UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de Marília

Dayane de Oliveira Martins

Estudo sobre a transformação de dados pessoais em dados pessoais sensíveis: análise da integração na coleta e de indícios do processamento

Marília - SP
2024

Dayane de Oliveira Martins

Estudo sobre a transformação de dados pessoais em dados pessoais sensíveis: análise da integração na coleta e de indícios do processamento

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação como parte das exigências para a obtenção do título de Mestre em Ciência da Informação pela Faculdade de Filosofia e Ciências, Universidade Estadual Paulista (UNESP), Campus de Marília.

Área de Concentração: Informação, Tecnologia e Conhecimento

Linha de Pesquisa: Informação e Tecnologia

Orientador (a): Ricardo César Gonçalves Sant'Ana

Marília - SP
2024

M386e

Martins, Dayane de Oliveira
Estudo sobre a transformação de dados pessoais em dados pessoais sensíveis : análise da integração na coleta e de indícios do processamento / Dayane de Oliveira Martins. -- Marília, 2024
131 p.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, Marília
Orientadora: Ricardo César Gonçalves Sant'Ana

1. Dados. 2. Dados pessoais. 3. Dados pessoais sensíveis. 4. Fator Integração. 5. Ciclo de Vida dos Dados. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Filosofia e Ciências, Marília. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Impacto potencial desta pesquisa

A presente pesquisa está em consonância com os Objetivos de Desenvolvimento Sustentável da Organização das Nações Unidas (ODS)[1], em especial o ODS 16.10. Os ODS representam um compromisso dos países-membros da Organização das Nações Unidas (ONU) em promover o desenvolvimento sustentável em todo o mundo. O ODS 16.10, em particular, tem por escopo:

> Garantir o acesso público à informação e proteger as liberdades fundamentais, de acordo com a legislação nacional e os acordos internacionais, promovendo, assim, a responsabilidade, a transparência, a participação e o Estado de Direito nas instituições nacionais e internacionais em todos os níveis.

Nesse contexto, o ODS em estudo visa fomentar o acesso público à informação, garantindo transparência ao cidadão, bem como fortalecendo os direitos e liberdades fundamentais. Na Sociedade em Rede[2], ao interagirem com as Tecnologias de Informação e Comunicação, informações (ou dados) sobre os cidadãos são coletadas, armazenadas, recuperadas e até mesmo descartadas pelos detentores dessas tecnologias (Sant'Ana, 2016). Contudo, os cidadãos que têm suas informações tratadas constantemente pelos detentores, não necessariamente conhecem o processo a que seus dados são submetidos ou autorizam que os detentores tenham acesso e utilizem uma quantidade substancial de informações pessoais.

A própria Constituição Federal Brasileira de 1988, em seu artigo 5º, LXXIX (Brasil, 1988), alçou o direito à proteção de dados como um direito fundamental do cidadão, isto é, uma garantia mínima necessária para que o cidadão viva de forma digna em sociedade. Para tanto, é necessário que os cidadãos tenham acesso a como seus dados são tratados, bem como tenham o controle sobre quem terá acesso aos seus dados, como quem irá compartilhá-los e por quanto tempo.

Assim, a presente pesquisa buscou estimular a crescente e constante consciência dos cidadãos e, sobretudo, dos usuários de plataformas digitais, acerca do tratamento de seus dados pessoais, auxiliando na efetivação do direito à proteção de dados, a partir da transparência no uso de dados.

---

[1] Fonte: Organizações das Nações Unidas (https://brasil.un.org/pt-br/sdgs).

[2] Sociedade em rede é um termo utilizado por Manuel Castells para descrever a configuração da era da informação, pois, segundo o sociólogo, "(...) as funções e os processos dominantes na era da informação estão cada vez mais organizados em torno de redes" (Castells, 2020, p. 553).

Potential impact of this research

The present research is in line with the Sustainable Development Goals (SDGs) of the United Nations, especially SDG 16.10[3]. The SDGs represent a commitment by United Nations member countries to promote sustainable development worldwide. SDG 16.10, in particular, aims to:

> Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements, thereby promoting accountability, transparency, participation, and the rule of law in national and international institutions at all levels.

In this context, the SDG under study aims to foster public access to information, ensuring transparency for citizens, as well as strengthening fundamental rights and freedoms. In the Network Society[4], as citizens interact with Information and Communication Technologies, information (or data) about citizens is collected, stored, retrieved, and even discarded by the holders of these technologies (Sant'Ana, 2016). However, citizens whose information is constantly processed by these holders do not necessarily know the process to which their data is subjected or authorize holders to access and use a substantial amount of personal information.

The Brazilian Federal Constitution of 1988, in its article 5, LXXIX (Brazil, 1988), elevated the right to data protection to a fundamental right of the citizen, that is, a minimum guarantee necessary for the citizen to live a dignified life in society. Therefore, it is necessary for citizens to have access to how their data is processed, as well as to have control over who will have access to their data, how they will be shared, and for how long.

Thus, the present research sought to stimulate the growing and constant awareness of citizens, and especially of digital platform users, regarding the treatment of their personal data, assisting in the realization of the right to data protection, through transparency in data usage.

---

[3] Source: United Nations (https://brasil.un.org/pt-br/sdgs).

[4] The Network Society is a term coined by Manuel Castells to describe the configuration of the information age, as, according to the sociologist, "(...) the dominant functions and processes in the information age are increasingly organized around networks" (Castells, 2020, p. 553).

Dayane de Oliveira Martins

Estudo sobre a transformação de dados pessoais em dados pessoais sensíveis: análise da integração na coleta e de indícios do processamento

Dissertação apresentada ao Programa de Pós-graduação em Ciência da Informação da Universidade Estadual Paulista “Júlio de Mesquita Filho” (Unesp), como requisito para a obtenção do título de Mestre em Ciência da Informação.

Área de Concentração: Informação, Tecnologia e Conhecimento

Linha de Pesquisa: Informação e Tecnologia

Banca Examinadora

_____
Prof. Dr. Ricardo César Gonçalves Sant’Ana
UNESP – Câmpus de Marília
Orientador

_____
Prof. Dr. José Eduardo Santarem Segundo
Universidade de São Paulo - Ribeirão Preto
Examinador interno

_____
Profª. Drª. Elaine Parra Affonso
Centro Estadual de Educação Tecnológica Paula Souza
Examinadora externa

Marília, 08 de março de 2024.

AGRADECIMENTOS

Uma de minhas músicas preferidas chama-se *Life is a song*, de autoria de Patrick Park. Nela, o compositor diz que “Talvez a vida seja uma canção, mas você está assustado para cantá-la sozinho” (*Maybe life is a song but you’re scared to sing along*). Referido trecho diz-me muito sobre como a vida pode ser mais leve, se tivermos pessoas para “cantarem” conosco.

Dessa forma, gostaria de agradecer a todos que sempre se fizeram presentes, de alguma forma, em minha jornada e, mais do que isso, acompanharam-me nesta canção, tornando minha caminhada mais leve e alegre.

Primeiramente, faço menção às bênçãos de Deus a mim concedidas. Dentre as mais importantes: a saúde que tornou o presente trabalho possível e minha família, sem a qual nenhuma realização seria completa.

Agradeço aos meus pais, Nilson e Eucy, por toda educação e pelo amor que sempre me dedicaram, bem como a minha única irmã, Daniela, por me ensinar o que é companheirismo.

Aos meus avós e a todos os familiares por todo carinho e cuidado.

Agradeço aos amigos de longa data e aos novos, bem como aos colegas de trabalho da empresa DPOnet.

Agradeço aos companheiros de pesquisa, hoje também amigos: Amanda Garcia, Nátally Barbosa, Paulo Martins e Danila Alencar.

Agradeço a Universidade Estadual Paulista “Júlio Mosquera Filho”, por me proporcionar um ensino de tamanha qualidade, que tornou possível o sonho do Mestrado.

Ao meu orientador Prof. Dr. Ricardo César Gonçalves Sant’Ana por toda dedicação e apoio desde as primeiras linhas deste trabalho e aos membros da banca, Prof. José Eduardo Santarem Segundo e Profª. Elaine Parra Affonso.

Por fim, agradeço ao meu marido, Heitor. Mais do que toda atenção e paciência, agradeço-lhe pelo companheirismo sincero, pelas doces palavras em momentos difíceis e, principalmente, por nosso amor que, a cada dia, me faz mais feliz.

RESUMO

A constante coleta de dados, em ambientes digitais, torna possível a identificação de uma pessoa física, cuja justificativa dos detentores é melhorar a experiência desses usuários ao utilizarem os serviços disponibilizados, sendo recuperados os chamados dados pessoais. A partir do estudo do Ciclo de Vida dos Dados, percebe-se que a coleta dos dados pessoais por detentores, após a interferência do fator integração, pode transformar dados pessoais em dados pessoais sensíveis que, em tese, não são coletados de forma direta e com o consentimento explícito do usuário. O compartilhamento de base de dados que envolva dados pessoais sensíveis com terceiros não autorizados pode levar a perseguições e discriminações, pois identificam preferências sexuais e afiliação religiosa dos usuários. Diante do exposto, o objetivo da presente dissertação é investigar indícios de como os dados pessoais, coletados por aplicações ou sítios eletrônicos, podem ser transformados em dados pessoais sensíveis, a partir do contexto em que estão inseridos. Para tanto, adotou-se a pesquisa de cunho descritivo, com abordagem qualitativa. Utilizou-se a triangulação metodológica, a partir do referencial teórico que abarca o Ciclo de Vida dos Dados, a fase de coleta de dados, o fator integração e a privacidade; pesquisa documental em legislações que amparam os conceitos de dados pessoais e dados pessoais sensíveis, bem como a análise das sanções aplicadas pelas Autoridades de Proteção de Dados Europeia, entre os anos de 2019-2023, às instituições que operam na União Europeia, relacionadas à violação do Regulamento Geral de Proteção de Dados (GDPR), a fim de apresentar indícios da transformação de dados pessoais em dados pessoais sensíveis, a partir do contexto em que estão inseridos. Foram levantados 2.039 casos de infrações ao GDPR, dos quais 129 estão relacionados ao artigo 9º da GDPR, isto é, estão relacionados ao tratamento incorreto de dados pessoais sensíveis. Foram destacados 12 casos em que há indícios de transformação de dados pessoais em dados pessoais sensíveis. Concluiu-se que há indícios de transformação de dados pessoais coletados por detentores em dados pessoais sensíveis, coletados por terceiros, a partir do compartilhamento de dados pessoais e após a interferência do fator integração.

Palavras–chave: Dados pessoais. Dados pessoais sensíveis. Fase de coleta. Fator integração.

ABSTRACT

The constant collection of data in digital environments makes it possible to identify an individual, with the justification from data holders being to enhance the users' experience when using the provided services, retrieving so-called personal data. From the study of the Data Life Cycle, it is observed that the collection of personal data by data holders, after the influence of the integration factor, can transform personal data into sensitive personal data that, in theory, is not collected directly and with the explicit consent of the user. The sharing of a database involving sensitive personal data with unauthorized third parties can lead to persecution and discrimination, as it reveals users' sexual preferences and religious affiliation. Given the above, the objective of this dissertation is to investigate indications of how personal data collected by applications or websites can be transformed into sensitive personal data based on the context in which they are embedded. To achieve this, a descriptive research with a qualitative approach was adopted. Methodological triangulation was employed, based on the theoretical framework covering the Data Life Cycle, the data collection phase, the integration factor, and privacy. Documentary research was conducted on legislation supporting the concepts of personal data and sensitive personal data, as well as an analysis of sanctions imposed by European Data Protection Authorities between 2019-2023 on institutions operating in the European Union related to violations of the General Data Protection Regulation (GDPR). The aim was to present evidence of the transformation of personal data into sensitive personal data based on the context in which they are embedded. A total of 2,039 GDPR infringement cases were identified, of which 129 were related to Article 9 of the GDPR, i.e., associated with the improper handling of sensitive personal data. Twelve cases were highlighted where there are indications of the transformation of personal data into sensitive personal data. It was concluded that there are indications of the transformation of personal data collected by data holders into sensitive personal data collected by third parties, following the sharing of personal data and after the influence of the integration factor.

Keywords: Personal data; Sensitive personal data. Collection phase. Integration factor.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CI	Ciência da Informação
COPPA	*Children's Online Privacy Protection Act of 1998*
CPF	Cadastro de Pessoa Física
CVD	Ciclo de Vida dos Dados
DPA	*Data Protection Authority*
EUA	Estados Unidos da América
FIPP	*Fair Information Practice Principles*
GDPR	*General Data Protection Regulation*
HIPAA	*Health Insurance Portability and Accountability Act of 1996*
HTTP	*Hype Text Tranfer Protocol*
IBGE	Instituto Brasileiro de Geografia e Estatística
IP	*Protocolo de Internet*
LGPD	Lei Geral de Proteção de Dados
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TIC	Tecnologias de Informação e Comunicação
UE	União Européia

SUMÁRIO

1 INTRODUÇÃO

A chamada revolução da tecnologia da informação foi responsável pela implementação de um processo de reestruturação de todo o sistema capitalista, no qual as Tecnologias de Informação e Comunicação (TIC) propiciam um fluxo praticamente instantâneo de troca de informações (Castells, 2020, p. 71). Assim,

> [...] uma revolução tecnológica concentrada nas tecnologias da informação começou a remodelar a base material da sociedade em ritmo acelerado. Economias por todo o mundo passaram a manter interdependência global, apresentando uma nova forma de relação entre a economia, o Estado e a sociedade em um sistema de geometria variável" (Castells, 2020, p.61).

