As Autoridades de Controle são órgãos públicos independentes designados pelos Estados Membros para resguardar os direitos e liberdades fundamentais das pessoas singulares relativos à proteção de dados pessoais e circulação de dados na União, funcionando então como fiscais da aplicação do RGPD. Pode-se contar com mais de uma autoridade nomeada por nação (art. 4, n.º 21, e, art. 51, n.º 1).

Curioso é o fato de que a maioria das nações europeias prevê uma única autoridade de proteção de dados, com exceção da Alemanha, da Suíça e do Reino Unido que possuem mais de uma; e, até pouco tempo, a Itália, que não possuía nenhuma autoridade nacional de controle, apenas um Registro Geral para o tratamento de dados pessoais[399]; atualmente, já designou sua autoridade.

As autoridades devem, outrossim, ser independentes, como a própria legislação europeia dispõe, sem influências externas, para cumprirem suas funções de proteção dos dados pessoais. Referida independência não quer dizer que as autoridades de controle devem se afastar dos seus respectivos Estados Membros, mas sim guardar certo nível de desvinculação à idoneidade das suas atribuições.

Mesmo porque, acerca desta questão, comenta Limberger, "o legislador não possui liberdade de criação total das administrações independentes, devendo concretizar os limites e estabelecer as garantias de tal modo que a utilização da informática respeite os direitos de honra e intimidade"[400]. Mundialmente, o nível de vinculação das autoridades de controle aos seus governos costuma variar bastante.

Neste diapasão, no tocante às Autoridades Nacionais com natureza fiscalizatória, em material jurisprudencial, encontra-se a Ação por incumprimento do Estado do TJUE, ainda sob à égide da Diretiva n.º 46/1995/CE, que abordou a

---

399 LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p.142.
400 Ibid., 146.

problemática do alcance da exigência de independência. No caso, a Comissão solicitava a declaração de violação pela Alemanha à Diretiva[401].

Restou declarada a violação e reconhecida e assegurada pelo TJUE a independência da Autoridade de Proteção de Dados da Alemanha, uma vez que a Diretiva está à serviço da proteção das pessoas singulares e do tratamento dos seus dados pessoais e não à serviço das autoridades públicas e de seus agentes, como espécie de regime estatutário especial.

Ademais, tecnicamente, elas trabalham em cooperação, todas entre si e com a Comissão, e aplicam com coerência as normas protetivas. Há determinação expressa para que, em caso de mais de uma autoridade de controle, nomeie-se uma representante nacional e que cada Estado-Membro notifique sobre as legislações adotadas à Comissão para haver uniformidade e atualização (art. 51, n.º 2 a 4).

Com nomeações mediante procedimentos transparentes, seus membros são nomeados pelo (i) Parlamento; (ii) Governo; (iii) Chefe de Estado; ou (iv) Organismo independente com poder de nomeação. Destacam-se pelas suas habilidades, experiências, conhecimentos e sigilo na área de proteção de dados pessoais e possuem, como regra, mandados não inferiores a 4 (quatro) anos (art. 54, n.º 1 e 2).

Conhecida como Autoridade de Controle Principal, sua competência para prossecução de atribuições e exercício de poderes está restrita ao território do seu próprio Estado-Membro, com exceção ao controle do tratamento de dados realizado pelos tribunais (art. 55, n.º 1 a 3), inclusive para certos casos de tratamentos transfronteiriços de dados pessoais (art. 56, n.º 1)[402].

Para identificá-la é preciso determinar a localização do estabelecimento principal ou estabelecimento único do responsável pelo tratamento ou do subcontratante na UE (art. 4, n.º 16), uma vez que a administração central é onde se decidem ou executam os tratamentos. A questão é aclarada nas explicações iniciais (36º Considerando) e minuciada em orientação do GT do art. 29[403].

---

401 TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão de 9 de março de 2010 (Grande Secção), Comissão/Alemanha (C-518/07, EU:C:2010:125).** Disponível em: <https://bit.ly/2NpUchT>. Acesso em: 30 jul. 2019.

402 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.

403 GT29. **Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante, adotadas em 13 de dezembro de 2016; com a última redação revista e adotada em 5 de abril de 2017.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp244rev01_pt.pdf>. Acesso em: 14 jul. 2019. p. 4-5.

Ademais, cada autoridade de controle é competente para tratar reclamações apresentadas ou potenciais violações ao RGPD causadas por estabelecimentos nacionais ou afetas aos titulares de dados dentro do próprio Estado-Membro. Deverá haver uma interlocução, notificação e decisão entre autoridade principal e "secundária" sobre quem atuará no caso concreto (art. 56, n.º 2 a 6).

Suas atribuições envolvem conscientização, cientificação, notificação, aconselhamento, orientação e acreditação; controle, execução e processamento de reclamações; cooperação e investigação de fatos relevantes; aprovação, autorização e adoção de cláusulas, requisitos, certificações; e redação, elaboração e conservação de documentos e registros internos (art. 57, n.º 1, "a" a "v").

Seus poderes investigativos (art. 58, n.º 1), poderes corretivos (art. 58, n.º 2), poderes consultivos e autorizativos (art. 58, n.º 3) e suas obrigações garantistas (art. 58, n.º 4 a 6) estão especificadas no Regulamento. Dentre tais obrigações, ressalta-se a de apresentação de relatório anual de atividades, contendo eventual listagem de violações notificadas e medidas aplicadas (art. 59)[404].

Uma relação completa de todas as Autoridades Nacionais de Proteção de Dados Europeias pode ser encontrada no *repositório online* da Comissão Europeia, contendo a titulação dos órgãos, seus respectivos países, logradouros públicos, informações de contato telefônico, eletrônico e *websites* e diretores/presidentes responsáveis, nos idiomas europeus correspondentes[405].

### 3.4.3 Responsável pelo tratamento de dados e subcontratantes

De acordo com a definição do RGPD, o responsável pelo tratamento de dados (*Controller*) é pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, individual ou coletivamente, estabelece as finalidades e os meios de tratamento de dados pessoais, conforme disposições constantes no direito da UE ou no direito dos Estados Membros (art. 4, n.º 7)[406].

---

[404] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.

[405] COMISSÃO EUROPEIA. **Proteção de dados na UE.** Autoridades nacionais de proteção de dados. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt>. Acesso em: 15 jul. 2019.

[406] Regulamento n.º 679/2016, op. cit., não paginado.

Semelhante conceito consta no Regulamento n.º 1.725/2018, apesar do foco no tratamento e circulação de dados feitos pelos órgãos, instituições e organismos da UE e não por pessoas singulares e coletivas (art. 3º, n.º 8). Nele é disposto ainda sobre a responsabilidade destes sujeitos públicos, incluindo análise de riscos, aplicação de medidas técnicas e certificações de cumprimento (art. 26, n.º 1 ao 3)[407].

Interessante destacar que as empresas/organizações, quando determinam em conjunto com uma ou mais organizações o porquê e como os dados serão tratados, são conjuntamente tidas como responsáveis. Devem para tanto celebrar contrato/acordo para assim funcionarem e os principais aspectos deste acordo devem ser comunicados aos titulares de dados.

A figura do subcontratante (*Processor*) também é reconhecida pelo RGPD. Um subcontratante, segundo definição legal, é "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes" (art. 4º n.º 8)[408]. Geralmente o subcontratante é terceiro externo à empresa, mas podem atuar junto a estas.

Há disposições gerais acerca dos subcontratantes (art. 28, n.º 1 ao 10), tratamento de dados pelos responsáveis e pelos subcontratantes, sob a autoridade destes (art. 29), e dos registros de atividades de tratamento como nomes, contatos, finalidades dos tratamentos, categorias de titulares, dados pessoais, destinatários, inclusive se estrangeiros, prazos e técnicas adotadas (art. 30 n.º 1, "a" a "g")[409].

Seguindo as diretrizes de cooperação entre as autoridades de controle e os EPDs, por força do RGPD, os responsáveis pelo tratamento de dados, e os subcontratantes sob as suas supervisões, igualmente devem cooperar com a autoridade de controle, quando solicitados por estas, para prosseguimento das suas atividades em prol da proteção e circulação dos dados pessoais (art. 31)[410].

---

[407] UNIÃO EUROPEIA. **Regulamento (UE) 1.725, do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE (Texto relevante para efeitos do EEE.). Disponível em: <https://eur-lex.europa.eu/eli/reg/2018/1725/oj>. Acesso em: 14 jul. 2019.

[408] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.

[409] Ibid., não paginado.

[410] Ibid., não paginado.

### 3.4.4 Encarregado pela Proteção de Dados

O Encarregado pela Proteção de Dados – EPD (*Data Protection officer*) é a pessoa designada pelas organizações envolvidas com o tratamento de dados pessoais, cuja função é necessária sempre que houver massivo processamento de dados pessoais e sensíveis que exija aconselhamento, monitorização e observância das normas de segurança e proteção dos dados[411].

O conceito de EPD não é inovação trazida pelo RGPD. A nomeação de EPD já era prevista na Diretiva n.º 46/1995/CE, embora não houvesse obrigatoriedade de nomeação. Esta prática foi cultivada pelos Estados Membros com o passar do tempo e desde sempre incentivada pelo GT 29, que defendia sua figura como facilitadora de conformação normativa e vantagem competitiva às empresas[412].

O RGPD trouxe consigo normas mais rígidas sobre os EPDs (art. 37 em diante), tornando obrigatória sua nomeação nos casos de (i) tratamento realizado por autoridade ou órgão público (exceto tribunais); (ii) tratamento que demande controle regular/sistemático[413] em grande escala[414]; e (iii) tratamento relativo a dados sensíveis ou a condenações penais em grande escala (art. 37, n.º 1, "a" a "c")[415].

Complementar ao RGPD, o Regulamento n.º 1.725/2018 dispõe sobre os critérios para designação dos EPDs pelos órgãos, organismos e instituições da UE

---

411 PORTAL DO DPO - Encarregado de Protecção de Dados. **Glossário RGPD.** Disponível em: <https://www.portaldodpo.pt/glossario/>. Acesso em: 15 jul. 2019.

412 GT29. **Orientações sobre os encarregados da proteção de dados (EPD), adotadas em 13 de dezembro de 2016; com a última redação revista e adotada em 5 de abril de 2017.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf>. Acesso em: 14 jul. 2019. p. 5.

413 **Controle Regular e sistemático:** "A noção de controlo regular e sistemático dos titulares dos dados não está definida no RGPD, mas inclui claramente todas as formas de seguimento de perfis na internet, designadamente para fins de publicidade comportamental. [...] Na interpretação do GT 29, <<regular>> significa, neste caso, uma ou mais das seguintes características: contínuo ou que ocorre a intervalos específicos num determinado período; recorrente ou repetido em horários estipulados; constante ou periódico. Na interpretação do GT 29, <<sistemático>> significa, neste caso, uma ou mais das seguintes características: que ocorre de acordo com um sistema; predefinido, organizado ou metódico; realizado no âmbito de um plano geral de recolha de dados; efetuado no âmbito de uma estratégia [...]". (Ibid., p. 24-25).

414 **Grande escala:** "O RGPD não define o que constitui um tratamento de grande escala. O GT 29 recomenda que, em especial, os seguintes fatores sejam tomados em consideração para determinar se o tratamento é efetuado em grande escala: número de titulares de dados afetados – como número concreto ou em percentagem da população em causa; o volume de dados e/ou alcance dos diferentes elementos de dados objeto de tratamento; a duração, ou permanência, da atividade de tratamento de dados; o âmbito geográfico da atividade de tratamento [...]". (Ibid., p. 24).

415 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.

(art. 43, n.º 1 ao 5), as posições dos EPDs (art. 44, n.º 1 ao 9) e, obviamente, sobre as funções dos EPDs (arts. 45, n.º 1 ao 3)[416]. Os mesmos tópicos normativos são abordados pelo RGPD (art. 37, n.º 1 ao 7; art. 38, n.º 1 ao 6; e art. 39, n.º 1 ao 2)[417].

Especificamente, são funções que competem aos EPDs: (i) informar e aconselhar os responsáveis pelo tratamento sobre suas obrigações; (ii) controlar a conformidade de normas dos Estados Membros com as da UE, além de repartir responsabilidades, sensibilizar e formar técnicos atuantes no tratamento e realizar auditorias; e (iii) aconselhar no solicitado sobre avaliações de impacto.

Estão ainda entre suas atribuições: (iv) cooperar com as autoridades de controle; e (v) servir como intermediador com as autoridades de controle quanto às consultas e consultas prévias. E, assim como para demais autoridades, os EPDs devem considerar os riscos inerentes às operações de tratamento no tocante à sua natureza, âmbito, contexto e finalidades (art. 39, n.º 1 ao 2)[418].

Tendo em vista o exposto, observa-se o quão importante são estas estruturas de proteção de dados instituídas pelo RGPD, em especial as autoridades de controle, que não apenas assumem o papel de resguardar a proteção dos segredos comerciais e industriais, mas também e, com rigor redobrado, a proteção dos ciberconsumidores em razão das tecnicidades de segurança de dados pessoais.

Não bastasse a atuação fiscalizatória, a competência delas abarca atribuições jurídicas – ao apreciar petitórios dos próprios prejudicados – e procedimentais – ao editar regulamentos e trâmites internos -, além de ações proativas – ao promover a cooperação entre outras autoridades de controle -, que elevam o nível de integridade e confiabilidade da segurança de dados pessoais.

---

[416] UNIÃO EUROPEIA. **Regulamento (UE) 1.725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE (Texto relevante para efeitos do EEE.). Disponível em: <https://eur-lex.europa.eu/eli/reg/2018/1725/oj>. Acesso em: 14 jul. 2019.

[417] Regulamento n.º 679/2016, op. cit., não paginado.

[418] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.

## 3.5 Segurança de dados pessoais

Tendo em vista este universo jurídico e digital e este viés protetivo e securitário que circunda a temática, a questão da violação de dados pessoais é um dos pontos-chave, o grande conectivo de todos os eixos da dissertação. O *personal data breach* interligará a proteção da privacidade dos consumidores com o inovador Regulamento europeu e com a necessidade de normatização a respeito destes incidentes de segurança no MERCOSUL, que serão trabalhados adiante.

### 3.5.1 Incidentes de segurança, violações de segurança e violações de dados

A discussão conceitual moderna sobre incidentes de segurança virtuais - cujo principal exemplo são as falhas, quebras, brechas ou violações de dados (*data breach*) - é uma tarefa complexa e não apenas por questões técnicas. O que em determinado nicho global consideram como um ataque à segurança pode ser considerado apenas ameaça à segurança em outra localidade. Isto ainda quando não se confundem as noções de incidentes de segurança e de violações de dados.

A engenharia destes incidentes de segurança serve a diversos propósitos. A motivação maliciosa pode apenas explorar vulnerabilidades técnicas e trabalhar com programação binária para obtenção de ganhos financeiros ilícitos, como pode também explorar características comportamentais e processuais, deflagrando tendências, moldando condutas, registrando protestos, atrapalhando investigações, destruindo e forjando evidências e toda sorte de vantagens indevidas imagináveis.

Portanto, não existe muito consenso entre as comunidades, razão pela qual as definições não são mundialmente uniformizadas. Contudo, existem algumas orientações internacionalmente reconhecidas, que funcionam mais como guias práticos condizentes às diretrizes de matéria de segurança, como o (i) ISO/IEC 27001: 2005; (ii) o SO/IEC 27035:2011; (iii) o NIST SP 800-61; (iv) o CMU/SEI-2004-TR-015; e (v) os padrões do BSI[419].

[419] **Padrões internacionais reconhecidos para incidentes de segurança:** ISO/IEC 27001:2005 – Information technology – security techniques – information security management systems – requirements. SO/IEC 27035:2011 (revising ISO/IEC TR 18044:2004) Information technology – security techniques – information security incident management. Standards of individual Member States (for instance BSI). NIST SP 800-61 Computer security incident handling guide recommendations of the US Department of Commerce, National Institute of Standards and Technolog. and CMU/SEI-2004-TR-015 Report on defining incident management processes for computer security incident response teams (CSIRTs).

Predomina a utilização do raciocínio dos grupos concêntricos para delimitar a relação de pertencimento ou causa-consequência dos incidentes de segurança (*security incidente)*, das falhas de segurança (*security breach*) e das violações de dados (*data breach*). O incidente de segurança, correspondente ao círculo mais amplo, envolve a violação de segurança, condizente ao círculo intermediário, que por sua vez engloba as violações de dados, o menor e mais interno dos círculos[420].

Tendo em vista a interligação e a distinção destes eventos e sua importância para melhor compreensão das violações de dados pessoais (*personal data breaches*), imperiosa sua diferenciação/classificação conforme os padrões internacionalmente aceitos, a começar pelo evento mais genérico e menos gravoso até o mais específico e gravoso, seguindo a lógica dos conjuntos. A análise segue os estudos da Direção-Geral de Políticas Internas Europeia[421].

Segundo definição do ISO/IEC 27005:2018, o incidente de segurança "é uma ocorrência identificada em sistema, serviço ou estado de rede indicando uma possível violação de política ou falha de segurança de SI, ou uma conhecida situação que pode ser relevante à segurança". Ele é indicado por "uma isolada ou série de indesejáveis eventos de segurança informacional com probabilidade de comprometer operações de negócios e ameaçar a segurança da informação"[422].

O US-CERT SP 800-61 define incidente de segurança como "o ato de violar explícita ou implicitamente uma política de segurança"[423]. O guia RFC 2350 o trata como "qualquer evento adverso que comprometa algum aspecto da segurança do

---

[420] EUROPEAN PARLIAMENT. The Directorate-general For Internal Policies: Policy Department A: Economic and Scientific Policy, Industry, Research and Energy. **Data and Security Breaches and Cyber-Security:** Strategies in the EU and its International Counterparts. Disponível em: < http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-ITRE_NT(2013)507476>. Acesso em: 19 jul. 2019. p. 30-36. p. 16.

[421] *Direção-Geral de Políticas Internas Europeia (IPOL):* é o órgão "responsável pela organização do trabalho das comissões parlamentares no domínio das políticas internas e pela contribuição para o exercício e desenvolvimento dos poderes legislativo e de controlo do Parlamento Europeu". (EUROPEAN PARLIAMENT. **The Secretary General. Directorate-general For Internal Policies of the Union.** Disponível em: <http://www.europarl.europa.eu/the-secretary-general/en/organisation/directorate-general-for-internal-policies-of-the-union>. Acesso em: 19 jul. 2019). (tradução nossa).

[422] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management.** Disponível em: <https://www.iso.org/standard/75281.html>. Acesso em: 19 jul. 2019. (tradução nossa).

[423] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **SP 800-61 Rev. 2 - Computer Security Incident Handling Guide.** Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>. Acesso em: 19 jul. 2019. p. 6. (tradução nossa).

computador ou da rede"[424] e, especifica, o guia NIST SP 800-61, sê-lo "uma violação ou iminente ameaça de políticas de segurança computacionais; aceitáveis usos de políticas ou práticas de segurança padrão"[425], definição comparável à da ENISA.

Os incidentes de segurança podem ser (i) maliciosos (negações de serviços, ameaças avançadas persistentes, desfigurações de *websites,* ataques internos, engenharias sociais, danificadores de integridade da cadeia suplementar etc.), (ii) acidentes (erros humanos e complexidades do ciberespaço); (iii) causas naturais (indisponibilidades causadas por tsunamis, tempestades, "clarões solares" etc.); (iv) causas físicas (atos de terrorismo, danos ao cabeamento subaquático etc.)[426].

A quebra, falha ou violação de segurança (*security breach*) "ocorre quando um provedor violou suas obrigações de segurança", uma vez que os responsáveis pelos tratamentos de dados devem "aplicar as medidas técnicas e organizacionais suficientes para garantir a segurança dos dados que processam"[427]. Não tendo sido tomadas as precauções devidas, haverá uma quebra de segurança, mesmo não havendo qualquer perda de dados.

Tentativas conceituais são encontradas na experiência legislativa internacional. Na proposta para a *NIS Directive*, diz-se acontecer uma violação de segurança "quando um provedor tiver violado seus deveres de segurança conforme a diretiva" (art. 3, n.º 2). Na *e-Privacy Directive* n.º 202/58/2002 (emendada em 2009), diz-se que ela "conduz à uma acidental ou ilegal destruição, perda, alteração, divulgação, acesso, transferência, conservação ou processamento (art. 4º)[428].

Na *Trust Services Regulations*, identificada, porém não definida, a violação de segurança é descrita como "uma perda de integridade que tenha significativo impacto na confiança do serviço prestado e nos dados pessoais lá mantidos" (art. 15). E, na *US Defence Industrial Base Pilot Guidance*, é tida como "qualquer circunstância ou

---

[424] NETWORK WORKING GROUP. **Request for Comments: 2350 - Expectations for Computer Security Incident Response.** Disponível em: <https://www.ietf.org/rfc/rfc2350.txt >. Acesso em: 19 jul. 2019. (tradução nossa).

[425] NIST, SP 800-61 Rev. 2, op. cit., p. 6. (tradução nossa).

[426] EUROPEAN PARLIAMENT. The Directorate-general For Internal Policies: Policy Department A: Economic and Scientific Policy, Industry, Research and Energy. **Data and Security Breaches and Cyber-Security:** Strategies in the EU and its International Counterparts. Disponível em: < http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-ITRE_NT(2013)507476>. Acesso em: 19 jul. 2019. p. 30-36.

[427] Ibid., p. 39. (tradução nossa).

[428] Ibid., p. 38. (tradução nossa).

evento com o potencial de adversamente impactar operações de uma organização [...], seus recursos, indivíduos ou nações [...]"[429].

Depreende-se, contudo, inexistir uma clara conceituação legal para violação de segurança, mas ela transmite a ideia da existência de certo risco, de potencial danosidade que, ainda que não resulte em prejuízos com dados efetivos, ultrapassa a esfera de simples incidente de segurança. Sua nomenclatura e contexto traduzem maior sensação de urgência, de executividade de conduta, de menor generalidade invasiva e de inobservância de obrigação.

Ao se adentrar no campo de incidentes de segurança e elevar o nível de especificidade das violações de segurança as relacionadas com dados e informações, é possível se deparar com uma violação de dados (*data breach*), um antigo estorvo documental, convertido em grande impasse virtual com a evolução da tecnologia da comunicação e da cibernética e, em tempos atuais, um catastrófico problema técnico-securitário, jurídico-legislativo e individual-governamental.

Segundo definição da ENISA, uma violação de segurança "[...] refere-se a incidentes que envolvem a divulgação e disseminação ilegais de dados do usuário". Estas violações são tratadas como "[...] incidentes bem-sucedidos que conduzem à perda de dados anteriormente existentes, uma vez que quando uma violação de dados é analisada, o incidente já alcançou seu êxito"[430]. São os principais responsáveis por ameaças e ataques cibernéticos modernos.

Uma violação de dados, segundo descrição do *US Health Insurance Portability and Accountability Act*, é uma inadmissível "[...] utilização ou divulgação, sob as normas de privacidade, que compromete a segurança ou a privacidade das informações de saúde de tal forma que [...] ofereça risco significativo de danos financeiros, de reputação ou prejuízos a outros indivíduos"[431]. Embora seja com enfoque na saúde o conceito citado, estes dados podem ser de qualquer área.

A ENISA menciona como principais agentes causadores de violações de dados, como já listado em tópicos anteriores, os (i) cibercriminosos, bastante atuantes

---

[429] Ibid., p. 38. (tradução nossa).
[430] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). **Data breaches.** Disponível em: <https://etl.enisa.europa.eu/#/>. Acesso em: 19 jul. 2019. Não paginado. (tradução nossa).
[431] EUROPEAN PARLIAMENT. The Directorate-general For Internal Policies: Policy Department A: Economic and Scientific Policy, Industry, Research and Energy. **Data and Security Breaches and Cyber-Security:** Strategies in the EU and its International Counterparts. Disponível em: < http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-ITRE_NT(2013)507476>. Acesso em: 19 jul. 2019. p. 38.

no ciberespaço; (ii) ciberguerrilheiros, grupos com motivações defensivas; (iii) ciberterroristas, grupos com motivações destrutivas, propagandistas e de recrutamento; (iv) hacktivistas; (v) agentes internos; (vii) programadores aprendizes; (viii) corporações nacionais e multinacionais; e até por (ix) Estados Nacionais[432].

A agência elenca os principais ataques - que não divergem muito dos casos dolosos de incidentes e violações de segurança, senão pelo seu propósito e enfoque nos dados - relacionados com as violações de dados: (i) roubo de identidade; (ii) vazamento de dados; (iii) "ataques internos"; (iv) programas mal-intencionados; (v) "pescagem de dados"; (vi) perda, furto, dano ou manipulação física de dados; (vii) envio e publicação massiva de anúncios; e (viii) ataques *online*[433].

### 3.5.2 Violação de dados pessoais

Da mesma forma que uma violação de dados transmite uma sensação de maior especificidade e periculosidade que um incidente de segurança, uma violação de dados pessoais[434] (*personal data breach*) transmite as mesmas impressões quando comparado com uma violação de dados gerais. Isto implica a conclusão de que uma violação de dados pessoais é uma violação de dados e, antes disso, um incidente de segurança, mas que os dois eventos não são *personal data breaches.*

A violação de dados pessoais, manifestada na grande maioria dos casos através de vazamentos clandestinos, às margens da legislação aplicável e quase sempre proveniente do submundo do cibercrime[435], recebe cada vez mais atenção nos ambientes corporativos, nas mídias tradicionais e alternativas, alcança escalas governamentais, tornando-se políticas regionais e agendas globais e, aos poucos, desperta a consciência dos ciberconsumidores, que são os mais interessados.

Sua danosidade à privacidade e à intimidade do titular dos dados pode ser irreversível, violando direitos humanos e fundamentais e, portanto, dispositivos legais internacionais e nacionais. Eis o porquê atualmente não é espantoso que seja uma temática recorrente nos noticiários, pauta de conferências e congressos renomados e

---

[432] ENISA, op. cit., não paginado.
[433] ENISA, op. cit., não paginado. (tradução nossa).
[434] Vide tópico 2.5 desta dissertação, sobre dados pessoais e dados sensíveis, para informações complementares.
[435] Vide tópico 2.4 desta dissertação, sobre criminalidade de dados, para informações complementares.

objeto de proteção jurídica de considerável número de projetos, diretrizes, regulamentos e legislações mundo afora.

A nomenclatura recebida é igualmente sugestiva, não esconde mistérios ou guarda trocadilhos técnicos tais como o incidente ou violação de segurança podem ocasionar, inclusive sua significação não parece destoar muito nas legislações onde vem sendo tipificada ou incorporada. Ela é comumente relacionada com o tratamento automatizado de dados de pessoais, associada com procedimentos desautorizados e inconsequentes e motivada por razões dolosas ou culposas.

O RGPD enuncia uma das suas mais conhecidas definições: é "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (art. 4, n.º 12)[436]. A Diretiva n.º 46/1995, se comparada às noções securitárias do RGPD[437], sequer dispunha de um conceito expresso para "violação de dados pessoais".

Como já explorado alhures, a segurança de dados pessoais é reforçada por princípios de tratamento automatizados no Regulamento[438]. São, então, compatíveis, porque o dado pessoal deve ser tratado de forma que "garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»[439])" (art. 5º, n.º 1, "f")[440].

O conceito de violação de dados pessoais vincula algumas noções com significados precisos. "Destruição", por exemplo, diz respeito aos dados que são extintos ou deixam de existir em formato utilizável pelo responsável pelo seu tratamento; já o "dano" indica a alteração ou corrupção dos dados, afetando sua

---

436 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 13 jul. 2019.

437 Vide tópico 3.5.1 desta dissertação, sobre incidentes de segurança, violações de segurança e violações de dados, para informações complementares.

438 Vide tópico 2.7 desta dissertação, sobre princípios da proteção de dados, para informações complementares.

439 Vide tópico 2.7.6 desta dissertação, sobre princípios da integridade e da confidencialidade, para informações complementares.

440 Regulamento n.º 679, de 27 de abril de 2016, op. cit., não paginado.

completude; e a "perda" se refere aos dados existentes, mas indisponíveis, inacessíveis ou não mais em propriedade do responsável pelo tratamento[441].

E a periculosidade destas violações destrutivas, danosas ou perdíveis reside em uma série de possíveis consequências aos titulares, aos consumidores que confiaram seus dados pessoais, sobretudo seus dados sensíveis, aos responsáveis pelo tratamento e viram o serviço prestado ser convertido em prejuízos físicos, psicológicos, materiais ou imateriais raramente reversíveis. Justificada está a preocupação do RGPD com medidas preventivas e contramedidas paliativas.

Algumas violações de dados pessoais podem ser: (i) perda do controle dos dados; (ii) limitações de direitos e liberdades; (iii) discriminação generalizada (racial, étnica, política, religiosa, filosófica, ideológica, sexual, médica, econômica, criminal etc.; (iv) roubo e usurpação de identidade; (v) perdas e desvantagens financeiras e sociais; (vi) destruição de reputação; (vii) quebra de sigilo profissional; (viii) inversão não autorizada da pseudonimização etc. (Considerações n.º 75 e n.º 85)[442]

Visando a precaver e minimizar estas consequências diretas e indiretas sobre os titulares, o RGPD determina a adoção de medidas técnicas e organizativas pelos responsáveis pelo tratamento dos dados pessoais (e subcontratantes) para garantir o nível de segurança adequado ao risco da violação. Elas determinam providências cabíveis e levam em conta as técnicas avançadas disponíveis, custos de aplicação, natureza, âmbito, contexto, finalidade, probabilidade e gravidade (art. 32)[443].

Prossegue o RGPD listando alguns exemplos de medidas organizativas e técnicas: (i) pseudonimização e cifragem de dados pessoais; (ii) permanência e conformidade dos sistemas e serviços de tratamento com os princípios protetivos; (iii) restauração de disponibilidade e acesso aos dados tempestiva no caso de problemas físicos e técnicos; e (iv) processo avaliativo de regular eficácia das medidas técnicas e organizativas utilizadas (art. 32, n.º 1, "a" a "d")[444].

---

441 GT29. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017 e Revistas e adotadas pela última vez em 6 de fevereiro de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf>. Acesso em: 20 jul. 2019. p. 7.

442 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016, do Parlamento Europeu e Conselho.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 19 jul. 2019.

443 Ibid., não paginado.

444 Ibid., não paginado.

O Regulamento estabelece ainda, para obtenção do nível de segurança adequada e ponderação de riscos, que os responsáveis pelo tratamento de dados (e subcontratantes) tenham especial cuidado com consequências de destruição, perda e alteração de dados pessoais, bem como com as atividades de divulgação, acesso desautorizado, transmissão e conservação de dados (art. 32, n.º 2)[445]. O enfoque particular não deve excluir o cuidado com outras formas de tratamento.

Mas não houve preocupação nesta legislação protetiva de dados pessoais apenas com seus titulares. Há dispositivo que serve de comprovante de que os responsáveis pelo tratamento (e subcontratantes) cumpriram suas obrigações corretamente se seguirem as normativas do Código de Conduta (art. 40) e as demonstrarem às autoridades (art. 32, n.º 3), uma vez que existente uma hierarquia, inclusive para fins de acesso de dados a particulares (art. 32, n.º 4)[446].

Neste contexto, visando a proteger o ciberconsumidor, o RGPD exsurge para prevenir a ocorrência, minimizar os impactos e penalizar os responsáveis. A prevenção é perceptível pela "segurança do tratamento dos dados pessoais" (art. 32) ora exposta; a minimização dos impactos pela "notificação à autoridade de controle, comunicação ao titular dos dados e avaliação de impactos" (arts. 33 a 35), em caso de violações de dados pessoais[447], será abordada na sequência.

### 3.6 Notificação de violação de dados pessoais

Uma vez esclarecidas questões conceituais de incidentes e de violações de segurança e questões técnico-legais sobre violações de dados e de dados pessoais (e sensíveis), possível seguir com as medidas protetivas instituídas pelo novo regulamento europeu, a começar com a notificação de violação de dados pessoais à autoridade de controle e ao titular dos dados e ciberconsumidores.

No que diz respeito à notificação de violação de dados pessoais à autoridade de controle, para que seja preciso qualquer notificação de violação de dados pessoais é preciso que alguma violação desta natureza tenha acontecido previamente.

---

445 Ibid., não paginado.
446 Ibid., não paginado.
447 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016, do Parlamento Europeu e Conselho.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 21 jul. 2019.

Constatando-a, o responsável pelo tratamento deverá cientificar a autoridade de controle (art. 55º) sobre o fato em até 72 (setenta e duas) horas depois que o tenha chegado ao seu conhecimento[448].