O protagonismo ocupado pela informação, na Sociedade em Rede, já fora dominado, outrora, pela terra (Sociedade Agrícola), pela produção fabril (Sociedade Industrial) e, no contexto Pós-Segunda Guerra, pelos serviços oferecidos (Bioni, 2021).

Castells (2020), contudo, acredita que ter a informação como elemento central da organização social, econômica, política e cultural não é proveniente da Sociedade em Rede, sendo o maior diferencial desta Sociedade a existência de base microeletrônica para suporte à informação. Com efeito, a organização da informação ganhou com a Internet um novo facilitador, visto que esse suporte mostra-se um mecanismo eficiente de coleta, armazenamento e recuperação de informações. Segundo Brandão (2004):

> Como uma tecnologia em constante desenvolvimento, o papel e a importância conferidos à Internet vêm se alterando ao longo do tempo. Laudon (1999) destaca quatro papéis fundamentais da Internet: a aceleração do acesso às informações, a melhoria de comunicação e colaboração entre pessoas, a aceleração da divulgação de novos conhecimentos e do ritmo das descobertas científicas e a facilitação do comércio eletrônico, das transações comerciais e dos serviços aos clientes (Brandão, 2004, p.92).

O surgimento das tecnologias digitais, impulsionadas, sobretudo, pela expansão e popularização da internet, contribuiu para a modificação da organização social, econômica, política e cultural humana, bem como das relações interpessoais. As TIC possibilitam aos usuários realizar atividades de forma *online*: compras são feitas em plataformas eletrônicas, de qualquer lugar do mundo; cursos virtuais para aprendizado de línguas estrangeiras são disponibilizados nos mais diversos formatos; são oferecidas sessões de psicoterapia *online*; mensagens são trocadas instantaneamente.

O usuário tende também a buscar constantemente pelos mais diversos tipos de informações em seus dispositivos eletrônicos, em especial os móveis, realizando, por exemplo, pesquisas antes de consumir de fato um produto ou serviço. Contudo, nesse processo não vislumbra-se apenas o usuário buscando por informação, mas também deixando diversas informações a seu respeito ao interagirem com as plataformas digitais, ocasião em que as plataformas obtém mais dados dos usuários do que ele imagina (Affonso; Oliveira; Sant'Ana, 2017).

As TIC, assim, mostram-se como o motor propulsor que torna possível a geração e tratamento massivo e ininterrupto de informação e, sobretudo, de dados. Diante disso, é inegável que a busca por informações sofreu uma atualização na Sociedade em Rede, sobretudo em decorrência do impulsionamento das tecnologias digitais, sendo capazes de processar um volume jamais imaginado de dados (Sant'Ana, 2016).

As atividades realizadas pelos usuários em ambientes digitais acarreta na geração de dados que podem ser atrelados a comportamentos e preferências dos usuários ou, como cunhado por Westin (1967), *data shadow*[5]*,* pois *a* "(...) simples locomoção com um *smartphone* no bolso, ou vestindo um relógio inteligente, pode gerar dados como a quantidade de passos, o caminho percorrido, a frequência cardíaca, a altura, o peso e os locais frequentados" (Bagatini; Guimarães; Sant'Ana, 2021, p. 3).

Dessa forma, os mais diversos tipos de dados passaram a ser tratados massivamente, potencializando o tratamento de diversos e incontáveis dados, ocasião em que são coletados, armazenados e recuperados em volume, variedade e velocidade (e.g., *Big Data*) (Sant'Ana, 2016, p. 117).

Os dados em si são puramente objetivos, não apresentam alta carga semântica intrínseca e são independentes do usuário, constituindo, contudo, matéria-prima para uma série de possíveis interpretações, bem como medidas ou fatos que são representados por números, palavras, sons e até imagens que poderão sustentar a produção de novas informações (Souza; Almeida, 2021).

A Ciência da Informação (CI) deve voltar seus estudos aos dados, visando contribuir para que o acesso e uso intenso de dados se desenvolva da mais forma mais equilibrada possível, a partir da delimitação das fases envolvidas no acesso e

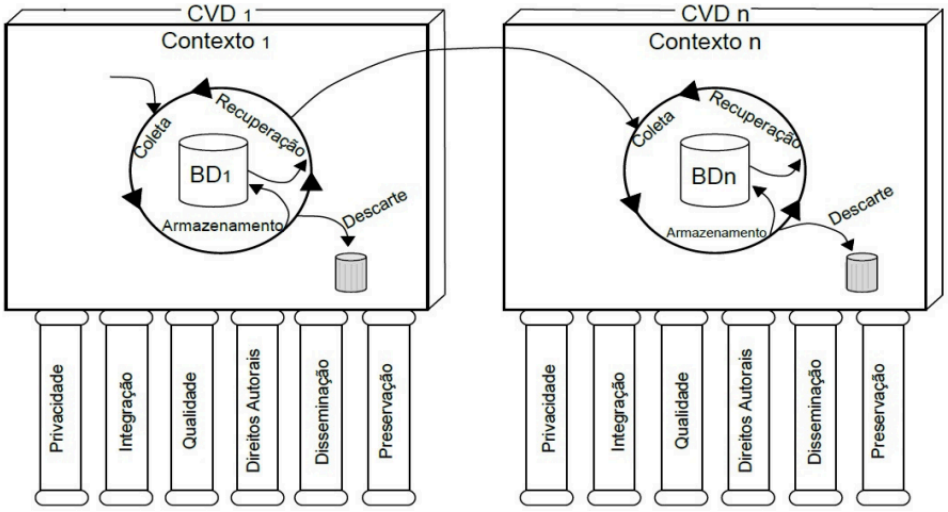
[5] Trata-se de termo cunhado por Alan Westin em que, metaforicamente, o conjunto de fatos e opiniões registrado em um banco de dados é associado a uma pessoa, acompanhando-a.

uso dos dados, bem como os atores envolvidos (Sant'Ana, 2016). Para tanto, Sant'Ana (2016) propõe o chamado Ciclo de Vida dos Dados - CVD, que busca identificar e estudar fatores e características do processo de uso e acesso de dados, propiciando uma ampliação do equilíbrio entre os atores envolvidos no processo, bem como a máxima otimização do uso dos dados (Sant'Ana, 2016).

Assim, os estudos de Sant'Ana (2016) contribuem para estruturação da análise de dados, propondo a delimitação de fases envolvidas no acesso e uso dos dados como forma de apresentar os diferentes momentos (fases) e fatores envolvidos neste processo.

O CVD, segundo os estudos de Sant'Ana (2016), é composto das seguintes fases: coleta, armazenamento, recuperação e descarte. Cada uma dessas fases é permeada por fatores transversais, quais sejam: Privacidade, Integração, Qualidade, Direitos Autorais, Disseminação e Preservação, conforme representado na Figura 1, a seguir.

Figura 1 - Ciclo de Vida dos Dados para a Ciência da Informação.



Fonte: Sant'Ana (2016).

Cada uma das fases propostas por Sant'Ana (2016) possuem características próprias, as quais podem ser indagadas diferentes questões. Na fase de coleta, por exemplo, busca-se perceber quais são os dados coletados em determinada atividade; de que forma; visando qual finalidade; qual o volume de dados envolvidos nessa operação, dentre outras. Na fase de armazenamento, por sua vez, estuda-se quais são os dados que serão armazenados; por quanto tempo; com qual finalidade; quais dados são descartados após a coleta; por qual razão; em que local serão armazenados, dentre outras. Na fase de recuperação, almeja-se compreender como

tais dados são recuperados; com quem são compartilhados; quais serão disponibilizados; como será feito o acesso, dentre outras. Na fase de descarte, por mim, observa-se quais dados serão descartados definitivamente; quais as formas a serem utilizadas para o descarte, dentre outras.

Segundo os estudos de Tanenbaum e Wetherall (2011), o crescimento tecnológico frenético ensejou no desaparecimento das diferenças entre as fases de coleta, armazenamento e recuperação, tornando as questões ocorridas nesse processo praticamente inseparáveis, intangíveis e abstraídas para o usuário (Affonso, 2018).

Nesse sentido, o fator integração explicitado no CVD mostra-se preponderante ao presente estudo, uma vez que "[...] os dados podem ser combinados, recombinados e usados por áreas multidisciplinares, ser unificados, integrados e interoperados em rede" (Monteiro; Segundo; Sant'Ana, 2016, p. 13). Assim, ao serem recuperados, os dados podem apresentar um grau de interação que componha um todo, representando um valor de uso maior se comparado ao uso individual (Sant'Ana, 2016).

Diante da notória possibilidade de coletar, armazenar e recuperar dados, a economia se adaptou e passou a ter dados como um dos seus principais ativos, permitindo com que as empresas e governos possam, por exemplo, direcionar seus serviços ao público mais propenso ao seu consumo, isto é, os dados em si não possuem nenhum valor, mas sim a informação que deles possa ser extraída, a ser utilizada para algum fim econômico. Para tanto, é necessário conhecer a fundo os donos dos dados que receberão, por exemplo, ofertas direcionadas, instaurando-se o que é conhecido por "capitalismo de vigilância" (Zuboff, 2019, p. 97), isto é, a constante e infindável extração de dados, mesmo que além do necessário.

A partir da análise de dados coletados em atividades realizadas pelos usuários de *online,* por exemplo, é possível que os dados armazenados, mesmo de diferentes entidades, sejam integrados entre si, passando a ser recuperados (ou coletados por outros detentores) como um conjunto de dados, um todo mais complexo em relação ao que foi coletado e armazenado.

A integração desses dados pode torná-los capazes de identificar uma pessoa natural, a partir de determinado contexto, gerando informações além daquelas explicitadas somente nos dados atomizados.

Em situações dessa natureza, os dados poderão ser classificados como sendo dados pessoais, oportunidade em que a vida do indivíduo pode ser exposta aos detentores dos dados coletados, considerando, ainda, o contexto em que os indivíduos estão inseridos. Nesse sentido,

> A opacidade estabelecida no processo de coleta de dados faz com que o usuário se limite a identificar o papel do detentor de dados, que não é visto como um atacante ou um ator que irá se beneficiar com o acesso aos dados. Assim, as ameaças aos dados pessoais não estão apenas na disponibilização desses para a sociedade, mas o próprio detentor passa a ter o apoderamento dessa coleta, caracterizando a quebra de privacidade (Affonso, 2018, p. 32).

O dicionário Houaiss (2001, p. 817-818) aponta que o contexto tem origem latina (“contextus”), verbo “entrelaçar” (“contexere”) ou “reunir tecendo”, derivado de “tecer” (“texere”), sendo referenciado como a “inter-relação de circunstâncias que acompanham um fato ou situação”.

Assim, o termo possui vários sentidos: i. Contexto linguístico ou verbal: é o suporte, oral ou escrito, da informação, no qual as palavras ou frases (“unidades linguísticas”) estão inseridas; ii. Contexto situacional: refere-se ao conhecimento do usuário acerca da língua, bem como de sua habilidade em usar esse conhecimento em suas relações sociais; está ligado ao “contexto social”; iii. Contexto extralinguístico: refere-se aos “dados extralinguísticos” importantes a realização do “ato de comunicação linguística”.

O contexto envolve, portanto, tanto a soma dos “conhecimentos” prévios do emissor e do receptor sobre determinado assunto, como as “crenças e pressuposições subjacentes” ao assunto (Foresti; Varvakis; Vieira, 2018).

Mais do que isso, por meio desses dados integrados, pode ser possível identificar a origem racial ou étnica, a convicção religiosa, a opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, situação clínicas, genéticas, a vida sexual e identificar a biometria de uma pessoa natural, caracterizando o tratamento dos chamados dados pessoais sensíveis (Brasil, 2018), sem o conhecimento do usuário acerca da coleta dessas informações. Nesse sentido, para Wolfgang Hoffman-Riem:

> O principal fenômeno da ubiquidade da tecnologia da informação é o desequilíbrio de poderes entre o indivíduo e os organismos que processam os dados pessoais e a consequente perda de controle individual sobre o fluxo de seus dados (Hoffman-Riem, 2014, p. 79).

A possibilidade de identificação de uma pessoa natural, direta ou indiretamente, por meio da integração de dados, sobretudo de forma massificada por meio de dispositivos eletrônicos, trouxe a necessidade de regulação normativa pelos Estados, por intermédio de leis e atos normativos, que visam proteger e regulamentar o tratamento de dados pessoais e, consequentemente, a privacidade dos titulares desses dados, uma vez que

> [...] no mundo atual, a tecnologia atua em dois flancos distintos e adversos: por um lado, ajuda a moldar uma sociedade mais evoluída e mais bem informada; em contrapartida, conduz as pessoas a uma maior fragilidade quanto às suas informações pessoais, expondo-as, muitas vezes, a abusos de toda ordem, tendo por suporte seus próprios dados pessoais (Gamiz, 2012, p. 26).

Assim, permeado pelas questões de integração de dados coletados pelos detentores, os indícios do fator integração na transformação de dados pessoais em dados pessoais sensíveis, apresentam-se, a seguir, o problema, os objetivos, a justificativa, a delimitação do tema e a metodologia desta pesquisa.

1.1 Problema de Pesquisa

A constante coleta de dados pessoais em ambientes digitais por detentores de dados, cuja justificativa é melhorar a experiência desses usuários ao utilizarem os serviços disponibilizados, enseja na construção de um perfil detalhado desses usuários, incluindo também dados pessoais sensíveis, a partir da integração de bases de dados, podendo ensejar na quebra de privacidade (Affonso, 2018).

Na Noruega, em 2020, um estudo coordenado por um grupo de defesa ao direito do consumidor, o *Norwegian Consumer Council*, gerou relatório *Out of Control: How consumers are exploited by the online advertising industry* (Forbrukerrådet, 2020). No documento, o grupo debate como dez aplicativos, *Grindr* (namoro), *OkCupid* (namoro), *Happn* (namoro), *Tinder* (namoro), *Clue* (ciclo menstrual), *MyDays* (ciclo menstrual), *Perfect365* (maquiagem), *My Talking Tom 2* (infantil), *Qibla Finder* (religioso) e *Wave Keyboard* (teclado), enviam dados pessoais de seus usuários para pelo menos 135 (cento e trinta e cinco) empresas parceiras, visando o direcionamento de conteúdo publicitário.

O relatório identificou que as aplicações compartilhavam dados pessoais com parceiros comerciais, tais como: gênero, idade, IDs de publicidade, endereços de IP, localizações de GPS e dados do comportamento do usuário dentro da

aplicação. Os dados em questão não têm, em tese, natureza de dado pessoal sensível.

Contudo, a partir da interferência do fator integração pode gerar dados pessoais sensíveis, pois o aplicativo *Grindr*, por exemplo, é voltado para indivíduos que se reconhecem como homossexuais e, mesmo que a aplicação disponibilize a terceiros, como parceiros comerciais, apenas dados cadastrais, o contexto em que esses usuários estão inseridos, qual seja, a participação em uma aplicação voltada exclusivamente a determinado público, enseja na disponibilização (mesmo que indireta) de um novo dado: orientação sexual. Nesse sentido,

> Em alguns casos, o compartilhamento generalizado de dados pessoais pode tornar-se uma questão de segurança física. Por exemplo, usuários do aplicativo de namoro *Grindr* foram localizados e visados em países onde a homossexualidade é ilegal. Atributos de *proxy* como dados de localização e interesses, que são frequentemente usados para fins comportamentais de publicidade, também pode revelar informações confidenciais relacionadas a tópicos como preferências sexuais ou crenças religiosas. Se os dados pessoais forem divulgados a centenas de empresas, os governos repressivos podem precisar apenas de obter acesso aos bancos de dados de um deles, a fim de identificar indivíduos ou realizar vigilância em larga escala (Forbrukerrådet, 2020, p. 52, tradução livre).[6]

Ainda de acordo com o relatório do grupo noruegês (Forbrukerrådet, 2020), o compartilhamento de base de dados que envolva dados pessoais sensíveis com terceiros não autorizados pode levar a perseguições, discriminações e ser uma questão de segurança física, posto que identificam preferências sexuais e afiliação religiosa dos usuários.

Considerando o cenário brevemente descrito, a presente pesquisa indaga: é possível coletar dados pessoais sensíveis, a partir da transformação de dados pessoais anteriormente coletados, em decorrência da interferência do fator integração?

---

[6] No original, "*In some cases, widespread sharing of personal data can become a matter of physical safety. For example, users of the dating app Grindr have been located and targeted in countries where homosexuality is illegal.140 Proxy attributes such as location data and interests, that are often used for behavioural advertising, could also reveal sensitive information related to topics such as sexual preferences or religious beliefs.141 If personal data is spread to hundreds of companies, repressive governments may only need to gain access to the databases of one of these in order to single out individuals, or perform large scale surveillance*" (Forbrukerrådet, 2020).

1.2 Objetivo Geral

Investigar indícios de como os dados pessoais, coletados por aplicações ou sítios eletrônicos, podem ser transformados em dados pessoais sensíveis, a partir da interferência do fator integração.

1.3 Objetivos Específicos

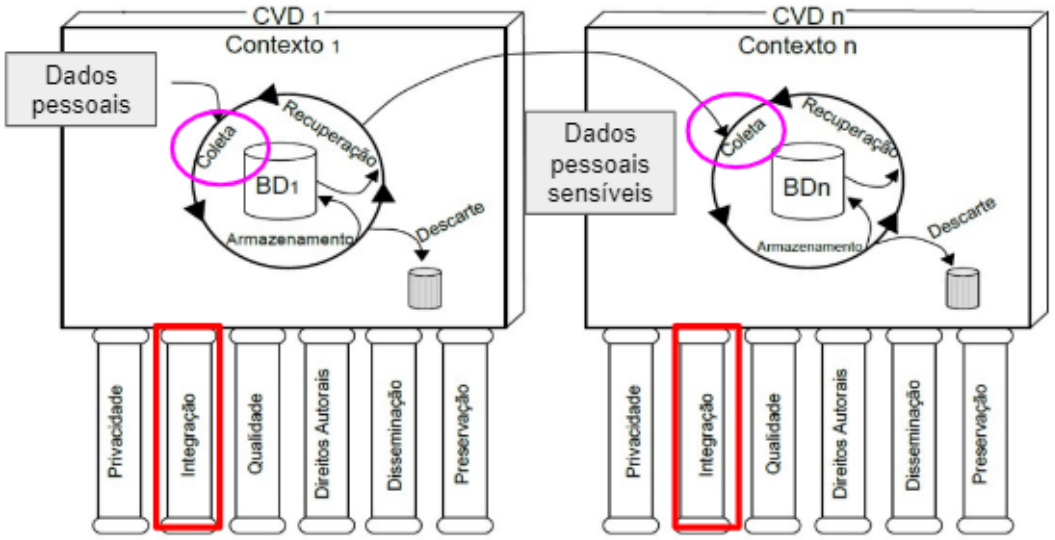
a) Identificar aspectos relacionados a dados pessoais e dados pessoais sensíveis;
b) Indicar os requisitos legais envolvidos no tratamento de dados pessoais;
c) Estudar o papel das Autoridades de Proteção de Dados em caso de descumprimento dos requisitos legais;
d) Descrever o papel do fator integração na fase de coleta de dados;
e) Analisar casos em que organizações foram punidas por Autoridades de Proteção de Dados por tratar dados pessoais sensíveis sem os requisitos legais necessários, a fim de investigar indícios de transformação de dados pessoais em dados pessoais sensíveis.

1.4 Delimitação

A presente pesquisa está delimitada na fase de coleta do CVD (Sant'Ana, 2016), com foco no fator de integração, uma vez que busca identificar indícios da transformação de dados pessoais, coletados por aplicações ou sítios eletrônicos, em dados pessoais sensíveis, a partir do contexto em que estão inseridos, isto é, a partir da interferência da integração de bases de dados.

Nesse sentido, a Figura número 2 demonstra o que o trabalho em tela propõe-se a analisar: como dados pessoais são coletados por aplicações e sítios eletrônicos, muitas vezes com a anuência de seus titulares (CVD 1), mas ao serem compartilhados (fase de recuperação) com outros detentores de dados (CVD n), tais detentores coletam, no CVD n, mais do que os dados pessoais coletados no CVD 1, coletam também dados pessoais sensíveis, senão vejamos:

Figura 2 - Elementos-chaves abordados na pesquisa



Fonte: Adaptado de Sant'Ana (2016, p. 123)

Assim, busca-se compreender o papel do fator integração nesse processo, sobretudo o contexto em que os dados pessoais são coletados, a fim de entender a eventual possibilidade de detentores coletarem, no CVD n, mais dados do que aqueles solicitados aos usuários de aplicações e sítios eletrônicos, no CVD 1.

A presente pesquisa é sustentada pelos seguintes elementos: i. referencial teórico, a partir da publicação de trabalhos que estudam ciclo de vida dos dados, com destaque para a fase de coleta e o fatos integração; ii. legislações que trata-se da proteção de dados pessoais e dados pessoais sensíveis; iii. análise de decisões de Autoridades de Proteção de Dados europeias, relacionadas à violação do artigo 9º da GDPR, a fim de apresentar indícios da transformação de dados pessoais em dados pessoais sensíveis, sob influência do fator integração.

Portanto, não é objeto do presente trabalho abordar as outras fases e fatores do CVD, tampouco as técnicas de integração de bases de dados, as consequências da transformação para os usuários, caso identificada, ou, ainda, se referidos usuários possuem ciência do processo de transformação.

Por fim, a autora entendeu que não caberia a Revisão Sistemática de Literatura como procedimento metodológico da presente pesquisa, uma vez que os procedimentos metodológicos que tornaram a pesquisa possível foi estabelecida em pesquisa bibliográfica, a partir de conceitos específicos, tais como ciclo de vida dos dados, coleta de dados, fator integração; documental, a partir do estudo de legislações que trazem conceitos de dados pessoais e dados pessoais sensíveis e

análise de conteúdo, visando investigar possíveis de indícios de transformação de dados pessoais em dados pessoais sensíveis, de forma que os objetivos geral e específicos foram devidamente atendidos.

1.5 Motivação pessoal e Justificativa

A motivação pessoal que levou a autora a se aprofundar no presente tema é contribuir com a construção da cultura da proteção de dados, no Brasil, a partir da efetiva conscientização dos titulares de como seus dados são tratados. Assim, almeja-se que as pessoas compreendam como o uso (possivelmente) indiscriminado de dados pessoais, sobretudo por grandes corporações, pode violar sua privacidade.

Durante os estudos da autora, ao longo do programa de Pós-Graduação, a autora debruçou-se sobre o estudo de dados, sobretudo os dados pessoais, capazes de identificar pessoas físicas.

Seus estudos foram voltados para os aspectos relacionados à ausência de efetiva transparência por parte dos detentores de sítios eletrônicos e aplicações, impedindo que os usuários tenham informações claras, precisas e facilmente acessíveis acerca das operações de tratamentos realizadas com os dados coletados por diversos meios, como a partir de *cookies*, gerando assimetria informacional e dificultando o exercício da autodeterminação informativa.

Nesse sentido, a investigação da transformação de dados pessoais em dados pessoais sensíveis, a partir do fator integração, pode contribuir socialmente e culturalmente para alertar os usuários sobre uma possível quebra de privacidade, posto que os dados pessoais coletados indiretamente podem ensejar em informações mais robustas, cujo domínio não está nas mãos do titular e sim dos detentores.

A presente pesquisa não tem como objetivo investigar a eventual quebra de privacidade, pois para chegar a esse estágio, foi necessário um passo interior, objeto deste trabalho, qual seja, investigar se há indícios de que dados pessoais sensíveis são coletados por detentores, mesmo que de forma indireta.

O presente estudo também justifica-se por sua relevância social. A pesquisa TIC Domicílios 2022 evidenciou que 149 (cento e quarenta e nove) milhões de indivíduos, com idade superior a 10 (dez) anos, no Brasil, são usuários de Internet

(CETIC, 2022). Indivíduos esses que têm seus dados pessoais coletados por aplicações e sítios eletrônicos, enquanto interagem em ambientes digitais.

O contínuo e incessante monitoramento do “capitalismo de vigilância”, entretanto, ensejou no que Frank Pasquale (2015, p. 09) chama de *one-way-mirror*, isto é, o fato de que o Governo e o mercado, especialmente as grandes corporações, conhecerem os usuários que consomem seus produtos e serviços, mas esses usuários pouco sabem sobre quem os monitora, quais dados têm sobre eles, para quais finalidades são utilizados, bem como que tais dados podem ser combinados entre si, isto é, todo o ciclo de vida dos nossos dados dentro das grandes organizações é opaco, caracterizando a chamada insciência do usuário na coleta de dados (Affonso, 2018).

O direito à proteção de dados é um direito fundamental autônomo expresso na Constituição Federal de 1988, em seu artigo 5º, LXXIX (Brasil, 1988), reconhecido pela Emenda Constitucional 115, de 10 de fevereiro de 2022. Dessa forma, a crescente consciência dos usuários acerca do tratamento de seus dados, sobretudo em aplicações digitais, auxilia na efetivação desse direito, o que também demonstra ser uma contribuição da presente pesquisa em âmbito social.

O Supremo Tribunal Federal (STF), em 2020, já havia reconhecido o direito à proteção de dados como direito fundamental autônomo. Na oportunidade, o STF suspendeu a aplicação da Medida Provisória 954/2018, que obrigava as operadoras de telecomunicações a compartilharem com o Instituto Brasileiro de Geografia e Estatística (IBGE) dados dos usuários de telefonia móvel, como nome, celular e endereço, visando a formulação de estatística oficial durante a pandemia Sars-Cov-2 (Covid-19).