Não sendo transmitida tempestivamente dentro dos 03 (três) dias, a notificação deverá ser acompanhada das razões que motivaram o atraso, o que demonstra a preocupação do legislador com a urgência da violação, com o *timing* do ato notificador, para contramedidas paliativas, e com a transparência e fiscalização das obrigações dos responsáveis pelos tratamentos.

No mesmo dispositivo abre exceção à desnecessidade de notificação da violação dos dados pessoais à autoridade de controle se ela não for suscetível de ocasionar riscos aos direitos fundamentais e liberdades individuais dos seus titulares (art. 33, n.º 1). Determina ainda que ao próprio responsável pelo tratamento deve se reportar/notificar o subcontratante em caso de tais violações (art. 33, n.º 2)[449].

Os requisitos que devem fazer parte da notificação também são listados pelo RGPD: (i) descrição da natureza da violação; (ii) as categorias e margem de titulares afetados[450]; (iii) categorias e média de bancos de dados afetados[451]; (iv) nome e

---

[448] *Conhecimento da violação de dados pessoais:* "[...] O GT29 considera que se deve considerar que um responsável pelo tratamento teve <<conhecimento>> quando tem um grau razoável de certeza de que ocorreu um incidente de segurança que afetou dados pessoais. [...] Nalguns casos, será relativamente claro desde o início se ocorreu uma violação, ao passo que noutros poderá ser necessário algum tempo para apurar se foram afetados dados pessoais. No entanto a ênfase deve estar na ação imediata para investigar um incidente, a fim de determinar se os dados pessoais foram de facto violados e, em caso afirmativo, tomar medidas de reparação e notificar, se necessário" (GT29. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017 e Revistas e adotadas pela última vez em 6 de fevereiro de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf>. Acesso em: 21 jul. 2019. p. 11).

[449] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016, do Parlamento Europeu e Conselho.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 21 jul. 2019.

[450] *Categorias de titulares de dados pessoais:* "[...] O GT29 sugere que as categorias de titular de dados digam respeito aos vários tipos de pessoas singulares cujos dados pessoais foram afetados por uma violação: dependendo dos descritores utilizados, pode incluir, entre outros, crianças e outros grupos vulneráveis, pessoas com deficiência, trabalhadores ou clientes [...]". (GT29. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679**, adotadas em 3 de outubro de 2017 e Revistas e adotadas pela última vez em 6 de fevereiro de 2018. Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf>. Acesso em: 21 jul. 2019. p. 15).

[451] *Categorias de registros de dados pessoais*: "[...] podem referir-se a diferentes tipos de registros que o responsável pelo tratamento pode tratar, como dados relativos à saúde, registros escolares informações relativas à ação social dados financeiros, números de contas bancárias, números de passaporte, etc.". (Ibid., p. 15).

contato dos encarregados pela proteção; (v) consequências prováveis da violação; e (vi) medidas de reparação e medidas atenuantes tomadas (art. 33, n.º 3)[452].

O Regulamento finaliza esta medida de segurança estendendo ao responsável pelo tratamento (ou subcontratante) a prestação de todas as informações em parcelas, se impossível fornecê-las imediata e simultaneamente (art. 33, n.º 4). Também determina que sejam documentadas quaisquer violações, efeitos e medidas tomadas para posterior análise de autoridade (art. 33, n.º 5)[453].

No tocante à comunicação de violação de dados pessoais ao titular dos dados, O RGPD, intensificando sua preocupação com os cidadãos, determina que, havendo violação de dados pessoais e havendo perigo de risco elevado para os direitos e liberdades dos seus titulares, a própria pessoa singular deverá ser notificada, sem demora injustificada, pelo responsável pelo tratamento (art. 34, n.º 1)[454]. Presume-se aqui seu direito à informação para tomada das medidas cabíveis.

Os requisitos a serem observados nesta notificação ao titular prejudicado não diferem muito dos solicitados à notificação à autoridade de controle, exigindo além daqueles, a descrição em linguagem aclarada e simplória da natureza da violação de dados pessoais, dispensando ciência apenas das categorias de titulares de dados pessoais e categorias de registros de dados pessoais (art. 34, n.º 2)[455].

O RGPD cria tríplice condição nas quais este dever de comunicação ao titular é dispensado; quais sejam: (i) aplicação de medidas capazes de impedir terceiros de compreender referidos dados; (ii) aplicação de tratamento que garanta a extinção do risco elevado aos direitos e liberdades dos titulares; e (iii) implicação de esforço desproporcional, bastando comunicação pública eficaz (art. 34, n.º 3, “a” a “c”)[456].

Na hipótese de violação constatada e notificação ao titular não realizada pelo responsável pelo tratamento, percebendo provável risco elevado aos direitos e liberdades daquele, a autoridade de controle, fazendo uso da sua cadeia de comando,

---

[452] Regulamento n.º 679, de 27 de abril de 2016, op. cit., não paginado.
[453] Regulamento n.º 679, de 27 de abril de 2016, op. cit., não paginado.
[454] Regulamento n.º 679, de 27 de abril de 2016, op. cit., não paginado.
[455] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016, do Parlamento Europeu e Conselho.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 21 jul. 2019.
[456] Ibid., não paginado.

pode exigir do responsável que proceda à notificação, bem como pode concluir pela sua desnecessidade (art. 34, n.º 4)[457].

Questão interessante diz respeito às investigações policiais acerca das circunstâncias da violação de dados pessoais, uma vez que a divulgação precoce de informações pode dificultar o processo de apuração dos fatos (considerando n.º 88)[458]. Neste sentido, o GT29 sugere que o responsável deve atrasar a notificação até o findar das investigações, mas fazê-la imediatamente após a conclusão delas[459].

### 3.7 Avaliação de impacto sobre a proteção de dados

O RGPD não conceituou o que seja a Avaliação de Impacto sobre a Proteção de Dados (AIPD) na sua relação de categorias operacionais (art. 4º). Todavia, o GT29 a define como sendo um "processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais [...]"[460].

Segundo a legislação, a AIPD deve ser realizada especialmente nos casos que envolva um tratamento (ou conjunto semelhante deles) de dados pessoais (e/ou sensíveis) baseado em novas tecnologias que possam surtir elevados riscos aos direitos e liberdades dos seus titulares. Deve considerar, para este intento preventivo, critérios como natureza, âmbito, contexto, destinação, tecnologia disponível e custos de aplicação (art. 35, n.º 1, e, considerações n.º 84 e 90)[461].

Destaca-se que, apesar de a AIPD ser realizada antes do início do tratamento dos dados pessoais, este processo avaliativo é contínuo, pois dinâmico também é o

---

457 Ibid., não paginado.
458 Ibid., não paginado.
459 GT29. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679**, adotadas em 3 de outubro de 2017 e Revistas e adotadas pela última vez em 6 de fevereiro de 2018. Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf>. Acesso em: 21 jul. 2019. p. 17.
460 GT29. **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**, adotadas em 4 de abril de 2017; Revistas e adotadas pela última vez em 4 de outubro de 2017. Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf>. Acesso em: 21 jul. 2019. p. 4.
461 UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016, do Parlamento Europeu e Conselho.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 21 jul. 2019.

avanço das tecnologias, seja para o tratamento de dados, seja para o cometimento de violações maliciosas. É preciso que a AIPD esteja sujeita a mudanças[462], mesmo porque ao efetuar uma avaliação se requer o máximo de informação disponível, inclusive pareceres dos encarregados da proteção de dados (art. 35, n.º 2)[463].

A realização de uma AIPD não é sempre necessária. Mas será obrigatória nos casos de: (i) avaliação sistemática de aspectos individuais relativos aos titulares, inclusa a definição de perfis, quando para produzirem efeitos jurídicos; (ii) operações de tratamento em escala massiva de categorias especiais de dados sensíveis (art. 9, n.º 1) e dados penais e infracionais (art. 10); ou (iii) controle sistemático de zonas acessíveis ao público em grande escala (art. 35, n.º 3, "a" a "c")[464].

Sugere o GT29 que esse rol de situações obrigatórias não é exaustivo e elenca uma série de nove critérios para que sejam avaliados se o tratamento de dados pessoais pode efetivamente implicar em elevado risco aos seus titulares. As hipóteses referidas são baseadas em disposições iniciais (considerandos n.º 71, 75 e 91) e disposições específicas de segurança de dados pessoais (arts. 35, n.º 1 e 3, "a" a "c") do RGPD.

São eles: (i) avaliação e classificação; (ii) decisões automatizadas com efeitos jurídicos; (iii) controle sistemático; (iv) dados sensíveis ou muito pessoais; (v) dados tratados em grande escala; (vi) aclaramento de correspondências ou combinação de conjuntos de dados; (vii) dados relativos a titulares vulneráveis; (viii) soluções inovadoras ou aplicação de soluções tecnológicas ou organizacionais; e (ix) não exercer direito, contratar ou usar serviço[465].

O RGPD determina que a autoridade de controle elabore e publicite listagem de operações de tratamento sujeitas ao requisito da AIPD (art. 35, n.º 4), bem como listagem de operações de tratamento não obrigatória de análise pela AIPD (art. 35, n.º 5), devendo sê-las comunicadas ao Comitê (art. 68). E, antes de serem adotadas

---

462 GT29, op. cit., p. 17.
463 Regulamento n.º 679/2016, op. cit., não paginado.
464 Regulamento n.º 679/2016, op. cit., não paginado.
465 GT29. **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**, adotadas em 4 de abril de 2017; Revistas e adotadas pela última vez em 4 de outubro de 2017. Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf>. Acesso em: 21 jul. 2019. p. 10-12.

referidas listagens, a autoridade efetuará um controle de coerência (art. 63), se houver bens, serviços ou definições em questão (art. 35, n.º 6)[466].

Ademais, o RGPD demanda que a avaliação inclua ao menos (i) uma decisão sistemática, o interesse e a finalidade das operações de tratamento; (ii) uma avaliação da necessidade e proporcionalidade delas em relação aos seus objetivos; (iii) uma avaliação dos riscos aos direitos e liberdades dos titulares; e (iv) as medidas e procedimentos de combate os riscos para proteção dos dados pessoais e conformação com as disposições legais (art. 35, n.º 7)[467].

Responsáveis pelo tratamento (e subcontratantes) devem ainda cumprir as diretrizes do Código de Conduta (art. 40) para realização de uma AIPD (art. 35, n.º 8); podem solicitar opiniões dos titulares (ou seus representantes) se adequado à situação (art. 35, n.º 9)[468]; e detém certa flexibilidade para considerar satisfatório o tratamento com aprovação de um critério, em que pese o GT29 sugira orientação no sentido de haja aprovação de vários critérios[469].

### 3.8 Consulta prévia

Como abordado antes, o RGPD exige a realização de uma AIPD quando a operação de tratamento de dados pessoais implicar elevado risco para os direitos e liberdades das pessoas singulares. O responsável pelo tratamento dos dados avalia os riscos e identifica medidas para saná-los/atenuá-los, entretanto, existem casos nos quais precisará consultar a autoridade de controle (art. 36, n.º 1)[470].

Quando da consulta, o responsável pelo tratamento deve comunicar à autoridade de controle alguns elementos: (i) repartição de obrigações entre responsável, corresponsável e subcontratante; (ii) finalidades e meios de tratamento

---

[466] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016, do Parlamento Europeu e Conselho.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 21 jul. 2019.

[467] Ibid., não paginado.

[468] Ibid., não paginado.

[469] GT29, op. cit., p. 12.

[470] UNIÃO EUROPEIA. **Regulamento n.º 679, de 27 de abril de 2016, do Parlamento Europeu e Conselho.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 21 jul. 2019.

previstos; (iii) medidas e garantias previstas; (iv) os contatos dos EPDs; (v) a AIPD prevista; e (vi) eventuais informações solicitadas (art. 36, n.º 3, “a” a “e”)[471].

É perceptível a hierarquia de comando nesta medida de segurança de dados. Mesmo que não consultada, se a autoridade de controle considerar que o responsável pelo tratamento (ou subcontratante) não identificou ou suficientemente atenuou os riscos de violação de dados pessoais, expedirá ela própria orientações para tomada de providência no prazo máximo de 08 (oito) semanas (art. 36, n.º 2)[472].

Os próprios Estados Membros podem consultar a autoridade de controle durante a elaboração de medida legislativa ou medida regulamentar baseada nesta, se estiver relacionada com o tratamento de dados pessoais (art. 36, n.º 4). Podem, inclusive, ordenar que os responsáveis pelo tratamento de interesse público a consultem para obtenção de autorização prévia (art. 36, n.º 5)[473].

Imperioso ressaltar que este instituto da consulta prévia não se confunde com o direito de acesso (art. 15) do RGPD, segundo o qual o titular dos dados possui a faculdade de obter do controlador uma confirmação sobre se os dados pessoais referentes à sua pessoa estão sendo processados ou não e, em caso afirmativo, solicitar acesso aos respectivos dados pessoais.

Ademais, uma das principais vantagens em se estudar estas ferramentas jurídico-tecnológicas reside no seu grande potencial preventivo e paliativo em relação às mazelas causadas pelas violações de proteção de dados pessoais. Muitas delas são criações modernas desenvolvidas para combate a problemas cada vez mais complexos, futurísticos e perigosos.

Como consabido, não há maiores dúvidas que existe um descompasso entre o avanço informacional e a evolução legislativa aplicável, razão pela qual o estudo das disparidades e das aproximações da temática entre ambos contribui para diminuição deste abismo cada vez mais evidente. A discussão ganha ainda reforço quando a preocupação com a proteção de dados pessoais se torna globalizada.

E um dos atuais focos de atenção à problemática, como já adiantado em linhas anteriores, é o cenário latino-americano e, em especial, o panorama mercosurenho e de seus países integrantes. Neste desiderato, o próximo capítulo trabalhará a questão

---

471 Ibid., não paginado.
472 Ibid., não paginado.
473 Ibid., não paginado.

da proteção de dados pessoais com este direcionamento, seguindo abordagem mais investigativa e comparativa.

# 4 ADOÇÃO DE NORMA REGIONAL NO MERCOSUL À LUZ DO RGPD

Os princípios explorados no primeiro capítulo, bem como os direitos e institutos investigados no segundo capítulo, constituem o arcabouço jurídico e os mecanismos securitários que protegem os dados pessoais dos ciberconsumidores e servem para compreensão e interpretação de critérios técnicos que serão utilizados para comparação das legislações protetivas de dados pessoais neste capítulo.

Portanto, neste capítulo será feito uma contextualização sobre a proteção de dados pessoais na América Latina, acompanhada de breve introdução da criação e da estrutura do MERCOSUL, bem como de uma investigação da produção legislativa mercosurenha sobre defesa do consumidor, comércio eletrônico e proteção de dados pessoais.

Na sequência, serão verificados os direitos internos argentino, brasileiro, paraguaio e uruguaio a respeito das suas legislações consumerista e protetiva de dados pessoais e, como estudo paralelo, também dos países falantes de língua portuguesa. Por derradeiro, será analisada, comparada e discutida a formulação de uma norma, no âmbito do MERCOSUL, seguindo os moldes do RGPD.

## 4.1 Proteção de dados pessoais na América Latina

Enquanto os europeus debatiam e otimizavam seu sistema de proteção de dados pessoais, a América Latina engatinhava nas discussões e regulamentações da matéria. Dispunha-se mais de resquícios de defesa civilista e consumerista em tempos pretéritos, com enfoque na proteção da privacidade particular e familiar e das correspondências. Posteriormente à produção legislativa europeia da terceira geração é que maiores avanços são percebidos.

Segundo Carrasquilla, o sistema de proteção de dados pessoais na América Latina possui uma particularidade que o diferencia dos modelos europeus, pois nela “inexiste um tratado internacional ou regulamento regional supranacional (nem no MERCOSUL nem na CAN) que regule a proteção dos dados pessoais ou a

transferência deles"[474], mesmo considerando que os sistemas legais latino-americanos compartilham a tradição do direito civil continental europeu[475].

O que predomina aqui, no entanto, é um reconhecimento constitucional do direito à proteção de dados. As constituições nacionais da região costumam incorporar, além do direito à privacidade, o recurso chamado de *habeas data*[476] - um instrumento à disposição dos cidadãos para acesso, conferência e transparência de informações governamentais ou públicas que lhes digam respeito -, ferramenta que faz às vezes do direito à consulta europeu.

Como exemplar primevo da proteção de dados, igualmente válido para dados pessoais em vista de sua amplitude, o *habeas data* esteve presente antes nas constituições da Argentina, Brasil, Colômbia, México, Peru e da Venezuela[477] - com pioneirismo devido aos brasileiros – e depois se enraizou para outras constituições vizinhas e se especializou conforme a tipagem do banco de dados nos quais estejam os dados disponíveis (privado ou público).

Em que pese as constituições latino-americanas não tenham previsões tão específicas sobre proteção de dados pessoais, não quer dizer que não tenham delimitado e protegido a matéria; dispuseram, em síntese, sobre acesso aos bancos de dados públicos e privados, de ciência à finalidade e destinação dos dados, além de atualização, retificação, supressão, destruição, cancelamento, confidencialidade, oposição, tratamento, circulação e recolocação dos dados[478].

---

474 CARRASQUILLA, Lorenzo Villegas. ***Protección de datos personales en América Latina:*** *retención y tratamiento de datos personales en el mundo de Internet. Capítulo tres.* p. 125-164. In: *Hacia una internet de censura: propuestas para América Latina* / compilado por Bertoni. – 1a. ed. – Buenos Aires: Universidad de Palermo – UP, 2012. Disponível em: <https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf>. Acesso em: 23 jul. 2019. p. 136-137 (tradução nossa).

475 SILVA, Alberto Jacob Cerda. ***Protección de datos personales y prestación de servicios en línea en América Latina.*** *Capítulo cuatro.* p. 165-180. In: *Hacia una internet de censura: propuestas para América Latina* / compilado por Bertoni. – 1a. ed. – Buenos Aires: Universidad de Palermo – UP, 2012. Disponível em:<https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf>. Acesso em: 23 jul. 2019. p. 167-168.

476 *Hebeas Data:* "[...] Literalmente: tenha os dados [...] Esta expressão, habeas data, é uma inovação de nossa Constituição Federal de 1988 (art. 5º, LXXII, a e b), que a criou com a finalidade de assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, ou para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo. [...]". (SANTOS, Washington dos. **Dicionário jurídico brasileiro**. – Belo Horizonte: Del Rey, 2001, p. 287).

477 MILANES, Valeria. ***El sistema de protección de datos personales em América Latina:*** *Oportunidades y desafíos para l os derechos humanos.* Volumen I. Córdoba: ADC, 2016. p. 5-40 Disponível em: <https://adcdigital.org.ar/wp-content/uploads/2017/06/Sistema-proteccion-datos-personales-LatAm.pdf>. Acesso em: 23 jul. 2019. p. 13.

478 VILLEGAS CARRASQUILLA, Lorenzo. ***Protección de datos personales en América Latina:*** *retención y tratamiento de datos personales en el mundo de Internet. Capítulo tres*. p. 125-164. In:

Angarita elaborou um completo mapa sobre a proteção de dados pessoais latino-americana, contendo as normas constitucionais e infraconstitucionais de 1985 a fevereiro de 2014 vigentes na região[479], as quais seguem transcritas alfabeticamente: Argentina (CN/1994, art. 43, Lei n.º 25.326/200 e Decreto 1.558/2001); Bolívia (CN/2004, art. 130); Brasil (CN/1988, art. 5º, "LXXII"); e Chile (Lei n.º 19.628/1999, Lei n.º 19.812/2002 e Lei n.º 20.575/2012).

Sequencialmente: Colômbia (CN/1991, art. 15 e Lei n.º 1.581/2012); Costa Rica (Lei n.º 8.968/2011); Equador (CN/1998, art. 94, CN/2008, arts. 66 e 92); Guatemala (CN/1985, art. 31); Honduras (CN/2005, art. 182); México (CN/2007, art. 6, CN/2009, art. 16 e Leis Federais de 2002 e 2010); Nicarágua (CN/1987, art. 26, Lei n.º 787/2012 e Decreto n.º 36/2012); Panamá (CN/2004, arts. 42 e 44); e Paraguai (CN/1992, art. 135, Lei n.º 1.682/2001 e Lei n.º 1.691/2002).

E, para concluir: Peru (CN/1993, arts. 2 e 200, Lei n.º 29.733/2011 e Decreto n.º 003/2013/JUS); República Dominicana (CN/2010, arts. 44 e 70 e Lei n.º 172/2013); Uruguai (Lei n.º 18.331/2008 e Decreto n.º 414/2009); e Venezuela (CN/1999, arts. 28 e 281). O estudo compilado, obviamente, não compreende todos os países da América Latina (20 países foram incluídos), assim como não contempla dispositivos, legislações e constituições supervenientes ao período analisado.

Pese ao exposto, as conclusões de Angarita são deveras interessantes: (i) "70% dos países da América Latina incorporaram em suas constituições disposições explícitas relativas aos aspectos relacionados com a proteção pessoal de dados" e que (ii) "100% das previsões constitucionais incorporaram o direito de acesso aos dados pessoais pelo titular e 92,85% mencionaram explicitamente os 'dados pessoais' ou 'informação pessoal'"[480]. Isto demonstra uma média acima do esperado.

Seus estudos estatísticos ainda revelam que (iii) "85,71% estabeleceram o direito do titular de solicitar retificação ou correção de informações, enquanto 64,28% garantiram o direito constitucional de solicitar a supressão, eliminação, destruição ou

---

*Hacia una internet de censura: propuestas para América Latina* / compilado por Bertoni. – 1a. ed. – Buenos Aires: Universidad de Palermo – UP, 2012. Disponível em: <https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf>. Acesso em: 23 jul. 2019. p. 137-138.

479 REMOLINA ANGARITA, Nelson. ***Mapa Latinoamericano sobre la protección de datos personales:*** *Constituciones y normas generales (1985-2014/Feb)*. In: *Latin America and protection of personal data: facts and figures.* Bogotá: Universidade de Los Andes. Disponível em: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/2014-marcha-Latin-America-data-protection-1985-2012-facts-and-figures-Remolina.pdf>. Acesso em: 23 jul. 2019. p. 7.

480 Ibid., p. 2. (tradução nossa).

cancelamento de dados pessoais" e que (iv) "64,28% consideram a atualização da informação como um direito do titular de dados"[481]. Conquanto acima de 50% é perceptível uma significativa diminuição na presença destes direitos.

Outros números aferíveis são que (v) "57,14% estabeleceram o 'habeas data' e 7,14% a 'ação de amparo' e a 'ação de proteção de privacidade'"; que (vi) "50% incorporaram o direito a saber a finalidade por trás do processamento dos dados pessoais e 21,42% o direito de saber o uso desse tipo de informação"; que (vii) "28,57% consideram a confidencialidade de dados pessoais um direito humano" e que (viii) "14,28% classificam a proteção de dados pessoais expressamente"[482].

Sobre as legislações de proteção de dados, o estudo permite concluir ainda que (ix) "100% dos países possuem leis de proteção de dados setoriais, entre outros, registros médicos e censo populacional"; que (x) "50% deles têm leis abrangentes de proteção de dados"; que (xi) "100% das leis gerais de proteção de dados regem a transferência internacional de dados pessoais, mas só 12,5% se referem à coleta internacional de informações pessoais"[483].

Os números indicam uma maior preocupação dos países latino-americanos com a proteção de dados gerais, muito embora alguns deles esbocem constitucionalmente menções e instituam medidas à proteção de dados pessoais ou a alguns dos direitos a ela inerentes. Uma última constatação é que no período de 2010-2014, o número de leis protetivas de dados gerais aumentou significativamente e que a legislação europeia foi a maior influência na América Latina[484].

Em verdade, a tendência de os países latino-americanos preferirem legislar inicialmente no plano constitucional sobre proteção de dados pessoais (e também não pessoais), englobando-os como direitos fundamentais, remete mais às estruturas constitucionais espanhola e portuguesa e, por lógica histórica e geográfica, ao processo de colonização/exploração destes países na região, do que a um alinhamento direto com os documentos internacionais.

---

[481] REMOLINA ANGARITA, Nelson. ***Mapa Latinoamericano sobre la protección de datos personales:*** *Constituciones y normas generales (1985-2014/Feb)*. In: *Latin America and protection of personal data: facts and figures.* Bogotá: Universidade de Los Andes. Disponível em: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/2014-marcha-Latin-America-data-protection-1985-2012-facts-and-figures-Remolina.pdf>. Acesso em: 23 jul. 2019. p. 3. (tradução nossa).
[482] Ibid., p. 3-4. (tradução nossa).
[483] Ibid., p. 6. (tradução nossa).
[484] Ibid., p. 6.

Destaca Milanes que este constitucionalismo latino-americano com enfoque protetivo se deve a três principais fatores: (i) ao reconhecimento do direito à proteção de dados pessoais como direito autônomo; (ii) à concessão de remédios constitucionais para a referida proteção; e (iii) ao reconhecimento legal e concessão de ações não unicamente relacionadas ao setor público, mas também contra atores não estatais, seguindo a tradição constitucional europeia[485].

Como baluarte deste processo cabe mencionar os seguintes conjuntos de princípios e guias elaborados por diversos organismos e instâncias internacionais, elencados por Milanes[486]: (i) Diretrizes sobre Arquivos Informatizados de Dados Pessoais para resolução pela Assembleia Geral da Organização das Nações Unidas[487]; (ii) Resolução sobre Privacidade na Era Digital adotada pela Assembleia Geral da Organização das Nações Unidas (2016)[488]. Continuando: (iii) Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais da Organização para Cooperação e Desenvolvimento Econômico (OCDE, publicada em 1980 e atualizada em 2013)[489]; (iv) Proposta de Declaração de Princípios de Privacidade e Proteção de Dados Pessoais nas Américas, adotada pelo Comitê Jurídico Interamericano da Organização dos Estados Americanos[490].

E, ainda: (v) Marco de Privacidade para a Organização Internacional de Cooperação Econômica da Ásia-Pacífico (APEC)[491]; (vi) Considerações de privacidade para protocolos da Internet, solicitação de comentários n.º 6973 (RFC) do

---

485 MILANES, Valeria. **El sistema de protección de datos personales em América Latina:** Oportunidades y desafíos para l os derechos humanos. Volumen I. Córdoba: ADC, 2016. p. 5-40 Disponível em: <https://adcdigital.org.ar/wp-content/uploads/2017/06/Sistema-proteccion-datos-personales-LatAm.pdf>. Acesso em: 23 jul. 2019. p. 13.

486 Ibid., p. 10-11.

487 UNITED NATIONS. General Assembly. **A/RES/45/95, 68th plenary meeting, 14 December 1990,** Guidelines for the regulation of computerized personal data files. Disponível em: <https://www.un.org/documents/ga/res/45/a45r095.htm>. Acesso em 24 jul. 2019.

488 Id. General Assembly. **A/C.3/71/L.39/Rev.1, Seventy-first session, Third Committee, Agenda item 68 (b), 16 November 2016,** The right to privacy in the digital age. Disponível em: <https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1>. Acesso em: 24 jul. 2019.

489 ORGANISATION FOR EUROPEAN ECONOMIC CO-OPERATION (OCDE). **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. Acesso em: 24 jul. 2019.

490 Id. **OEA/Ser.Q, CJI/doc. 474/15 rev.2, 26 marzo 2015**, Informe del Comité Jurídico Interamericano - Privacidad y Protección de Datos Personales. Disponível em: <http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf>. Acesso em: 24 jul. 2019.

491 ASIA-PACIFIC ECONOMIC COOPERATION (APEC). **APEC#205-SO-01.2, December 2005**. Privacy Framework. Disponível em: <http://bit.ly/1zRV0QK>. Acesso em: 24 jul. 2019.

*Internet Engineering Working Group* (IETF)[492]; (vii) Padrões Internacionais de Proteção de Dados Pessoais e Privacidade adotados na 31ª Conferência Internacional de Proteção de Dados e Autoridades de Privacidade[493]. Adiante e ao arremate: (viii) Padrões de Privacidade em um Mundo Global - Declaração da Sociedade Civil (Madri, Espanha, 2009)[494].

Deixa claro a autora que as influências citadas não são exaustivas e, certamente, como já esclarecido nos capítulos anteriores, o impacto da Diretiva n.º 46/1995/CE e de seu substituto, o Regulamento (UE) n.º 679/2016, estimularam sobremaneira o avanço legislativo dos países latino-americanos na matéria. Neste sentido, comenta Silva:

> O modelo latino-americano de proteção de dados pessoais está em um estágio de transição. Anos atrás, verificava-se através de dispositivos constitucionais, aos quais foi incorporado maior ou menor número de leis, o que tornou uma regulação fragmentária e por vezes inconsistentes. Hoje, nas principais economias da região, essa proteção constitucional se sobrepõe a uma regra geral que regula o processamento de informações pessoais, seja ela privada ou não. Como resultado dessa sobreposição de medidas constitucionais e legais, a proteção de dados pessoais parece fortalecida na América Latina, embora seja necessário fortalecer a aplicação efetiva da lei.[495]

Mesmo que haja uma sensação de atraso, mister reiterar a criação da Rede Iberoamericana de Proteção de Dados (RIPD - 2003), efetivado na XIII Reunião de Cúpula, em Santa Cruz de la Sierra – Bolívia. Trata-se de instituição com natureza de fórum de discussão direta e de aprovação de decisões e documentos sobre proteção

---

[492] INTERNET ENGINEERING WORKING GROUP (IETF). **RFC n.º 6973, July 2013.** Privacy Considerations for Internet Protocols. Disponível em: <https://tools.ietf.org/html/rfc6973>. Acesso em: 24 jul. 2019.

[493] CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD. **Resolución de Madrid, 5 de Noviembre de 2009.** Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf>. Acesso em: 24 jul. 2019.

[494] ESPAÑA. **La Declaración de la Sociedad Civil, 3 de Noviembre de 2009.** Estándares de Privacidad en un Mundo Global. Disponível em: <https://thepublicvoice.org/madrid-declaration/es/>. Acesso em: 24 jul. 2019.

[495] SILVA, Alberto Jacob Cerda. ***Protección de datos personales y prestación de servicios en línea en América Latina.*** *Capítulo cuatro.* p. 165-180. In: *Hacia una internet de censura: propuestas para América Latina* / compilado por Bertoni. – 1a. ed. – Buenos Aires: Universidad de Palermo – UP, 2012. Disponível em:<https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf>. Acesso em: 24 jul. 2019. p. 170.

de dados; além de promover ainda encontros anuais, seminários, *workshops* e diversas outras atividades relacionadas[496].

Como mencionado no capítulo inicial, no 15º Encontro Ibero-Americano de Proteção de Dados (2017), que foi organizado pela RIPB e pelo Conselho de Transparência do Chile, aprovou-se o chamado "Padrões de Proteção de Dados Pessoais para os Estados Ibero-Americanos", alcançando a meta estipulada ao cumprimento do acordo relacionado à criação de proposta cooperativa de proteção de dados pessoais adotado, na XXV Cúpula Ibero-Americana na Colômbia (2016).

Este conjunto de diretrizes almeja a realização de iniciativas regulatórias de proteção de dados pessoais aos países integrantes que não contenham legislações sobre a temática, cumprindo desta forma a premissa estratégica convencionada pela RIPD (2016), plasmada no documento "RIPD 2020", aprovado em Montevidéu, que estimula o fortalecimento e a adequação dos processos regulatórios na região mediante parametrizações.

Neste documento padronizador, reitera-se uma vez mais, atribui-se *status* de direito fundamental à proteção de dados pessoais (1ª Consideração), assegurando a integridade dos direitos e liberdades fundamentais à vida privada, familiar e intimidade (2ª Consideração), em caráter altamente prioritário (11ª Consideração), com ressalvas ao interesse público e de terceiros, quando não constatadas arbitrariedades, e com respeito aos ideais democráticos (12ª Consideração)[497].

## 4.2 Proteção de dados pessoais no MERCOSUL

Tendo em vista a rápida contextualização da situação protetiva de dados pessoais na América Latina realizada, investiga-se melhor agora a produção legislativa do MERCOSUL sobre proteção de dados pessoais que, conforme será explorado, é bastante relacionada com a defesa do consumidor, com o comércio eletrônico, com políticas regionais e processos harmonizadores normativos.

---

[496] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Encontros Ibero-Americanos.** Iniciação. Disponível em: <http://www.redipd.org/actividades/encuentros/index-idpt-idphp.php>. Acesso em: 14 mar. 2019.

[497] REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Padrões de Proteção de Dados Pessoais para os Estados Ibero-Americanos, de 20 de junho de 2017.** Disponível em: < http://www.redipd.es/documentacion/common/Estandares_PORTUGUES.pdf>. Acesso em: 15 mar. 2019.