Em análise preliminar, a Ministra Rosa Weber afirmou que apesar da gravidade da crise sanitária então vivenciada, a solicitações das informações não estabelecia qualquer mecanismo de proteção que assegura o sigilo, a higidez e o anonimato dos dados compartilhados. Além disso, a Ministra entendeu que não há interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telecomunicações, não sendo definido o objetivo da utilização dos dados coletados, o que poderia representar uma limitação às liberdades individuais.

O compartilhamento de dados sem o consentimento ou, no mínimo, a ciência dos usuários é uma preocupação latente entre os estudiosos do tema. O

sociólogo Vance Packard (1967) alerta acerca do apoderamento de dados pessoais por detentores:

> [...] o maior perigo em um banco de dados centralizado seria a possibilidade de colocar um poder tão grande nas mãos de pessoas que podem apertar alguns botões de computadores. Quando os detalhes de nossas vidas são armazenados em um computador central ou em outros grandes sistemas de armazenamentos, todos nós nos sujeitamos, de certa forma, ao controle exercido pelos operadores destas máquinas (Packard, 1967, p. 40, tradução nossa)[7].

Enquanto área do conhecimento responsável por investigar a informação tanto nos âmbitos individual, institucional, quanto social (Silva; Nathansohn; 2018), a contribuição dos estudos da CI neste processo mostra-se necessária, tornando o presente trabalho com relevância científica.

Os estudos da CI evoluíram e ultrapassaram a recuperação da informação científica, por exemplo. A partir da concepção adotada no texto *Information science: what is it?* de Borko (1968), a CI apresenta-se como uma ciência interdisciplinar que investiga as propriedades do comportamento da informação, bem como as forças que governam seus fluxos, os processos e a otimização de sua acessibilidade e uso.

Enquanto ciência social aplicada, a CI busca soluções que amparem a necessidade informacional da sociedade, visando esclarecer um problema social concreto, qual seja, o da informação (Le Coadic, 2004). Assim, o campo investigativo da CI preocupa-se com o corpo de conhecimento relacionado à coleta, armazenamento, organização, recuperação, compartilhamento, transformação e utilização da informação (Borko, 1968).

Cunha e Cavalcanti (2008) entendem o termo dado como "a menor representação convencional e fundamental de uma informação (fato, noção, objeto, nome próprio, número, estatística, etc.) sob forma analógica ou digital", ensejando na necessidade da CI rever e/ou ampliar seu quadro referencial sobre as possibilidades interpretativas acerca do conceito de dados (Santos;Sant'Ana, 2013).

Os dados são considerados parte integrante da informação e, por isso,

> A vinculação do conceito de dados com o processo de geração de informação, que apresenta maior carga semântica, é muito presente, principalmente na ciência da computação, ao considerar a

[7] No original, "*The most disquieting hazard in a central data bank would be the placing of so much power in the hands of the people in a position to push computer buttons. When the details of our lives are fed into a central computer or other vast file-keeping systems, we all fall under the control of the machine's managers to some extent*".

> informação como elemento intermediário entre o dado (básico e estruturado) e o conhecimento (complexo e com alta carga semântica), conforme reforça a definição de Dorn (1981), de que os dados são a matéria prima para o desenvolvimento de informações (Santos;Sant'Ana, 2013, p. 202).

A interdisciplinaridade inerente à CI (Borko, 1968; Saracevic, 1996) permite a aproximação com o Direito, ao esclarecer o conceito de dado, bem como em situações em que o conceito de dado se refere a dado pessoal, pois, a partir do entendimento do que é um dado pessoal, torna-se possível saber se a legislação protetiva de dados pessoais será avocada (Bioni, 2021), bem como o papel do usuário em todo em esse processo e reduzir eventual assimetria informacional entre os usuários e àqueles que detém seus dados pessoais, chamados de agentes de tratamento pela legislação brasileira.

Assim, a presente pesquisa tem contribuição científica, uma vez que a CI pode e deve voltar os seus estudos aos dados, visando contribuir para que o acesso e uso intenso de dados se desenvolva da mais forma mais equilibrada possível, a partir da delimitação das fases envolvidas no acesso e uso dos dados, bem como os atores envolvidos (Sant'Ana, 2016).

1.6 Procedimentos metodológicos

A presente pesquisa é de cunho descritivo, com abordagem qualitativa. Para tanto, adotou-se a triangulação metodológica como o uso de múltiplos métodos, a fim de estudar e analisar, de forma interpretativa, o problema de pesquisa ora proposto (Denzin, 1988). Nesse sentido,

> A triangulação é uma abordagem metodológica que requer um desenho de pesquisa, cujo desenvolvimento pode contar com técnicas de recolha de dados diferentes, tanto com instrumentos para a pesquisa quantitativa quanto para a pesquisa qualitativa ou ainda mobilizando instrumentos quantitativos e qualitativos em uma mesma pesquisa. Ela tem se mostrado competente porque permite coletar informações a partir de fontes, espaços e tempos diferentes. Pode ainda triangular teorias e pesquisadores de distintas áreas do conhecimento (Figaro, 2014).

Visando investigar como os dados pessoais coletados por aplicações e sítios eletrônicos podem ser transformados em dados pessoais sensíveis, a partir da interferência do fator integração do Ciclo de Vida dos Dados, foram adotados os procedimentos a seguir:

1.6.1 Pesquisa bibliográfica

Iniciou-se com a pesquisa bibliográfica, pois, de acordo com Lima e Mioto (2007), a pesquisa bibliográfica relaciona um conjunto estruturado de procedimentos que visam buscar o objeto de estudo. Assim, utilizou-se a pesquisa bibliográfica para explanar acerca:

a) as principais definições de dados, dados Pessoais e dados Pessoais Sensíveis, suas diferenças, bem como a relevância prática da diferenciação, sobretudo baseado em legislações protetivas de dados (Sant'Ana; Santos, 2002, 2015; Sant'Ana, 2016, Affonso, 2018; Doneda, 2021, 2015; Mayer-Scönberge, 1997; Bioni, 2019; Rodotà, 2008; Mulholland, 2021);

b) o Ciclo de Vida dos Dados, com foco na fase de coleta e no fator integração (Sant'Ana, 2016; Affonso, 2018; Milagre, 2021; Monteiro; Segundo; Sant'Ana, 2016; Affonso, 2018; Segundo, 2014; Segundo; Coneglian, 2016).

1.6.2 Pesquisa documental

De acordo com Gil (2008, p. 51), a pesquisa documental é próxima à pesquisa bibliográfica, sendo percebida a diferença na natureza das fontes, uma vez que "[...] a pesquisa documental vale-se de matérias que não receberam ainda um tratamento analítico [...] tais como: documentos oficiais, reportagens de jornal, cartas, contratos, etc." (Gil, 2010, p. 51). Nesse sentido, a pesquisa documental nos útil para analisar os seguintes documentos:

a) Documentos jurídicos

A pesquisa documental também foi utilizada, mediante análise de documentos jurídicos, como leis, regulamentos e jurisprudências, visando identificar como tem sido aborda a questão dos dados pessoais e dados pessoais sensíveis, indicando os requisitos legais envolvidos no tratamento de dados pessoais, bem como o papel das Autoridades de Proteção de Dados em caso de descumprimento dos requisitos legais. As coletas ocorreram no mês de julho de 2023, sendo considerado:

- Cenário internacional: A presente pesquisa identificou e explanou as principais leis e os principais regulamentos que abordam as questões de dados pessoais e dados pessoais sensíveis: Estados Unidos, França, Europa,

Austrália, Canadá, Argentina, Uruguai e Suíça. A identificação das legislações ocorreu por meio de busca nos sites governamentais dos países supracitados.

- Cenário nacional: Foi identificada e explanada acerca da Lei Geral de Proteção de Dados brasileira, bem como os conceitos trazidos pela legislação para dados pessoais e dados pessoais sensíveis. A identificação ocorreu por meio de consulta ao sítio do governo federal, especificamente Planalto.gov. As jurisprudências foram identificadas mediante busca nos sítios eletrônicos do Superior Tribunal de Justiça e Supremo Tribunal Federal.

b) Decisões de Autoridades de Proteção de Dados Europeias

Foram analisadas as sanções aplicadas pelas Autoridades de Proteção de Dados Europeia, entre os anos de 2019-2023, às instituições que operam na União Europeia, relacionadas à violação do artigo 9º da GDPR, a fim de apresentar indícios da transformação de dados pessoais em dados pessoais sensíveis, a partir do contexto em que estão inseridos (fator integração), coletadas no sítio eletrônico *Enforcement Tracker* (Enforcement, 2023).

Registra-se que foi utilizada uma base de dados relacionada à UE, uma vez que a legislação de proteção de dados brasileira, por estar vigente há 3 (três) anos, período considerado recente, publicou uma única sanção, imposta pela Autoridade Nacional de Proteção de Dados brasileira, até o fechamento da presente pesquisa, em setembro de 2023.

De acordo com o sítio eletrônico *Enforcement Tracker*[8] (2023), foram aplicadas, até setembro de 2023, 2.039 (dois mil e trinta e nove) sanções foram aplicadas, sendo 1.824 (mil oitocentos e vinte e quatro) sanções pecuniárias na UE, representando um montante de 4 bilhões de euros, o que representa uma maturidade e experiência das autoridades em questão.

Nesse contexto, a técnica de coleta de dados utilizada na pré-análise foi a base de dados disponibilizada no sítio eletrônico *Enforcement Tracker* (2023), que possui 2.039 (dois mil e trinta e nove) casos de sanções mapeadas, até o fechamento deste estudo, em setembro de 2023. Contudo, realizou-se um filtro, disponibilizado pelo próprio sítio eletrônico, e da totalidade de casos mapeados pela

[8] Disponível em: https://www.enforcementtracker.com/.

plataforma, foram encontrados 129 (cento e vinte e nove) casos relacionados ao artigo 9º da GDPR, isto é, casos que estão relacionados a dados pessoais sensíveis, que foram analisados a partir da Análise de Conteúdo, a seguir descrita.

1.5.3 Análise de Conteúdo

A **Análise de Conteúdo** também atende às pretensões do estudo em comento, posto que não almeja-se discutir se os usuários sabem como funciona o ciclo de vida de seus dados coletados por aplicações e sítios eletrônicos. Mas sim, demonstrar os indícios da transformação de dados pessoais em dados pessoais sensíveis, por meio da análise das sanções aplicadas pelas Autoridades de Proteção de Dados Europeia, entre os anos de 2019-2023, a partir do contexto em que estão inseridos ou pela integração de bases de dados, sendo analisados 129 (cento e vinte e nove) casos.

Nesse contexto, Bardin (2011, p. 15) nos explica que:

> O que é a análise de conteúdo atualmente? Um conjunto de instrumentos metodológicos cada vez mais sutis em constante aperfeiçoamento, que se aplicam a 'discursos' (conteúdos e continentes) extremamente diversificados. O fator comum destas técnicas múltiplas e multiplicadas - desde o cálculo de frequências que fornece dados cifrados, até a extração de estruturas traduzíveis em modelos - é uma hermenêutica controlada, baseada na dedução: a inferência.

Assim, iniciamos pela **Pré-Análise**, oportunidade em que trabalhou-se os conceitos necessários para o presente estudo, como dados pessoais; dados sensíveis; coleta e fator integração, visando aprofundar o contexto social em que os dados estão estão inseridos, sobretudo em ambientes digitais, a partir dos conceitos e considerações já trabalhados anteriormente por autores referências e especialistas na área, como Affonso, 2018; Sant'Ana; Santos, 2002, 2015; Sant'Ana, 2016, Affonso, 2018; Doneda, 2021, 2015; Mayer-Scönberge, 1997; Bioni, 2019; Rodotà, 2008; Mulholland, 2021.

Para além disso, aprofundou-se também nas legislações mundiais e suas respectivas definições que abordam dados pessoais e dados pessoais sensíveis, sendo imprescindível entender seu mecanismo a partir do Ciclo de Vida dos Dados, cujo conceito foi cunhado por Sant'Ana (2016).

A coleta supracitada é de suma importância, pois em momento posterior será possível iniciar uma categorização de quais sanções aplicadas na União

Europeia, dentre os anos de 2019-2023, estão relacionadas a dados pessoais sensíveis (artigo 9º).

Para tanto, utilizou-se a base de dados disponibilizada pelo sítio eletrônico *Enforcement Tracker*, filtrados os casos relacionados ao artigo 9º do Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* - GDPR). O sítio eletrônico traz uma visão geral das sanções aplicadas pelas autoridades de proteção de dados na União Europeia (UE) às organizações, públicas e privadas, que agiram em desacordo com o da UE, por Autoridades de Proteção de Dados (*Data Protection Authority* - DPA, em inglês). A plataforma ressalta que o

> [...] objetivo é manter esta lista o mais atualizada possível. Como nem todas as multas são tornadas públicas, é claro que esta lista nunca poderá estar completa, e é por isso que apreciamos qualquer indicação de outras multas e penalidades do GDPR (Enforcement, 2023, tradução nossa).

A lista contém as sanções impostas em decorrência do descumprimento da GDPR, não sendo catalogados descumprimentos às leis nacionais/não europeias, tampouco leis que não sejam de proteção de dados (por exemplo, leis de concorrência/leis de comunicação eletrônica) ou de legislações já revogadas.