Dedica-se antes, com objetivo de localizar e delimitar a temática, à breve introdução sobre o histórico de criação e estrutura institucional do MERCOSUL e esclarecimentos a respeito dos seus membros fundantes e suspensos, das nações em processo de adesão e das nações associadas, para então seguir explorando a produção legislativa de proteção de dados pessoais do bloco.

### 4.2.1 Histórico de criação e estrutura institucional do MERCOSUL

O MERCOSUL é um bloco econômico que surgiu por iniciativa da integração regional da América Latina no final da década de 1980[498]. Foi criado em 1991, pelo Tratado de Assunção[499], mas somente em 1995, com a vigência do Protocolo de Ouro Preto, é que os Estados Partes criaram sua personalidade jurídica. Trata-se agora de uma Organização Internacional[500].

O MERCOSUL teve como membros fundantes a Argentina, Brasil, Paraguai e Uruguai e tem como objetivos gerais (i) a livre circulação de bens, serviços e fatores produtivo; (ii) o estabelecimento de uma tarifa externa comum; (iii) a adoção de uma política comercial comum; (iv) a coordenação de políticas macroeconômicas e setoriais; e (v) o compromisso de harmonização legislativa (art. 1º)[501].

Promove ainda ações para alcançar, como objetivos específicos, (i) o aumento e diversificação de bens e serviços com padrões mútuos de qualidade; (ii) o fomento científico e tecnológico coordenado; (iii) o desenvolvimento sustentável dos recursos regionais através de pautas comuns; e (iv) o aumento da participação dos setores privados no processo de integração[502].

Houve, com motivações distintas, o processo de adesão da Venezuela ao MERCOSUL, que teve seu início em 2005. Buscava-se, segundo Varella, uma complementação econômica e novos incentivos para uma maior integração

---

498 MERCOSUL. **Composição, objetivos e estrutura institucional.** Disponível em: <http://www.mercosul.gov.br/saiba-mais-sobre-o-mercosul>. Acesso em: 17 jul. 2019.
499 TRATADO de Assunção. **Tratado para a constituição de um Mercado Comum entre a República Argentina, a República Federativa do Brasil, a República do Paraguai e a República Oriental do Uruguai, de 26 de março de 1991.** Disponível em: <http://www.rau.edu.uy/mercosur/tratapt.htm>. Acesso em: 17 jul. 2019.
500 VARELLA, Marcelo D. **Direito internacional público.** – 6. ed. – São Paulo: Saraiva, 2016. p. 387.
501 Tratado de Assunção, op. cit., não paginado.
502 REIS, Jair Teixeira de. **Resumo de direito internacional e comunitário.** 3. ed. – Niterói: Impetus, 2011. p. 145-146.

regional[503]. Foi um longo processo de adesão e que restou concluído apenas com a Decisão CMC n.º 27/2012[504], quando lhe foi concedida a condição de Estado-Parte.

A ratificação do Protocolo de Adesão da República Bolivariana da Venezuela ao MERCOSUL veio anos depois (04/07/2016)[505], mas não tardou para que os Estados Partes decidissem suspendê-la (12/2016)[506], por tempo indeterminado, diante do seu descumprimento à cláusula de compromisso democrático do Protocolo de Ushuaia (art. 4º)[507], perdendo seus direitos de participação no bloco econômico.

A Bolívia está atualmente em processo de adesão, já contando com a aprovação dos Chefes de Estado[508]. Colômbia, Chile, Equador, Peru, Guiana e Suriname não são integrantes do MERCOSUL, contudo, possuem acordos de Complementação Econômica com o bloco para redução tarifária em diversos setores, mantendo, portanto, a condição de Estados Associados[509].

A estrutura institucional do MERCOSUL, com as alterações realizadas pelo Protocolo de Ouro Preto, é composta por órgãos decisórios e órgãos não decisórios. Os com capacidade decisória são o Conselho do Mercado Comum (CMC), o Grupo de Mercado Comum (GMC) e a Comissão de Comércio do MERCOSUL (CCM). Os sem capacidade decisória são o Parlamento do MERCOSUL (PARLASUL), o Foro Consultivo Econômico-Social (FCES), a Secretaria Administrativa do MERCOSUL (SAM), o Tribunal Permanente de Revisão (TPR) e o Instituto de Políticas Públicas em Direitos Humanos do MERCOSUL (IPPDH)[510].

O Protocolo Adicional ao Tratado de Assunção, dispôs ainda sobre a possibilidade de criação de órgãos auxiliares para consecução dos objetivos do

---

503 VARELLA, op. cit., p. 387-388.
504 MERCOSUL. **CMC/DEC n.º 27, de 30 de julho de 2012.** Adesão da República da Venezuela ao Mercosul. Disponível em: <http://www.mdic.gov.br/arquivos/dwnl_1377717164.pdf>. Acesso em: 18 jul. 2019.
505 Id. **Protocolo de adesão da República Bolivariana da Venezuela ao MERCOSUL**. Disponível em: <http://www.mdic.gov.br/arquivos/dwnl_1377717219.pdf>. Acesso em: 18 jul. 2019.
506 MERCOSUL. **Decisão sobre a suspensão da Venezuela no MERCOSUL**. Disponível em: <https://www.mercosur.int/pt-br/decisao-sobre-a-suspensao-da-republica-bolivariana-da-venezuela-no-mercosul/>. Acesso em: 18 jul. 2019.
507 Id. **Protocolo de Ushuaia sobre compromisso democrático no Mercosul, Bolívia e Chile.** Disponível em: <https://www.mercosur.int/documento/protocolo-de-ushuaia-sobre-compromisso-democratico-no-mercosul-bolivia-e-chile/>. Acesso em: 20 jul. 2019.
508 O Uruguai depositou o Instrumento de Ratificação do Protocolo de Adesão do Estado Plurinacional da Bolívia ao MERCOSUL em 17/05/2017. O Paraguai depositou referido Instrumento de Ratificação em 13/08/2018. Brasil e Argentina ainda não ratificaram o Protocolo de Adesão. Disponível em: <http://www.mre.gov.py/tratados/public_web/DetallesTratado.aspx?id=wPEBvbgLt4cMYaxJfUrS/w==&em=lc4aLYHVB0dF+kNrtEvsmZ96BovjLlz0mcrZruYPcn8=>. Acesso em: 30 jul. 2019.
509 VARELLA, Marcelo D. **Direito internacional público.** – 6. ed. – São Paulo: Saraiva, 2016. p. 388.
510 MERCOSUL. **Organograma.** Disponível em: <https://www.mercosur.int/pt-br/quem-somos/organograma-mercosul/>. Acesso em: 30 jul. 2019.

processo de integração (art. 1º, parágrafo único)[511]. Fazem parte da estrutura institucional do MERCOSUL alguns importantes órgãos temáticos como: "Reuniões de Ministros, Subgrupos de Trabalho, Reuniões Especializadas, Grupos "ad hoc", o Comitê de Cooperação Técnica, o Tribunal Arbitral "ad hoc" e os Tribunais Judiciários de cada Estado-parte".[512]

Uma vez que sinteticamente explorado o histórico de criação, os Estados Partes, os parceiros comerciais regionais e a organização do MERCOSUL e diante da necessidade de integração regional, de harmonização legislativa e, em especial para esta dissertação, de proteção do consumidor e de seus dados pessoais, dedica-se agora à análise da produção legislativa do MERCOSUL sobre o tema.

### 4.2.2 Produção legislativa de proteção dados pessoais no MERCOSUL

Considerando que a formação de um bloco econômico em um mundo globalizado pressupõe a proteção do ciberconsumidor[513] como etapa necessária para obtenção da uma integração econômica e que inexiste previsão específica no tratado de constituição do MERCOSUL a este respeito, é evidente que mecanismos protetivos consumeristas precisavam ser desenvolvidos[514].

Relata Vieira que a primeira preocupação do MERCOSUL com o direito do consumidor surgiu com proposta institucional na Reunião de Ministros de Justiça dos Estados Partes (1995)[515]. Todavia, o tema ganhou destaque no âmbito do GMC, com

---

511 Id. **Protocolo de Ouro Preto** - Protocolo Adicional ao Tratado de Assunção sobre a Estrutura Institucional do Mercosul. Disponível em: <http://portal.antaq.gov.br/wp-content/uploads/2016/12/Protocolo-de-Ouro-Preto.pdf>. Acesso em: 18 jul. 2019.

512 KERBER, Gilberto. **Mercosul e Supranacionalidade:** um estudo à luz das legislações constitucionais. Dissertação (Mestrado em Direito). UFSC: Florianópolis, 2000. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/78226/170264.pdf?sequence=1&isAllowed=y>. Acesso em: 30 jul. 2019. p. 30.

513 *Ciberconsumidor:* "[...] o consumidor é um destinatário final contratante, um sujeito mudo que atua a qualquer hora, em qualquer língua, de qualquer idade, identificado por uma chave PIN, por uma assinatura eletrônica, por um número de cartão de crédito ou por impressões biométricas. Para não falar da coletividade de consumidores, que intervêm na relação de consumo, para haver recebido do provedor uma oferta em um CD, em um *spam* por *e-mail*, na televisão, etc." (MARQUES, Cláudia Lima. Proteção do consumidor brasileiro no comércio eletrônico e a chamada nova crise do contrato: por um direito do consumidor aprofundado. In: **Revista de Direito do Consumidor.** N.º 57. Jan./Mar. 2006. p. 36. [tradução nossa]).

514 VIEIRA, Luciane Klein. **La hipervulnerabilidad del consumidor transfronterizo y la función del Derecho Internacional Privado.** – 1 ed. Ciudad Autónoma de Buenos Aires: La Ley, 2017. p. 164.

515 MERCOSUL. **CMC/DEC. n.º 1, de 5 de agosto de 1995.** Reunião de Ministros. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

a criação SGT-10, vinculado à Coordenação de Políticas Macroeconômicas, onde foi criada a Comissão de Estudos do Direito do Consumidor (1993)[516].

Prossegue esclarecendo que referida Comissão foi transformada no Comitê Técnico n.º 7º (CT-7) da CCM, que as competências da Comissão lhe foram transferidas[517] e que, desde sua criação (1995)[518], o CT-7 é o órgão responsável pela proposição de harmonizações legislativas e uniformizações de políticas no MERCOSUL, com relação ao direito do consumidor, cujo trabalho rendeu uma série de projetos protetivos consumeristas[519].

A primeira normativa proposta pelo CT-7, resultante na Resolução n.º 126/1994, recomendava a adoção de medidas de proteção ao consumidor compatíveis com padrões internacionais, o tratamento do consumidor como agente económico vulnerável e a confecção de regulamento sobre a matéria (art. 1º); e que, enquanto não fosse ele aprovado, as leis de cada país seriam aplicáveis (art. 2)[520].

Ficou acordado que o Regulamento do Consumidor do MERCOSUL seria aprovado em capítulos. Neste desiderato, houve proposição de cinco normativas pelo CT-7 que restaram aprovadas pelo GMC. A Resolução n.º 123/1996/GMC regulava questões conceituais consumeristas[521]. A Resolução n.º 124/1996/GMC adotava uma relação não fechada de direitos básicos do consumidor[522]. Por sua vez, a Resolução n.º 125/1996/GMC regulava a proteção à saúde e segurança do consumidor[523]. A Resolução n.º 126/1996/GMC disciplinava o regime de publicidade enganosa e

---

516 VIEIRA, op. cit., 165.

517 *Atribuições do CT-7:* "[...] são discutidos, no âmbito do CT 7, os seguintes temas: a) propostas e projetos para a harmonização de legislações; b) ações de proteção e defesa dos consumidores; c) intercâmbio de informações e know how a respeito de políticas e projetos desenvolvidos pelos Estados; d) elaboração de marcos normativos; e) ações de educação sobre proteção e defesa do consumidor; f) tarefas com o objetivo de aprofundar a integração e melhorar os direitos e interesses dos consumidores da região". (AMARAL JÚNIOR, Alberto do; VIEIRA, Luciane Klein. A proteção internacional do consumidor no Mercosul. In: **Revista de Direito do Consumidor.** vol. 106 – jul-ago 2016. p. 4).

518 MERCOSUL. **CCM/DIR. n.º 1, de 14 de fevereiro de 1995.** Criação de Comitês Técnicos. Disponível: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

519 VIEIRA, Luciane Klein. **La hipervulnerabilidad del consumidor transfronterizo y la función del Derecho Internacional Privado.** – 1 ed. Ciudad Autónoma de Buenos Aires: La Ley, 2017. p. 166.

520 MERCOSUL. **GMC/RES. n.º 126, de 16 de dezembro de 1994.** Defesa do Consumidor. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

521 Id. **GMC/RES. n.º 123, de 14 de dezembro de 1996.** Defesa do consumidor – Conceitos. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

522 Id. **GMC/RES. n.º 124, de 14 de dezembro de 1996.** Defesa do consumidor – Direitos Básicos. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

523 Id **GMC/RES. n.º 125, de 14 de dezembro de 1996.** Defesa do consumidor – Proteção à saúde e segurança do consumidor. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

publicidade comparativa[524]. E, enfim, a Resolução n.º 127/1996/GMC trazia normas tocantes à garantia contratual[525], posteriormente substituída pela Resolução n.º 42/1998/GMC, que regulava a questão do certificado de garantia[526].

Seguiram-nas a Resolução n.º 21/2004/GMC sobre o direito à informação do consumidor nas transações comerciais virtuais[527]; a Resolução n.º 45/2006/GMC sobre publicidade enganosa[528]; a Resolução n.º 01/2010/GMC sobre proteção da saúde e da segurança de consumidores e usuários[529]; e a Resolução n.º 34/2011/GMC, também sobre definições[530], inclusive a de consumidor transfronteiriço[531].

Impende agora verificar o mais atual conteúdo legislativo aprovado pelo GMC sobre a matéria. A investigação normativa pretendida concentrará esforços no pertintente à defesa do ciberconsumidor, do comércio eletrônico e dos dados pessoais. O repositório *online* do órgão armazena atos resolutivos desde 1991 e, portanto, uma análise completa extrapolaria o tempo e espaço disponíveis, razão pela qual a investigação será limitada aos documentos compilados de 2010 a 2019.

Para começar, na já citada Resolução n.º 01/2010/GMC, relativa à proteção da saúde e da segurança de consumidores, tratou-se sobre a periculosidade e nocividade de produtos e serviços disponíveis no mercado, sendo resolvido que devem os fornecedores e nações comunicar, quando cientes estiverem, aos consumidores e

---

524 Id. **GMC/RES. n.º 126, de 14 de dezembro de 1996.** Defesa do consumidor – Publicidade. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

525 MERCOSUL. **GMC/RES. n.º 127, de 14 de dezembro de 1996.** Defesa do consumidor – Garantia contratual. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

526 Id. **GMC/RES. n.º 42, de 08 de dezembro de 1998.** Defesa do consumidor – Garantia contratual. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

527 Id. **GMC/RES. n.º 21, de 08 de outubro de 2004.** Direito à informação do consumidor nas transações comerciais efetuadas através da internet. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

528 Id. **GMC/RES. n.º 45, de 24 de novembro de 2006.** Proteção da Saúde e da Segurança de Consumidores e Usuários – Aspectos Operativos. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

529 Id. **GMC/RES. n.º 01, de 09 de abril de 2010.** Publicidade enganosa. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

530 Id. **GMC/RES. n.º 34, de 16 de dezembro de 2011.** Defesa do Consumidor – Conceitos básciso. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

531 *Consumidor transfronteiriço:* "[...] uma relação de consumo será transfronteiriça quando consumidor e provedor estão domiciliados em Estados distintos, o que configura a internacionalidade do contrato, que pode estar conectada a dois ou mais ordenamentos jurídicos". (VIEIRA, Luciane Klein. **La hipervulnerabilidad del consumidor transfronterizo y la función del Derecho Internacional Privado.** – 1 ed. Ciudad Autónoma de Buenos Aires: La Ley, 2017. p. 69. [tradução nossa]).

autoridades, acerca dos riscos a que estejam sujeitos, bem como investigar e implementar as medidas de notificação previstas (arts. 1º ao 3º)[532].

O documento dispõe sobre o dever de notificação das autoridades e do direito à informação dos consumidores, prerrogativa esta comparável, por exemplo, com o direito do titular de dados pessoais de ser notificado, pelo responsável pelo tratamento (ou subcontratante), em caso de violação de segurança privada. O quesito "proteção à saúde", contudo, não parece ter o condão de se equiparar à proteção dos dados médicos ou genéticos previstos no RGPD.

No ano conseguinte, com a Resolução n.º 34/2011/GMC, foram reajustadas as definições aplicáveis às relações consumeristas nos Estados Partes como parte do processo de atualização e harmonização de legislações na área de defesa do consumidor. Conceitos básicos como os de consumidor, fornecedor, produto, serviço e, técnicos, como os de relação de consumo, dever de informação e oferta vinculante foram discriminados na resolução (art. 1º, "a" a "g")[533].

A resolutiva também esclarece (i) que o nível de proteção do consumidor poderá ser mais elevado nos territórios dos Estados Partes, a critério de cada um, servindo a resolução apenas como nivelação protetiva mínima (art. 2º); e (ii) elenca os órgãos nacionais competentes de cada delegação para implementação da resolução (art. 3º)[534]. A mesma tendência uniformizadora é sentida quanto aos princípios norteadores do direito do consumidor.

Esta modernização e padronização terminológica traz benefícios de ordem prática e jurídica ao evitar imprecisões e equívocos nas operações e relações de consumo causadas por distintas concepções. Contribui, ainda, para que haja maior equidade nas negociações ao tratar cada sujeito, objeto, direito e obrigação consumerista, guardadas suas particularidades, sem prejuízo de interpretação entre as nações mercosurenhas.

Mais recentemente, com a Resolução n.º 18/2018/GMC foi criado o Setor de Tecnologias da Informação e Comunicação (STIC) (art. 1º), órgão responsável por, dentre outras funções, (i) implementar processos de renovação tecnológica (art. 2º,

---

532 MERCOSUL. **GMC/RES. n.º 01, de 9 de abril de 2010.** Proteção da saúde e da segurança de consumidores e usuários - aspectos operativos. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019. p. 1-2.

533 Id. **GMC/RES. n.º 34, de 16 de dezembro de 2011.** Defesa do Consumidor - Conceitos Básicos. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019. p. 1-2.

534 Ibid., p. 2.

"a"); (ii) administrar e dar suporte aos serviços de correio eletrônico (art. 2º, "b"); e (iii) implantar políticas de segurança e processos de proteção informáticos (art. 2º, "c"). Sua incorporação é dispensada aos Estado Partes (art. 4º)[535].

Na Resolução n.º 36/2019/GMC, buscando intensificar a harmonização de legislações na área da defesa do consumidor no âmbito do MERCOSUL, reconheceu-se a vulnerabilidade dos consumidores no mercado e a integração do sistema de proteção ao consumidor com as normas nacionais e internacionais através da atualização dos princípios fundamentais protetivos (art. 1º), devendo sê-la incorporada no ordenamento jurídico dos Estados Partes até 15/01/2020 (art. 23)[536].

Destaque especial aos princípios do/da (i) acesso ao consumo (art. 1º, n.º 3); (ii) transparência dos mercados (art. 1º, n.º 4); (iii) proteção especial para consumidores em situação vulnerável e de desvantagem (art. 1º, n.º 6); (iv) respeito à dignidade da pessoa humana (art. 1º, n.º 7); (v) prevenção de riscos (art. 1.º, n.º 8), não discriminação (art. 1º, n.º 9); (vi) informação (art. 1º, n.º 11); (vii) harmonização (art. 1, n.º 12); e da (viii) equiparação de direitos (art. 1, n.º 14)[537].

Os princípios supramencionados guardam afinidade direta com os princípios da proteção de dados pessoais, mesmo porque o ciberconsumidor não deixa de ser uma categoria de consumidor e a disponibilização de seus dados pessoais aos responsáveis pelo tratamento (e subcontratantes) não deixa de ser uma categoria de consumo de prestação de serviço. Os princípios reforçam, desta forma, não apenas os direitos do consumidor, mas toda segurança, comércio e contratação eletrônica.

Com a Resolução n.º 37/2019/GMC, específica sobre o ciberconsumidor e com propósitos análogos à resolução anterior, garantiu-se aos ciberconsumidores os direitos "à informação clara, suficiente, verídica e de fácil acesso sobre o provedor, o produto e/ou serviço e transação realizada" (art. 1º)[538], assim como a disponibilização *online* de um conjunto de 12 informações técnicas pelo provedor, para visualização e contratação justa e transparente pelos usuários (art. 2º, "I" a "XII")[539].

---

[535] MERCOSUL. **GMC/RES. n.º 19, de 16 de junho de 2018.** Setor de tecnologias da informação e comunicação. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019. p. 1-3.

[536] Id. **GMC/RES. n.º 36, de 15 de julho de 2019.** Defesa do Consumidor: princípios fundamentais. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019. p. 1.

[537] Ibid., p. 1-3.

[538] Id. **GMC/RES. n.º 37, de 15 de julho de 2019.** Defesa do consumidor proteção ao consumidor no comércio eletrônico. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019. p. 1. (tradução nossa).

[539] Ibid., p. 1-2.

Preocupou-se ainda referida resolutiva com: (i) a visibilidade, idoneidade e inalterabilidade dos termos da contratação (art. 3º); (ii) a simplicidade do vocabulário, enaltecimento de cláusulas importantes e não referenciamento a outros documentos (art. 4º); (iii) a criação de mecanismos de correção e confirmação de dados introduzidos, para evitar imprecisões e consentimento tácito (art. 5º); e (iv) o direito de arrependimento, atendimento e solução de controvérsias (art. 6º a 8)[540].

Não foi esquecido do aspecto transfronteiriço da (v) proteção do ciberconsumidor, tampouco das diretrizes de cooperação entre agências protetoras e demais organismos dos Estados Partes (art. 9º). Dispôs, em vista do rearranjo das fronteiras aos modernos canais de informação e comércio, sobre (vi) provedores atuantes sob diversos domínios de *internet* (art. 10º); e (vii) o prazo até 15/01/2020 à incorporação do resolvido no direito interno dos Estados Partes (art. 11º) [541].

A atualização principiológica consumerista e a regulação de parâmetros do comércio eletrônico, com foco no sujeito vulnerável da relação, é um inequívoco progresso para fins de harmonização legislativa no âmbito do MERCOSUL e de nivelação dos regramentos nacionais e regionais com os padrões internacionais vigentes. Ademais, fazem sentido suas publicações simultâneas, assim como suas idênticas datas para internalização pelos Estados Partes.

Retrocedendo um pouco, cabe registrar que considerando as mudanças globais - decorrentes do progresso tecnológico e informático e resultantes em uma nova economia digital -, o estimular do comércio eletrônico para atualização e recolocação do MERCOSUL no comércio exterior e o repensar das políticas comerciais, jurídicas e tributárias dos Estados Partes, resolveu-se, através da Resolução n.º 43/2000/ GMC, criar o Subgrupo de Trabalho sobre Comércio Eletrônico (SGT-13) como um foro independente do GMC (art. 1º)[542].

O SGT-13 tem como objetivos “coordenar as posições nacionais, fortalecendo o relacionamento externo do bloco nesta matéria”, que estava defasada, bem como “contribuir para o melhoramento do marco jurídico, fiscal, de meios de pagamento e infra-estrutura, necessário para o rápido desenvolvimento intrazona do comércio

---

[540] MERCOSUL. **GMC/RES. n.º 37, de 15 de julho de 2019.** Defesa do consumidor proteção ao consumidor no comércio eletrônico. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019. p. 2.

[541] Ibid., p. 2.

[542] Id. **GMC/RES. n.º 43, de 28 de junho de 2000.** Grupo Ad Hoc sobre comércio eletrônico. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019. p. 1.

eletrônico" (art. 2º)[543], comércio este onde transitam incontáveis informações pessoais e onde os dados constituem as modernas moedas de troca.

Tendo em vista a existência de 26 atas do SGT-13 - referentes à I a XVI Reuniões Oridinárias, respectivamente aos anos de 2001 a 2018, com acesso público disponível, com exceção das de 2018 - e que cada uma delas possui suas próprias agendas, arquivos consolidados e arquivos anexos, optou-se por um recorte investigativo das publicações depositadas de 2007-2019, delimitação esta tida como suficiente para aferimento do panorama legislativo do MERCOSUL.

Seguindo este enfoque, cronologicamente, tem-se a Ata n.º 001/2007, da XVIII Reunião Ordinária do SGT-13[544], cujas pautas principais discutiam (i) o projeto de cooperação MERCOSUL-UE; (ii) a situação da incorporação das normativas aprovadas pelo GMC; (iii) o intercâmbio de informação com a Venezuela; (iv) a proteção de dados pessoais; (v) a análise de documentos sobre retificação de comunicações eletrônicas; e (vi) a questão do certificado de origem eletrônica[545].

Destaca-se o Projeto ALADI/2000-2006 que buscava o aumento de competências e a intensificação do uso das TICs entre os grupos tomadores de decisões do setor público e da sociedade civil no MERCOSUL, mediante ações comuns de capacitação, desenvolvimento de infraestrutura de TIC relacionado à formação e aplicações do comércio eletrônico no bloco. O Brasil, coordenador do projeto, informou sobre a aprovação da iniciativa pela Direção Técnica da UE, apresentando cronograma para sua implementação.

Houve ainda manifestação dos países mercosurenhos, em relação à situação da incorporação das normativas aprovadas pelo GMC - sendo a referente ao "Direito à Informação ao Consumidor em Transações feitas através da Internet" a que mais

---

543 MERCOSUL. **GMC/RES. n.º 43, de 28 de junho de 2000.** Grupo Ad Hoc sobre comércio eletrônico. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019. p. 1.

544 *Projeto Mercosul Digital:* "O Mercosul Digital nasceu com o objetivo de preencher vazios detectados, buscando estabelecer uma política comum, capacitar recursos especializados em TICs e trabalhar por uma simetria estrutural entre os quatro países para favorecer o comércio regional e, assim, potencializar a integração do MERCOSUL. Está inserido no documento de estratégia regional da Comissão Europeia que estabelece o marco estratégico da cooperação da Comunidade Europeia com o MERCOSUL para o período 2007-2013, tendo como beneficiários quatro membros-plenos do GMC: Argentina, Brasil, Paraguai e Uruguai" (BRASIL. Ministério da Ciência Tecnologia e Inovação. **Comércio Eletrônico:** estados e diagnósticos no Mercosul. Disponível em: <http://www.ludovinolopes.com.br/website/wp-content/uploads/2014/02/MD-Publica_Comercio-Eletronico-RelatorioFinal.pdf>. Acesso em: 25 jul. 2019. p. 13).

545 MERCOSUL. XVIII Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 01, de 17-18 de maio de 2007.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/364>. Acesso em: 25 jul. 2019. p. 1-6.

importa a esta investigação –, no sentido de que ainda estão em processo de internalização. Comentou-se também sobre as discussões do Projeto de Proteção de Dados Pessoais e Livre Circulação de Dados (2006) da Argentina, mas apenas foi decidido que os países enviassem relatórios sobre a discussão da proposta.

Na mesma reunião, houve apresentação pelo Brasil do Projeto Piloto de Certificado de Origem Eletrônica, com a finalidade de contribuir para o fortalecimento da iniciativa em curso, no âmbito da Associação Latino-Americana de Integração (ALADI), havendo concordância das demais delegações, com orientações para que trabalhassem para alcançar este objetivo.

Segundo a Ata n.º 002/2007, da XIX Reunião Oridinária do SGT-13, dominaram a pauta a retomada de temas pretéritos como (i) a situação de incorporação de resoluções aprovadas; e (ii) novas discussões sobre o projeto de cooperação MERCOSUL-UE, incluindo mudanças procedimentais na sua execução e a deliberação sobre a criação de um guia prático.

No mesmo evento, retornaram à discussão sobre (iii) o Projeto de Certificação Digital, com novos avanços, trocas de experiências e ideia para formalização de fórum periódico; e (iv) o Projeto de Proteção e Circulação de Dados Pessoais, onde demonstraram interesse no acordo a Argentina, Uruguai e a Venezuela (ainda não suspensa), mas o Brasil postergou qualquer decisão por não ter debatido internamente a questão ainda, comprometendo-se a realizar a devida consulta[546].

Conforme a pauta da Ata n.º 001/2008, da XX Reunião Ordinária do SGT-13, houve algumas inovações nos temas discutidos e deliberados. Deram-se prosseguimento nas tratativas referentes (i) ao Projeto de Cooperação MERCOSUL-UE; (ii) ao comércio eletrônico; (iii) à proteção de dados pessoais; e a (iv) outros assuntos, como a faturação eletrônica e o selo/carimbo de tempo e sincronismo[547].

No que alude ao projeto cooperativo, concordaram as delegações presentes na apresentação de uma resolução ao GMC para designação de autoridade gestora dos trabalhos. Em relação ao comércio eletrônico, as delegações apresentaram relatórios sobre o *status* da pesquisa no setor em seus respectivos países. E a Argentina,

---

[546] MERCOSUL. XIX Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 02, de 13-14 de setembro de 2007.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/1707>. Acesso em: 25 jul. 2019. p. 1-7.

[547] Id. XX Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 01, de 27-28 de maio de 2008.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/296>. Acesso em: 25 jul. 2019. p. 1-4.

sempre pioneira nesta área, reiterou seu interesse na criação de um padrão regional sobre proteção de dados pessoais.

Nesta mesma ocasião, a delegação argentina ressaltou a importância do *Selo PDP* e que a Argentina já recebera esta certificação europeia de nível protetivo (desde 2003), consoante os parâmetros da Diretiva n.º 46/1995/CE, sendo considerada, portanto, um dos únicos cinco países do mundo na época a ter este selo de reconhecimento. A delegação brasileira, sempre interessada, mas pouco proativa, manifestou-se no sentido de estudar a possibilidade no próximo semestre.

No semestre consecutivo, observam-se da Ata n.º 002/2008, da XXI Reunião Ordinária do SGT-13, novas empreitadas digitais na pauta do encontro, a exemplo da (i) informatização no setor jurídico; e da (ii) integração do comércio eletrônico via logística postal. Retomaram discussões sobre (iii) o carimbo temporal e sincronizador; (iv) a nota fiscal eletrônica; bem como sobre (v) o sistema de apoio ao exportador, a proteção de dados pessoais e o Projeto MERCOSUL-EU[548].

Os destaques da reunião foram os anúncios das delegações brasileira e uruguaia. Representantes de setores brasileiros apresentaram a situação do comércio eletrônico do país, incluindo a sincronização certificada, o que foi bem recebido pelas demais delegações, que manifestaram desejo de criar autoridades e serviços de carimbo de tempo. Também noticiou a Receita Federal a implantação da Nota fiscal Eletrônica no país, visando à informatização de instrumentos contábeis.

No que diz respeito à proteção de dados pessoais, a delegação uruguaia informou a criação de sua lei de proteção de dados pessoais, não restrita ao escopo comercial, mas expansível a todas as esferas informáticas, bem como a estrutura e o órgão de controle e promessa de apresentação de relatório de comparação do seu sistema legal com a proposta normativa anteriormente feita pela Argentina. As demais delegações manifestaram interesse no prosseguimento das discussões.

Ademais, ocorreram exposições sobre o cenário de informatização de processos judiciais e cartórios nacionais, com explicações sobre aspectos regulatórios no âmbito federal. E, voltando às discussões do Projeto MERCOSUL Digital, destacou sua diretoria seu objetivo na promoção de políticas e estratégias comuns e inerentes

---

548 MERCOSUL. XXI Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 02, de 23-24 de setembro de 2008.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/237>. Acesso em: 25 jul. 2019. p. 1-4.

à Sociedade da Informação para redução do desnível digital das tecnologias entre os países mercosurenhos.

Ato contínuo, na Ata n.º 001/2009, da XXII Reunião Ordinária do SGT-13, constavam como temas da pauta: (i) a formulação de plano de trabalho para avanço na realização de acordos mútuos de assinaturas eletrônicas; (ii) a inclusão de segmento de padrões gerais de interoperabilidade no Projeto MERCOSUL Digital, bem como sua harmonização de critérios; (iii) a apresentação do *status* dos Estados Membros sobre proteção de dados pessoais[549].

No que diz respeito à proteção de dados pessoais, o Uruguai asseverou a importância do trabalho em bloco para abordar problemas vinculados à temática. O Paraguai informou sobre o anteprojeto de comercio eletrônico que se encontra em andamento, que vai contemplar a proteção de dados pessoais. O Brasil, informou que o tema é prioridade em sua agenda e que pretende concluir a negociação no próximo semestre.

Na sequência, depreende-se da Ata n.º 001/2010, da XXIII Reunião Oridinária do SGT-13, que houve (i) nova apresentação pela delegação brasileira sobre o Projeto MERCOSUL Digital; (ii) análise da metodologia pela qual o SGT-13 conduziria aludido projeto; (iii) a criação de comitê técnico para assistência quando preciso; e (iv) discutida a situação das assinaturas digitais em cada país, tendo todas as delegações, salvo a argentina, revelado expressivo progresso[550].

O que entende disso é que o consenso das delegações sobre o MERCOSUL Digital sinalizou uma pontecialização da integração entre os Estados Partes - especialmente no tocante à harmonização legislativa – e uma aproximação do MERCOSUL às políticas, tecnologias e aos modelos normativos europeus. Uma interação neste sentido, a exemplo da pauta sobre firmas digitais, impliciaria cedo ou tarde na revisão de questões afetas à defesa do consumidor e aos dados pessoais.

A menção nesta mesma ata do consenso das nações mercosurenhas sobre a redação de um projeto de lei para proteção dos dados pessoais não desmente este pensamento. Sem numeração e intitulado “Medidas para a Proteção de Dados

---

549 MERCOSUL. XXII Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 01, de 10-11 de dezembro de 2009.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/1187>. Acesso em: 25 jul. 2019. p. 1-9.

550 Id. XXIII Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 01, de 27-28 de maio de 2010.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/2081>. Acesso em: 25 jul. 2019. p. 1-3.

Pessoais e sua Livre Circulação", o projeto sujeito à aprovação pelo GMC guarda notória semelhança com as disposições da Diretiva n.º 46/1995/CE, instrumento responsável na época pela proteção de dados pessoais europeus.

A similitute entre ambos os documentos é conferível desde sua justificativa nos direitos e liberdades fundamentais e na contribuição com o progresso econômico, social e tecnológico até sua estrutura e texto normativo. Foram introduzidas as definições técnicas, o âmbito de aplicação, os princípios protetivos, a classificação e qualidade dos dados, o consentimento e tratamentos de dados, os direitos dos titulares, a transferência internacional, dentre os fatores indissociáveis[551].

Conforme a Ata n.º 002/2010 da XXIV Reunião Ordinária do SGT-13, percebe-se, pelo registrado à época, no quesito proteção de dados pessoais, que o Brasil lançava debate público sobre o projeto de lei proposto sobre o assunto; que o Uruguai analisava aspectos jurídicos oriundos de consultas internas; e que o Paraguai estava antecipado na aprovação do outrora acordado; e isto demonstra uma aparente uniformidade de posições e descompasso temporal das delegações[552].

Discutiu-se ainda, na mesma reunião, sobre: (i) o tema da resolução eletrônica de conflitos, aquiescendo as delegações no avanço de estudos; (ii) a postergação da discussão da questão logística do comércio eletrônico; (iii) diversos aspectos regionais do desenvolvimento tecnológco em TICs; (iv) a segurança informática aplicada aos *webservices* para intercâmbio de informações; (e) o projeto MERCOSUL digital; e (f) a coordenação de certificação digital[553].

No tocante à questão da segurança informática, encabeçada pela delegação argentina, ainda que com anseios comerciais e normativos, percebe-se indício de uma preocupação com a circulação de dados transfronteiriços, tendo em vista a necessidade de validação de dados do comércio intra-zona. E, novamente, pelo relatado, as demais delegações seguem com unicidade de posições, porém revelam ainda estarem em estágio de consulta e de articulação interna.

Segundo a Ata n.º 001/2017 da XXV Reunião Ordinária do SGT-13, discutiu-se (i) o intercâmbio de informações relevantes sobre o comércio eletrônico, com

---

551 MERCOSUL. XXIII Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 01, de 27-28 de maio de 2010.** Anexo IV - Acesso Público: Projeto de Decisão s/n de Proteção de Dados Pessoais. Disponível em: <https://documentos.mercosur.int/reuniones/doc/2081>. Acesso em: 25 jul. 2019. p. 1-8.

552 Id XXIV Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 02, de 6-7 de dezembro de 2010.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/3628>. Acesso em: 25 jul. 2019. p. 1.

553 Ibid., p. 1-2.

esclarecimento da situação dos respectivos países na matéria, para posterior compilação; (ii) a negociação de possível protocolo de comércio eletrônico em nível de MERCOSUL; e houve até (iii) a proposição, pela delegação argentina, de novas competências ao subgrupo e de acordo bilateral sobre firmas digitais[554].

Dentre as competências sugeridas estão a assinatura digital, a proteção de dados e os direitos do ciberconsumidor, que condizem com as temáticas prioritárias da pauta: (i) princípios de acesso e uso da *internet*, transferência de informações e interconexão para transações comerciais; (ii) proteção de dados pessoais; (iii), mecanismos de proteção e cooperação; (iv) autenticação e assinaturas digitais; (v) localizações, vedações e estímulos; e (vii) spams (Anexo III)[555].

Quanto ao acordo de reconhecimento mútuo de certificados de firmas digitais, consta do arquivo (Anexo V) que ele objetiva outorgar o mesmo valor jurídico e probatório das assinaturas manuscritas às eletrônicas (art. 1º) quando emitidas por prestadores de serviços certificados e consoante os padrões internacionais (art. 3º). Houve previsão no documento, inclusive, de avaliação e harmonização operativa (art. 4º) e de criação de sistema de acreditação e controle (art. 5º)[556].

A proposição marca não apenas uma avanço harmonizador legislativo e fortalecedor protetivo do consumidor, mas consagra a extensão destas conquistas ao ciberconsumidor e ao comércio digital, pois envolve questões de (i) controle de acesso a serviços e perfis (art. 4, “a”); (ii) setorização de tratamentos específicos (art. 4, “b”); (c) mecanismos de segurança de dados e informações sensíveis (art. 4º, “c”); (d) mecanismos de criação e armazenamento de registros (art. 4º, “d”)[557]. Engloba, ainda, questões de (e) mecanismos de segurança para integridade dos dados e processos críticos (art. 4º, “e”); (f) mecanismos de segurança física e lógica das instalações (art. 4º, “f”)[558]; dentre outros aspectos tocantes à proteção de dados, dados pessoais e dados sensíveis, o que evidencia uma maior preocupação do MERCOSUL com a

---

554 MERCOSUL. XXV Reunião Ordinária do SGT-13**. GMC/SGT-13/ATA n.º 01, de 10 de novembro de 2017.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/6458>. Acesso em: 25 jul. 2019. p. 1-2.

555 Id. XXV Reunião Ordinária do SGT-13**. GMC/SGT-13/ATA n.º 01, de 10 de novembro de 2017.** Anexo III - Acesso Público: Lista de Temas Prioritários. Disponível em: <https://documentos.mercosur.int/reuniones/doc/6458>. Acesso em: 25 jul. 2019. p. 1.

556 Id. XXV Reunião Ordinária do SGT-13**. GMC/SGT-13/ATA n.º 01, de 10 de novembro de 2017.** Anexo V - Acesso Público: Proposta de Acordo Bilateral em Matéria de Reconhecimento Mútuo de Certificados de Assinatura Eletrônica – apresentado pela Argentina. Disponível em: <https://documentos.mercosur.int/reuniones/doc/6458>. Acesso em: 25 jul. 2019. p. 8-10.

557 Ibid., p. 9.

558 Ibid., p. 9.

regulação da matéria, ainda que incidentalmente ou de forma acessória a outras inovações tecnológicas.

Assim, são perceptíveis e notáveis os esforços do MERCOSUL, ainda que a curto passo e em descompasso, no sentido de harmonizar as normas de proteção do consumidor, do ciberconsumidor e do consumidor transfronteiriço; e que a proteção de dados pessoais já está inclusa nas suas pautas e em discussão nas suas reuniões, ainda que incidentalmente. Parece que, no entanto, os próprios direitos internos dos Estados Partes estão se modernizando com maior celeridade.

Para melhor compreender este cenário jurídico regional, nos tópicos seguintes serão explorados os históricos legislativos argentino, brasileiro, paraguaio e uruguaio sobre a defesa do (ciber)consmuidor e, principalmente, sobre a proteção de dados pessoais. Reitera-se que a legislação venezuelana não fará parte da análise adiante, em vista da sua suspensão do MERCOSUL, por tempo indeterminado, em virtude da ruptura da ordem democrática pactuada pelo país.

### 4.3 A proteção de dados pessoais na Argentina

A Argentina tem se preocupado com o direito do consumidor desde 1993, quando publicou a Lei n.º 24.240/1993 (Lei de Defesa do Consumidor)[559]. Até então a proteção do consumidor derivava das normas do Código Civil.

A aprovação desta lei é fruto de uma ferrenha luta política pela obtenção de um sistema orgânico de proteção ao consumidor[560]. Entretanto, a proteção de dados pessoais não foi contemplada na lei como um direito do consumidor.

Foi somente sete anos depois que o país promulgou a Lei n.º 25.326/2000[561], com a finalidade de normatizar a proteção dos dados pessoais, com sua respectiva regulamentação pelo Decreto n.º 1.558/2001[562].

---

[559] ARGENTINA. **Ley n.º 24.240, de 13 de Octubre de 1993.** Defensa del Consumidor. Normas de Protección y Defensa de los Consumidores. Autoridad de Aplicación. Procedimiento y Sanciones. Disposiciones Finales. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/638/texact.htm>. Acesso em: 20 jul. 2019.

[560] FELLOUS, Beyla Esther. **Proteção do consumidor no Mercosul e na União Europeia**. – São Paulo: Editora Revista dos Tribunais, 2003. p. 158.

[561] ARGENTINA. **Ley n.º 25.326, de 30 de Octubre de 2000**. Proteccion de los datos personales. Disponível em: <https://www.oas.org/juridico/PDFs/arg_ley25326.pdf>. Acesso em 20 jul.2019.

[562] Id. **Decreto Reglamentario n.º 1.558, de 29 de novembro de 2001.** Disponível em: < http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=D31E6955E0657D42EF16E6061748B221?id=70368>. Acesso em: 20 jul. 2019.

Curioso é o fato que a legislação argentina demorou anos para tratar da matéria de proteção de dados pessoais e, ainda assim, é considerada como pioneira dentre todos os demais Estados Partes do MERCOSUL[563].

Referida legislação contém 48 artigos, subdivididos em sete capítulos. Em seu bojo, traz disposições gerais, objetivo e conceitos (Capítulo I); princípios gerais de proteção de dados (Capítulo II); direitos dos titulares de dados (Capítulo III).

E, disciplina também: usuários e responsáveis pelos arquivos, registros e banco de dados (Capítulo IV); órgãos de controle (Capítulo V); sanções (Capítulo VI); e ação de proteção de dados pessoais (Capítulo VII).

A própria redação legal menciona como objetivo a obtenção de proteção de dados com amplitude, envolvendo, o processamento de dados públicos e privados e a garantia da privacidade e acesso à informação (art. 1º):

> O objetivo desta lei é a proteção abrangente de dados pessoais armazenados em arquivos, registros, bancos de dados ou outros meios técnicos de processamento de dados, sejam públicos ou privados, destinados a fornecer informações, para garantir o direito de honrar a privacidade das pessoas, bem como o acesso às informações registradas sobre elas, de acordo com o disposto no artigo 43, terceiro parágrafo da Constituição Nacional[564].

Dentre os conceitos argentinos relacionados à proteção de dados, destaca-se o conceito de “dados pessoais” e “dados sensíveis”. Os dados pessoais são quaisquer tipos de dados referentes às pessoas singulares determinadas ou determináveis e, os considerados sensíveis, são os dados pessoais que revelam origem racial e étnica, opiniões políticas, convicções religiosas, filosóficas ou morais, afiliação sindical e informações sobre saúde ou vida sexual (art. 2º)[565].

Os princípios gerais determinados na legislação são os seguintes: (i) legalidade dos arquivos de dados (devem estar registrados, observando em sua operação os princípios definidos); (ii) qualidade dos dados (devem ser verdadeiros, apropriados, relevantes e não excessivos; e a coleta não pode ser feita por meios fraudulentos ou injustos); (iii) finalidade (não podem ser utilizados para outros fins); atualização

---

563 DA SILVA, Felipe Stribe. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria, 2015. Dissertação. Universidade Federal de Santa Maria (UFSM). p. 76.

564 ARGENTINA. **Ley n.º 25.326, de 30 de Octubre de 2000. Proteccion de los datos personales**. Disponível em: <https://www.oas.org/juridico/PDFs/arg_ley25326.pdf>. Acesso em 20 jul.2019.

565 Ibid., não páginado.

(devem ser precisos e atualizados); (iv) idôneos (dados parcialmente incorretos ou incompletos deverão supridos e substituídos); (v) conservação limitada (devem ser armazenados para fins de acesso pelo titular e deverão ser destrúidos quando desnecessários) (art. 4º)[566].

O tratamento de dados deverá ser autorizado expressamente pelo titular dos dados, no entanto, há exceções algumas previstas (art. 5º). Na coleta de dados pessoais, os titulares devem ser informados de maneira expressa e clara (art. 6º). Nenhuma pessoa pode ser obrigada a fornecer dados sensíveis, salvo se houver interesse geral e houver autorizado legal. Segundo a lei, inclusive, é proibido formar arquivos passíveis de revelar dados sensíveis e dados referentes a registros criminais, cujo tratamento compete apenas às autoridades competentes (art. 7º)[567].

Ademais, dados relativos à saúde, públicos ou privados, podem ser coletados, respeitando-se os princípios do segredo profissional (art. 8º). Há também preocupação como a adoção de medidas técnicas para garantir a segurança dos dados tanto pelos responsáveis quanto pelos usuários (art. 9º). E, em clara alusão ao RGPD, proibiu-se a transferência de dados pessoais, de qualquer categoria, para países ou organizações internacionais ou supranacionais que não forneçam níveis adequados de proteção (art. 12), mas há ressalvas legais (art. 12, n.º 2)[568].

Aos titulares dos dados pessoais foram garantidos os direitos à informação, ao acesso, ao conteúdo da informação, à retificação, à atualização e à exclusão (arts. 13 ao 16). Igualmente há ressalvas, mormente quando o interesse público, a segurança pública, os processos investigativos, administrativos ou judiciais, dentre outras hipótese de exceção, conflitam com o exercício desses princípios (art. 17)[569].

No que diz respeito ao órgão de controle da proteção de dados da Argentina, é preciso registrar que ele sofreu modificações estruturais ao longo dos anos. Acerca delas, cabe mencionar a pesquisa realizada pelo IDEC[570], que objetivou analisar, de

---

[566] ARGENTINA. **Ley n.º 25.326, de 30 de Octubre de 2000. Proteccion de los datos personales**. Disponível em: <https://www.oas.org/juridico/PDFs/arg_ley25326.pdf>. Acesso em 20 jul.2019.
[567] Ibid., não paginado.
[568] Ibid., não paginado.
[569] Ibid., não paginado.
[570] *Instituto Brasileiro de Defesa do Consumidor (IDEC):* "Trata-se de uma Associação de consumidores fundada em 1987. Não possui fins lucrativos. É independente de empresas, governos ou partidos políticos. Os recursos financeiros para o desenvolvimento de suas atividades têm sua origem nas contribuições dadas pelos seus associados. O Idec também desenvolve projetos que recebem recursos de organismos públicos e fundações independentes, como Fundação Ford e Open Society Foundation. Esse apoio não compromete a independência do Instituto. O Idec é membro pleno da *Consumers International* e faz parte do Fórum Nacional das Entidades Civis de Defesa do Consumidor e

maneira comparada, arquiteturas institucionais de Autoridades de Proteção de Dados Pessoais já existentes em países da América Latina, especificamente, das situadas na Argentina, Uruguai e Colômbia.

O órgão de controle foi, inicialmente, criado pela Lei n.º 25.326/2000 (art. 29) e, posteriormente, regulamentado pelo Decreto n.º 1.558/2001. Com sua regulamentção, sofreu alteração de nomenclatura, deixando de ser chamado de *Dirección Nacional de Protección de Datos Personales*.

Designado pelo Poder Executivo Nacional, por um período de 04 (quatro) anos, este órgão pertencia à Administração Direta e estava subordinado ao Ministério da Justiça. Em 2017, sua estrutura foi modificada e ele recebeu *status* de órgão da Administração indireta, tendo sido integrado à Agencia de *Acceso a La Información Publica*[571].

A pesquisa analisou a autonomia administrativa, autonomia financeira, autonomia dos diretores e os poderes de cada país alvo. Sua conclusão foi de que, tanto na Argentina quanto no Uruguai - que são Estados Partes do MERCOSUL - não há um modelo de estrutura adequado. Em relação à Argentina, destaca:

> Na Argentina, a experiência com o órgão sem personalidade jurídica própria – implementado sob a justificativa de não aumentar despesas – fez com que, sete anos após concretizada, a autoridade necessitasse passar por uma reforma que alterou seu modelo para posicioná-la na administração indireta. Afinal, a vinculação representava uma limitação da incidência da lei, pelos riscos de haver ingerências hierárquicas e menores possibilidades para investigar e sancionar as infrações do poder público[572].

Ressalta a pesquisa, outrossim, que a vinculação do órgão à administração direta acaba influenciando e dificultando sua função como órgão fiscalizador, minando, por conseguinte, sua autonomia, muito embora conste na legislação que o órgão goze de independência:

---

Associação Brasileira de Organizações Não-Governamentais". (IDEC – Instituto de Defesa do Consumidor. **Quem somos**. Disponível em: <https://idec.org.br/quem-somos>. Acesso em: 22 jul. 2019).

[571] ARGENTINA. **Decreto n.º 746, de 25 de Septiembre de 2017**. Modificación de Funciones en Ministerios. Disponível em: <http://argentinambiental.com/legislacion/nacional/decreto-74617-modificacion-funciones-ministerios/>. Acesso em: 22 jul. 2019.

[572] SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. **Autoridades de Proteção de Dados na América Latina**. Disponível em: <http://www.portaldaprivacidade.com.br/2019/05/14/autoridades-de-protecao-de-dados-na-america-latina/>. Acesso em: 22 jul. 2019. p. 36.

> Tendo em vista estes exemplos, fica evidente que a vinculação da autoridade à administração direta e a livre nomeação dos membros pelo Presidente da República, sem participação da oposição, influencia sua eficácia e dificulta a concretização da independência enquanto órgão fiscalizador, em que pese na letra fria da lei estar disposta a autonomia do órgão[573].

A despeito disso, a recomendação do estudo é que o melhor modelo aplicável é aquele no qual a Autoridade de Controle tenha personalidade jurídica própria e esteja desvinculada da Administração Direta e que tenha o crivo da oposição para nomeação de seus membros. Neste sentido:

> Por outro lado, o melhor modelo é aquele cuja autoridade possua personalidade jurídica própria, estando desvinculada da administração direta, e a nomeação de seus membros passem pelo crivo da oposição, como no Congresso, ou admita a participação da sociedade civil nesta escolha. Vale destacar, nesse sentido, o processo de nomeação da autoridade argentina, em que é realizada uma audiência pública, possibilitando participação na decisão a todos os interessados. Tal modelo parece ter repercussões práticas, sendo o diretor da autoridade argentina bastante elogiado pelos entrevistados[574].

É curioso e imperioso registrar que, sob a égide da antiga Diretiva n.º 46/1995 (art. 25, n.º 6), a Comissão Europeia concedeu à Argentina uma titulação/certificação de país com nível adequado de proteção de dados pessoais, façanha pouco comum nos países latino-americanos à época[575]. Frise-se, contudo, que a legislação europeia de proteção de dados pessoais vigente é o RGPD[576].

Vale acrescentar, em matéria jurisprudencial, sobre julgado relacionado à violação de dados sensíveis ocorrido na Argentina e que chegou até a Corte Suprema de Justiça. Trata-se do Acórdão n.º 17/2019, que decidiu sobre caso de obtenção

---

[573] SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. **Autoridades de Proteção de Dados na América Latina:** um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. – São Paulo: IDEC, 2019. p. 36.

[574] Ibid., p. 37.

[575] COMISSÃO EUROPEIA. **Decisão n.º 490/2003/CE, de 30 de junho de 2003.** Decisão da Comissão relativa à adequação do nível de proteção de dados pessoais na Argentina. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32003D0490&from=EN>. Acesso em: 20 jul. 2019.

[576] A Argentina não possui ainda uma certificação/titulação de país com adequação de proteção de dados pessoais da UE com base no RGPD. O Japão foi o único país até o momento a receber este "referencial de adequação" da UE.

furtiva de dados sensíveis e envolveu os princípios de tratamento de dados e procedimento de interceptação e captação de comunicações[577].

## 4.4 A proteção de dados pessoais no Brasil

Parece salutar começar lembrando que, dentre todos os países mercosurenhos, é o Brasil o que primeiro criou uma legislação específica sobre matéria de direito do consumidor e o que possui o nível mais elevado de proteção nesta seara, inclusive antes da formação do bloco que integra[578].

A preocupação jurídica com os consumidores brasileiros ganhou um notável reforço constitucional desde a promulgação da CFRB/1988. Previsto no capítulo de direitos e deveres individuais e coletivos, o direito do consumidor foi alçado ao título de direito fundamental e sua promoção incumbida ao Estado (art. 5º, XXXII)[579].

Na mesma linha de proteção do sujeito vulnerável, concedeu-se ao cidadão o *habeas data*, remédio constitucional com dúplice finalidade de (i) garantir acesso às suas informações contidas em bancos de dados públicos ou do governo e de (ii) retificar dados em caso sigiloso, judicial ou administrativo (art. 5º, LXXII, "a" e "b")[580], sendo regulamentada pela Lei n.º 9.507/1997[581].

O direito do consumidor também recebeu, constitucionalmente, *status* de princípio geral da atividade econômica com objetivo de assegurar a dignidade da pessoa humana, a valorização do trabalho, a livre iniciativa e os preceitos da justiça social tamanha sua importância (art. 170, V)[582].

Para regulamentação e concretização da proteção consumerista foi promulgada a Lei n.º 8.078/1990, conhecida como Código de Defesa do Consumidor (CDC). Nele foram previstos seus direitos básicos como o resguardo contra serviços

---

577 ARGENTINA. Corte Suprema de Justicia de la Nacion. **Acordada n.º 17/2019, de 19 de junho de 2019.** Disponível em: <https://www.csjn.gov.ar/documentos/descargar/?ID=117364>. Acesso em: 30 jul. 2019.

578 FELLOUS, Beyla Esther. **Proteção do consumidor no Mercosul e na União Europeia.** – São Paulo: Editora Revista dos Tribunais, 2003. p. 160.

579 BRASIL. **Constituição da república federativa do brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 26 jul. 2019.

580 Ibid., não paginado.

581 Ibid. **Lei n.º 9.507 de 12 de novembro de 1997.** Dispõe sobre o regulamento do direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm>. Acesso em: 25 jul. 2019.

582 Ibid. não paginado.

considerados nocivos e a prestação clara de dados sobre eles (art. 6º, I a X)[583], com destaque à questão do banco de dados e cadastro (art. 43), demonstrando preocupação com os dados pessoais, arquivos de consumo e suas fontes, assim como com seus direitos de acesso, retificação e comunicação inerentes[584].

É importante mencionar a Lei n.º 12.414/2011 - que disciplinou a formação e consulta a bancos de dados com informações de adimplemento, de pessoais naturais e também de pessoas jurídicas, para formação de histórico de crédito, disciplinado conceitos, direitos, obrigações, dentre outras questões inerentes[585].

E também a Lei n.º 12.527/2011, com objetivo de regular o acesso a informações de variadas legislações, estabelecer procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios e conformar o tratamento de informações pessoais com os preceitos de transparência, respeito à intimidade, vida privada, honra, imagem, liberdades e garantias individuais[586].

Em decorrência da criminalidade envolvendo a *internet*, foi publicada a Lei n.º 12.737/2012 que dispõe sobre a tipificação criminal de delitos informáticos, como o crime de invasão de dispositivo informático (art. 154-A), um notável reforço à proteção do titular dos dados (inclusive pessoais e sensíveis), contribuindo para elevar seus direitos personalíssimos ao ambiente digital e tecnológico[587].

A proteção de dados pessoais foi, de fato, reconhecida com Lei n.º 12.965/2014 (Marco Civil da *Internet*). Estendeu-se com ela, aos ciberconsumidores, a defesa do consumidor (art. 2º, V), enrobustecendo a proteção da privacidade (art. 3º, II), a

---

583 BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 26 jul. 2019.

584 Id. **Lei n.º 8.078, de 12 de novembro de 1997.** Dispõe sobre o regulamento do direito ao acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm>. Acesso em: 29 jul.2019.

585 Id. **Lei n.º 12.414 de 09 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 26 jul. 2019.

586 Id. **Lei n.º 12.527 de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Aceso em: 26 jul. 2019.

587 Id. **Lei n.º 12.737 de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 25 jul. 2019.

proteção dos dados pessoais (art. art. 3º, III), a segurança e o funcionamento das redes de dados conforme padrões internacionais (art. 3º, V)[588].

Apostava a mesma legislação na promoção do acesso à informação (art. 4, II), da adoção de novas tecnologias e modelagens de acessibilidade e interoperabilidade entre aplicações e bases de dados (art. 4º, III e IV), bem como da padronização de conceitos inerentes (art. 5º)[589].

Não se furtou ainda à fixação dos direitos e garantias aos ciberconsumidores, maximizando as disposições constitucionais e consumeristas de inviolabilidade da vida particular e da vida familiar (art. 7º, I), do fluxo de comunicações pela *internet* (art. 7º, II) e das comunicações privadas armazenadas (art. 7º, III)[590].

Tampouco ficou silente acerca da claridade e completude das contratações eletrônicas de prestação de serviços (art. 7º, VI), do fornecimento de dados a terceiros sem consentimento livre, expresso e informado (art. 7º, VII) e sobre o gerencialmente, processamento e tratamento de dados pessoais (art. 7º, VIII a X)[591].

E dedicou uma seção inteira à proteção de registros, dados pessoais, comunicações privadas, incluindo tecnicidades de coleta, guarda e responsabilização, com grande enfoque nas obrigações dos provedores, mas pouco enfoque na circulação e categorias de dados pessoais (art. 10 a 21)[592].

Ciente da complexidade e particularidade da temática, o próprio Marco Civil da *Internet* determinou a regulamentação das questões afetas aos dados pessoais (art. 3º, inciso III). Não obstante a extraordinária melhoria da proteção do (ciber)consumidor trazida, os dados pessoais tardou a ser disciplinado. A propósito, Boff e Fortes ressaltam sua contribuição à modernização do direito.

> O Marco Civil representa o maior avanço normativo diretamente vinculado ao uso da internet na vida civil brasileira. Ele trouxe consigo algumas das respostas legislativas que contribuem para o fortalecimento do Estado Democrático de Direito e, principalmente, do reconhecimento de direitos e de sua extensão para a internet. Inevitavelmente, a instituição do Marco Civil da Internet também trouxe ao meio jurídico o debate sobre a necessidade de uma norma jurídica

---

588 BRASIL. **Lei n.º 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 25 jul. 2019.
589 Ibid., não paginado.
590 Ibid., não paginado.
591 Ibid., não paginado.
592 Ibid., não paginado.

> que recepcionasse e reconhecesse direitos, dentro do contexto da internet no Brasil[593].

Pensando adiante, tramitavam projetos nacionais objetivando estabelecer definições e providências acerca dos dados pessoais. O Projeto de Lei n.º 4.060/2012 da Câmara dos Deputados (art. 7º, I e IV)[594], o Projeto de Lei n.º 330/2013 do Senado Federal (art. 3º, I e II)[595], o Projeto de Lei n.º 5.276/2016 do Poder Executivo (art. 5º, I)[596] e o Decreto n.º 8.771/2016 (art. 14, I e II)[597].

Contudo, foi com a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) que se oficializou o significado de "dado pessoal" como sendo "informação relacionada a pessoa natural identificada ou indetificável" (art. 5º, I), com redação bastante semelhante ao RGPD. Percebe-se ainda a tipificação da categoria especial de dado pessoal, o chamado "dado pessoal sensível"[598].

O referido termo corresponde ao "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político [...]". Também seriam elementos identificadores o "dado referente à saúde ou à vida sexual, dado genético ou biométrico", para todos os casos, "quando vinculado a uma pessoa natural" (art. 5º, II)[599].

A LGPD contém 65 artigos e está dividida em 10 Capítulos, a saber: disposições preliminares (Capítulo I); tratamento de dados pessoais (Capítulo II);

---

[593] BOFF, Salete Oro; FORTES, Vinícius Borges. **Internet e proteção de dados pessoais:** uma análise das normas jurídicas brasileiras a partir das repercussões do caso nsa vs. Edward Snowden. Cadernos do Programa de Pós-Graduação em Direito da UFGRS, volume 11, 2016. p. 358.

[594] BRASIL. **Projeto de Lei n.º 4.060, de 13 de junho de 2012.** Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 18 fev. 2019. Tramitando como Projeto de Lei n.º 53/2018 no Senado Federal, foi aprovado e transformado na Lei n.º 13.709/2018.

[595] Id. **Projeto de Lei n.º 330, de 13 de agosto de 2013.** Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. O projeto foi arquivo em razão da deliberação do Projeto de Lei n.º 53/2018 que tramitava em conjunto.

[596] Id. **Projeto de Lei n.º 5.276, de 13 de maio de 2016.** Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. O projeto foi arquivo em razão da aprovação do Projeto de Lei nº 4.060/2012 sobre a mesma temática.

[597] Id. **Decreto n.º 8.771, de 11 de maio e 2016.** Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 26 jul. 2019.

[598] Id. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 26 jul. 2019.

[599] Ibid., não paginado.

direitos do titular (Capítulo III); tratamento de dados pessoais pelo Poder Público (Capítulo IV); transferência internacional de dados (Capítulo V); e agentes de tratamento de dados pessoais (Capítulo VI)[600].

Sequencialmente: segurança e boas práticas (Capítulo VII); fiscalização (Capítulo VIII); Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (Capítulo IX); e disposições finais e transitórias (Capítulo X)[601]. Cabe registrar que vários artigos do Capítulo IX sofreram vetos e que nova lei disporia a respeito.

É naturalmente perceptível a grande semelhença da estrutura da LGPD com o modelo europeu do RGPD, com pouquíssimas diferenças terminológicas entre ambos. Em verdade, como já discutido em linhas pretéritas, desde a vigência da Diretiva n.º 46/1995/CE os padrões europeus já eram fonte de referência normativa mundial na matéria. Com o RGPD, a tendência é ser uma influência ainda maior[602].

Indispensável mencionar a Medida Provisória n.º 869/2018[603], recentemente convertida na Lei n.º 13.853/2019[604], que realizou modificações na Lei n.º 13.709/2018 (LGPD), com objetivo de melhor explorar tecnicidades pendentes e regulamentar dispositivos vetados, mormente no tocante à natureza jurídica, vinculação, composição, estrutura, orçamentos, poderes e atribuições da ANPD.

A situação do veto alertou os estudiosos e autoridades regionais, muito embora houvesse promessa de sua regulamentação. O alerta reside nos prejuízos do funcionamento de uma lei de proteção de dados pessoais sem uma autoridade nacional para fiscalização. O problema se irradiaria, possivelmente, ainda em corte bilionário de investimentos e baixa competitividade no mercado internacional.

---

600 BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 26 jul. 2019.

601 Ibid., não paginado.

602 Veja-se que a legislação nem estrou em vigência e que diversos são os julgados sobre violações de dados pessoais nos tribunais brasileiros desde o ano passado. A título de contribuição jurisprudencial, chamaram atenção o Recurso Especial nº 1.660.168-RJ do STJ, sobre direito ao esquecimento e o Pedido de providência n.º 0004068-95.2015.2.00.0000 do CNJ, sobre exclusão de dados pessoais de candidatos a cargos públicos.

603 BRASIL. **Medida Provisória n.º 869, de 27 de dezembro de 2018.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 26 jul. 2019.

604 Id. **Lei n.º 13.853 de 08 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm>. Acesso em: 26 jul. 2019.

Ademais, ocasionou bastante preocupação a questão da autonomia apenas técnica e decisória da ANPD (art. 55-B). A discussão é relativizada, contudo, pelo dispositivo acrescido que fixa sua natureza jurídica como transitória, passível de transformação em órgão da administração pública federal indireta e sujeita ao regime autárquico especial, vinculada à chefia do Poder Executivo (art. 55-A)[605].

Neste sentido, invoca-se novamente a pesquisa realizada pelo IDEC sobre as autoridades de controle. Ela conclui que o modelo de autoridade independente, com autonomia completa, desvinculado da administração direta, é o recomendado para o funcionamento do órgão, para que ele consiga efetivar a proteção dos direitos humanos e fundamentais de proteção de dados pessoais do ciberconsumidor[606].