Assim, conhecidas as sanções pecuniárias relacionadas ao artigo 9º, do GDPR, no total 129 (cento e vinte e nove) casos, foi possível separar as sanções, oportunidade em que uma segunda fase da pesquisa foi iniciada: **exploração do material.** A fase de exploração compreende a codificação e categorização do material que compõe o *corpus* de análise, feita a partir de critérios previamente estabelecidos (análise categorial).

Nesse sentido, iniciou-se-á uma análise geral, por meio de observação sistemática de cada decisão que gerou a sanção, disponibilizada nos sítios eletrônicos das autoridades de proteção de dados e catalogadas pela *CMS.Law GDPR Enforcement Tracke*r. Nesta oportunidade, far-se-á também um recorte das unidades de registro e de contexto, criando categorias, isto é, separando as decisões que impuseram sanções por caso, país, ano, dados coletados, tipos de dados transformados.

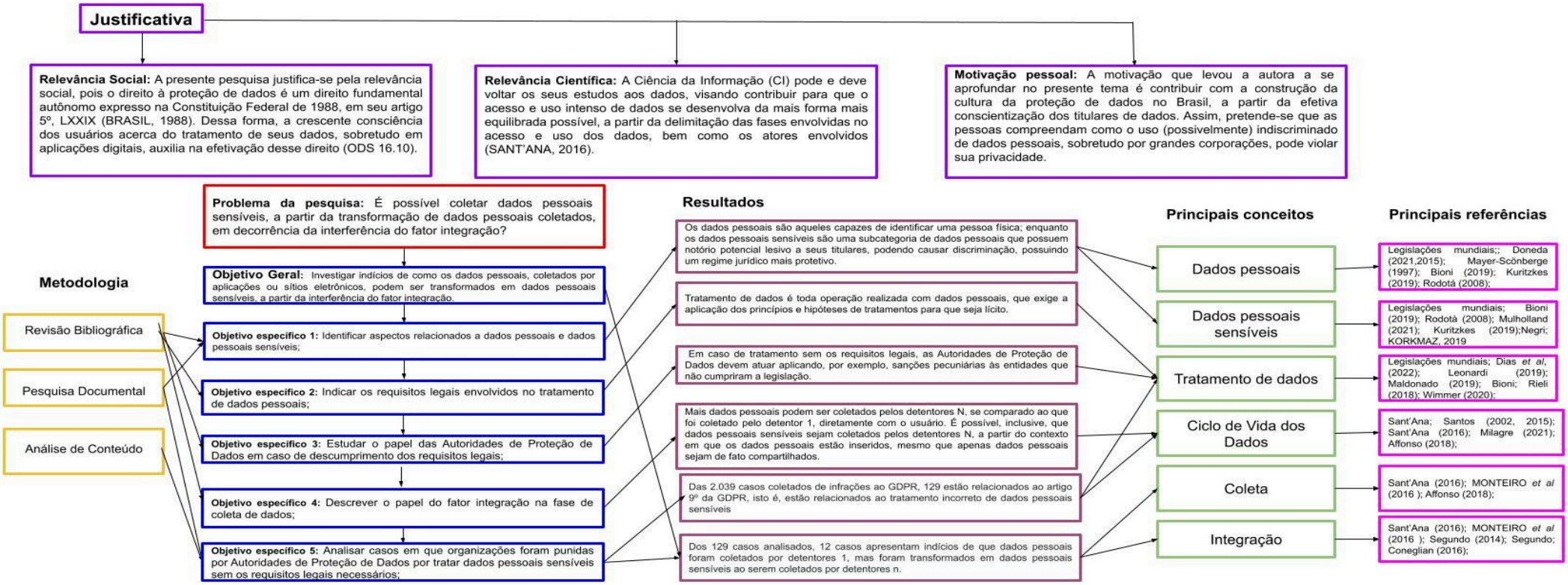
Criadas as categorias, é possível comparar quais decisões afirmaram que houve tratamento de dados sensíveis de forma indireta, ou seja, a partir do contexto ou da integração de bases de dados em que os dados pessoais estavam sendo tratados, transformou-os em dados pessoais sensíveis.

Por fim, a última fase poderá ser iniciada: **Tratamento dos resultados**. Nesta fase, é possível tratar os resultados obtidos, condensando todas as informações obtidas na exploração do material em tabelas e gráficos. Assim, é possível aferir quais das decisões das autoridades europeias afirmam que houve a transformação de dados pessoais em dados pessoais sensíveis, mesmo que não coletados ou disponibilizados de forma direta.

1.7 Estrutura da Pesquisa

Estruturalmente, a presente pesquisa está disposta em nove seções que explicitam os temas constituintes do presente trabalho, conforme Diagrama Estrutural apresentado na Figura 3, senão vejamos:

Figura 3 - Diagrama estrutural da dissertação de mestrado



Fonte: Adaptado de Sant'Ana, 2022.

O trabalho é composto por 6 seções. A seção 1, intitulada “Introdução”, tem a função de apresentar e delimitar o escopo da pesquisa, expondo o contexto em que o presente trabalho se insere, bem como sua relevância social e científica. Nesta seção, também é abordado o problema de pesquisa, a justificativa, objetivos gerais e específicos, bem como os procedimentos metodológicos aplicados para o seu desenvolvimento e a presente estrutura da pesquisa.

A seção 2, denominada “**DADOS, DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS**” expõe os conceitos de dados, abordando a questão de dados pessoais e dados pessoais sensíveis, a partir das legislações mundiais, conforme proposto no primeiro objetivo específico. A seção em tela traz a construção dos conceitos de dados pessoais, fundamentada nas quatro gerações de leis que tutelam a proteção de dados, trazendo reflexões sobre a construção e consolidação do termo em diversos países. Além disso, é apresentado o conceito de dados pessoais sensíveis, uma subcategoria de dados pessoais, criados a partir da prática do direito.

A seção 2 traz, ainda, a diferenciação prática entre dados pessoais e dados pessoais sensíveis, a partir da investigação nas mais diferentes legislações mundiais. O conceito de dados pessoais é tido como sendo aqueles que por meio de seu tratamento é possível relacioná-lo à uma pessoa natural, identificada ou identificável, sintetizado no Quadro 1, enquanto os dados pessoais sensíveis, a seu turno, compõe uma subcategoria de dados pessoais e possuem notório potencial lesivo a seus titulares, podendo causar-lhes discriminação.

Nesse contexto, essa categoria atrai um regime jurídico mais protetivo. Assim, sintetizou-se no Quadro 2 as definições trazidas pelas legislações protetivas de dados acerca dos conceitos de dado sensível. A seção aborda, ainda, uma comparação entre dados pessoais e dados pessoais sensíveis, conforme legislações pesquisadas (Quadro 3) e traz a relação entre os tipos de dados (Figura 3).

A seção 3, nomeada **OS ATORES E REQUISITOS LEGAIS ENVOLVIDOS NO TRATAMENTO DE DADOS PESSOAIS** explora os agentes de tratamentos envolvidos no tratamento de dados pessoais, os princípios e hipóteses legais de tratamento de dados pessoais, bem como o papel das Autoridades Nacionais de Proteção de Dados Pessoais, relacionados ao segundo e terceiros objetivos específicos. Na presente seção busca-se descrever um breve panorama das autoridades de proteção de dados europeias e latino americanas, em especial a

brasileira, evidenciando suas atribuições, atuação, tais como a aplicação de sanções pecuniárias, em caso de infração por entidades às leis de proteção de dados. A importância dessa seção está relacionada à seção 6, que visa apurar sanções aplicadas pelas autoridades de proteção de dados europeias, entre os anos de 2019-2023, relacionando-se o objetivo da presente pesquisa, qual seja, o de investigar como os dados pessoais, coletados por aplicações e sítios eletrônicos, podem ser transformados em dados pessoais sensíveis.

A seção 4, "**A FASE DE COLETA DE DADOS PESSOAIS E O FATOR INTEGRAÇÃO NO CVD**", explana acerca do CDV, suas fases, em especial a fase de coleta, bem como o fator integração, conforme proposto no quarto objetivo específico. Esse fator, pertencente ao CVD, permeia todas as fases do CVD, havendo um destaque para as fases de coleta, armazenamento e recuperação, na presente pesquisa, a partir da integração de diferentes bases de dados. Em que pese não ser objeto da presente pesquisa dissertar acerca das técnicas de integração de bases de dados, destacou-se o papel desse fator no CVD, sobretudo podendo gerar novos dados que, em tese, não foram coletados diretamente do usuário.

A seção 5 dispõe acerca da "**APRESENTAÇÃO DOS RESULTADOS**", obtidos por meio da análise de sanções aplicadas por Autoridades de Proteção de Dados Europeias, a fim de verificar indícios de transformação de dados pessoais em dados sensíveis, conforme quinto objetivo específico, oportunidade em que poderá aferir se a presente pesquisa alcançou seu objetivo geral.

A seção 6 apresenta as "**CONSIDERAÇÕES FINAIS**" da pesquisa.

2 DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Santos e Sant'Ana (2002) conceituam o termo dado como "[...] um elemento básico, formado por signo ou conjunto finito de signos que não contém, intrinsecamente, um componente semântico, mas somente elementos sintáticos". Os dados, compostos pela tríade EAV, podem ser estruturados por entidade e atributo (EA), podendo ser identificados através da granularidade mais fina de determinado contexto, oportunidade em que a tríade se forma por meio do valor (Santos; Sant'Ana 2015). Considera-se como dado, na presente pesquisa,

> uma unidade de conteúdo necessariamente relacionada a determinado contexto e composta pela tríade entidade, atributo e valor, de tal forma que, mesmo que não esteja explícito o detalhamento sobre contexto do conteúdo, ele deverá estar disponível de modo implícito no utilizador, permitindo, portanto, sua plena interpretação (Santos; Sant'Ana, 2015, p. 205).

Assim, o termo dado é considerado nesta pesquisa como o elemento básico na geração de uma informação, sendo composto pela pela tríade entidade - atributo - valor (EAV). Nesses termos, a tríade é composta por por um conjunto mínimo de símbolos que pode ser tomado como uma unidade de conteúdo, sendo necessário ser identificado o contexto a que pertence (Santos; Sant'Ana, 2015).

Os dados em si são puramente objetivos, não apresentam alta carga semântica intrínseca e são independentes do usuário, constituindo, contudo, matéria-prima para uma série de possíveis interpretações, bem como medidas ou fatos que são representados por números, palavras, sons e até imagens que poderão sustentar a produção de novas informações (Souza; Almeida, 2021).

A informação em sua concepção mais ampla, está fora do escopo desta pesquisa e, a seu turno, está além do que está representado pelo dado, chegando ao limiar da cognição, a partir de determinado contexto (Doneda, 2021). Assim "[...] Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo - daí que a informação carrega em si também um sentido instrumental, no sentido de redução de um estado de incerteza" (Doneda, 2021, p.140). Já o conceito de conhecimento, também além da delimitação deste texto, pode ser entendido como a aplicação e o uso produtivo da informação (Boisot, 1998).

2.1 A identificação dos dados pessoais

A partir da criação de novos métodos e técnicas decorrentes do advento e evolução da informática e das consequentes mudanças políticas e sociais, percebe-se uma transformação no tratamento de dados, que passa por uma mudança quantitativa e qualitativa, uma vez que:

> [...] o diferencial que a informatização proporcionou ao tratamento de dados pessoais apresenta perfis quantitativo e qualitativo: um baseado na 'força bruta', no poder de processar mais dados em menos tempo, e o outro, na aplicação de técnicas sofisticadas a este processamento de forma a obter resultados mais valiosos (Doneda, 2021, p.155).

Nesse contexto, é possível que, por intermédio dos dados, seja possível a identificação de uma pessoa natural, a partir de determinado contexto, gerando informações além daquelas explicitadas somente nos dados atomizados. Em situações dessa natureza, os dados poderão ser classificados como sendo dados pessoais, oportunidade em que o Estado passa ter uma maior preocupação com o tratamento desses dados, uma vez ser possível a violação da privacidade dos indivíduos.

Kuritzkes (2019) enfatiza que apesar da notória necessidade de regulamentação para o tratamento de dados coletados de forma *online*, os legisladores encontram dificuldades em elaborar normas suficientemente abrangentes para governar a coleta de dados. Lawrence Lessig (2006) argumenta que os dados pessoais são tratados frequentemente como mercadoria pelas companhias, e que a coleta e o processamento de dados pessoais podem ter consequências negativas para a privacidade. Por isso:

> A inserção de dados pessoais do cidadãos em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações da vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita a sua intimidade; ao mesmo tempo, o cidadão objeto dessa discriminada colheita de informações, muitas vezes, sequer sabe da existência dessa atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo (STJ, 1996).

A aplicação de leis que protegem dados pessoais preconiza a análise inicial do próprio conceito de dado, muitas vezes confundido com o conceito de informação

pelas legislações (Doneda, 2021). O Conselho da Europa, na Convenção 108 de 28 de janeiro de 1981, primeiro instrumento internacional vinculante que protege o indivíduo contra abusos que possam acompanhar a coleta e o processamento de dados pessoais, além de regular o fluxo transfronteiriço de dados pessoais, também trouxe como sendo dado pessoal toda informação relacionada a um indivíduo identificado ou identificável.