A pesquisa indica que, ainda durante a vigência da Medida Provisória, a falta de autonomia administrativa foi criticada pelas autoridades argentina e uruguaia. O histórico destes países, ambos inicialmente vinculados, demonstrou que os argentinos precisaram fazer mudanças ao modelo de administração indireta e os uruguaios, ainda vinculado, tiveram conflitos de interesses com o Executivo[607].

As consequências são inúmeras e variadas segundo a pesquisa, havendo: "[...] dificuldade na identificação dos principais atores do mercado e dos principais riscos sociais das inovações tecnológicas, bem como penosidade em dar efetividade às investigações realizadas"[608]. A própria nomeação dos integrantes dos órgãos prejudicaria a qualificação das equipes operadoras da autoridade de controle.

A título de comparação, a Autoridade de Controle da UE, como já mencionado outrora, possui total independência, sem sujeições a influências externas, diretas ou indiretas, no desempenho de suas funções, sem contar que dispõe de recursos humanos, técnicos e financeiros, instalações e infraestruturas necessárias ao desenvolvimento de suas funções.

Parece prematuro tecer conclusões a este respeito no cenário brasileiro, haja vista a criação deveras recente do órgão. Conquanto as autoridades mencionadas guardem, majoritariamente, semelhanças entre si e todas (mais adiante será visto

---

[605] **Lei n.º 13.853 de 08 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm>. Acesso em: 26 jul. 2019.

[606] SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. **Autoridades de Proteção de Dados na América Latina:** um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. – São Paulo: IDEC, 2019. p. 36-37.

[607] Ibid., p. 36-37.

[608] Ibid., p. 37.

sobre a uruguaia e paraguaia) demonstrem seguir os parâmetros europeus do RGPD, estas projeções vizinhas servem de indícios que não devem ser ignorados.

### 4.5 A proteção de dados pessoais no Paraguai

O Paraguai não previa em sua Constituição (1967) a proteção do consumidor, diferentemente dos demais Estados Partes do MERCOSUL[609]. Foi somente com sua reforma constitucional (1992) que foi garantido o direito individual ou coletivo de reivindicar das autoridades públicas medidas de defesa do consumidor ou de interesses da comunidade tocantes à qualidade de vida e ao patrimônio (art. 38º)[610].

Uma legislação específica sobre proteção do consumidor paraguaio surgiu seis anos depois, com a promulgação da Lei n.º 1.334/1998 (*Lei de Defensa del Consumidor y del Usuário*), com o objetivo precípuo de defender "sua dignidade, saúde, segurança e interesses econômicos" (art. 1)[611]. Sua elaboração foi baseada nas legislações consumeristas brasileiras e argentinas.

A citada lei paraguaia possui 54 artigos voltados à proteção dos consumidores, normas estas consideradas irrenunciáveis, não transacionáveis, não convencionáveis e prevalentes a quaisquer usos, costumes, práticas contrárias (art. 2º) relativos à oferta de bens e serviços (Capítulo III e IV), à proteção contratual e creditícia (Capítulo V e VI) e à saúde e segurança (Capítulo VII)[612].

Em matéria de proteção de dados pessoais, esclarece Gamarra que, apesar dos avanços tecnológicos terem alcançado o Paraguai e que em 2001 "o Poder Legislativo tenha iniciado o processo de regulamentação específica da matéria, ainda não foram incorporados ao direito positivo regras nacionais e abrangentes que protegem o direito à autodeterminação informativa de maneira eficaz"[613].

---

609 FELLOUS, Beyla Esther. **Proteção do consumidor no Mercosul e na União Europeia**. – São Paulo: Editora Revista dos Tribunais, 2003. p. 171.

610 PARAGUAY. **Constitución de la República de Paraguay, de 20 de junio de 1992.** Disponível em: <http://www.oas.org/juridico/mla/sp/pry/sp_pry-int-text-const.pdf>. Acesso em: 23 jul. 2019.

611 Id. **Ley n.° 1.334, de 27 de octubre de 1998.** Ley de Defensa del Consumidor y del Usuario. Disponível em: <http://www.bacn.gov.py/leyes-paraguayas/897/de-defensa-del-consumidor-y-del-usuario>. Acesso em: 23 jul. 2019. (tradução nossa).

612 Ibid., não paginado.

613 MARECOS GAMARRA, Adriana Raquel. *La protección de datos de carácter personal em el Paraguay.* In: **Revita Jurídica UCA Law Review.** Universidad Católica "Nuestra Señora de la Asunción" - Facultad de Ciencias Jurídicas y Diplomáticas, 2017. p 623-654. Disponível em: <https://www.pj.gov.py/ebook/monografias/nacional/informatico/Adriana-Marecos-Proteccion-de-datos-Py.pdf>. Acesso em: 30 jul. 2019. p. 2.

Registra Gamarra que, a título de disciplina constitucional, os paraguaios tinham previsto: o direito à expressão da personalidade (art. 25); direito à intimidade pessoal e familiar, respeito à vida privada, garantida, portanto, a proteção da intimidade, dignidade e imagem privada das pessoas (art. 33); além da autodeterminação informativa (art. 45) e do recurso de *habeas data* (art. 135)[614].

Não havia tutela específica até o momento e, neste sentido, pertinente é o comentário do Instituto de Investigações Jurídicas ao dizer ser "[...] incompreensível como no Paraguai, especificamente no auge do seu potencial econômico, não ter conseguido preencher este vazio, mas que o germe da proteção de dados está rondando fortemente [...]"[615]. O *upgrade* normativo paraguaio veio aos poucos.

Em matéria de proteção de dados pessoais, os paraguaios publicaram a Lei n.º 1.682/2001 (Regulamento de Proteção de Dados de Caráter Privado), trata-se, contudo, de legislação bastante enxuta, estruturada com apenas uma dúzia de artigos que contemplam, principalmente, alguns direitos dos titulares, formas de tratamento de dados e conceituações (arts.1° ao 12)[616].

Consta da lei, quanto aos *datos sensibles*, ser "proibida a divulgação de dados sensíveis de pessoas que são explicitamente individualizadas ou individualizáveis" e que são considerados dados sensíveis as informações "raciais ou étnicas, as preferências políticas, os de estado de saúde individual, as crenças religiosas, filosóficas ou morais; a intimidade sexual" e, de forma geral, "todos que fomentam preconceito e discriminação, ou afetam a dignidade, privacidade, intimidade doméstica e imagem privada de indivíduos ou famílias" (art. 4°)[617].

Sua *vacatio legis* foi de 06 (seis) meses após a publicação, tempo considerado suficiente para que as empresas, entidades e indivíduos pudessem se adaptar às disposições, operações, registros, sistemas de informação e divulgação (art. 11)[618]. O

---

[614] Ibid., p. 4.
[615] PARAGUAY. Corte Suprema de Justicia. Instituto de Investigações Jurídicas. **Protección de Datos Personales:** edición com aporte de jurisprudencia internacional. - Tomo II, p. 458, ISBN 978-99953-41-21-3. Asunción, 2014, p. 10. Disponível em: <https://www.pj.gov.py/ebook/libros_files/Proteccion-de-datos-personales-Tomo-II.pdf>. Acesso em: 30 jul. 2019.
[616] Id. **Ley n.º 1.682, de 16 de janeiro de 2001.** Reglamenta la Información de Carácter Privado. Disponível em: <http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado>. Acesso em: 24 jul. 2019.
[617] Ibid., não paginado. (tradução nossa).
[618] PARAGUAY. **Ley n.º 1.682, de 16 de janeiro de 2001.** Reglamenta la Información de Carácter Privado. Disponível em: <http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado>. Acesso em: 24 jul. 2019.

prazo parece bastante curto se comparado com os 03 (três) anos concedidos pela Diretiva n.º 46/1995/CE e com os 02 (dois) anos pelo RGPD.

No ano seguinte, por meio da Lei n.º 1.969/2002, houve modificações e ampliações de alguns artigos da lei Paraguai em comento (arts. 1º e 2º, por exemplo), como o aumento do rol de tratamentos dedos pessoais, a criação de exceções de tratamento aos bancos de dados e fontes de informações jornalísticas e à liberdade de expressão, bem como o fortalecimento do direito de acesso.

Gamarra elenca ainda como normas defensivas (i) a proteção da intimidade (art. 143) da Lei n.º 1.160/1997 (Código Penal Paraguaio); (ii) a participação do Paraguai no Projeto MERCOSUL Digital; (iii) a tipificação de grave violação de dados pessoais em serviços de certificação (art. 44, "d") na Lei n.º 4.610/2012; (iv) a vedação expressa de dados pessoais por atividade comercial (art. 6º) na Lei n.º 4.868/2013 (Lei do Comércio Eletrônico); (v) a proteção contra transmissão de dados pelos responsáveis pelo tratamento (art. 9º) da Lei n.º 1.682/2002, modificada pela Lei n.º 5.443/2015; e (vi) a proteção contra publicidade desautorizada de usuários de serviços de telefonia móvel (art. 1º) da Lei n.º 5.830/2017[619].

Inexiste legislação criando qualquer órgão para funcionar como "autoridade de proteção de dados", verifica-se, no entanto, que o Tribunal Civil e Comercial são os órgãos competentes para a aplicação das sanções. No âmbito da Corte Suprema de Justicia e dos Tribunais Civil e Comercial do Paraguai, a título de jurisprudência nacional, há uma série de discussões sobre o *habeas data*.

Um destes posicionamentos, constante no Acordo e Sentença n.º 477/1997[620], diz respeito à ilicitude da sua utilização (do *habeas data*) para pré-construir provas para processos posteriores quando deveriam funcionar como instrumento de proteção do patrimônio documental inviolável das pessoas; outro deles, constante no Acordo e Sentença n.º 84/1998[621], no âmbito do Tribunal de Apelação Civil e Comercial, que

---

[619] MARECOS GAMARRA, Adriana Raquel. *La protección de datos de carácter personal em el Paraguay.* In: **Revita Jurídica UCA Law Review.** Universidad Católica "Nuestra Señora de la Asunción" - Facultad de Ciencias Jurídicas y Diplomáticas, 2017. p 623-654. Disponível em: <https://www.pj.gov.py/ebook/monografias/nacional/informatico/Adriana-Marecos-Proteccion-de-datos-Py.pdf>. Acesso em: 30 jul. 2019. p. 5-9.

[620] CORTE SUPREMA DE JUSTICIA. Sala Constitucional. **Acuerdo y Sentencia n.º 477, de 1º de 1997.** Disponível em: <https://www.csj.gov.py/jurisprudencia/>. Acesso em: 30 jul. 2019.

[621] PARAGUAY. Tribunal de Apelación. Civil y Comercial. **Acuerdo y Sentencia n.º 84, de 10 de novimbre de 1998.** Marco Riera Hunter. Disponível em: <http://www.csj.gov.py/jurisprudencia/>. Acesso em: 30 jul. 2019.

recrimina a utilização de *habeas datas* para impugnar resoluções judiciais ao invés de servir ao propósito de proteger os direitos das pessoas.

### 4.6 A proteção de dados pessoais no Uruguai

O Uruguai não previa a proteção do consumidor em sua Constituição. A situação só veio a mudar com a promulgação da Lei n.º 17.189/1999, que estabeleceu suas normas relativas "*a las relaciones de consumo*"[622], legislação esta estruturada em 52 artigos e subdivididos em 15 capítulos.

De acordo com a legislação, são concedidos os seguintes direitos aos consumidores (art. 6°): (i) a proteção da vida, saúde e segurança contra os riscos causados por práticas no fornecimento de produtos e serviços considerados perigosos ou prejudiciais; (ii) educação e divulgação sobre o consumo adequado de produtos e serviços, a liberdade de escolha e igualdade de tratamento quando contratados; (iii) informação suficiente, clara e verdadeira em espanhol e sem prejuízo de que outras línguas também possam ser usadas[623].

Além dos direitos de (iv) proteção contra publicidade enganosa, métodos coercivos ou desleais no fornecimento de produtos e serviços e cláusulas abusivas nos contratos de adesão, cada um dentro dos limites estabelecidos nesta lei; (v) a associação em organizações cujo propósito específico é a defesa do consumidor e ser representado por elas; (vi) a efetiva prevenção e compensação de danos materiais e extradicionais; e (vii) acesso aos órgãos judiciais e administrativos para a prevenção e reparação de danos através de procedimentos ágeis e eficazes, nos termos previstos nos respectivos capítulos desta lei[624].

Desta listagem de direitos estendidos ao consumidor, observa-se a ausência dos direitos relacionados à proteção de dados pessoais, situação deveras semelhante com o ocorrido com a legislação dos outros três Estados Partes do MERCOSUL anteriormente analisados, demonstrando realmente ser a proteção de dados um direito moderno regionalmente.

---

[622] URUGUAY. **Ley n.º 17.189, de 07 de setembro de 1999.** Dictanse normas relativas a las relaciones de consumo. Em: <https://legislativo.parlamento.gub.uy/temporales/leytemp2082340.htm>. Acesso em: 24 jul. 2019.
[623] Ibid., não paginado.
[624] Ibid., não paginado.

Esta insuficiência protetiva foi suprida posteriormente com a edição e publicação da Lei n.º 18.331/2008 sobre "*Protección de Datos Personales y Acción de "Habeas Data*"[625]*.* Sua estrutura está disposta em 49 artigos, subdivididos em 9 capítulos. Nas disposições gerais há previsão expressa aos dados pessoais e sua elevação ao título de direito humano (art. 1º): "Direito humano.- O direito à proteção de dados pessoais é inerente à pessoa humana, por isso está incluída no artigo 72 da Constituição da República"[626].

Com relação ao seu âmbito material, a lei é aplicada "a dados pessoais registrados em qualquer meio que os torne suscetível de tratamento, e para todas as modalidades de uso posterior destes dados por esferas públicas ou privadas"[627]. São descritas também as definições dos termos técnicos aplicáveis e relacionados ao tratamento de dados pessoais.

A principiologia inerente à proteção dos dados pessoais igualmente foi contemplada. Foram prescritos os princípios da legalidade, veracidade, finalidade, consentimento informado prévio, segurança de dados, reserva e da responsabilidade (Capítulo II). E, relativo aos direitos dos titulares de dados pessoais, destacam-se os direitos à informação, acesso, retificação, atualização, inclusão e supressão de dados (Capítulo III).

Ademais, foram insertos dispostivos específicos sobre tratamentos de dados (Capítulo IV) e daqueles realizados pelos órgãos públicos (Capítulo V), a exemplo das normas para criação, modificação ou supressão de bases de dados de órgãos públicos, enquanto as de orgãos privados envolvem pessoas físicas e jurídicas e tratamentos como a criação, modificação ou exclusão (Capítulo VI).

A legislação também instituiu a autoridade de controle nacional, a Agência Descentralizada para o Desenvolvimento do Governo de Gestão Eletrônica e da Sociedade do Informação e Conhecimento (AGESIC), dotado da mais ampla autonomia técnica, a Unidade de Controle de Dados Regulatórios e Pessoais"

---

[625] URUGUAY. **Ley n.º 18.331, de 18 de agosto de 2008.** Protección de Datos Personales y Acción de Habeas Data. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008/29>. Acesso em: 25 jul. 2019.
[626] Ibid., não paginado. (tradução nossa).
[627] Ibid., não paginado (tradução nossa).

(Capítulo VII). Referido órgão de controle possui poderes técnicos, no entanto, não são poderes decisórios (art. 34)[628].

Derradeiramente, há previsão de ações de proteção de dados pessoais, a ação de Habeas Data, reconhecida como o "direito efetivo para tomar conhecimento dos dados referenciados a sua pessoa e de seu propósito e uso, que são registrados em bancos de dados públicos ou privado"[629].

No mesmo ano da publicação da legislação, parte da matéria foi regulamentada pelo Decreto n.º 664/2008[630], criando o Registro de Bancos de Dados Pessoais responsáveis pela Unidade Reguladora e Controle de Dados Pessoais (URCDP). A regulamentação sobre a proteção de dados pessoais foi complementada no ano consecutivo com o Decreto n.º 414/2009[631].

Este último decreto está estruturado em 41 artigos, subdivididos em 5 Títulos, com grande detalhamento normativo. Veja-se, por exemplo, sobre sua aplicação "à proteção de dados pessoais das pessoas físicas, direta ou indiretamente, por meio de qualquer informação acústica numérica, alfabética, gráfica, fotográfica ou qualquer outro tipo que se refira a eles"[632].

Guardando grande semelhança coma redação da Diretiva n.º 46/1995/CE, apresenta novas conceitos operacionais, aborda o consentimento dos titulares, a segurança dos dados, as obrigações do repensável pela base de dados ou pelo tratamento, que deve utilizar as medidas técnicas e organizacionais que sejam mais adequadas à integridade, confidencialidade e disponibilidade do tratamento[633].

Acresce-se aos direitos dos titulares de dados pessoais de acesso, atualização, retificação, inclusão, supressão, os relativos à comunicação e transferência de dados. A estrutura orgânica da autoridade de controle é definida (art. 31), bem como suas atribuições (art. 23)[634]. São descritas, outrossim, as normas de atuação do registro e os princípios da Administração Pública (art. 29)[635].

---

628 URUGUAY**. Ley n.º 18.331, de 18 de agosto de 2008. Protección de Datos Personales y Acción de Habeas Data.** Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008/29>. Acesso em: 25 jul. 2019.
629 Ibid., não paginado.
630 Id. **Decreto n.º 664, de 22 de dezembro de 2008.** Cria o registro de base de dados pessoais. Disponível em: <https://www.impo.com.uy/bases/decretos/664-2008>. Acesso em: 25 jul. 2019.
631 Id. **Decreto n.º 414, de 31 de agosto de 2009.** Regulamenta a Lei de Proteção de Dados. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>. Acesso em: 25 jul. 2019.
632 Ibid., não paginado. (tradução nossa).
633 Ibid., não paginado.
634 Ibid., não paginado.
635 Ibid., não paginado.

Impende salientar a respeito do resultado da pesquisa realizada pelo IDEC[636] sobre a Autoridade de Proteção de Dados do Uruguai. Consta do documento que a mesma realmente possui só autonomia técnica, não sendo independente para tomada de decisões, senão veja-se no excerto abaixo:

> No Uruguai, a autoridade é vinculada à Presidência e os diretores são indicados livremente pelo presidente. Apesar da "autonomia técnica" garantida por lei, no entanto, foram apontados conflitos de interesses, tendo em vista que o Poder Executivo e seus projetos também deveriam ser investigados pela autoridade. Estando diretamente vinculados, as decisões poderiam facilmente ser enviesadas e os membros, influenciados politicamente. Ainda assim, caso comparada com o modelo previsto pela Medida Provisória nº 869/2018, a autoridade uruguaia resguarda mais autonomia por ser um órgão "desconcentrado".

A análise sobre a figura da autoridade de controle uruguaia, realizada por Guidi em seu estudo, igualmente destaca que ela não possui poder decisório, apenas competência jurisdicional ou de resolução de conflitos. Nas suas palavras:

> Uma última característica da Autoridade de Proteção de Dados uruguaia é de grande relevância para o presente mapeamento: a inexistência de competência jurisdicional ou de resolução de conflitos. Ao contrário de modelos como o europeu, a Autoridade uruguaia não tem poder decisório para determinar certa conduta a um ente, público ou privado, que entre em conflito com um cidadão. Ao invés disso, a Autoridade deve informar, ao cidadão que a procure com uma querela, sobre os meios judiciais a sua disposição para buscar a tutela adequada de seus direitos. Não há, pois, uma instância administrativa dedicada a questões relacionadas a proteção de dados, sendo tais casos direcionados ao Poder Judiciário em geral, que pode ser acionado exclusivamente pelo titular dos dados[637].

Diante da ausência de meios administrativos de solução de controvérsias, resta ao titular dos dados buscar guarida legal no Poder Judiciário. Nesse sentido, e como visto anteriormente, a Lei n.º 18.331/2008 traz em seu bojo a ação de *Habeas Data* para que o titular tenha direito de tomar conhecimento de seus dados pessoais que foram registrados em banco de dados públicos ou privados.

---

[636] SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. **Autoridades de Proteção de Dados na América Latina:** um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. – São Paulo: IDEC, 2019. p. 36.

[637] GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 11 jul. 2019. p. 18.

Em que pese o a atuação do Judiciário tenha um papel mais ativo no processo de garantia da proteção de dados pessoais, importante é o fato de que o Uruguai, assim como a Argentina, adquiriu certificação europeia, sob à égide da Diretiva n.º 46/1995/CE acerca do seu nível de proteção ideal para transferência de dados com a EU, conforme a Decisão de Execução da Comissão (21/08/2012)[638].

Inobstante, também é válido ressaltar que a Diretiva n.º 46/1995/CE já está mais em vigor. Foi substituída pelo RGPD, o que faz com a certificação, tanta da Argentina quanto do Uruguai, esteja relativamente defasa, senão veja-se:

> O modelo uruguaio de regulação e proteção de dados pessoais guarda semelhanças com o modelo europeu, mesmo considerando que sua lei geral de proteção tomou sua inspiração da Diretiva 95/46/CE da União Europeia, modelo hoje praticamente ultrapassado, tanto pelo desenvolvimento do sistema uruguaio quando do próprio sistema europeu, com sua recente reforma. Não obstante, algumas diferenças são fundamentais, tanto na adoção inicial quanto nos caminhos adotados em um e noutro contexto[639].

Agora que analisadas as legislações de proteção de dados pessoais dos Estados Partes do MERCOSUL, é factível que todas as quatro nações possuem alguma normativa sobre a matéria, seja em âmbito constitucional ou em âmbito infraconstitucional, o que possibilita uma análise comparativa entre elas, conforme poderá ser conferido mais adiante na dissertação.

## 4.7 A proteção de dados pessoais em países de língua portuguesa

Contribuindo para verificação da viabilidade de uma normatização harmônica sobre proteção de dados pessoais em comunidades, os apontamentos de Masseno a respeito do nivelamento legislativo protetivo em Portugal e em outros países falantes de língua portuguesa servirão como fontes de direito comparado, nesta dissertação, tendo em vista sua pertinência temática e sua pesquisa atualizada.

---

[638] COMISSÃO EUROPEIA. **Decisão de Execução n.º 484/2012/UE, de 21 de agosto de 2012,** nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32012D0484&from=EN>. Acesso em: 20 jul. 2019.

[639] GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 11 jul. 2019. p. 17.

No artigo em questão, intitulado “A proteção de dados pessoais em Portugal e nos outros países de Língua Portuguesa: uma cartografia das fontes legislativas”[640], o autor referido realiza uma investigação legislativa, procurando reportar, objetivamente, os avanços e atrasos nos respectivos direitos internos dos países lusófonos e, de forma concomitante, apontar similitudes e diferenças entre eles.

No estudo, de um dos lados, é utilizado Portugal como referência, já sob a égide do RGPD e, de outro lado, a comunidade lusitana, unida pelos fatores linguístico e colonial, porém dispersa em geografia, desprovida de uma formação em bloco econômico como o MERCOSUL ou a UE - considerando todos os seus integrantes - e cada qual com suas próprias legislações.

Foram analisadas por Masseno as normas de proteção de dados pessoais, além das de Portugal, as de Angola, Brasil, Cabo Verde, Guiné-Bissau, Macau, Moçambique, São Tomé e Príncipe e Timor-Leste. E, considerando estas nações, importa trazer algumas das informações compiladas pelo autor e tecer alguns comentários sobre as conclusões pontuadas pelo autor.

A começar pela experiência portuguesa, o autor faz um apanhado das três gerações de proteção de dados pessoais influentes no país: na primeira, destaca a Lei n.º 10/1991, o dispositivo constitucional de *utilização da informática* (art. 35º) e a Convenção de Estrasburgo n.º 108/1981; na segunda, o microssistema normativo composto pela Diretiva n.º 46/1995/CE, transposta pela Lei n.º 67/1998[641].

E, na terceira geração, pela tríade substituta daquela, o Regulamento n.º 679/2016 - sobre proteção de dados pessoais e livre circulação de dados -, a Diretiva n.º 680/2016 - com enfoque na prevenção, investigação, detecção e execução para fins penais - e a Diretiva 681/2016 – sobre utilização dos dados dos registros de identificação dos passageiros[642].

No tocante à experiência de Cabo Verde, comenta Masseno haver previsão constitucional específica à utilização de meios informáticos, à proteção de dados pessoais (art. 44) e ao *habeas data* (art. 45), revelando enunciados mais detalhados

---

[640] MASSENO, Manuel David Rodrigues. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa: uma cartografia das Fontes Legislativas. **Revista Direito & TI – Debates Contemporâneos**: Porto Alegre, 2018.
[641] Ibid., p. 1-2.
[642] Ibid., p. 1.

que a própria constituição portuguesa. Destaca ainda as Leis n.º 41/2013, 42/2013 e 86/2015, especialmente a primeira, com conteúdo próximo ao europeu[643].

Acerca da experiência brasileira, ressalta os dispositivos constitucionais de proteção à vida privada, honra e imagem (art. 5º, "X") e de previsão do *habeas data* (art. 5º, LXXII), criticando sua ausência de regulamentação em três décadas; a Lei n.º 12.965/2014 (Marco Civil da *Internet*) - que trouxe limites ao tratamento de dados – e o Decreto n.º 8.771 – com a definição de dado pessoal e tratamento de dados[644].

Realça ainda as regras constantes na Lei n.º 8.078/1990 (CDC) e a Lei n.º 12.527/2011 (Lei de Acesso à Informação Públicas), ponderando que até então a proteção brasileira estava restrita apenas à intimidade, vida privacidade e segurança de dados. Culpa a dimensão continental, a jurisprudência fragmentária e a falta de regulamentação brasileira pelas mazelas[645].

Não obstante a atualidade do artigo de Masseno, desde a sua elaboração e publicação, ocorreu a entrada em vigência da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), com redação dada pela Lei n.º 13.853/2019, e a criação da Autoridade Nacional de Proteção de Dados (ANPD) brasileiros, cobrindo a defasagem histórica mencionada pelo estudioso.

No tocante à experiência de Macau, assinala haver previsão na Lei Básica da Região Administrativa Especial de Macau da República da China (1993)[646] de direito à reserva da intimidade e vida familiar (art. 30) e liberdade e sigilo dos meios de comunicação (art. 32), concretizados pela Lei n.º 08/2005. Elogia sua proximidade ao modelo europeu e critica a falta de independência da autoridade de controle[647].

Quanto à experiência de Angola, Masseno encontra previsão constitucional (art. 32 e 69), mas nada específico à proteção de dados pessoais. A deficiência foi suprida pela Lei n.º 22/2011, pelo Decreto n.º 214/2016 e pela Lei n.º 07/2017, revelando que a legislação do país seguiu os padrões portugueses e europeus. Demonstra receio quanto à independência não garantida do órgão de controle[648].

---

643 MASSENO, Manuel David Rodrigues. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa: uma cartografia das Fontes Legislativas. **Revista Direito & TI – Debates Contemporâneos**: Porto Alegre, 2018. p. 4.
644 Ibid., p. 6.
645 Ibid., p. 6.
646 Macau é uma região autônoma situada na costa sul da China continental. Embora tenha sido colonizada e administrada por Portugal até 1999, Macau não é reconhecida como Estado, mas sim como uma Região Administrativa Especial da China.
647 MASSENO, op. cit., p. 4.
648 MASSENO, op. cit., p. 5.

Relativo à experiência de São Tomé e Príncipe, também sem previsão constitucional específica (art. 24), o país já está alinhado com os modelos português e europeu, a exemplo das suas Leis n.º 03/2016 e 70/2017 que dispõem sobre a proteção de dados pessoais e autoridade nacional de controle, órgão este que não sofre interferência governamental[649].

No tocante à experiência do Moçambique, um reforço legislativo ainda é esperado. A Lei n.º 03/2017 regula as transações eletrônicas de dados, mas não há maiores garantias aos titulares de dados pessoais. O que há é o resguardo da privacidade (art. 41) e regras de uso da informática (art. 71). Percebe Masseno uma maior influência inglesa e um enfoque na questão dos deveres dos provedores[650].

A respeito da experiência do Timor-Leste, não diferindo muito da situação angolana, porém mais próximo à constituição portuguesa que aquela, o país já tinha disposto sobre a proteção de dados pessoais na constituição (art. 38). Todavia, carecendo de uma legislação específica, regula a matéria com projeções protetivas através das Leis n.º 05/2010, 01/2015 e 06/2016[651].

Derradeiramente, acerca da experiência de Guiné-Bissau, percebe-se uma proteção de dados pessoais quase incipiente. Há previsão constitucional de direito à reserva da intimidade da vida particular e familiar (art. 44, n.º 1), no entanto, nada explícito sobre o tratamento de dados, inclusive em nível infraconstitucional. Justifica Masseno este fato na instabilidade do governo e do parlamento do país[652].

Muito embora não tenha o estudo pretensão de formular ilações a respeito de uma uniformização ou sistematização normativa entre estes países, o conteúdo e conclusões nele constantes permitem tecer algumas considerações interessantes ao cerne da dissertação. E são parcos os estudos comparativos sobre o assunto em razão da sua atualidade, conquanto a temática esteja em evidência no momento.

Pois bem, antes algumas constatações. A primeira delas reside na inegável força da constitucionalização da proteção da privacidade nos países colonizados por Portugal. Segundo o estudo de Masseno, dispositivos desta natureza estão presentes

---

649 MASSENO, Manuel David Rodrigues. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa: uma cartografia das Fontes Legislativas. **Revista Direito & TI – Debates Contemporâneos**: Porto Alegre, 2018. p. 5.
650 Ibid., p. 5.
651 Ibid., p. 5.
652 Ibid., p. 6.

em todas as constituições nacionais analisadas. Obviamente, algumas com maior intensidade ou abrangência e outras com maior tecnicidade.

Mas fato é que a praxe legislativa portuguesa de inserção de dispositivos constitucionais, a título de direitos fundamentais e em celebração dos direitos humanos reconhecidos, exerceu notável influência sobre as outrora colônias que estiveram sob seu domínio imperial. Não é espantoso que a tradição legislativa tenha sido preservada e que haja certa semelhança com a Constituição de Portugal.

Barroso já sustentava que, em relação ao Legislativo, a constitucionalização "(i) limita sua discricionariedade ou liberdade de conformação na elaboração das leis em geral e (ii) impõe-lhe determinados deveres de atuação para realização de direitos e programas constitucionais"[653]. E o que se observa do estudo de Masseno é a regulamentação e atualização deste direito à privacidade.

O consenso majoritário é que proteção de dados pessoais derivou do direito à privacidade e a realidade moderna, a economia digital e a sofisticação dos direitos estão conduzindo todas as nações à necessidade de regulamentação da matéria. E assim o está sendo: vejam-se as recentes legislações aprovadas. Esta é a segunda constatação, de que há uma massiva normatização dos dados pessoais.

Veja-se, no tocante às datas, a aprovação das legislações protetivas de dados pessoais (ou congêneres) citadas por Masseno: Cabo Verde (2001, 2013 e 2015); Macau (2005 e 2007); Angola (2011, 2016 e 2017); São Tomé e Príncipe (2016 e 2017); Moçambique (2017); Timor-Leste (2010, 2015 e 2016); e Brasil (2014, 2016, 2018 e 2019), este acrescido das últimas legislações aprovadas.

Com exceção de Guiné-Bissau - pelos motivos expostos - e ciente de que algumas destas normativas de dados pessoais (e congêneres) elencadas – pelas suas respectivas datas de aprovação - tenham seguido os padrões protetivos portugueses anteriores ao RGPD (2016) - os padrões da Diretiva 46/1995/CE (1995) -, a conclusão de que esta tendência é intensa e crescente é plausível.

As próprias menções no artigo de Masseno quanto à criação e regulamentação das autoridades nacionais de proteção de dados pessoais e à preocupação latente quanto à independência ou vinculação delas aos órgãos governamentais - outra

---

[653] BARROSO, Luís Roberto. **Neoconstitucionalismo e constitucionalização do direito:** o triunfo tardio do direito constitucional no Brasil. Disponível em: <http://www.luisrobertobarroso.com.br/wp-content/uploads/2017/09/neoconstitucionalismo_e_constitucionalizacao_do_direito_pt.pdf>. Acesso em: 27 jul. 2019. p. 17.

constatação observada – demonstram seu emparelhamento com os padrões do RGPD da UE.

Ademais, em um exercício de comparação, no qual Portugal representasse a UE - e o RGPD fosse a norma vigente - e os países de língua portuguesa representassem os Estados Membros da UE - e estivessem sujeitos às normas deste megabloco -, eventual processo de uniformização legislativo seria facilitado em razão da supranacionalidade[654].