A Diretiva 95/46/CE, promulgada pelo Parlamento Europeu e do Conselho, de 24 de outubro de 1995 (União Europeia, 1995), dispôs acerca do tratamento de dados em âmbito europeu, a fim de cada país membro do bloco europeu tenha uma legislação protetiva de dados pessoais, bem como cada Estado-membro da União Europeia possua uma autoridade de proteção de dados própria, competente para supervisionar e fiscalizar o tratamento de dados.

O texto legal em estudo trouxe a definição de dado pessoal, como sendo: "qualquer informação relativa a uma pessoa singular identificada ou identificável". Em seu artigo 2º, a Diretiva em estudo acrescenta, ainda, que uma pessoa natural é identificável ao ser associada "[...] a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social" (União Europeia, 1995).

O Relatório do Fórum Econômico Mundial (*World Economic Forum)* define como o dado pessoal os dados (e metadados) criados por e sobre as pessoas, abrangendo: dados oferecidos voluntariamente, como perfis em redes sociais); dados observados, como: dados de localização emitidos por celulares; e dados inferidos, como pontuação de crédito (Wef, 2011, p.7).

O léxico "dado", para fins legais, pode ter conotação reducionista (identificado) ou expansionista (identificável). Para os reducionistas, somente é considerado dado pessoal, os dados únicos, isto é, por intermédio de apenas um único dado é possível identificar uma pessoa natural de forma imediata, direta e específica, sem a necessidade de associação de dados (Bioni, 2021), a saber: nome completo, imagem, documentos, como CPF, RG, dentre outros.

A visão expansionista, por sua vez, permite um alargamento da conceituação do termo dado pessoal, uma vez que por meio da combinação de dados é possível identificar um indivíduo, tais como: características físicas, preferências pessoais, hábitos de consumo, profissão, dentre outros.

Affonso e Sant'Ana (2017) destacam que os dados podem ser armazenados em uma única relação R, no qual R possui um esquema relacional R (a1, a2, a3,...an), em que a1 é um atributo do domínio Di, com i = 1,...,n. Assim,

> Na perspectiva da divulgação de dados dos indivíduos, os atributos em R podem ser classificados da seguinte forma (CAMENISCH; FISCHER-HÜBNER; RANNENBERG,2011; SAMARATI, 2001): a) **Identificadores** (I): atributos que identificam unicamente os indivíduos (ex.: CPF, Nome, Número da Identidade); b) **Semi-identificadores** (SI): atributos que podem ser combinados com dados externos e expor o indivíduo, ou ainda reduzir a incerteza sobre suas identidades (ex.: data do nascimento, CEP, cargo, função, tipo sanguíneo); Fung et al. (2010) e Run et al. (2012) corrobora com a ideia de que os semiidentificadores é um conjunto de atributos que quando combinados podem identificar o registro. Para exemplificar os semi-identificadores Sweeney (2002) relata a seguinte situação: Dado um conjunto de elementos em uma entidade U, na entidade-especificada T (A1,...,An), c:U T e g: T U', onde UU'. O semi-identificador de T, escrito QT, é o conjunto de atributos {A1,...,Aj} {A1,...,An} onde pi U ambos que g(c(pi)[QT])=pi. c) **Atributos sensíveis** (AS): ou também chamados de confidenciais, representam os atributos que contêm informações sensíveis sobre os indivíduos (ex.: doenças, salário, exames médicos, lançamentos do cartão de crédito) (VIMERCATI et al., 2012) (Affonso; Sant'Ana, 2017, p. 24).

Dessa forma, é possível que dados pessoais sejam disponibilizados para o público, como para fins estatísticos, mas tendo os identificadores únicos removidos, visando garantir a privacidade dos sujeitos que participaram de uma pesquisa científica, por exemplo (Run *et al.,* 2012). Contudo, ainda é possível identificar indivíduos a partir da combinação de dados de outras bases de dados, como, por exemplo, dados públicos sem identificadores únicos combinados com outros dados publicados em uma base de dados privada (Affonso; Sant'Ana, 2017).

2.2 As gerações de leis de proteção de dados

A partir dos estudos realizados, sobretudo, por Mayer-Scönberge (1997) e Doneda (2021), é possível descrever quatro diferentes gerações de leis que tutelam a proteção de dados, o que contribui para análise da evolução desse direito ao longo do tempo, bem como possibilita a reflexão acerca da construção e consolidação do termo "dados pessoais".

As leis da chamada primeira geração são datadas da década de 1970 e são vinculadas à tutela de dados em relação ao tratamento realizado pelos Estados, que detinham, à época, o monopólio dos grandes bancos de dados pessoais. As

legislações em estudo referiam-se, sobretudo, acerca da concessão de autorizações para criação de banco de dados e o controle exercido pelo Estado e suas unidades administrativas sobre eles (Doneda, 2021).

A primeira legislação local de proteção de dados foi a chamada Lei do *Land* alemão, da cidade de Hesse, na Alemanha (1970). Ainda na Europa, em 1973, a Suécia promulgou o Estatuto para banco de dados (*Datalag),* primeira lei nacional de proteção de dados (Doneda, 2021).

À medida que a tecnologia avançava, a partir dos anos de 1960 e 1970, tornou-se mais fácil que as agências governamentais cruzassem dados pessoais dos cidadãos, mantidos pelos governos federais para as mais diversas finalidades, como cadastros em sistema de saúde, entidades tributárias, educacionais e para fins criminais. Nesse contexto, os Estados Unidos promulgaram o *Privacy Act* (1974), que visava a regulamentação da criação e o uso de banco de dados computadorizados que, de alguma forma, impactam o direito à privacidade. Segundo o *Privacy Act* (EUA, 1974):

> 4. o termo “registro” significa qualquer item, coleção ou agrupamento de informações sobre um indivíduo mantido por uma agência, incluindo, mas não limitado a, sua educação, transações financeiras, histórico médico e criminal ou profissional e que contenha seu nome, ou o número de identificação, símbolo ou outro particular de identificação atribuído ao indivíduo, como impressão digital ou de voz ou fotografia;[9]

A legislação em comento, portanto, conceitua o termo dado de forma expansionista, posto que considera como dado qualquer item, coleção ou agrupamento de informações referentes a educação, transações financeiras, histórico médico, criminal ou profissional, que contenha o nome de uma pessoa natural ou seu número de identificação, símbolo ou outro meio de identificação que poderá ser atribuído a um indivíduo.

A primeira geração de leis seguiu até 1977, tendo como marco a promulgação da *Bundesdatenschutzgesetz,* Lei da República Federativa da Alemanha sobre proteção de dados pessoais (Doneda, 2021).

Contudo, logo as leis da primeira geração tornaram-se obsoletas, posto que uma multiplicidade dos centro de tratamento de dados estava ocorrendo em todo o

---

[9] Tradução livre. No original “*the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;”*

mundo, isto é, em decorrência do avanço tecnológico, o tratamento de dados pessoais estava deixando de ser uma atividade privativa do Estado (Lugati; Almeida, 2020). Nesse sentido, a “Figura do grande irmão" (uma única e centralizada base de dados - Estado) é diluída pela de pequenos irmãos, a saber, bancos de dados dispersos no plano estatal e privado (Bioni 2021).

Assim, uma segunda geração de leis estava surgindo, preocupadas não mais com a estrutura dos bancos de dados e o fenômeno computacional, mas com a possibilidade do cidadão exercer seu direito à privacidade. Nesse contexto, as legislações permitiam que o cidadão participasse do processo de tratamento de dados, por meio de seu consentimento (Bioni, 2021).

O conceito de dado pessoal, contudo, não sofreu muitas alterações. Em 1978, por exemplo, a França promulgou a chamada *La Loi Informatique et Libertés* (França, 1978), seguida pela lei austríaca, portuguesa e espanhola. A Lei francesa caracterizava, em seu artigo 4º, um dado como sendo uma

> Informação que permita, sob qualquer forma, direta ou indiretamente, a identificação das pessoas singulares a quem se aplica, quer o tratamento seja efetuado por pessoa singular, quer por pessoa moral.[10]

A definição ora exposta, todavia, teve sua vigência encerrada em 2004. A *La Loi Informatique et Libertés* sofreu uma série de reformas, passando a adotar, entre os anos de 2004 e 2018, o seguinte conceito

> Dados pessoais são quaisquer informações relativas a uma pessoa singular identificada ou que possa ser identificada, direta ou indiretamente, por referência a um número de identificação ou a um ou mais elementos que lhe sejam específicos. Para determinar se uma pessoa é identificável, é necessário considerar todos os meios que permitam sua identificação disponíveis ou aos quais o controlador ou qualquer outra pessoa possa ter acesso.[11]

Em ambas as definições, é caracterizado como dado pessoal tanto as informações relativas a uma pessoa identificada, como as que podem identificar um sujeito, oportunidade em que a visão expansionista já era adotada desde 1978 e

---

[10] Tradução Livre. No original: “*Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit,* directement ou non*, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale”.*

[11] Tradução Livre. No original *“Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.*

permaneceu até 2018, ocasião em que a França passa a seguir as diretrizes do *General Data Protection Regulation* de 2018.

Percebe-se, ainda, que a legislação traz como sinônimos dado e informação, sendo o dado pessoal qualquer informação relativa à pessoa física identificada ou que pode ser identificada. Contudo, o dado pessoal constitui uma unidade de conteúdo que, quando relacionado a determinado contexto, poderá identificar uma pessoa natural.

As leis de segunda geração também ficaram ultrapassadas, uma vez que eram focadas no fornecimento de dados pelo próprio cidadão e, caso esse cidadão, não concedesse o seu consentimento para o tratamento de dados, ele acabaria sendo excluído de certas atividades sociais (Doneda, 2021).

A terceira geração, observada a partir da década de 1980, manteve o cidadão como protagonista da tutela de proteção de dados, mas deu enfoque em garantir a efetividade do direito à proteção de dados e não somente na liberdade do indivíduo em fornecer dados (Doneda, 2021). A presente geração é representada pela decisão do Tribunal Constitucional Alemão (1983) que, pela primeira vez, trouxe o conceito de autodeterminação informativa, como sendo o “direito de manter controle sobre as suas informações e de determinar a maneira de construir sua esfera particular” (Rodotà, 2008, p. 15).

Assim, a clássica sequência “pessoa-informação-sigilo” é superada pela sequência “pessoa-informação-circulação-controle”, cuja “circulação controlada” de dados passa a imperar (Rodotà, 2008, p. 93).

Nesse cenário, o tratamento de dados pessoais passou a ser visto como um processo, que não era encerrado com a coleta dos dados pelos agentes de tratamento, a partir da permissão dos titulares de dados. A participação dos titulares passou a envolver o conhecimento consciente das fases sucessivas do processo de tratamento (Doneda, 2021). Contudo, as leis da terceira geração não eram muito acessíveis, sobretudo diante dos custos envolvidos para exercer os direitos relacionados à proteção de dados pessoais.

Assim, a quarta geração de leis de proteção de dados pessoais procura focar não apenas no controle individual, mas também difuso, buscando proteger a coletividade de tratamentos abusivos e ilícitos, a partir da criação de instrumentos e mecanismos jurídicos, como autoridades que fiscalizam o tratamento de dados, a

inversão do ônus da prova para o agente de tratamento, restrição no tratamento de dados, em especial, os sensíveis, dentre outros (Bioni; Silva; Martins, 2022).

Na Austrália, o *Privacy Act* (Austrália,1988) trouxe a definição de "*personal information*" como sendo a "informação ou opinião sobre um **indivíduo identificado, ou um indivíduo que seja razoavelmente identificável**, seja a informação ou opinião verdadeira ou não; e se a informação ou opinião está registrada de forma relevante ou não" (Austrália, 1988, grifo nosso).

Em 21 de outubro de 1998, o governo do presidente americano Bill Clinton, assinou o chamado *Children's Online Privacy Protection Act* of 1998 - COPPA (EUA, 1998), que entrou em vigor em 21 de abril de 2000. Essa legislação proíbe atos ou práticas injustas ou enganosas relacionadas à coleta, uso e/ou divulgação de informações pessoais de e sobre crianças na Internet, tendo por definição de informações pessoais aquelas informações individualmente identificáveis sobre um indivíduo coletadas online, incluindo: nome e sobrenome; a casa ou outro endereço físico, incluindo o nome da rua e o nome de uma cidade ou vila; Informações de contato on-line; tela ou nome de usuário onde funciona da mesma maneira que as informações de contato on-line; Um número de telefone; Um número de Seguro Social; Um identificador persistente que pode ser usado para reconhecer um usuário ao longo do tempo e em diferentes sites ou serviços online. Tal identificador persistente inclui, mas não está limitado a, um número de cliente mantido em um cookie, um endereço de Protocolo de Internet (IP), um processador ou número de série do dispositivo ou identificador exclusivo do dispositivo; Uma fotografia, vídeo ou arquivo de áudio onde tal arquivo contém a imagem ou voz de uma criança; Informações de geolocalização suficientes para identificar o nome da rua e o nome de uma cidade ou vila; ou Informações sobre a criança ou os pais dessa criança que o operador coleta online da criança e combina com um identificador descrito nesta definição.