Supondo agora que Portugal representasse o MERCOSUL - e que o RGPD fosse um projeto legislativo desejável - e os países de língua portuguesa representassem os Estados Partes deste bloco - e que este projeto fosse indispensável ao avanço da Integração -, necessário seria a realização de uma harmonização legislativa e internalização da norma devido ao modelo operante de intergovernabilidade[655].

Há diferença entre os institutos da supranacionalidade, característico da UE, e da intergovernabilidade, característico do MERCOSUL. Enquanto este prioriza as políticas e interesses do bloco - transmitindo ideia de vinculação e verticalização normativa –, aquela prima pela tomada de decisão consensual – transmitindo ideia de desvinculação e horizontalização normativa. Neste sentido, comenta Gomes:

> Objetivamente, a diferença primordial entre o modelo integracionista da União Européia e do Mercosul está no instituto da supranacionalidade, que é condição para a existência da UE, pois permite que as políticas sejam fixadas segundo os interesses da Comunidade e que suas instituições atuem com autonomia na defesa desses interesses; enquanto no Mercosul vigora o sistema de intergovernabilidade, em que os procedimentos de funcionamento do

---

654 *Supranacionalidade:* "Tradução política de actos provenientes de órgãos independentes dos órgãos políticos nacionais, mas que os vinculam, quer no plano interno, quer no plano externo. Decorrem tais actos da aplicação prática de tratados aprovados pelos Estados, no pleno uso dos seus poderes soberanos, em que se aceita a limitação (muitas vezes confundida com partilha) desses mesmos poderes. Temos como exemplo os actos legislativos provenientes dos órgãos da União Europeia, que vêm assumindo um papel de cada vez maior relevo no plano da produção legislativa, substituindo em inúmeros domínios os órgãos legislativos nacionais" (SOUSA, Fernando de. **Dicionário de Relações Internacionais**. ed. 954. Santa Maria da Feira: Edições Afrontamento, 2005. p. 182).

655 *Intergovernabilidade:* "As decisões tomadas no âmbito dos órgãos de integração dos Estados-membros estão vinculadas a procedimentos internos de cada Estado-parte do bloco, logo são tomadas por governos nacionais, que estão sujeitos ao controle dos seus respectivos Parlamentos nacionais". (KERBER, Gilberto. **Mercosul e Supranacionalidade:** um estudo à luz das legislações constitucionais. Dissertação (Mestrado em Direito). UFSC: Florianópolis, 2000. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/78226/170264.pdf?sequence=1&isAllowed=y>. Acesso em: 30 jul. 2019. p. 30.

> bloco econômico são regidos pelos princípios do Direito Internacional Público.[656]

E, necessário sendo uma harmonização, quanto menor for o número de discrepâncias e de assimetrias entre os dispositivos das legislações internas, menor será o número de supressões ou atenuações que precisarão ser feitas para aproximá-las e coordená-las, para que funcionem e sirvam ao seu propósito de fortalecer o processo de integração do bloco.

Por exemplo, o fato destes países utilizarem o mesmo idioma, no caso, a língua portuguesa, tende a diminuir o número de variações conceituais ou interpretações terminológicas, facilitando o processo de harmonização. Ainda, o fato de suas legislações internas de proteção de dados pessoais indicarem significativa similaridade com os padrões europeus, é um grande passo neste sentido.

Conquanto o autor ressalte a existência de desníveis de regulação entre estes países[657], variando eles entre combinações de presença ou ausência de dispositivos constitucionais sobre privacidade particular, familiar e sigilo de comunicações eletrônicas e de leis gerais de proteção de dados pessoais, o que predomina é o espelhamento normativo nos modelos portugueses e europeus.

Obviamente, um processo de harmonização é mais complexo do que o exercício de suposição acima proposto, visto que inúmeras variáveis precisam ser consideradas; mas como bem descreve Masseno em seu artigo, trata-se de "uma realidade consolidada e suas réplicas" e, portanto, com os devidos "ajustes", uma normatização no âmbito do MERCOSUL seria possível.

---

[656] GOMES, Eduardo Biacchi. **A supranacionalidade e os blocos econômicos**. Revista da Faculdade de Direito UFPR. v. 38, n. 0, 2003. p. 159-183. Disponível em: <http://dx.doi.org/10.5380/rfdufpr.v38i0.1767>. Acesso em: 30 jul. 2019. p. 171.

[657] Masseno aponta no estudo quatro níveis diferentes nas regulações dos países falantes de língua portuguesa. O primeiro nível, caracterizado por uma disciplina constitucional expressa e uma lei geral de proteção de dados pessoais (Portugal, Cabo Verde e Angola); o segundo nível de regulação, caracterizado por uma disciplina constitucional expressa e ausência de lei geral de proteção de dados pessoais (Moçambique e Timor-Leste); o terceiro nível, caracterizado pela existência de uma lei geral de proteção de dados pessoais e ausência de disciplina constitucional (Macau e São Tomé e Príncipe); e o quarto nível, caracterizado pela ausência de disciplina constitucional expressa e de uma lei geral de proteção de dados (Guiné-Bissau e Brasil). Reitera-se que com a aprovação da Lei n.º 13.709/2018 (LGPD) e da provável aprovação da PEC n.º 17/2019, para inclusão da proteção de dados pessoais como direito fundamental, segundo os próprios critérios de Masseno, o país se enquadraria no primeiro nível de regulação.

## 4.8 A viabilidade da adoção de uma norma mercosurenha à luz do RGPD

Com a finalidade de constatar se as legislações de proteção de dados pessoais dos Estados Partes do MERCOSUL possuem majoritária similitude entre si - ou se elas apresentam muitas disparidades uma com a outra - e de mensurar o grau de facilitação ou dificultação para uma possível harmonização legislativa sobre a temática regionalmente para defesa do consumidor e combate ao *personal data breach*, far-se-á na sequência uma análise comparativa de determinados critérios técnicos relacionados à proteção de dados pessoais.

Insta reiterar que uma harmonização legislativa se refere à um processo conformador de disposições constantes nas respectivas leis dos países integrantes de uma comunidade sobre um problema ou temática de mútuo interesse para que, mediante a adoção de normativa em nível regional, se obtenha um bom funcionamento, desenvolvimento e coesão de regramentos nacionais distintos ao suavizar discrepâncias e eliminar conflitualidades[658]. No mesmo sentido, acerca deste método, comentam Amorim, Carvalho e Diz:

> A harmonização pode ser definida como a adoção, em nível comunitário de regras que tendem a assegurar o bom funcionamento do mercado Comum e de normas que devem se conformar com as legislações nacionais. Neste caso, estaríamos na presença de uma legislação em duas fases: uma comunitária, que se impõe aos Estados-Membros e outra, nacional, que cria direitos e impõe obrigações aos particulares conforme previsto nas normas do direito interno[659].

É neste contexto geral que a hipótese de uma harmonização normativa sobre proteção de dados pessoais no MERCOSUL deve ser analisada. Partindo do princípio que esta harmonização é plausível, vale-se como terceira teoria de base dos critérios de "nivelação legislativa protetiva entre países pertencentes ao mesmo bloco econômico", de Stribe (2015)[660], e dos apontamentos sobre "modelos normativos de

---

[658] OLIVEIRA, Renata Fialho de. **Harmonização Jurídica no Direito Internacional.** São Paulo: Quartier Latin, 2008. p. 23.

[659] DIZ, Jamile Bergamaschine Mata; AMORIM, Letícia Balsamão; CARVALHO, Karen Patrícia. Harmonização das normas de defesa do consumidor no Mercosul. In: **Revista de Ciências Humanas.** v. 1, n. 1 p. 60-67, fevereiro/julho. Universidade Federal de Viçosa - UFV: 2001. Disponível em: < https://www.locus.ufv.br/handle/123456789/13059>. Acesso em: 30 jul. 2019. p. 66.

[660] DA SILVA, Felipe Stribe. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria, 2015. Dissertação. Universidade Federal de Santa Maria (UFSM).

proteção de dados pessoais entre países falantes de língua portuguesa" de Masseno (2018)[661], anteriormente abordado.

Stribe utilizou em seu estudo seis critérios técnicos para dimensionar o grau de nivelação ou de desnível entre as legislações de proteção de dados pessoais nos direitos internos dos países do MERCOSUL, a saber: (i) conceituação de dados pessoais e sua classificação/espécies; (ii) regulamentação do uso de dado sensível; (iii) consentimento do usuário para captação e uso de dados conforme finalidade prevista; (iv) veracidade dos dados pessoais registrados; (v) procedimentos para acesso e retificação de dados; (vi) existência e atribuição de órgão de controle .

Realizando minuciosa análise das respectivas legislações dos países do MERCOSUL de acordo com referidos parâmetros, o autor conseguiu encontrar divergências e simetrias normativas e, através destes contrastes legislativos, pôde diagnosticar as possibilidades e desafios à uma harmonização da proteção dos dados pessoais entre os Estados Partes. Todavia, o estudo não traça comparativos com o RGPD, tampouco considera a recente LGPD brasileira, ambos inexistentes na época, razão pela qual o estudo aqui será atualizado em moldes parecidos.

Dentre os critérios técnicos niveladores utilizados por Stribe, serão considerados apenas cinco critérios para fim de análise legislativa comparativa: (i) conceituação de dados pessoais e sua classificação; (ii) regulação do uso de dados sensíveis; (iii) consentimento do titular dos dados pessoais; (iv) procedimento para acesso, retificação e uso dos dados pessoais; e (v) existência e atribuições de órgão de controle. Não será contemplado o critério técnico de veracidade dos dados pessoais registrados usado pelo autor[662].

---

[661] MASSENO, Manuel David Rodrigues. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa: uma cartografia das Fontes Legislativas. **Revista Direito & TI – Debates Contemporâneos**: Porto Alegre, 2018.

[662] A decisão para não inclusão nesta análise do critério técnico de "veracidade dos dados pessoais registrados", dentre outros possíveis para inserção, se deve à intenção de se evitar a repetição de argumentos comparativos, visto que ele está ligado ao princípio da exatidão/atualização que, por sua vez, está relacionado com o direito do titular de dados à retificação de seus dados pessoais, o qual se acredita trazer à discussão uma ideia de maior rigor protetivo que aquele. A justificativa também reside no intuito de evitar a saturação de critérios no cotejo, que já naturalmente esgotaria o espaço disponível, o que não se tem pretensão, mesmo porque inúmeros são os direitos, obrigações, modelos, técnicas, atribuições, variáveis etc. constantes nas legislações de proteção de dados pessoais dos países mercosurenhos que poderiam ser convertidos em critério técnicos e, portanto, serem passíveis de apreciação. O recorte comparativo é limitado considerando a relevância ao nível de proteção adequado e a preferência de Stribe na escolha dos critérios técnicos, inclusive porque se pretende atualizar o estudo no possível.

Como já enunciado alhures, as legislações adiante apreciadas serão as últimas leis de proteção de dados pessoais vigentes da Argentina (Lei n.º 25.326/2000), do Brasil (Lei n.º 13.709/2018), do Paraguai (Lei n.º 1.682/2001) e do Uruguai (Lei n.º 18.331/2008). Frise-se, uma vez mais, que eventuais normas venezuelanas sobre a temática não serão contempladas em virtude da sua suspensão do bloco econômico, por tempo indeterminado, por descumprimento da cláusula de compromisso democrático.

### 4.8.1 Conceituação de dados pessoais e sua classificação

O critério analisado de conceituação de dados pessoais foi escolhido em função de ser elemento indecomponível sobre os quais todo o RGPD, e, a bem da verdade, toda a legislação de proteção de dados pessoais está estruturada.

Em relação ao primeiro critério sobre a conceituação de “dados pessoais” constatou-se que a Argentina, Brasil e Uruguai possuem conceitos semelhantes. Para esses países, dados pessoais são quaisquer tipos de dados referentes a pessoas singulares determinadas ou determináveis. Destaca-se que o Paraguai não adota o conceito de dados pessoais.

Um Regulamento de Proteção de Dados Pessoais a nível de MERCOSUL, com conceituação de dados pessoais mais abrangente favorecerá o direito interno do Paraguai, tendo em vista possibilitar ao país uma melhor segurança na proteção dos dados dos consumidores.

Em relação à conceituação de dados sensíveis semelhantes foram identificados na Argentina, Brasil, Paraguai e Uruguai. No entanto, observa-se que na Argentina e no Uruguai não há menção sobre os dados pessoais sensíveis que possam causar dano ao titular do direito, como menciona Stribe, sendo esta a “principal característica do dado sensível, isto é, potencialidade de causar discriminação do titular, denotando-se, portanto, que o rol de dados considerados sensíveis poderia ser taxativo e não meramente exemplificativo”[663].

Conforme a Lei n.º 13.709/2018 (art. 11, §1º): “aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que

[663] DA SILVA, Felipe Stribe. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria, 2015. Dissertação. Universidade Federal de Santa Maria (UFSM). p. 126.

possa causar dano ao titular, ressalvado o disposto em legislação específica". Em relação ao Paraguai, este menciona sobre tratamento de dados pessoais sensíveis que possam promover "preconceitos e discriminação ou afetam a dignidade, privacidade doméstica e imagem de indivíduos ou famílias" (art. 4º da Lei 1.682/2001) [664].

### 4.8.2 Regulação do uso de dados sensíveis

O critério analisado de regulação de dados sensíveis foi escolhido em função de ser também um elemento essencial, por tratar de dados específicos, como (origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; dados relacionados com a saúde; dados relativos à vida sexual ou orientação sexual da pessoa).

Na análise sobre a regulamentação relativa ao tratamento do uso de dados sensíveis, com a finalidade de não causar discriminação ou dano ao titular, constatou-se que na Argentina, Brasil e Uruguai, países nos quais ninguém é obrigado a fornecer dados sensíveis. No entanto, há exceções previstas nas legislações dos países.

Na Argentina, um dado pode ser tratado como sensível caso seja de interesse geral, autorizado por lei, sendo proibida a formação de arquivos que possam revelar dados sensíveis. Assim, dados referentes a registros criminais só poderão ser tratados por autoridades públicas competentes e dados relativos à saúde (públicos ou privados) coletados se respeitado os princípios do segredo profissional.

No Brasil, o rol de exceções é mais amplo do que o da Argentina, tal como se pode facilmente constatar a partir da análise da legislação brasileira: cumprimento de obrigação legal; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; proteção da vida ou da incolumidade física do titular ou de terceiros; tutela da saúde, exclusivamente, em

---

[664] PARAGUAY. **Ley n.º 1.682, de 16 de enero de 2001.** Reglamenta la información privada. Visto em:<http://www.redipd.org/legislacion/common/legislacion/paraguay/Ley_1682_de_2001.pdf>.Acesso em: 30 jul. 2019. (tradução nossa).

procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária e a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (art. 11).

No Paraguai, observa-se a proibição da divulgação, mas inexiste menção ao tratamento de dado sensível. Neste sentido, o art. 4º da Lei 1.682/2001 menciona a proibição da divulgação de dados sensíveis de pessoas individualizadas ou individualizáveis. Conceitua como dados sensíveis, as informações de cunho raciais e étnicas; preferências políticas; estado de saúde; crenças religiosas, filosóficas ou morais; intimidade sexual e em geral aquelas que fomentam preconceito e discriminação ou afetam a dignidade, privacidade, intimidade e imagem do indivíduo. Entende-se, desse modo, que de maneira nenhuma poderá haver divulgação de dados sensíveis, pois não há menção na lei sobre possíveis exceções. Se não há de fato exceção à regra, há proteção definitiva do titular.

Em relação ao Uruguai, verifica-se que os dados confidenciais só podem ser tratados quando tiver interesse geral, autorizados por lei ou mandato legal; quando forem tratados para fins estatísticos ou científicos. Em relação à saúde, os dados podem ser tratados mediante o sigilo profissional.

Diante do exposto, observa-se que a Argentina, Brasil e Uruguai se assemelham no quesito de tratamento de dados em situações autorizadas por lei, mas o Uruguai acrescenta a situação do “mandato legal”; no tratamento de informações relacionadas à saúde, o direito dos países referidos é similar, no entanto, somente a Argentina e o Paraguai mencionam o sigilo profissional; no que tange ao tratamento para fins estatísticos e científicos, percebe-se que nada consta na Argentina a este respeito. Já na legislação brasileira há menção de realização de estudo por órgão de pesquisa, subentende-se haver relação com estatística e pesquisa, assemelhando-se, portanto, com a legislação uruguaia.

Constata-se que nesse critério, Argentina e Uruguai, se assemelham no geral, protegendo a violação de dados sensíveis que possam prejudicar a personalidade do titular. O Brasil se sobressai por apresentar um rol mais amplo de exceções no tratamento de dados sensíveis, o que aparenta ser um ponto negativo, pois, nesse caso, as regras não são mais tão protetivas. Como bem destaca Stribe, a “grande dificuldade surge das exceções a esta regra, sobretudo considerando o alto grau de amplitude conceitual”. O Uruguai, por sua vez, não esclarece como se dá o tratamento de dados pessoais sensíveis, apenas proíbe a sua comunicação.

### 4.8.3 Consentimento do usuário

O critério analisado referente ao consentimento do usuário foi escolhido por estar interligado à autonomia, pois caso contrário o mercado dominaria tudo.

Na análise desse critério, observa-se, regra geral, que na Argentina, Brasil e Uruguai, se exige o consentimento expresso e escrito. Entre estes países, destaca-se a regulamentação do Brasil, que prevê “consentimento escrito ou por outros meios que demonstrem a manifestação da vontade” (art. 8º Lei 13.709/2018).

O Paraguai, como visto anteriormente, não normatiza o tratamento de dados sensíveis e também não menciona como se daria o consentimento do titular para o tratamento destes, mas como a divulgação dos dados é proibida e não consta exceção, o consentimento, teoricamente, não seria algo necessário.

Vantajosa seria a harmonização legislativa ao Paraguai neste aspecto, porquanto relativizaria a inflexibilidade do consentimento e da divulgação de dados pessoais, que podem prejudicar a análise dos casos concretos com nuances fáticas e até mesmo engessar o funcionamento, a operabilidade, de certos mecanismos de tratamento designados na própria legislação.

### 4.8.4 Direito de acesso, retificação e uso

O critério analisado de procedimento para acesso, retificação e uso dos dados foi escolhido em função de estar ligado aos direitos fundamentais, humanos, consumeristas e principiologia relacionada à proteção de dados pessoais. Importa utilizá-lo para verificar se as legislações concedem aos titulares dos dados estes direitos e mensurar o nível de proteção e adequação.

Observou-se que Argentina, Brasil e Uruguai possuem direitos dos titulares devidamente expressos em suas legislações. A Argentina e o Uruguai possuem direitos semelhantes como acesso de informação, retificação, atualização ou exclusão. No Brasil, foi constatado um rol maior de direitos em relação aos direitos dos titulares de dados, na medida em que se concedem os mesmos direitos que nos demais países, acrescentando-se alguns outros como: anonimização, bloqueio ou eliminação de dados desnecessários; portabilidade de dados; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado

de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (art. 18).

Nesse último item vale comentar que a lei não esclarece quais consequências seriam essas. No Paraguai, por exemplo, não foi constatado direitos dos titulares. Depreende-se destas constatações que, para uma harmonização legislativa, a consideração de rol exemplificativo de direitos do titular seria mais benéfica, razão pela qual deveria ser considerada a da legislação brasileira.

Diante do exposto, concluiu-se que dentre os países do MERCOSUL, o Brasil possui um rol maior de direitos, no entanto os direitos básicos de acesso, retificação, atualização ou exclusão são comuns no direito interno dos Estados, com exceção do Paraguai - que não apresenta direitos em sua lei de proteção de dados pessoais.

### 4.8.5 Existência e atribuições de órgão de controle

O critério de atribuições de órgão de controle foi escolhido para análise em função de estar ligado à fiscalização, pois não há proteção de dados sem controle.

No quinto e último critério definido para verificar se as legislações analisadas possuem existência e atribuição de órgão de controle, observou-se a seguinte estrutura nos países em análise:

Com relação à Argentina, será necessário esclarecer resumidamente, a trajetória do seu órgão de controle, tendo em vista ter se modificado ao longo dos anos. Inicialmente foi criado um órgão denominado “Órgão de Controle”, através do art. 29 da Lei 25.326/2000, cujo objetivo era de controlar a execução das ações para cumprimento da lei, com uma série de atribuições de caráter conciliatório, bem como punitivo. Sua autonomia era funcional com atuação como órgão descentralizado no âmbito do Ministério da Justiça e dos Direitos Humanos da nação. Dirigido por um diretor, selecionado pela experiência na área, por um período de 4 (quatro) anos.

Com a regulamentação da Lei nº 25.326/2000, por meio do Decreto nº 1.55/2001, passou o referido órgão a ser denominado “Direção Nacional de Proteção de Dados Pessoais – DNPDP”, órgão da Administração Direta. Em 2017, com a publicação do Decreto nº 746/2017, que tratava das modificações dos Ministérios, passou o referido órgão para a Administração Indireta. Diante do exposto, observa-se que a Argentina, possui a Direção Nacional de Proteção de Dados Pessoais, com atribuições previstas em lei, no entanto, não possui poder de decisão.

Em relação ao Brasil, como já comentado anteriormente, o país também possui uma história em torno da criação do seu órgão de controle. Através da Lei 13.709/2018 (LGPD), semelhante à do RGPD da UE, foi criado o órgão denominado “Autoridade Nacional de Proteção de Dados - ANPD”, mas o artigo não passou pela votação do Congresso, sendo vetado. Sendo assim, toda a regulamentação em torno da criação do órgão foi vetada também. Mais adiante, com a publicação da MP 869/2018, por sua vez convertida na Lei n.º 13.853/2019, recente, criou-se a Autoridade Nacional de Proteção de Dados - ANPD, mas o artigo não passou pela votação do Congresso, sendo vetado. A ANPD possui autonomia técnica e decisória, é um órgão da Administração Pública Federal vinculado à Presidência da República. Importante esclarecer que a sua natureza é transitória em função da possibilidade de se transformar pelo Poder Executivo Federal em entidade da Administração Indireta, após 2 (dois) anos da entrada em vigor da norma que o criou, em 28 de dezembro de 2018.

O Órgão é composto pelo Conselho Diretor, Conselho Nacional de Proteção de Dados Pessoais, Corregedoria, Ouvidoria, órgão de assessoramento jurídico e unidades administrativas. Tem atribuições conciliatórias, de conscientização, fiscalização, edição de normas, punição, entre outras mencionadas no art. 55-J. Destaca-se que a ANPD tem a competência exclusiva no que se refere à proteção de dados pessoais.

No tocante ao Paraguai, observou-se não constar um órgão de controle com denominação de “Autoridade de Proteção de Dados” ou congênere, como é padrão enxergado em grande maioria dos países que a criam, contudo, há um Tribunal Civil e Comercial competente na matéria para a aplicação das sanções.

Ademais, registra-se que o Uruguai possui um Órgão de Controle descentralizado, denominado Agência para o Desenvolvimento do Governo de Gestão Eletrônica e da Sociedade da Informação e do Conhecimento – AGESIC, com ampla autonomia técnica, vinculada à Unidade de Regulação e Controle de Dados Pessoais. Dirigido por um Conselho de três membros (Diretor Executivo, mais dois membros designados pelo Executivo, mediante seleção por competência).

No quesito atribuições, pode-se dizer que se assemelha aos demais países ao ser constatado que trata da conciliação, edição de normas, censo, controles, conscientização, todavia, não foi notada a função de aplicação de sanções. É previsto

ainda na legislação a possibilidade de entrar com ação de *habeas data*, para fazer valer seus direitos sobre os dados pessoais.

Diante da análise da existência ou não de órgão de controle, independentemente de sua denominação, constatou-se que a Argentina, Brasil e Uruguai possuem suas autoridades designadas, com atribuições semelhantes e que o Paraguai não a possui, apesar de dispor de tribunais específicos para aplicações das penalidades. Sendo assim, um regulamento geral de proteção de dados pessoais em nível de MERCOSUL contribuiria para o direito interno do Paraguai.

Por fim, considerando os cinco critérios analisados (conceituação de dados pessoais e sua classificação/espécie, regulamentação do uso de dado sensível, consentimento do usuário para captação de dados, procedimento para acesso e retificação e uso de dados e existência e atribuições de órgão de controle), percebe-se que Argentina, Brasil e Uruguai estão mais bem estruturados, em relação à legislação de proteção de dados. O Brasil, embora tenha sido o último a publicar lei especifica na área de proteção de dados, já previa em sua Constituição a proteção do direito do consumidor, *habeas data*, entre outros. E atualmente entende-se que possui a melhor estrutura de proteção de dados pessoais dentre os Estados Partes do MERCOSUL, revelando-se que a sua legislação se assemelha diretamente ao RGPD da UE. O Paraguai, por sua vez, ainda parece estar aquém dos demais Estados Partes em certos aspectos, cuja padronização lhe beneficiaria.

Já é sabido que para harmonizar legislação num processo de integração, a semelhança dos dispositivos constantes nas legislações internas dos Estados envoltos contribui sobremaneira para que a elaboração de uma norma regional seja facilitada, internalizada e alcance o propósito pelo qual foi idealizada, projetada, e, futuramente, adotada e executada. No caso em apreço, no qual foram definidos alguns critérios considerados mais relevantes, mas não todos os dispositivos das quatro legislações, perceptível foi que os quatro países são majoritariamente semelhantes em vários aspectos, mas divergentes em algumas nuances. E, não sendo iguais, as partes deverão encontrar um denominador comum para concretizar um regulamento geral para todos do bloco.

Teruchkin, em estudo realizado sobre a proteção dos consumidores, destaca bem essa situação em que ora se encontram os Estados Parte do MERCOSUL, em relação à proteção dos dados pessoais. Há a necessidade de harmonizar as legislações existentes em cada país, no entanto a discussão gira em torno de como

constituir uma unificação das normas, pois "quanto maiores forem as diferenças existentes entre as legislações protetoras dos consumidores dos países, mais complexas serão as dificuldades a serem enfrentadas para compatibilizá-las[665]".

Tendo em vista (i) que no Tratado de Assunção foi previsto como compromisso dos Estados Parte a harmonização de suas legislações, nas áreas pertinentes, para lograr o fortalecimento do Processo de Integração (art. 1º ); (ii) a insuficiência legislativa sobre matéria de proteção de dados pessoais no âmbito do MERCOSUL; (iii) a existência de regulamentação sobre a temática nos Estados Partes do MERCOSUL; entende-se como de grandiosa importância e necessidade a harmonização das legislações em um Regulamento Geral de Proteção de Dados do MERCOSUL, que possa facilitar o comércio de dados, possibilitando também a comunicação com a UE e, acima de tudo, proteger o direito do (ciber)consumidor contra os *personal data breaches.*

Um Regulamento Geral de Proteção dos Dados do MERCOSUL beneficiará as partes, em especial ao Paraguai que possui uma legislação de proteção de dados menos abarcadora e evoluída em relação aos demais países. Lembrando que o MERCOSUL, dentro do seu sistema de intergovernabilidade, exige que todos os tratados e acordos realizados sejam ratificados pelos Estados Partes.

Diante do exposto e considerando que o MERCOSUL já tem um expressivo acervo de legislações harmonizadas em matéria consumerista e de comércio eletrônico, acredita-se ser possível, portanto, harmonizar as quatro legislações referentes à proteção de dados pessoais e adotar uma norma regional para o bloco, espelhada no RGPD, feitos os devidos reajustes para aproximação/eliminação dos possíveis conflitos existentes entre elas, sem deixar de levar em consideração as vicissitudes e particularidades dos Estados da zona integrada.

---

[665] TERUCHKIN, Sônia Unikowsk. A proteção dos consumidores no Mercosul: algumas considerações. In: **Revista Indicadores Econômicos – IE** – v. 25. n.4., 1998. p. 278-293 Disponível em: <https://revistas.fee.tche.br/index.php/indicadores/article/view/1173>. Acesso em: 29 jul. 2019. p. 286-287.

## 5 CONSIDERAÇÕES FINAIS

Não parece mais espantoso que exista um choque entre privacidade e segurança dos dados pessoais e que isto desperte uma discussão entre intimidade, publicidade e modernidade. O advento da tecnologia da informação e do tratamento automatizado destes dados pessoais pode fazer com que eles sejam indevidamente terceirizados e/ou abusivamente utilizados e/ou até mesmo sequestrados/vazados.

E, neste cenário, de inquietude, desconfiança e vulnerabilidade se encontra o cidadão, o usuário, o consumidor, o internauta, o ciberconsumidor, o potencial prejudicado, cuja intimidade e privacidade foram violados ou estão à mercê de os ser. E resta a dúvida, que já ecoava no universo jurídico nas últimas décadas, e se estes aspectos digitais não fossem regulamentados?

Esta revolução tecnológica, seguida da evolução legislativa, revelou-se espontânea. No caso da proteção de dados pessoais, a realidade demonstrou estar o arcabouço legislativo clássico defasado, na medida em que ficou incapaz de tutelar os direitos de personalidade modernos satisfatoriamente em virtude das novas tendências e novos reclames tecnológicos.

Primeiro, pela complexidade técnica estranha ao direito; segundo, pelo processamento virtual dos dados pessoais quase às ocultas do seu portador. Nesta senda, perdido o vínculo físico entre o titular e sua informação pessoal, indispensável que o vínculo jurídico deste com aquela fosse preservado. E, para tanto, necessária a atualização das legislações de outrora.

Contudo, a vinculação jurídica entre o consumidor e seus dados pessoais não é o único problema. Houve uma sofisticação dos interesses, das causas e das técnicas de violação destas “informações”, a exemplo dos *phishing* (“pescaria”), *credential stuffing* (preenchimento de credenciais), *web app vulnerabilty* (vulnerabilidade de aplicativos web), *spam* (e-mails não solicitados), *malicious insider or outsider* (ameaças internas e externas), *insecure database* (banco de dados inseguros); *unauthorized access* (acesso não autorizado); *malware* (programas malignos), dentre tantos infindos outros.

Estes estratagemas, geralmente utilizados por um *hacker* ou *cracke*r - mas sem desconsiderar o fator humano, a imperícia técnica e o maquinário antiquado como eventuais causadores - acabam provocando uma *security breach* (falha de segurança) e, potencialmente, uma *data breach* (violação de dados), sendo este último caso

hipótese na qual os dados são ilegalmente acessados, sem autorização divulgados, muitas vezes mercantilizados ou barganhados, e até mesmo perdidos/apagados, com uma reversibilidade de danos baixíssima.

Foi pensando neste cenário contemporâneo e cotejando este panorama jurídico que, nesta dissertação, se objetivou verificar a viabilidade da adoção de uma norma, no âmbito do MERCOSUL, à luz RGPD, que defendesse os consumidores contra o *personal data breach* (as violações de dados pessoais).

Portanto, o problema de pesquisa que guiou a dissertação se referiu a: sob quais condições seria possível a adoção de uma norma, no âmbito do Mercosul, destinada a proteger o consumidor contra o *personal data breach*, aos moldes do RGPD? E a hipótese trabalhada, que responderia à referida problematização, apontava no sentido de que a viabilização do referido espelhamento normativo era possível no atual cenário do Mercosul diante da (i) insuficiência legislativa, no âmbito do Mercosul, em matéria de proteção de dados pessoais, ao passo que existiria uma forte tendência regional e internacional de normatização e padronização da temática; e da (ii) compatibilidade relativa de critérios técnicos das leis protetivas de dados pessoais dos Estados Partes do Mercosul entre si e com o RGPD.

Neste desiderato, um esforço foi feito para analisar legislações sobre proteção do consumidor e, especialmente, sobre proteção de dados pessoais, de países europeus chaves – das leis mais antigas até as mais atuais, visto que pioneiros nesta última área -, de países latino-americanos – para localizar a temática, traçar paralelos e encontrar pontos de convergência de interesses – dos países mercosurenhos – pois neles reside a problemática – e até de países falantes da língua portuguesa – para descobrir paralelos e fatores que auxiliem na realização de um processo de harmonização legislativa de proteção de dados pessoais.

Constatou-se nas investigações realizadas que o Regulamento n.º 679/2016/UE (RGPD) é o documento normativo com maior nível de atualização e proteção no quesito dados pessoais, um verdadeiro instrumento garantidor de direitos humanos e fundamentais, enfrentador de violações de segurança de dados e gestor para prevenção de incidentes futuros. Uma evolução necessária e bem-vinda da longeva Diretiva n.º 46/1995/CE.

Verificou-se que os Estados Partes do MERCOSUL (Argentina, Brasil, Paraguai e Uruguai têm buscado a proteção de dados pessoais. Explorando o histórico legislativo da proteção de dados no seu direito interno foi possível concluir que a

Argentina e o Uruguai foram os pioneiros na proteção de dados pessoais, recebendo, durante à égide da antiga Diretiva n.º 46/1995, a titulação/certificação de países com nível adequado de proteção de dados pessoais, façanha pouco comum nos países latino-americanos à época.

O Paraguai, durante o escrutínio normativo, revelou-se o Estado Parte que mais tardou para incluir a proteção do consumidor em disciplina constitucional, o que somente veio a ocorrer em 1992 e, no tocante aos dados pessoais, que apenas em 2001 foram publicadas as primeiras normatizações sobre a matéria.

O Brasil, muito embora seja exemplar no que diz respeito à proteção do consumidor, seja constitucional ou infraconstitucionalmente, não possuía uma legislação especifica para a proteção dos dados pessoais até a criação do Marco Civil da *Internet* e sua regulamentação. Não obstante sua tardia atualização, com a recente aprovação da Lei Geral de Proteção de Dados (LGPD), sobremaneira semelhante ao RGPD, é possível concluir que agora a legislação brasileira está melhor estruturada e oferece o maior nível protetivo dentro todos os Estados Partes.

Para comprovação ou denegação da hipótese de trabalho da dissertação, foi realizado um estudo de direito comparado, cotejando cinco critérios técnicos indispensáveis para uma possível harmonização legislativa de dados pessoais, a saber: (i) conceituação de dados pessoais; (iii) conceituação de dados sensíveis; (iii) consentimento do titular de dados; (iv) direitos de acesso, retificação e uso de dados; e (v) existência e atribuições dos órgãos de controle.

Percebeu-se, por meio da análise desses critérios, que a Argentina, o Brasil e o Uruguai estão melhores estruturados no que tange à proteção de dados pessoais e que o Paraguai, por sua vez, demonstra estar aquém em certos aspectos, no entanto, guarda equiparação na maioria dos critérios. E, comparando o nível de proteção fornecido pelo RGPD da UE, a legislação dos Estados Partes analisados ainda apresenta assimetrias.

Tendo em vista (i) que no Tratado de Assunção foi previsto como compromisso dos Estados Partes a harmonização de suas legislações, nas áreas pertinentes, para lograr o fortalecimento do Processo de Integração (art. 1º ); (ii) a insuficiência legislativa sobre matéria de proteção de dados pessoais no âmbito do MERCOSUL; (iii) a existência de regulamentação sobre a temática nos Estados Partes do Mercosul; entende-se como confirmada a hipótese de trabalho da dissertação, como suficientemente existente as condições capazes de propiciar uma harmonização

legislativa em um Regulamento Geral de Proteção de Dados do MERCOSUL, que possa facilitar o comércio de dados, possibilitar a comunicação com a UE e, acima de tudo, proteger o direito do consumidor contra os *personal data breaches.*

Conclui-se também que um Regulamento Geral de Proteção dos Dados Pessoais, no MERCOSUL, beneficiará as partes, em especial ao Paraguai que possui uma legislação de proteção de dados menos abarcadora e evoluída em relação aos demais países do bloco econômico.

Os benefícios da adoção de uma norma protetiva sobre a matéria impactarão sobremaneira e diretamente no cotidiano regional dos consumidores, já acostumados com a transmissão transfronteiriça, ainda não padronizada, de dados pessoais. Haverá maior segurança no tratamento e na circulação destes dados, uma vez que estendido a todos as medidas securitárias mais atuais e efetivas. A padronização facilitará ainda o processo de cooperação regional entre os órgãos de controle, cuja assistência se verá revertida em prol dos próprios consumidores.

As vantagens serão percebidas ainda com possível diminuição dos casos de violações de dados pessoais, uma vez que exponencialmente proporcionais ao baixo nível de proteção. E, ainda que não seja possível expurgar esta mazela digital, a medida de Avaliação de Impacto de Violação de Dados Pessoais contribuirá preventivamente e a notificação aos titulares de dados sobre a ocorrência do ato invasivo e a tomada de contramedidas urgentes pelos responsáveis (e subcontratantes) e autoridades competentes servirão para minimizar os efeitos e danos decorrentes.

Diante do exposto e considerando que o MERCOSUL já tem um expressivo acervo de legislações harmonizadas em matéria consumerista e de comércio eletrônico, verificou-se ser possível, portanto, harmonizar as quatro legislações referentes à proteção de dados pessoais e adotar uma norma regional para o bloco, espelhada no RGPD, feitos os devidos reajustes para aproximação/eliminação dos possíveis conflitos e assimetrias existentes entre elas.

Como contribuição prática desta dissertação e, possivelmente, como esboço inicial para eventual adoção de modelo normativo em matéria de proteção e circulação de dados pessoais a este cenário integracionista, foi elaborada uma proposta de Tratado baseada nos cinco critérios técnicos definidos e analisados nas quatro legislações de proteção de dados pessoais dos Estados Partes do MERCOSUL, no

modelo do Projeto de Decisão n.º 110 do MERCOSUL/CMC e inspirada nas disposições do Regulamento n.º 679/2016/UE (RGPD).

A Proposta segue adjunto à dissertação (Anexo-A) e, no seu diminuto corpo normativo, leva em consideração os dados pessoais, dados sensíveis, consentimento, acesso, retificação e atualização, uso dos dados e órgão de controle como critérios técnicos para harmonização legislativa em defesa do consumidor e de seus dados pessoais. Buscando conciliar as divergências, aproximar as semelhanças e afastar as incompatibilidades, a proposta segue o modelo europeu e vale-se mais, portanto, dos dispositivos constantes na legislação brasileira.

## REFERÊNCIAS

AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA. **Protección de datos personales.** Institucional. Disponível em: <https://www.argentina.gob.ar/aaip/datospersonales>. Acesso em: 14 mar. 2019.

ALENCAR, Ianara de Souza; PACHECO, Ludgard Vinicius Andrade; FERREIRA, Rodrigo leal. A Evolução do conceito de privacidade diante das novas tecnologias utilizadas nos correios eletrônicos (E-mail). Piauí: **Revista de Direito UNINOVAFAPI**. v. 1, n. 1., 2016.

AMADEO, Auletta Tommaso. **Riservatezza e tutela della personalità.** Milano: Giuffrè, 1978.

AMARAL JÚNIOR, Alberto do; VIEIRA, Luciane Klein. A proteção internacional do consumidor no Mercosul. In: **Revista de Direito do Consumidor.** vol. 106 – jul-ago 2016.

ARAÚJO, Alexandra Maria Rodrigues. **As transferências transatlânticas de dados pessoais:** o nível de proteção adequado depois de Schrems. Revista de Direitos Humanos e Democracia. Editora Unijuí, ano 5. n. 9. jan./jun, 2017. p. 201-236.

ARGENTINA. Buenos Aires. Corte Suprema de Justicia de la Nacion. **Expediente nº3536/2019.** Principios rectores para los procesos y procedimientos involucrados en la interceptación y captación de comunicaciones.-Disponível em: <https://www.csjn.gov.ar/documentos/descargar/?ID=117364

_____. **Decreto n.º 746, de 25 de Septiembre de 2017. Modificación de Funciones en Ministerios.** Disponível em: <http://argentinambiental.com/legislacion/nacional/decreto-74617-modificacion-funciones-ministerios/>. Acesso em: 22 jul. 2019.

_____. **Decreto Reglamentario n.º 1.558, de 29 de novembro de 2001.** Disponível em: < http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=D31E6955E0657D42EF16E6061748B221?id=70368>. Acesso em: 20 jul.2019.

_____. **Ley n.º 24.240, de 13 de Octubre de 1993.** Defensa del Consumidor. Normas de Protección y Defensa de los Consumidores. Autoridad de Aplicación. Procedimiento y Sanciones. Disposiciones Finales. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/638/texact.htm>. Acesso em: 20 jul. 2019.

_____. **Ley n.º 25.326, de 30 de Octubre de 2000.** Proteccion de los datos personales. Disponível em: <https://www.oas.org/juridico/PDFs/arg_ley25326.pdf>. Acesso em 20 jul.2019.

ASIA-PACIFIC ECONOMIC COOPERATION (APEC). **APEC#205-SO-01.2, December 2005.** Privacy Framework. Disponível em: <http://bit.ly/1zRV0QK>. Acesso em: 24 jul. 2019.

ASSEMBLEIA GERAL DA ONU. **Resolução 68/167, de 18 de dezembro de 2013** [on the report of the Third Committee (A/68/456/Add.2)]. O Direito à privacidade na era digital. Disponível em: < http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>. Acesso em: 21 fev. 2019.

_____. **Resolução 69/166, de 18 de dezembro de 2014** [on the report of the Third Committee (A/69/488/Add.2 and Corr. 1)]. O Direito à privacidade na era digital. Disponível em: < http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166>. Acesso em: 21 fev. 2019.

_____. **Resolução 70/186, de 22 de dezembro de 2015** [on the report of the Second Committee (A/70/470/Add.1)]. Diretrizes das Nações Unidas para proteção do consumidor. Disponível: < https://unctad.org/meetings/en/SessionalDocuments/ares70d186_en.pdf>. Acesso em: 14 mar. 2019.

_____. **Resolução n.º 217-A, inciso III, de 10 de dezembro de 1948.** Declaração Universal dos Direitos Humanos. Disponível em:<http://www.un.org/en/universal-declaration-human-rights/>. Acesso em: 21 fev. 2019).

ASSIS, Ana Cláudia Mrando Lopes; ASSIS, Vinicius de; ZUIN, Aparecida Luzia Alzira. **A dinâmica tecnológica e os desáfios na regulação do direito do consumo no Brasil.** p. 20-35. In: Desafios socioambientais das sociedades de consumo, informacional e tecnológica [recurso eletrônico] / Aidee Moser Torquato Luiz... [et al.]; organizadores, Pedro Abib Hectheuer, Bruna Borges Moreira Lourenço, Marcia Abib Hecktheuer. – Itajaí: UNIVALI, 2018.

BARRETO JUNIOR, I. F.; AULER, H.; BARBOSA, M. A. Hacktivismo e ativismo digital na sociedade da informação. In: Redes: **R. Eletr. Dir. Soc**., Canoas, v. 4, 2016, p. 126-146. Disponível em: <https://revistas.unilasalle.edu.br/index.php/redes/article/view/2318-8081.16.28/pdf>. Acesso em: 18 jul. 2019.

BARROSO, Luís Roberto. **Neoconstitucionalismo e constitucionalização do direito:** o triunfo tardio do direito constitucional no Brasil. Disponível em: <http://www.luisrobertobarroso.com.br/wp-content/uploads/2017/09/neoconstitucionalismo_e_constitucionalizacao_do_direito_pt.pdf>. Acesso em: 27 jul. 2019.

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

BLACKSTONE, William. **Commentaries on the Laws of England.** Oxford: Clarendon Press, 1765.

BOFF, Salete Oro; FORTES, Vinícius Borges. **Internet e proteção de dados pessoais:** uma análise das normas jurídicas brasileiras a partir das repercussões do caso nsa vs. Edward Snowden. Cadernos do Programa de Pós-Graduação em Direito da UFGRS, volume 11, 2016.

BOLESINA, Iuri; Rossoni Caroline. **A teoria dos círculos concêntricos e a proteção à vida privada:** análise ao caso Von Hannover Vs. Alemanha, julgado pela Corte Europeia de Direitos Humanos. In: XI Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea – VII Mostra de Trabalhos Jurídicos Científicos. 2014.

BRANDEIS, Louis; WARREN, Samuel. **The right to privacy**. In: 4 - Harvard Law Review 193, 1980.

BRASIL. Brasília. Conselho Nacional da Justiça- CNJ. **Pedido de Providência. Processo n.º 0004068-95.2015.2.00.0000.** Exclusão de dados pessoais de candidatos a cargos públicos. Requerente: Sérgio Iglesias Nunes de Souza. Requerido: Conselho Nacional de Justiça - CNJ. Relator: Cons. Valtércio de Oliveirai, 19 de outubro de 2018. Disponível em: <http://www.omci.org.br/jurisprudencia/272/concurso-publico-e-ferramenta-no-follow/>. Acesso em: 29 jul. 2019).

_____. **Constituição da república federativa do brasil de 1988.** Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 26 jul. 2019.

_____. **Decreto n.º 7.030, de 14 de dezembro de 2009.** Promulga a Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos Artigos 25 e 66. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Decreto/D7030.htm>. Acesso em: 28 jul. 2019.

_____. **Decreto n.º 8.771, de 11 de maio e 2016.** Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 26 jul. 2019.

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

_____. **Lei n.º 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 26 jul. 2019.

_____. **Lei n.º 9.507 de 12 de novembro de 1997.** Dispõe sobre o regulamento do direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm>. Acesso em: 25 jul. 2019.

_____. **Lei n.º 12.414 de 09 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 26 jul. 2019.

_____. **Lei n.º 12.527 de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Aceso em: 26 jul. 2019.

_____. **Lei n.º 12.737 de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 25 jul. 2019.

_____. **Lei n.º 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 25 jul. 2019.

_____. **Lei n.º 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 26 jul. 2019.

_____. **Lei n.º 13.853 de 08 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm>. Acesso em: 26 jul. 2019.

_____. **Medida Provisória n.º 869, de 27 de dezembro de 2018.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 26 jul. 2019.

_____. **Projeto de Lei n.º 4.060, de 13 de junho de 2012.** Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em:

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 26 jul. 2019.

_____. Rio de Janeiro. Tribunal de Justiça. **Recurso Especial nº 1.660.168 - RJ (2014/0291777-1).** Direito Civil. Obrigação de fazer. Recorrente: YAHOO! DO BRASIL INTERNET LTDA e GOOGLE BRASIL INTERNET LTDA. Recorrido: D P N. Relatora: Ministra Nanci Andrighi, 08 de maio de 2018. Disponível em: <http://www.omci.org.br/jurisprudencia/251/dados-pessoais-e-direito-ao-esquecimento/>. Acesso em: 29 jul. 2019).

CALHEIROS, Tânia da Costa; TAKADA, Thalles Alexandre. **Reflexões sobre a privacidade na sociedade da informação.** Londrina, v. 4, n. 1, p. 120 – 134, jan./jun. 2015.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. 7. ed. Coimbra: Almedina, 2003.

CASTELLS, Manuel. **A galáxia da Internet:** reflexões sobre a internet, os negócios e a sociedade. – Rio de Janeiro: Zahar, 2003.

CAVALCANTE, Rebeca Freitas. **Ciberativismo:** como as novas formas de comunicação estão a contribuir para a democratização da comunicação. Universidade Nova de Lisboa, 2010.

CHAGAS, Morgana Santos das. **Ciberterrorismo:** as possibilidades da expansão do terror nas relações internacionais. Monografia. João Pessoa: UEPB, 2012.

COMBREXELLE, Jean-Denis**. Les Limites du controle de la Commission natiolanes de l'informatique et des libertés dans le régime de la declaration.** RFDA, v. 13, n. 3, mai/juin.

COMISSÃO EUROPEIA. **COM n.º 043/Final/2018 – Comunicação da Comissão ao Parlamento Europeu e ao Conselho, de 24 de janeiro de 2018.** Maior proteção, novas oportunidades — Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0043>. Acesso em: 11 jul. 2019.

_____. **COM n.º 0627/Final/2015/0284, de 9 de dezembro de 2015.** Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A0627%3AFIN>. Acesso em: 30 jul. 2019.

_____. **COM n.º 0634/Final/2015/0287, de 9 de dezembro de 2015.** Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015PC0634>. Acesso em: 30 jul. 2019.

COMISSÃO EUROPEIA. **Decisão de Execução n.º 484/2012/UE, de 21 de agosto de 2012,** nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32012D0484&from=EN>. Acesso em: 20 jul. 2019.

_____. **Decisão n.º 490/2003/CE, de 30 de junho de 2003.** Decisão da Comissão relativa à adequação do nível de proteção de dados pessoais na Argentina. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32003D0490&from=EN>. Acesso em: 20 jul. 2019.

_____. **Sete coisas que as empresas da UE27 precisam de saber para se preparar para o Brexit.** Disponível em: <https://ec.europa.eu/info/sites/info/files/factsheet-preparing-withdrawal-brexit-preparedness-web_pt.pdf>. Acesso em: 5 jul. 2019.

_____. **Proteção de dados na UE.** Autoridades nacionais de proteção de dados. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt>. Acesso em: 15 jul. 2019.

CONSELHO DA UNIÃO EUROPEIA. **Decisão-Quadro n.º 977/2008/JAI do Conselho, de 27 de novembro de 2008**, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60), revogada a partir de 6 de maio de 2018. Disponível em: <https://www.consilium.europa.eu/pt/documents-publications/>. Acesso em: 29 jul. 2019.

CONSELHO EUROPEU. **O Brexit**. Disponível em: <https://www.consilium.europa.eu/pt/policies/eu-uk-after-referendum/>. Acesso em: 5 jul. 2019.

_____. **Convenção n.º 108, de 28 de janeiro de 1981**, relativa à Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Disponível em: <http://www.ministeriopublico.pt/instrumento/convencao-para-proteccao-das-pessoas-relativamente-ao-tratamento-automatizado-de-dados-2>. Acesso em: 15 fev. 2019.

_____. **Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 4 de novembro de 1950.** Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 3 jul. 2019.

_____. **Manual da legislação europeia sobre proteção de dados.** Agência dos Direitos Fundamentais da União Europeia, 2014.

_____. **Resolution 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector**, de 26 de setembro de 1973.

Disponível em: <https://www.coe.int/en/web/data-protection/legal-instruments>. Acesso em: 3 jul. 2019.

_____. **Resolution 29 on the protection of individuals vis-à-vis electronic data banks in the public sector**, de 20 de setembro de 1974. Disponível em: <https://www.coe.int/en/web/data-protection/legal-instruments>. Acesso em: 3 jul. 2019.

COOK, Timothy Donald. **Trecho do discurso recitado pelo CEO da Apple sobre privacidade e segurança, na conferência Champions of Freedom.** Evento organizado pelo EPIC e acontecido em 1º de junho de 2015, em Washington, D.C.

COSTA JÚNIOR, Paulo José da. **O direito de estar só:** tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995.

CRAVO, Daniela Copetti. **Direito à portabilidade de dados:** necessidade de regulação *ex ante* e *ex post*. Tese (Doutorado em Direito). UFRS: Porto Alegre, 2018. p. 172.

CRETELLA JÚNIOR, José. **Comentários à Constituição Brasileira de 1988.** Rio de Janeiro: Forense Universitária. 1988.

DA SILVA, Felipe Stribe. **A proteção jurídica dos dados pessoais nos países do Mercosul em face da segmentação comportamental:** um estudo comparado. Santa Maria, 2015. Dissertação. Universidade Federal de Santa Maria (UFSM).

DA SILVEIRA, Sérgio Amadeus. Ciberativismo, cultura hacker e o individualismo colaborativo. In: **Revista USP.** São Paulo, n.º 86, 2010, p. 28-39. Disponível em: <https://doi.org/10.11606/issn.2316-9036.v0i86p28-39>. Acesso em: 18 jul. 2019.

DE CUPIS, Adriano. **Il diritto alla riservatezza existe.** In: Foro Italiano - IV, 1954.

DENNING, Dorothy E. **Activism, hacktivism, and cyberterrorism:** The internet as a tool for influencing foreign policy. Chapter Eight. In: Networks and Netwars: The Future of Terror, Crime, and Militancy. 2002.

DEUTSCHLAND. **Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG).** Disponível em: <https://germanlawarchive.iuscomp.org/?p=712>. Acesso em: 8 jul. 2019.

_____. **Federal Commissioner for Data Protection and Freedom of Information.** Disponível em: <https://www.bfdi.bund.de/EN/Home/home_node.html>. Acesso em: 8 jul. 2019.

_____. **Deutscher Bundestag, 23 mai. 1949**. Disponível em: <https://www.btg-bestellservice.de/pdf/10080000.pdf>. Acesso em: 8 jul. 2019.

DIZ, Jamile Bergamaschine Mata; AMORIM, Letícia Balsamão; CARVALHO, Karen Patrícia. Harmonização das normas de defesa do consumidor no Mercosul. In: **Revista de Ciências Humanas.** v. 1, n. 1 p. 60-67, fevereiro/julho. Universidade

Federal de Viçosa - UFV: 2001. Disponível em: < https://www.locus.ufv.br/handle/123456789/13059>. Acesso em: 30 jul. 2019.

DOMINGUES, Elisabeth Júlio. **Os Ciberataques como um Novo Desafio para a Segurança:** o Hacktivismo. Instituto Superior de Ciências Policiais e Segurança Interna. Monografia. Lisboa, 2015.

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

_____. **Proteção dos dados pessoais como um direito fundamental.** v. 12, n. 2, p. 91-108, jul./dez. Joaçaba: Espaço Jurídico: 2011.

DRUMMOND, Victor Gameiro. **Internet, privacidade e dados pessoais.** – Rio de Janeiro: Editora Lumen Juris, 2003.

ESPAÑA. Conferencia internacional de autoridades de protección de datos y privacidad. **Resolución de Madrid, 5 de Noviembre de 2009. Estándares Internacionales sobre Protección de Datos Personales y Privacidad.** Disponível em: <https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf>. Acesso em: 24 jul. 2019.

_____. **Constitución Española, de 29 de diciembre de 1978**. Disponível em: <https://www.boe.es/eli/es/c/1978/12/27/(1)>. Acesso em: 9 jul. 2019.

_____. La Declaración de la Sociedad Civil, 3 de Noviembre de 2009. **Estándares de Privacidad en un Mundo Global.** Disponível em: <https://thepublicvoice.org/madrid-declaration/es/>. Acesso em: 24 jul. 2019.

_____. **Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.** Disponível em: <>. Acesso em: 9 jul. 2019.

_____. **Agencia Española de Portección de Datos – AEPD.** Disponível em: <https://www.aepd.es/index.html>. Acesso em: 9 jul. 2019.

_____.**Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.** Disponível em: <https://www.boe.es/buscar/doc.php?id=BOE-A-2013-128

FERNANDES, Milton. **Os direitos de personalidade:** estudos jurídicos em homenagem ao Professor Caio Mário da Silva Pereira. Rio de Janeiro: Forense, 1984.

_____. **Proteção civil da intimidade.** São Paulo: Saraiva, 1977.

EUROPEAN PARLIAMENT. The Directorate-general For Internal Policies: Policy Department A: Economic and Scientific Policy, Industry, Research and Energy. **Data and Security Breaches and Cyber-Security:** Strategies in the EU and its International Counterparts. Disponível em: <

http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-ITRE_NT(2013)507476>. Acesso em: 19 jul. 2019.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). **Data breaches.** Disponível em: <https://etl.enisa.europa.eu/#/>. Acesso em: 19 jul. 2019.

FELLOUS, Beyla Esther. **Proteção do consumidor no Mercosul e na União Europeia**. – São Paulo: Editora Revista dos Tribunais, 2003.

FRANCIE. **Loi n° 78-17, du 6 janier 1978, relative à l'informatique, aux fichiers et aux libertés.** Disponível em: < https://www.legislationline.org/legislation/country/30/section/legislation/topic/3?fbclid=IwAR1ULh2gH5ceIuOgSFkwqZwAj9nGn4msD6B2YXEiGutgAtFV7ppB3lJgDNg>. Acesso em: 7 jul. 2019.

_____. **Commission Nationale de l'Informatique et des Libertés - CNIL.** Disponível em: <https://www.cnil.fr/en/home>. Acesso em: 6 jul. 2019.

_____. **Code pénal,** as last amended by Loi n°2012-410 du 27 mars 2012. Disponível em: <http://www.legislationline.org/documents/action/popup/id/18094>. Acesso em: 7 jul. 2019.

_____. **Décret n°2005-1309 du 20 octobre 2005**, pris pour l'application de la loi n° 78-17 du 6
janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Disponível em: <https://www.legislationline.org/legislation/country/30/section/legislation/topic/3?fbclid=IwAR1ULh2gH5ceIuOgSFkwqZwAj9nGn4msD6B2YXEiGutgAtFV7ppB3lJgDNg>. Acesso em: 7 jul. 2019.

GILLENSON, Mark. L. **Fundamentos da gerência de banco de dados**. Tradução Acauan Fernandes, Elvira Maria Antunes Uchôa. – Rio de Janeiro: LTC, 2006.
GOMES, Carla de Marcelino; OLIVEIRA, Bárbara Nazareth; SANTOS, Rita Páscoa dos. **Os direitos fundamentais em Timor-Leste:** teoria e prática. 1. ed. Portugal: Coimbra Editora, 2015.

GOMES, Eduardo Biacchi. **A supranacionalidade e os blocos econômicos**. Revista da Faculdade de Direito UFPR. v. 38, n. 0, 2003. p. 159-183. Disponível em: <http://dx.doi.org/10.5380/rfdufpr.v38i0.1767>. Acesso em: 30 jul. 2019.

GT29 - Grupo de trabalho do art. 29º. **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, adotadas em 4 de abril de 2017; Revistas e adotadas pela última vez em 4 de outubro de 2017.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf>. Acesso em: 21 jul. 2019.

_____. **Orientações relativas à transparência na acepção do Regulamento 2016/679, adotadas em 29 de novembro de 2017; revistas e adotadas pela última vez em 11 de abril de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp260rev01_pt.pdf>. Acesso em: 11 jul. 2019.

_____. **Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante, adotadas em 13 de dezembro de 2016; com a última redação revista e adotada em 5 de abril de 2017.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp244rev01_pt.pdf>. Acesso em: 14 jul. 2019.

_____. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017 e Revistas e adotadas pela última vez em 6 de fevereiro de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf>. Acesso em: 20 jul. 2019

_____. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017; com a última redação revista e adotada em 6 de fevereiro de 2018.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf>. Acesso em: 13 jul. 2019.

_____. **Orientações sobre o direito à portabilidade dos dados, adotadas em 13 de dezembro de 2016; com a última redação revista e adotada em 5 de abril de 2017.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf>. Acesso em: 12 jul. 2019.

_____. **Orientações sobre os encarregados da proteção de dados (EPD), adotadas em 13 de dezembro de 2016; com a última redação revista e adotada em 5 de abril de 2017.** Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf>. Acesso em: 14 jul. 2019.

GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 11 jul. 2019.

HABERMAS, Jürgen. **Storia e critica della opinione pubblica.** 5. ed. Editore Laterza, 2006.

HOESCHL, Hugo César. **Alguns aspectos constitucionais da Lei n.9296/1996.** In: ROVER, Aires José (Org). Direito, Sociedade e Informática: limites e perspectivas da vida digital. Florianópolis: Boiteux, 2000.

HUBMANN, Heinrich. **Der zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion.** 1957.

INSTITUTO DE DEFESA DO CONSUMIDOR (IDEC). **Quem somos**. Disponível em: <https://idec.org.br/quem-somos>. Acesso em: 22 jul. 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27005:2018** – Information technology – Security techniques – Information security risk management. Disponível em: <https://www.iso.org/standard/75281.html>. Acesso em: 19 jul. 2019.

INTERNET ENGINEERING WORKING GROUP (IETF). **RFC n.º 6973, July 2013.** Privacy Considerations for Internet Protocols. Disponível em: <https://tools.ietf.org/html/rfc6973>. Acesso em: 24 jul. 2019.

ITALIA. **Codice Civile**, R.D. 16 marzo de 1942, n. 262. Disponível em: <https://www.brocardi.it/codice-civile/libro-primo/>. Acesso em: 7 jul. 2019.

_____. **Costituzione dela Repubblica Italianai (2012).** Disponível em: <https://www.senato.it/documenti/repository/istituzione/costituzione.pdf >. Acesso em: 7 jul. 2019.

_____. **Legge 7 agostos 1990, n. 241**, nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. Disponível em: <http://www.legislationline.org/documents/action/popup/id/7245>. Acesso 7 jul. 2019.

_____.**Garante per la protezione dei dati personali.** Disponível em: <https://www.garanteprivacy.it/web/guest/home/autorita>. Acesso em: 7 jul. 2019.

ITALY. **Legislative Decree n. º 196 of 30 June 2003, Personal Data Protection Code**. Disponível em: <https://www.legislationline.org/legislation/section/legislation/topic/3/country/22>. Acesso em: 7 jul. 2019.

_____ **Resolution n.º 217/01/CONS.** Regulation concerning the access to documents. Disponível em: <https://www.legislationline.org/legislation/section/legislation/topic/3/country/22>. Acesso em: 7 jul. 2019.

ITURRASPE, Jorge Mosset et. al. Daños. **Globalizacion – Estado – Economía.** Buenos Aires: Rubinzal-Culzoni, 2000.

JANAL, Ruth. **Data Portability:** a tale of two concepts. In: Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC). v. 8. Issue 1, ISSN 2190-3387, 2017. 29-69. Disponível em: <https://bit.ly/2q5Ut1u>. Acesso em: 30 jul. 2019.

KAKU, William Smith. **Internet e comércio eletrônico:** pequena abordagem sobre a regulação da privacidade. In: ROVER, Aires José (Org.) Direito, Sociedade e Informática: limites e perspectivas da vida digital. Florianópolis: Boiteaux, 2000.

KERBER, Gilberto. **Mercosul e Supranacionalidade:** um estudo à luz das legislações constitucionais. Dissertação (Mestrado em Direito). UFSC: Florianópolis, 2000. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/78226/170264.pdf?sequence=1&isAllowed=y>. Acesso em: 30 jul. 2019.

LACOMBE, Francisco José Masset et. al., **Administração Princípios e Tendências.** - São Paulo: Saraiva, 2003.

LEMOS, André. **Cidade Ciborgue:** As cidades na Cibercultura, vol. 8. - São Paulo: 2004

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** – Campinas: Millenium Editora, 2005.

LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

_____. Transparência Administrativa e Novas Tecnologias: o Dever de Publicidade, o Direito a ser informado e o Princípio Democrático. In: **Revista do Direito Administrativo.** v. 244. FGV: 2007, p. 248-263. Disponível em: <bibliotecariodigital.fgv.br>. Acesso em: 29 ago. 2019.

LINDON, Raymond. **Une création pretorienne:** Les droits de la personnalité. Paris: Dalloz, 1974.

LOCKE, John. **Segundo tratado sobre o governo civil:** ensaio sobre a origem, os limites e os fins verdadeiros do governo. Petrópolis: Vozes, 1999.

LUÑO, Antonio-Henrique Pérez. **Derechos humanos, estado de derecho y constituición**. Madrid: Tecnos, 2017.

MACHADO, Fernando Inglez de Souza; RUARO, Regina Linden. **Publicidade comportamental, proteção de dados pessoais e o direito do consumidor.** In: CONPEDI Law Review. Braga, vol. 14, n. 43, abr./jun., 2017. p. 421-440.

MACHADO, Joana de Moraes Souza. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista da Ajuris:** v. 41, n. 134, 2014.

MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. **Regulamento Geral de Proteção de Dados:** manual prático. Vida Económica: Porto, 2017.

MAIA, Luciano Soares. **A privacidade e os princípios de proteção do indivíduo.** In: XVI Congresso Nacional do CONPEDI, 2008, Belo Horizonte. Pensar Globalmente: Agir localmente. Florianópolis: Fundação Boiteux, 2008. v. 1.

MARECOS GAMARRA, Adriana Raquel. La protección de datos de carácter personal em el Paraguay. In: **Revita Jurídica UCA Law Review.** Universidad Católica “Nuestra Señora de la Asunción” - Facultad de Ciencias Jurídicas y Diplomáticas, 2017. p 623-654. Disponível em: <https://www.pj.gov.py/ebook/monografias/nacional/informatico/Adriana-Marecos-Proteccion-de-datos-Py.pdf>. Acesso em: 30 jul. 2019.

MARQUES. Cláudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor:** um estudo dos negócios jurídicos de consumo no comércio eletrônico. São Paulo: Revista dos Tribunais, 2004.

_____. Cláudia Lima. Proteção do consumidor brasileiro no comércio eletrônico e a chamada nova crise do contrato: por um direito do consumidor aprofundado. In: **Revista de Direito do Consumidor.** n.º 57. Jan./Mar. 2006.

MARQUES FILHO, Glenio Leitão. **Hackers e Crackers na Internet**: as duas faces da moeda. Revista eletrônica – Temática. – Ano VI, n.º 01, 2010, p. 18-30.

MARQUES, João; SILVEIRA, Alessandra. Do direito a estar só ao Direito ao esquecimento. Considerações sobre a proteção de dados pessoais informatizadas no Direito da União Europeia: sentido, evolução e reforma legislativa. In: **Revista da Faculdade de Direito UFPR.** v. 61, n. 3, 2016. p. 91-118. Disponível em: <https://revistas.ufpr.br/direito/article/view/48085/29828>. Acesso em: 30 jul. 2019. p. 111.