A Argentina promulgou a Lei de Proteção de Dados Pessoais, Lei 25.326, promulgada parcialmente em 4 de outubro de 2000 (Argentina, 2000), que tem por objeto a proteção integral dos dados pessoais armazenados em arquivos, registros, bancos de dado ou outros meios técnicos de tratamento de dados, sejam públicos

ou privados[12] (Argentina, 2000). Na legislação em comento, dados pessoais tem a definição bem próxima a europeia e são tidos como “informações de qualquer tipo referentes a pessoas com existência natural ou ideal, **específicas ou determináveis**”[13] (Argentina, 2000, grifo nosso).

O Uruguai promulgou sua legislação protetiva de dados pessoais em 18 de agosto de 2008, a Lei nº 18.331, nomeada de *Protección de datos personales y acción de “habeas data”* (Uruguai, 2008). Na supracitada legislação, a definição de dados pessoais pode ser vista no artigo 4º como sendo informação de qualquer tipo referida a uma pessoa física ou jurídica determinadas ou determináveis.

O *General Data Protection Law* (GDPR), (EU) 2016/679, promulgado em 25 de maio de 2018, legislação responsável por normatizar o tratamento de dados pessoais na Europa, define dados pessoais (*personal data)*, em seu 4º, como sendo

> ‘Dado pessoal’ é qualquer informação relacionada a uma pessoa natural **identificada ou identificável** (‘titular de dados); uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, por um identificador particular, como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos relacionados à natureza física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural (European, 2016, tradução nossa, grifo nosso)[14].

Seguindo a tendência mundial de tutelar os dados pessoais, o Brasil regulou a proteção de dados pessoais através da Lei 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), cuja vigência data de 18 de setembro de 2020, tendo as sanções administrativas entrado em vigor apenas a partir de agosto de 2021 (Brasil, 2018). A LGPD traz em seu artigo 1º seu principal escopo, qual seja, regular 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

---

[12] Tradução livre. No original: “La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados” (ARGENTINA, 2000).

[13] Tradução livre. No original: “*Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*”. (Argentina, 2000).

[14] Tradução livre. No original: “‘*Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*”(European Parliament; Council of the European Union, 2016).

> de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Para tanto, a legislação brasileira nos prestigiou, em seu artigo 5º, com a definição de dado pessoal como sendo:

> I - dado pessoal: informação relacionada a pessoa natural **identificada ou identificável** (Brasil, 2018).

A LGPD também adotou a visão expansionista, considerando dado pessoal todo o tipo de "informação" que está atrelado a uma pessoa natural, seja de forma direta (identificada) ou indireta (identificável).

Por meio da promulgação da Emenda Constitucional (EC) 115/2022, o direito à proteção de dados pessoais passou a integrar o rol de direitos e garantias fundamentais, que compõem as cláusulas pétreas, expressas na Constituição Federal (Brasil,1988). Assim, passa-se a ser "(...) assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Brasil,1988), conforme redação do artigo 5º, inciso LXXIX, da Carta Magna.

Desde a década de 1980, já na terceira geração de leis, as legislações ocidentais, organismos internacionais e blocos econômicos conceituam dados pessoais, a partir de uma visão expansionista, sendo considerado dado pessoal os dados por meio dos quais é possível identificar uma pessoa, seja de forma direta ou indireta (Bioni, 2021).

Contudo, caso a correlação entre um dado e uma pessoa demande um esforço desproporcional do agente de tratamento, o dado não poderá ser alçado à categoria de pessoal e sim de anônimo. Bioni (2021) esclarece que tanto a LGPD quanto o direito europeu adotaram um critério de razoabilidade para limitar o conceito expansionista de dados pessoais, não bastando que o indivíduo possa ser identificado, mas a partir de um contexto no qual ele está inserido ser possível, de forma razoável, identificá-lo de forma efetiva.

2.3 Dados pessoais sensíveis e as definições legais

Os dados pessoais podem ser agrupados em subcategorias, criadas a partir da prática do direito (Doneda, 2021). O tratamento de dados pessoais podem ensejar em informações que revelem, segundo Bioni (2021, p. 84), "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação", conferindo a esses dados o pertencimento a subcategoria de dados pessoais sensíveis.

A criação da subcategoria dados pessoais sensíveis ocorreu a partir da observação pragmática acerca dos diferentes efeitos produzidos a partir do tratamento de dados dessa natureza (Doneda, 2021), pois "um dado, em si, não é perigoso ou discriminatório - mas o uso que dele se faz, pode sê-lo" (Doneda, 2021, 148). Assim, a seleção de quais tipos de dados são considerados como sensíveis advém da constatação de que certos tipos de dados, quando tratados por terceiros, "[...] apresentariam um elevado potencial lesivo aos seus titulares, em uma determinada configuração social" (Doneda, 2021, p. 147).

Dessa forma, mais importante do que identificar o conteúdo do dado é aferir a potencialidade discriminatória no tratamento de determinados tipos de dados pessoais (Mulholland, 2021). Nesse sentido, cada ordenamento jurídico deve estabelecer seus dados pessoais sensíveis, isto é, quais dados tem a maior probabilidade de serem utilizados para fins discriminatórios e deixem o titular em posição vulnerável.

O Conselho da Europa, na Convenção 108 de 28 de janeiro de 1981, apresentou, em seu artigo 6º, os dados considerados "sensíveis", considerando seu processamento proibido, salvo nos casos em que os agentes de tratamento utilizassem salvaguardas, a serem determinadas por lei, em complemento à Convenção, visando a prevenção de riscos inerentes ao tratamento de dados pessoais sensíveis. Assim:

> O tratamento de: – dados genéticos; – dados pessoais relativos a infrações, processos penais e condenações e medidas de segurança conexas; – dados biométricos que identificam exclusivamente uma pessoa; – os dados pessoais pela informação que revelam relativos à origem racial ou étnica, opiniões políticas, filiação sindical, convicções religiosas ou outras, saúde ou vida sexual, só serão permitidos quando as garantias apropriadas estiverem consagradas na lei, complementando as da presente Convenção . 2. Essas salvaguardas devem prevenir os riscos que o tratamento de dados pessoais sensíveis possa representar para os interesses, direitos e liberdades fundamentais da pessoa em causa, nomeadamente o risco de discriminação (Council…1981).[15]

[15] Tradução livre. No original "*The processing of: – genetic data; – personal data relating to offences, criminal proceedings and convictions, and related security measures; – biometric data uniquely identifying a person; – personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention. 2 Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.*

A Diretiva 95/46/CE, no mesmo sentido, proibiu o tratamento de “certas categorias” de dados, em seu artigo 8º. O diploma legal em estudo afirma que os Estados-membros devem proibir o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

Ainda no artigo 8º, contudo, a própria Diretiva autoriza o tratamento de dados pessoais sensíveis, em caráter excepcional, caso o titular de dados dê consentimento explícito para o tratamento; para cumprimento de obrigações legais pelos agentes de tratamento; para proteção dos interesses vitais de pessoa natural; para dados tornados públicos pelo próprio titular e caso o tratamento for efetuada por associações ou organismos similares, sem fins lucrativos de carácter político, filosófico, religioso ou sindical, na condição de o tratamento disser unicamente respeito aos próprios membros desse organismo.

Em 1996, os Estados Unidos publicou a *Health Insurance Portability and Accountability Act of* 1996 (HIPAA) (EUA, 1996), que visa melhorar a eficiência e eficácia do sistema de saúde americano por meio da adoção de padrões nacionais para transações eletrônicas de assistência médica e conjuntos de códigos, identificadores exclusivos de saúde e segurança. A legislação não utiliza o termo sensível, mas entende como informações Protegidas de Saúde: Informações de saúde individualmente identificáveis que são transmitidas ou mantidas em qualquer forma ou meio (eletrônico, oral ou papel) por uma entidade coberta ou seus associados comerciais, excluindo certos registros educacionais e de emprego.

A Lei de Proteção de Dados Argentina (2000), a seu turno, considerou como dados pessoais sensíveis, os dados pessoais que revelam origem racial e étnica, opiniões políticas, convicções religiosas, filosóficas ou morais, filiação sindical e informações sobre saúde ou vida sexual.

No Uruguai, de forma semelhante, a legislação protetiva de dados pessoais traz os dados pessoais sensíveis como sendo os dados que revelam a origem racial e étnica, preferência políticas, convicções religiosas ou morais, filiação sindical, bem como informações referentes à saúde ou à vida sexual.

O GDPR (2018), em seu artigo 9º, considera como dados de categoria especial (ou sensíveis) aqueles que revelam raça ou origem étnica, opiniões políticas, religiosa ou filosófica, filiação sindical, dados genéticos, biometria, dados

referentes à saúde ou referentes à vida ou orientação sexual. No caso dos dados de saúde e genético,

> [...] não há dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado (Rodotà, 2008, 70).

Os dados biométricos também compõe a categoria de dados pessoais sensíveis, pois traços ou características do corpo humano, com o avanço da tecnologia, estão sendo usados para identificação direta e inequívoca de um indivíduo ou, nas palavras de Rodotà (2008, p. 94) as

> [...] inovações tecnológicas permitem uma renovada decomposição do corpo mediante a coleta de informações que reduzem a identidade do sujeito a um só detalhe – a um traço do rosto, ao reconhecimento da íris, impressões digitais (Rodotà, 2008).

Ainda no estudo da legislação européia de proteção de dados, o GDPR, em seu considerando 51, impõe que os dados que sejam, por sua natureza, sensíveis, devem ter proteção específica, pois o contexto a que esses dados podem ser submetidos podem acarretar em riscos significativos para os direitos e liberdades fundamentais. Em regra, a legislação europeia proíbe, via de regra, o tratamento de dados pessoais sensíveis. Nesse sentido, o artigo 9º expressamente alude que

> O tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para efeitos de identificação unívoca de uma pessoa singular, dados relativos à saúde ou dados relativos a uma pessoa singular a vida sexual ou a orientação sexual de uma pessoa devem ser proibidas.[16]

Contudo, a própria legislação em comento trouxe 10 (dez) circunstâncias, que têm caráter de excepcionalidade, e permitem o tratamento de dados pessoais sensíveis, tais como cumprimento de obrigação legal pelos agentes de tratamento, consentimento do titular, questões de saúde, dentre outras.

Para dados dessa natureza, a LGPD também alçou, no artigo 5º, inciso II, (Brasil, 2018) à categoria de sensíveis, isto é, dados referentes à origem racial ou

---

[16] Tradução livre. No original "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".*

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.

A separação entre dados pessoais e sensíveis, no Brasil, contribui para o cumprimento do princípio da não discriminação, constitucionalmente consagrado no artigo 3º, inciso IV, (Brasil, 1988), em que “Constituem objetivos fundamentais da República Federativa do Brasil, IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação” (Mulholland, 2021). Nesse sentido, Mulholland destaca que

> O princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam inequitativos. Esse princípio deve servir como base de sustentação da tutela dos dados pessoais sensíveis, especialmente quando estamos diante do exercício democrático e do acesso a direitos sociais, tais como o direito ao trabalho, à saúde e à moradia (Mulholland, 2018, p. 174).

Além disso, Rodotà (2008) preconiza que a tutela de dados pessoais sensíveis possibilita também a garantir e a efetivação do direito à saúde (dados genéticos ou sanitários), do direito à liberdade de expressão e de comunicação (dados sobre opiniões políticas), do direito à liberdade religiosa e de associação (dados sobre convicção religiosa e associação sindical), bem como de liberdade sexual.

No caso da LGPD, os dados pessoais sensíveis foram arrolados pelo legislador, não sendo expressamente definido, seja pelo próprio legislador, seja pela Autoridade Nacional de Proteção de Dados (ANPD), se o rol que elenca os dados pessoais sensíveis poderá ser estendido a outros tipos de dados que gerem discriminação aos usuários. Contudo, a LGPD estabeleceu um regime jurídico diferenciado, com institutos próprios, voltados a conferir maior proteção no tratamento de dados pessoais sensíveis (Mulholland, 2021).

No mesmo sentido, a LGPD, que sofreu forte influência da legislação protetiva de dados europeia, segue a mesma tendência ao conferir maior proteção aos dados pessoais sensíveis (Mulholland, 2021). De acordo com Rodotà (2008, p. 64),

> […] para garantir plenitude à esfera pública, determinam-se rigorosas condições de circulação destas informações, que recebem um fortíssimo estatuto “privado”, que se manifesta sobretudo pela

> proibição de sua coleta por parte de determinados sujeitos (por exemplo, empregadores) e pela exclusão de legitimidade de certas formas de coleta e circulação.

Nesse cenário, o rol de hipóteses legais que autorizam o tratamento de dados pessoais sensíveis mostra mais restritivo do que as hipóteses legais relacionadas aos dados pessoais não sensíveis, não sendo conferido aos agentes de tratamento a possibilidade de tratamento de dados pessoais sensíveis para fins de legítimo interesse e proteção ao crédito, por exemplo (Brasil, 2018).