MASSENO, Manuel David Rodrigues. A Proteção de Dados Pessoais em Portugal e nos Outros Países de Língua Portuguesa: uma cartografia das Fontes Legislativas. **Revista Direito & TI – Debates Contemporâneos**: Porto Alegre, 2018.

MAZZUOLI, Valério de Oliveira. **Curso de direito internacional público.** 5 ed., Editora RT, 2011.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor**. Revista de Direito do Consumidor.** São Paulo, v. 25, n. 106, jul./ago., 2016. p. 37-69.

_____. **Transparência e Privacidade:** violação e proteção de informação pessoal na sociedade de consumo. Universidade de Brasilia - UNB. Dissertação (Mestrado em Direito). 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em: 29 jul. 2019.

MERCOSUL. **CCM/DIR. n.º 1, de 14 de fevereiro de 1995.** Criação de Comitês Técnicos. Disponíivel: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **CMC/DEC. n.º 1, de 5 de agosto de 1995.** Reunião de Ministros. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **CMC/DEC n.º 27, de 30 de julho de 2012.** Adesão da República da Venezuela ao Mercosul. Disponível em: <http://www.mdic.gov.br/arquivos/dwnl_1377717164.pdf>. Acesso em: 18 jul. 2019.

_____. **Composição, objetivos e estrutura institucional.** Disponível em: <http://www.mercosul.gov.br/saiba-mais-sobre-o-mercosul>. Acesso em: 17 jul. 2019.

_____. **Decisão sobre a suspensão da Venezuela no MERCOSUL.** Disponível em: <https://www.mercosur.int/pt-br/decisao-sobre-a-suspensao-da-republica-bolivariana-da-venezuela-no-mercosul/>. Acesso em: 18 jul. 2019.

_____. **GMC/RES. n.º 01, de 9 de abril de 2010.** Proteção da saúde e da segurança de consumidores e usuários - aspectos operativos. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019.

_____. **GMC/RES. n.º 19, de 16 de junho de 2018.** Setor de tecnologias da informação e comunicação. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019.

_____. **GMC/RES. n.º 21, de 08 de outubro de 2004.** Direito à informação do consumidor nas transações comerciais efetuadas através da internet. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **GMC/RES. n.º 34, de 16 de dezembro de 2011.** Defesa do Consumidor - Conceitos Básicos. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019.

_____. **GMC/RES. n.º 36, de 15 de julho de 2019.** Defesa do Consumidor: princípios fundamentais. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019.

_____. **GMC/RES. n.º 37, de 15 de julho de 2019.** Defesa do consumidor proteção ao consumidor no comércio eletrônico. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019.

_____. **GMC/RES. n.º 42, de 08 de dezembro de 1998.** Defesa do consumidor – Garantia contratual. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **GMC/RES. n.º 43, de 28 de junho de 2000.** Grupo Ad Hoc sobre comércio eletrônico. Disponível em: <https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/>. Acesso em: 25 jul. 2019.

_____. **GMC/RES. n.º 45, de 24 de novembro de 2006.** Proteção da Saúde e da Segurança de Consumidores e Usuários – Aspectos Operativos. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **GMC/RES. n.º 123, de 14 de dezembro de 1996.** Defesa do consumidor – Conceitos. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **GMC/RES. n.º 124, de 14 de dezembro de 1996.** Defesa do consumidor – Direitos Básicos. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **GMC/RES. n.º 125, de 14 de dezembro de 1996.** Defesa do consumidor – Proteção à saúde e segurança do consumidor. Disponível em:

<https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **GMC/RES. n.º 126, de 16 de dezembro de 1994.** Defesa do Consumidor. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **GMC/RES. n.º 127, de 14 de dezembro de 1996.** Defesa do consumidor – Garantia contratual. Disponível em: <https://www.mercosur.int/documentos-y-normativa/normativa/>. Acesso em: 18 jul. 2019.

_____. **Organograma.** Disponível em: <https://www.mercosur.int/pt-br/quem-somos/organograma-mercosul/>. Acesso em: 30 jul. 2019.

_____. **Protocolo de Ouro Preto** - Protocolo Adicional ao Tratado de Assunção sobre a Estrutura Institucional do Mercosul. Disponível em: <http://portal.antaq.gov.br/wp-content/uploads/2016/12/Protocolo-de-Ouro-Preto.pdf>. Acesso em: 18 jul. 2019.

_____. **Protocolo de Ushuaia sobre compromisso democrático no Mercosul, Bolívia e Chile.** Disponível em: <https://www.mercosur.int/documento/protocolo-de-ushuaia-sobre-compromisso-democratico-no-mercosul-bolivia-e-chile/>. Acesso em: 20 jul. 2019.

_____. **Tratado de Assunção.** Tratado para a constituição de um Mercado Comum entre a República Argentina, a República Federativa do Brasil, a República do Paraguai e a República Oriental do Uruguai, de 26 de março de 1991. Disponível em: <http://www.rau.edu.uy/mercosur/tratapt.htm>. Acesso em: 17 jul. 2019.

_____. XVIII Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 01, de 17-18 de maio de 2007.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/364>. Acesso em: 25 jul. 2019.

_____. XIX Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 02, de 13-14 de setembro de 2007.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/1707>. Acesso em: 25 jul. 2019.

_____. XX Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 01, de 27-28 de maio de 2008.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/296>. Acesso em: 25 jul. 2019.

_____. XXI Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 02, de 23-24 de setembro de 2008.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/237>. Acesso em: 25 jul. 2019.

_____. XXII Reunião Ordinária do SGT-13. **GMC/SGT-13/ATA n.º 01, de 10-11 de dezembro de 2009.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/1187>. Acesso em: 25 jul. 2019.

_____. XXIII Reunião Ordinária do SGT-13**. GMC/SGT-13/ATA n.º 01, de 27-28 de maio de 2010.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/2081>. Acesso em: 25 jul. 2019.

_____. XXIV Reunião Ordinária do SGT-13**. GMC/SGT-13/ATA n.º 02, de 6-7 de dezembro de 2010.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/3628>. Acesso em: 25 jul. 2019.

_____. XXV Reunião Ordinária do SGT-13**. GMC/SGT-13/ATA n.º 01, de 10 de novembro de 2017.** Arquivos da ata. Disponível em: <https://documentos.mercosur.int/reuniones/doc/6458>. Acesso em: 25 jul. 2019.

MICROSOFT, Corporation. **Dicionário Prático de Informática.** 22. ed. Portugal: McGraaw-Hill, 2000.

MILANES, Valeria. **El sistema de protección de datos personales em América Latina:** Oportunidades y desafíos para l os derechos humanos. Volumen I. Córdoba: ADC, 2016. p. 5-40 Disponível em: <https://adcdigital.org.ar/wp-content/uploads/2017/06/Sistema-proteccion-datos-personales-LatAm.pdf>. Acesso em: 23 jul. 2019.

MILL, John Stuart. **A liberdade/utilitarismo.** 1. ed. Martins Fontes, 2000.

MIRANDA, Jorge Manuel Moura Loureiro de. **Direitos Fundamentais:** Introdução Geral. Lisboa: Diversos, 1999.

MITNICK, Kevin David; SIMON, William L. **A Arte de Enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Ed. Pearson, 2003.

MONIZ, Graça Canto. **Finalmente:** coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD. UNIO - EU Law Journal, Braga, Vol. 4, No. 2, julho 2018, pp 119-131. Disponível em: <http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Gra%C3%A7a%20Canto%20Moniz.pdf>. Acesso em: 6 jul. 2019.

NASCIMENTO, Aline Tiduco Hossaka Molette. **Direito à vida privada e à intimidade do portador do HIV e sua proteção no ambiente de trabalho.** Curitiba, 2009.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **SP 800-61 Rev. 2 - Computer Security Incident Handling Guide.** Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>. Acesso em: 19 jul. 2019.

NETWORK WORKING GROUP. **Request for Comments: 2350 - Expectations for Computer Security Incident Response.** Disponível em: <https://www.ietf.org/rfc/rfc2350.txt >. Acesso em: 19 jul. 2019.

OCDE. Organização para a Cooperação e Desenvolvimento Econômico. **Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais, de 1º de outubro de 1980.** Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf>. Acesso em: 14 mar. 2019.

ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA). **OEA/Ser.Q, CJI/doc. 474/15 rev.2, 26 marzo 2015**, Informe del Comité Jurídico Interamericano - Privacidad y Protección de Datos Personales. Disponível em: <http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf>. Acesso em: 24 jul. 2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Convenção de Viena sobre o Direito dos Tratados / Vienna Convention on the Law of Treaties, de 22 maio de 1969.** Disponível em: <https://treaties.un.org//doc/source/docs/A_CONF.39_11_Add.2-E.pdf >. Acesso em: 3 jul. 2019.

ORTIZ, Paula Jervis. Internet de las cosas y protección de datos personales. **Revista Chilena de derecho y tecnología.** Centro de estudios en derecho informático. Universidad de Chile ISSN 0719-2584. Vol. 4. num. 2. (2015) p. 9-51. DOI 10.5354/0719-2584.2015.37509.

PARAGUAY. **Constitución de la República de Paraguay, de 20 de junio de 1992.** Disponível em: <http://www.oas.org/juridico/mla/sp/pry/sp_pry-int-text-const.pdf>. Acesso em: 23 jul. 2019.

_____. Corte Suprema de Justicia. Instituto de Investigações Jurídicas. **Protección de Datos Personales:** edición com aporte de jurisprudencia internacional. - Tomo II, p. 458, ISBN 978-99953-41-21-3. Asunción, 2014, p. 10. Disponível em: <https://www.pj.gov.py/ebook/libros_files/Proteccion-de-datos-personales-Tomo-II.pdf>. Acesso em: 30 jul. 2019.

PARAGUAY. Asunción. Corte Suprema de Justicia. Sala Constitucional. Accion de Inconstitucionalidad em el Juicio: "ESTABLECIMIENTOS PACU CUA S.R.L. C/ ENTIDAD BINACIONAL YACYRETA S/ HABEAS DATA". **Acuerdo y Sentencia n.º 477, de 1º de 1997.** Disponível em: <https://www.csj.gov.py/jurisprudencia/>. Acesso em: 30 jul. 2019.

_____. **Ley n.° 1.334, de 27 de octubre de 1998.** Ley de Defensa del Consumidor y del Usuario. Disponível em: <http://www.bacn.gov.py/leyes-paraguayas/897/de-defensa-del-consumidor-y-del-usuario>. Acesso em: 23 jul. 2019.

_____. **Ley n.º 1.682, de 16 de janeiro de 2001.** Reglamenta la Información de Carácter Privado. Disponível em: <http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado>. Acesso em: 24 jul. 2019.

_____. Tribunal de Apelación. Civil y Comercial. **Acuerdo y Sentencia n.º 84, de 10 de novimbre de 1998.** Marco Riera Hunter. Disponível em: <http://www.csj.gov.py/jurisprudencia/>. Acesso em: 30 jul. 2019.

PEREIRA, J.; DAL MAGRO, E. C.; CARRES, A. F. N. **Terrorismo e ciberterrorismo:** uma análise frente a nova legislação brasileira de combate ao terror. Paraná: Unioeste, 2017.

PETER, Rob; CORONEL, Carlos. **Sistemas de banco de dados: projeto de implementação e gerenciamento**; revisão técnica Ana Paula Appel; [tradução All Tasks]. 8. ed. – São Paulo: Cengage Learninh, 2011.

PEZZI, Ana Paula Jacobus. **A necessidade de proteção dos dados pessoais nos arquivos de consumo:** em busca da concretização do direito à privacidade. Monografia. UNISINOS: São Leopoldo, 2007. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf>. Acesso em: 11 mar. 2019.

PORTAL DO DPO - Encarregado de Protecção de Dados. **Glossário RGPD.** Disponível em: <https://www.portaldodpo.pt/glossario/>. Acesso em: 15 jul. 2019.

PORTUGAL. **Constituição da República Portuguesa.** Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 9 jul. 2019.

_____. **Lei n.º 10/91 - Lei da Protecção de Dados Pessoais face à Informática.** Disponível em: <https://www.cnpd.pt/bin/legis/nacional/lei_1091.htm>. Acesso em: 9 jul. 2019.

_____.**Lei n.º 67/98 - Lei da Protecção de Dados Pessoais.** Disponível em: <https://www.cnpd.pt/bin/legis/nacional/LPD.pdf>. Acesso em: 9 jul. 2019.

_____. **Comissão Nacional de Protecção de Dados – CNPD**. Disponível em: <https://www.cnpd.pt/index.asp>. Acesso em: 9 jul. 2019.

_____. **Lei n.º 12/2005 – Lei de Informação Genética Pessoal e Informação de Saúde.** Disponível em: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1660&tabela=leis>. Acesso em: 9 jul. 2019.

_____. **Lei n.º 109/2009 – Lei do Cibercrime.** Disponível em: <https://www.cnpd.pt/bin/legis/nacional/LEI109_2009_CIBERCRIME.pdf>. Acesso em: 9 jul. 2019.

REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. **Encontros Ibero-Americanos.** Iniciação. Disponível em: <http://www.redipd.org/actividades/encuentros/index-idpt-idphp.php>. Acesso em: 14 mar. 2019.

_____. **Padrões de Proteção de Dados Pessoais para os Estados Ibero-Americanos,** de 20 de junho de 2017**.** Disponível em: < http://www.redipd.es/documentacion/common/Estandares_PORTUGUES.pdf>. Acesso em: 15 mar. 2019.

REIS, Jair Teixeira de. **Resumo de direito internacional e comunitário.** 3. ed. – Niterói: Impetus, 2011.

REMOLINA ANGARITA, Nelson. **Mapa Latinoamericano sobre la protección de datos personales:** Constituciones y normas generales (1985-2014/Feb). In: Latin America and protection of personal data: facts and figures. Bogotá: Universidade de Los Andes. Disponível em: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/2014-marcha-Latin-America-data-protection-1985-2012-facts-and-figures-Remolina.pdf>. Acesso em: 24 jul. 2019.

RIPOL CARULLA, Santiago**. Las libertades de información y de comunicación em europa.** Madrid: Tecnos, 1995.

RÖDER, Karl David August. Classic Reprint Series: **Grundzüge des Naturrechts oder der Rechtsfilosofie.** Londres: Forgotten Books, 2018.

RODOTÁ, Stefano. **A vida na sociedade de vigilância.** A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

_____. **Repertorio difine secolo**. Bari: Laterza, 1999. p. 62. SAMPAIO, José Adércio L. Direito à intimidade e à vida privada. Belo Horizonte: Del Rey, 1999.

_____, Stefano. **Tecnologie e diritti.** Bologna: Il Mulino, 1995.

_____. **Un Codice per L'Europa? Diritti nazionali, diritto europeo, diritto globale**. In: Codici. Uma reflessioni di fine millennio. Paolo Cappellini Bernardo Sordi (orgs.). Milano: Giuffrè, 2002, p. 564.

RODRIGUES, Luciana Ribeiro; PIMENTA, Francisco José Paoliello. **Discussões sobre o conceito de ciberativismo e suas práticas atuais através de uma abordagem pragmaticista.** Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. XXXVIII Congresso Brasileiro de Ciências a Comunicação – Rio de Janeiro, RJ – 2015

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família da comunicação e informações pessoais. Belo Horizonte: Del Rey, 1998.

SAMUEL, Alexandra Whitney. **Hacktivism and the Future of Political Participation.** Cambridge, Harvard university, 2004. Disponível em: <http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-frontmatter.pdf>. Acesso em: 18 jul. 2019.

SANTA MARIA, José Serpa de. **Direitos da personalidade e a sistemática civil geral.** Campinas: Julex, 1987.

SANTOS DOS, Washington. **Dicionário jurídico brasileiro.** – Belo Horizonte: Del Rey, 2001.

SILVA, Alberto Jacob Cerda. **Protección de datos personales y prestación de servicios en línea en América Latina.** Capítulo cuatro. p. 165-180. In: Hacia una internet de censura: propuestas para América Latina / compilado por Bertoni. – 1a. ed. – Buenos Aires: Universidad de Palermo – UP, 2012. Disponível em:<https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf>. Acesso em: 23 jul. 2019.

SILVA, José Luís Moreira. **Novo Dicionário de Termos Europeus.** Disponível em: <http://euroogle.com/dicionario.asp?definition=835>. Acesso em: 29 jul. 2019.

SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. **Autoridades de Proteção de Dados na América Latina:** um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. – São Paulo: IDEC, 2019.

SINGHAL, Anoop; WINOGRAD, Theodore; SCARFONE, Karen. NIST – National Institute of Standards and Technology. **Guide to Secure Web Services SP 800-95.** Computer Security Resource Center (CSRC), 2007. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf>. Acesso em: 18 jul. 2019.

SKOUDIS, Ed. **Counter hack:** a step-by-step guide to computer attacks and effective defenses. In: Prentice Hall series in computer networking and distributed systems. Upper Saddle River: PH PTR: 2002.

SOMASUNDARAM, G; SHRIVASTAVA, A.; EMC Education Services. **Armazenamento e Gerenciamento de Informações.** São Paulo: Bookman, 2012.

SOUSA, Fernando de. **Dicionário de Relações Internacionais.** ed. 954. Santa Maria da Feira: Edições Afrontamento, 2005.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas; tradução Daniel Vieira; revisão técnica Paulo Sérgio Licciardi, Messer Barreto, Rafael Misoczki. – 6. ed. São Paulo: Pearson Education do Brasil, 2015.

TRIBUNAL CONSTITUCIONAL ALEMÃO. **Sentença de 15/12/1983, BJC n.º 33, jan. 1984.** Reclamação Constitucional contra Ato Normativo. Disponível em: < https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877>. Acesso em: 29 jul. 2019.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Decisão Prejudicial,** Maximilian Schrems c. Data Protection Commissioner. (processo C-362/14). Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564999613096&uri=CELEX:62014CA0362 >. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 6 de novembro de 2003 (Assembleia Plenária),** Bodil Lindqvist (C-101/01, EU:C:2003:596). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564992216541&uri=CELEX:62001CJ0101>. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 8 de abril de 2014 (Grande Secção),** Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564946739627&uri=CELEX:62012CA0293>. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 9 de março de 2010 (Grande Secção), Comissão/Alemanha (C-518/07, EU:C:2010:125).** Disponível em: <http://curia.europa.eu/juris/document/document.jsf;jsessionid=49FD75BA8078823EAA163FA45B4B37F4?text=&docid=79752&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=6024610>. Acesso em: 30 jul. 2019.

_____. **Decisão Prejudicial de 9 de novembro de 2010 (Grande Secção),** Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564948498369&uri=CELEX:62009CJ0092>. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 11 de dezembro de 2014**, František Ryneš contra Úřad (C-212/13, EU:C:2014:2428). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564976362204&uri=CELEX:62013CJ0212>. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 13 de maio de 2014 (Grande Secção),** Google Spain e Google (C-131/12, EU:C:2014:317). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 17 de outubro de 2013,** Michael Schwarz (C-291/12, EU:C:2013:670). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564948616770&uri=CELEX:62012CA0291>. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 21 de dezembro de 2016 (Grande Secção),** Tele2 Sverige (processos apensos C-203/15 e C-698/15, EU:C:2016:970. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1564950891168&uri=CELEX:62015CJ0203>. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 29 de junho de 2010 (Grande Secção**), Comissão/Bavarian Lager (C-28/08 P, EU:C:2010:378). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62008CJ0028>. Acesso em: 29 jul. 2019.

_____. **Decisão Prejudicial de 30 de maio de 2006 (Grande Secção)**, Parlamento/Conselho (C-317/04 e C-318/04, EU:C:2006:346). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/SUM/?qid=1564976182834&uri=CELEX:62004CJ0317_SUM>. Acesso em: 29 jul. 2019.

TUCCI, Rogério Lauria. **Direitos e garantias individuais no Processo Penal Brasileiro.** São Paulo: Saraiva, 1993.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia, 2000/C 364/01, de 18 de dezembro de 2000.** Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 21 fev. 2019.

_____. **Diretiva n.º 24/2006/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006**, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. Disponível em: <http://data.europa.eu/eli/dir/2006/24/oj>. Acesso em: 29 jul. 2019.

_____. **Diretiva n.º 58/2002/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002**, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). Disponível em: <http://data.europa.eu/eli/dir/2002/58/oj>. Acesso em: 29 jul. 2019.

_____. **Diretiva n.º 46/1995/CE do Parlamento Europeu e do Conselho**, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 15 fev. 2019.

_____. **Diretiva n.º 66/1997/CE do Parlamento Europeu e do Conselho**, de 15 de dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações. Disponível em: <http://data.europa.eu/eli/dir/1997/66/oj >. Acesso em: 7 jul. 2019.

_____. **Diretiva (EU) n.º 680/2016 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível em: <http://data.europa.eu/eli/dir/2016/680/oj>. Acesso em: 10 jul. 2019.

_____. **Diretiva (UE) n.º 681/2016 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0681>. Acesso em: 29 jul. 2019.

_____. **Posição Comum n.º 31/2000/CE, de 25 de Maio de 2000, adoptada pelo Conselho** deliberando nos termos do procedimento previsto no artigo 251.o do Tratado que institui a Comunidade Europeia, tendo em vista a adopção de um regulamento do Parlamento Europeu e do Conselho que altera o Regulamento

(CEE) n.o 2913/92 do Conselho, que estabelece o Código Aduaneiro Comunitário. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1562447137990&uri=CELEX:52000AG0031>. Acesso em: 6 jul. 2019.

_____. **Regulamento n.º 45/2001/CE do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000**, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001R0045>. Acesso em: 14 jul. 2019.

_____. **Regulamento (UE) n.º 679/2016, de 27 de abril de 2016 do Parlamento Europeu e do Conselho**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 15 fev. 2019.

_____. **Regulamento (UE) n.º 1.725/2018 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE (Texto relevante para efeitos do EEE.). Disponível em: <https://eur-lex.europa.eu/eli/reg/2018/1725/oj>. Acesso em: 14 jul. 2019.

_____. **Tratado da União Europeia (Tratado de Maastricht), 29 jul.1992.** Disponível em: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF>. Acesso em: 14 mar. 2019.

_____. **Tratado de Lisboa (2007/C 306/01)**, que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, de 13 de dezembro de 2007. Disponível em: < http://data.europa.eu/eli/treaty/lis/sign>. Acesso em: 3 jul. 2019.

_____. **Tratado sobre o Funcionamento da União Europeia, n.º 22/47, de 13 de dezembro de 2007, Parlamento Europeu e Conselho**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12012E%2FTXT>. Acesso em: 21 fev. 2019.

UNITED KINGDOM. Public General Acts. **Data Protection Act 1998 c.35.** Disponível em: <http://www.legislation.gov.uk/ukpga/1984/35/contents>. Acesso em: 4 jul. 2019.

_____. Public General Acts. **Data Protection Act 1998 c.29.** Disponível em: <http://www.legislation.gov.uk/ukpga/1998/29/contents>. Acesso em: 5 jul. 2019

_____. Statutory Instruments. **Data Protection Act 1987 n. 2028.** Disponível em: < http://www.legislation.gov.uk/uksi/1987/2028/contents/made>. Acesso em: 5 jul. 2019.

_____. Public General Acts. **Data Protection Act 2018 c.12.** Disponível em: <http://www.legislation.gov.uk/ukpga/2018/12/contents>. Acesso em: 5 jul. 2019.

UNITED NATIONS. General Assembly. **A/C.3/71/L.39/Rev.1, Seventy-first session, Third Committee, Agenda item 68 (b), 16 November 2016**, The right to privacy in the digital age. Disponível em: <https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1>. Acesso em: 24 jul. 2019.

_____. General Assembly. **A/RES/45/95, 68th plenary meeting, 14 December 1990**, Guidelines for the regulation of computerized personal data files. Disponível em: <https://www.un.org/documents/ga/res/45/a45r095.htm>. Acesso em 24 jul. 2019.

UNITED STATES OF AMERICA. Records, computers and the rights of citizens. **Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973.** Disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm>. Acesso em: 15 mar. 2019.

URUGUAY. **Decreto n.º 414, de 31 de agosto de 2009.** Regulamenta a Lei de Proteção de Dados. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>. Acesso em: 25 jul. 2019.

_____. **Decreto n.º 664, de 22 de dezembro de 2008.** Cria o registro de base de dados pessoais. Disponível em: <https://www.impo.com.uy/bases/decretos/664-2008>. Acesso em: 25 jul. 2019.

_____. **Ley n.º 17.189, de 07 de setembro de 1999.** Dictanse normas relativas a las relaciones de consumo. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp2082340.htm>. Acesso em: 24 jul. 2019.

_____. **Ley n.º 18.331, de 18 de agosto de 2008.** Protección de Datos Personales y Acción de Habeas Data. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008/29>. Acesso em: 25 jul. 2019.

VARELLA, Marcelo D. **Direito internacional público**. – 6. ed. – São Paulo: Saraiva, 2016.

VIEIRA, Luciane Klein. **La hipervulnerabilidad del consumidor transfronterizo y la función del Derecho Internacional Privado.** – 1 ed. Ciudad Autónoma de Buenos Aires: La Ley, 2017.

VILLEGAS CARRASQUILLA, Lorenzo. **Protección de datos personales en América Latina:** retención y tratamiento de datos personales en el mundo de Internet. Capítulo tres. p. 125-164. In: Hacia una internet de censura: propuestas

para América Latina / compilado por Bertoni. – 1a. ed. – Buenos Aires: Universidad de Palermo – UP, 2012. Disponível em: <https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf>. Acesso em: 23 jul. 2019.

## ANEXO A – PROPOSTA DE TRATADO

**MERCOSUL/CMC/P. DEC. N°**

## MEDIDAS PARA A PROTEÇÃO E LIVRE CIRCULAÇÃO DE DADOS PESSOAIS[666]

**TENDO EM VISTA:** O Tratado de Assunção e o Protocolo de Ouro Preto.

**CONSIDERANDO[667]:**

Que os sistemas de tratamento de dados estão a serviço do homem e que devem, qualquer que seja a nacionalidade ou a residência das pessoas singulares, respeitar suas liberdades e direitos fundamentais, em particular, a intimidade, e contribuir para o progresso econômica e social, para o desenvolvimento da Integração, assim como para o bem-estar dos indivíduos.

Que o tratamento dos dados pessoais dentro do Mercosul, nos diferentes setores da atividade econômica e social, somado ao avanço das tecnologias de informação, facilita o tratamento e intercâmbio de dados.

Que o fortalecimento da cooperação científica e técnica, assim com o estabelecimento coordenado de novas redes de telecomunicações entre os Estados Partes exigem e facilitam a circulação transfronteiriça de dados pessoais.

Que, em virtude disso, é necessário adotar um conjunto de medidas que protejam com efetividade, modernidade e regionalmente os consumidores em relação ao tratamento e à circulação de dados pessoais.

**O CONSELHO DO MERCADO COMUM DECIDE:**

**Artigo 1 -** Aprovar as "Medidas para a Proteção e Circulação dos Dados Pessoais" que constam como anexo e fazem parte da presente Decisão.

**Artigo 2 -** Os Estados Partes deverão incorporar a presente Decisão em seus ordenamentos jurídicos nacionais, conforme artigos 6 e 7.

---

[666] Proposta de Tratado baseada nos cinco critérios (dados pessoais; dados sensíveis; consentimento do usuário; acesso, retificação e atualização, uso dos dados; e órgão de controle) definidos e analisados na dissertação com base nas legislações de proteção de dados pessoais dos Estados Partes do Mercosul, no modelo do Projeto de Decisão n.º 110 do Mercosul/CMC, na Resolução n.º 21/2004/GMC e inspirada nas disposições do Regulamento (EU) n.º 679/2016 (RGPD).

[667] Redação de considerandos baseada no modelo do Projeto de Decisão n.º 110 do Mercosul/CMC.

# ANEXO

# MEDIDAS PARA A PROTEÇÃO E LIVRE CIRCULAÇÃO DE DADOS PESSOAIS

## CAPÍTULO I – DISPOSIÇÕES GERAIS

### Artigo 1 – Objeto

O presente tratado dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[668].

### Artigo 2 – Definições[669]

I - **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;

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.

## CAPÍTULO II – DISPOSIÇÕES ESPECÍFICAS

### Artigo 3 – Consentimento

I - O tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular[670].

II - O consentimento não será necessário quando[671]:

a) Os dados são obtidos de fontes de acesso público irrestrito;

b) São recolhidos para o exercício de funções próprias dos poderes do Estado ou em virtude de uma obrigação legal;

c) Estas são listagens cujos dados se limitam ao nome, documento de identidade nacional, identificação de imposto ou pensão, ocupação, data de nascimento e endereço;

---

668 Objetivo baseado na Lei brasileira n.º 13.709/2018 (LGPD).
669 Conceitos de dados pessoais/dados sensíveis baseados na brasileira Lei n.º 13.709/2018 (LGPD).
670 Consentimento baseado na Lei brasileira n.º 13.709/2018 (LGPD).
671 Consentimento não necessário baseado na Lei argentina n. 25.326/2000.

d) Derivam de uma relação contratual, científica ou profissional do proprietário dos dados, e resultam necessários para o seu desenvolvimento ou cumprimento;

e) Estas são as operações realizadas pelas instituições financeiras e as informações que receber de seus clientes.

**Artigo 4 – Direito de acesso, retificação, atualização e supressão[672]**

I **-** Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

II - O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

a) acesso aos dados;

b) correção de dados incompletos, inexatos ou desatualizados;

c) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 3, inciso II, desta Decisão.

**Artigo 5 – Órgão de controle**

I – Os Estados Partes disporão que uma ou mais autoridades públicas serão criadas[673], sem aumento de despesa[674], para se encarregar da fiscalização da aplicação em seu território das disposições adotadas por eles na aplicação da presente Decisão[675]. Estas autoridades exercerão suas funções com plena autonomia técnica e decisória[676].

II - A natureza jurídica da ou das autoridades de controle serão transitórias, podendo ser transformadas pelo Poder Executivo dos respectivos Estados Partes em entidades da administração pública federal indireta (ou equivalente na estrutura de órgãos dos Estados Partes), submetidas à regime autárquico especial (ou equivalente nos regimes jurídicos dos Estados Partes) e vinculadas à Chefia do Executivo[677].

---

**672** Direito de acesso, retificação, atualização e supressão baseados na Lei brasileira n.º 13.709/2018 (LGPD).

673 Multiplicidade de autoridades de controle de proteção de dados inspirada no Regulamento n.º 679/2018/UE da União Europeia.

674 Disposição orçamentária baseada na Lei brasileira n.º 13.709/2018 (LGPD).

675 Disposição baseada no modelo do Projeto de Decisão n.º 110 do CMC do Mercosul

676 Disposição sobre autonomias baseada na Lei brasileira n.º 13.709/2018 (LGPD).

677 Disposição adaptada da Lei brasileira n.º 13.709/2018 (LGPD) em razão de possível designação de mais de uma autoridade de controle e conforme as características de vinculação/desvinculação das autoridades de controle já existentes e atuantes na Argentina e no Uruguai.

III - A avaliação quanto à transformação de que dispõe o n. II deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ou das autoridades de controle no território dos Estados Partes[678].

IV – Os Estados Partes disporão que se consulte os respectivos órgãos de controle no momento da elaboração das medidas regulamentares ou administrativas relativas à proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais[679].

## CAPÍTULO III – DISPOSIÇÕES FINAIS E TRANSITÓRIAS[680]

### Artigo 6 – Cooperação

As autoridades nacionais de cada Estado Parte, responsáveis pela proteção de dados pessoais, intercambiarão a informação necessária para facilitar a aplicação da presente normativa.

### Artigo 7 – Internalização

Os Estados Partes do MERCOSUL deverão incorporar o presente Tratado aos seus ordenamentos jurídicos nacionais antes de 30 de julho de 2021.

### Artigo 8 – Vigência

O Tratado terá duração indefinida e entrará em vigor 30 (trinta) dias após a data do depósito do terceiro instrumento de ratificação. Os instrumentos de ratificação serão depositados ante o Governo da República do Paraguai.

O Governo da República do Paraguai notificará ao Governo de cada um dos demais Estados Partes a data de entrada em vigor do presente Tratado.

**CMC – Rio do Sul, 30/07/2019**

---

678 Disposição sobre prazo transformação baseado na Lei brasileira n.º 13.709/2018 (LGPD).
679 Disposição sobre regulamentação baseada no modelo do Projeto de Decisão n.º 110 do Mercosul/CMC.
680 Disposições finais e transitórias baseadas na Resolução n.º 21/2004/GMC.