2.4 Dados pessoais e dados pessoais sensíveis: diferenciação e relevância prática

A partir da investigação nas mais diferentes legislações, tanto a aplicada em âmbito nacional, quanto as internacionais, é possível considerar os dados pessoais como aqueles que por meio de seu tratamento é possível relacioná-lo à uma pessoa natural, identificada ou identificável, conforme sintetizado no Quadro 1, a seguir:

Quadro 1 - Dados pessoais: definições em legislações

Dados Pessoais			
Definição	**Legislação**	**Origem**	**Ano**
Registro significa qualquer item, coleção ou agrupamento de informações referentes a educação, transações financeiras, histórico médico, criminal ou profissional, que contenha o nome de uma pessoa natural ou seu número de identificação, símbolo ou outro meio de identificação atribuído a um indivíduo (tradução nossa).	Privacy Act	Estados Unidos	1974
Informações que permitam, sob qualquer forma, direta ou indiretamente, a identificação das pessoas singulares a quem se aplicam, quer o tratamento seja efetuado por pessoa singular ou por pessoa jurídica (tradução nossa).	*La Loi Informatique et Libertés*	França	1978
Toda informação relacionada a um indivíduo identificado ou identificável.	Convenção 108	Europa	1981
Informação ou opinião sobre um indivíduo identificado, ou um indivíduo que seja razoavelmente identificável, seja a informação ou opinião verdadeira ou não; e se a informação ou opinião está registrada de forma relevante ou não	*Privacy Act*	Austrália	1988
Qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de	Diretiva 95/46/CE	Europa	1995

identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.			
Informações individualmente identificáveis sobre um indivíduo coletadas online, incluindo: nome e sobrenome; a casa ou outro endereço físico, incluindo o nome da rua e o nome de uma cidade ou vila; Informações de contato on-line; tela ou nome de usuário onde funciona da mesma maneira que as informações de contato on-line; Um número de telefone; Um número de Seguro Social; Um identificador persistente que pode ser usado para reconhecer um usuário ao longo do tempo e em diferentes sites ou serviços online. Tal identificador persistente inclui, mas não está limitado a, um número de cliente mantido em um cookie, um endereço de Protocolo de Internet (IP), um processador ou número de série do dispositivo ou identificador exclusivo do dispositivo; Uma fotografia, vídeo ou arquivo de áudio onde tal arquivo contém a imagem ou voz de uma criança; Informações de geolocalização suficientes para identificar o nome da rua e o nome de uma cidade ou vila; ou Informações sobre a criança ou os pais dessa criança que o operador coleta online da criança e combina com um identificador descrito nesta definição.	COPPA	Estados Unidos	1998
Informações de qualquer tipo referentes a pessoas com existência natural ou ideal, específicas ou determináveis.	*Ley de Protección de los Datos Personales*	Argentina	2000
Dados pessoais são quaisquer informações relativas a uma pessoa singular identificada ou que possa ser identificada, direta ou indiretamente, por referência a um número de identificação ou a um ou mais elementos que lhe sejam específicos. Para determinar se uma pessoa é identificável, é necessário considerar todos os meios para permitir sua identificação, disponíveis ou aos quais o controlador ou qualquer outra pessoa possa ter acesso (tradução nossa).	*La Loi Informatique et Libertés*	França	2004
Informação de qualquer tipo referida a uma pessoa física ou jurídica determinadas ou determináveis (tradução nossa).	*Protección de datos personales y acción de "habeas data"*	Uruguai	2008
Dados (e metadados) criados por e sobre as pessoas, abrangendo: dados oferecidos voluntariamente, como perfis em redes sociais); dados observados, como: dados de localização emitidos por celulares; e dados inferidos, como pontuação de crédito (tradução nossa).	Fórum Econômico Mundial (*World Economic Forum)*	Suíça (organismo internacional)	2011

Qualquer informação relacionada a uma pessoa natural identificada ou identificável (‘titular de dados); uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, por um identificador particular, como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos relacionados à natureza física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural (tradução nossa).	*General Data Protection Law* (GDPR)	Europa	2016
Informação relacionada a pessoa natural identificada ou identificável;	Lei Geral de Proteção de Dados Pessoais (LGPD)	Brasil	2018

Fonte: Elaborado pela autora.

Os dados pessoais sensíveis, por sua vez, compõe uma subcategoria de dados pessoais que possuem notório potencial lesivo a seus titulares, podendo causar-lhes discriminação, atraindo um regime jurídico mais protetivo ante os riscos que envolvem seu tratamento (Negri; Korkmaz, 2019). Assim, selecionou-se no Quadro 2 abaixo as definições trazidas pelas legislações protetivas de dados acerca dos conceitos de dado sensível.

Quadro 2 - Dados pessoais sensíveis: definições em legislações.

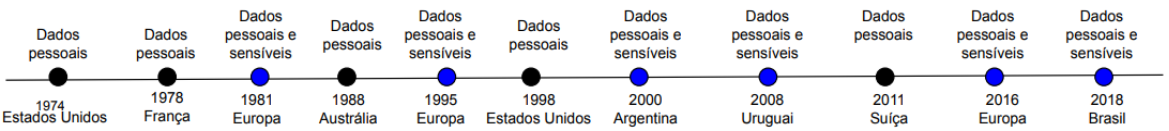
Dados pessoais sensíveis			
Definição	**Legislação**	**Origem**	**Ano**
O tratamento de: – dados genéticos; – dados pessoais relativos a infrações, processos penais e condenações e medidas de segurança conexas; – dados biométricos que identificam exclusivamente uma pessoa; – os dados pessoais pela informação que revelam relativos à origem racial ou étnica, opiniões políticas, filiação sindical, convicções religiosas ou outras, saúde ou vida sexual, só serão permitidos quando as garantias apropriadas estiverem consagradas na lei, complementando as da presente Convenção . 2. Essas salvaguardas devem prevenir os riscos que o tratamento de dados pessoais sensíveis possa representar para os interesses, direitos e liberdades fundamentais da pessoa em causa, nomeadamente o risco de discriminação (tradução nossa).	Convenção 108	Europa	1981
Dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação	Diretiva 95/46/CE	Europa	1995

Dados pessoais sensíveis			
sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.			
Dados pessoais que revelam origem racial e étnica, opiniões políticas, convicções religiosas, filosóficas ou morais, filiação sindical e informações sobre saúde ou vida sexual (tradução nossa)..	*Ley de Protección de los Datos Personales*	Argentina	2000
Dados que revelam a origem racial e étnica, preferência políticas, convicções religiosas ou morais, filiação sindical, bem como informações referentes à saúde ou à vida sexual (tradução nossa).	*Protección de datos personales y acción de "habeas data"*	Uruguai	2008
Dados que revelam raça ou origem étnica, opiniões políticas, religiosa ou filosófica, filiação sindical, dados genéticos, biometria, dados referentes à saúde ou referentes à vida ou orientação sexual. (tradução nossa).	*General Data Protection Law* (GDPR)	Europa	2016
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.	Lei Geral de Proteção de Dados Pessoais (LGPD)	Brasil	2018

Fonte: Elaborado pela autora.

Dessa forma, é possível compilar os quadros 1 e 2 na linha do tempo abaixo, em que mostra os países selecionados na presente pesquisa, o ano de sua legislação protetiva de dados, bem como quais delas trazem o conceito de dados pessoais sensíveis, senão vejamos:

Figura 4 - Linha do tempo das legislações protetivas de dados.



Fonte: Elaborado pela autora.

A partir das conceituações trazidas pelas legislações, é possível inferir que todo dado sensível é, em essência, um dado pessoal. Contudo, os dados pessoais sensíveis são capazes de gerar discriminação aos seus titulares e, por isso, estão relacionados, em geral, a 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.

Contudo, a classificação rígida desses dados pode deixar sem a devida proteção outros dados que também tem potencial discriminatório.

No caso dos dados “relacionados à vida sexual”, por exemplo, pode ser interpretado como "orientação sexual", ou seja, a "vida sexual" pode ser interpretada de forma restrititva como sendo apenas os aspectos centrais de como as pessoas experimentam o próprio sexo, excluindo a identidade de gênero do grupo de dados pessoais sensíveis, bem como das proteções inerentes a essa categoria (FICO *et al*, 2021). Assim, apesar da forma como as legislações propõe a definição de dados pessoais e dados pessoais sensíveis, podemos sintetizar no quadro 3 abaixo a diferença entre dados pessoais e dados pessoais sensíveis:

Quadro 3 - Diferenciação entre dados pessoais e sensíveis.

Dados pessoais	dados pessoais sensíveis
São dados que, independentemente da forma de tratamento, podem ser relacionados a uma pessoa natural identificada ou identificável, isto é, aquela que pode ser identificada a partir da combinação de um conjunto de dados.	São dados pessoais com potencial socialmente discriminatório, tais como, mas não se reduzindo a dados relativos à 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.

Fonte: Elaborado pela autora.

Tanto os dados pessoais quanto a subcategoria de dados pessoais sensíveis podem ser utilizados para identificar ou descrever um indivíduo, tendo por maior diferença o nível de sensibilidade e o grau de privacidade e segurança que exigem.

Acerca do tema, Daniel Solove (2008) entende que, caso os dados pessoais sensíveis sejam divulgados, causarão danos mais significativos, se comparado com os dados pessoais, em decorrência do seu potencial lesivo superior. Em geral, a divulgação do resultado de um exame de saúde (dado sensível de saúde), por exemplo, a terceiros não autorizados pode acarretar em exposição de usuário (que tem seu diagnóstico publicado sem sua vontade) do que um a divulgação de um CPF (dado pessoal).

O esclarecimento desses conceitos revela uma importante aplicabilidade prática. Em decorrência da notória potencialidade lesiva aos direitos fundamentais no tratamento de dados pessoais sensíveis, a própria LGPD (Brasil, 2018), em seu artigo 46, estabelece que a ANPD deverá estabelecer medidas de segurança,

técnicas e administrativas aptas mínimas a serem implementadas por agentes de tratamento, a fim de proteger os dados pessoais, sobretudo os sensíveis, de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

O conceito de dado adotado pela CI e o conceito adotado pelas legislações protetivas de dados podem ser aproximados e relacionados. As legislações, em geral, cometem imprecisão técnica ao alçar o conceito de dado como sendo uma informação e até mesmo trazendo os dois termos como sinônimos. Contudo, a presente pesquisa considera o dado como parte integrante da informação e não um sinônimo dela, uma vez que a informação é dotada de uma maior carga semântica (Santos; Sant'Ana, 2015).

O conceito de dado, na CI, é trazido, como vimos, a partir da tríade entidade, atributo e valor (e, a, v), em que o dado é uma unidade de conteúdo, relacionado a um contexto. Segundo Santos e Sant'Ana (2015) o conjunto mínimo de símbolos pode ser tomado como uma unidade de conteúdo, sendo necessário a identificação do contexto a que pertence.

> Como ilustração, pode-se pensar em um tipo documental de entidade livro <e> que contém o atributo título<a> que se instancia pelo valor "As Tecnologias da Inteligência"<v> como um elemento da entidade de um caso concreto. Ou ainda, exemplificando com a inclusão de outros atributos desta entidade, podemos considerar o caso deste livro<e> que tem como autor<a> "Pierre Lévy"<v>, com total de páginas<a> 204<v>, do qual se pode abstrair a seguinte estrutura:
> <e,a,v>
> <Livro,Título,As Tecnologias da Inteligência>
> <Livro,Autor,Pierre Lévy>
> <Livro,Página,204> (Santos; Sant'Ana, 2015, p. 205).

Nesse contexto, os dados pessoais, protegidos pelas legislações aqui estudadas que adotam uma visão expansionista, também podem ser percebidos a partir da tríade entidade, atributo e valor, vez que a partir do relacionamento estabelecido entre os elementos que compõem a tríade é possível identificar uma pessoa física, tornando o dado pessoal.

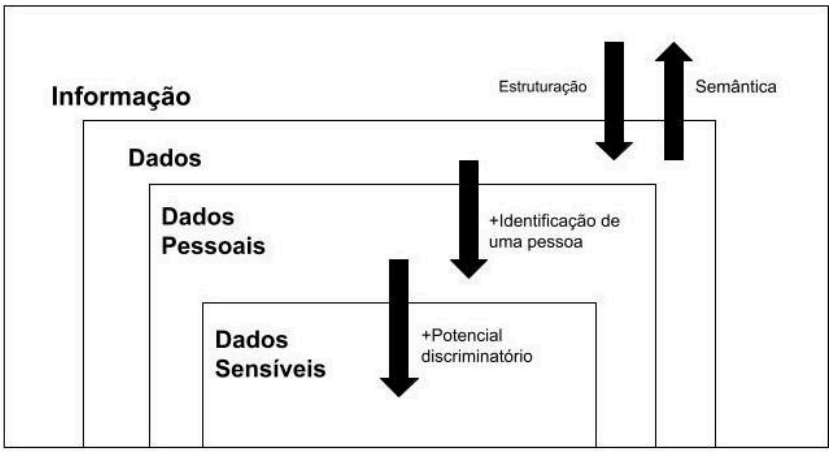
Assim, os dados, como parte integrante da informação, são estruturados por um esquema composto pela entidade e atributo (e,a), a partir de determinado contexto, tácito ou explícito, sendo identificados como dados por representarem a granularidade mais fina de um determinado contexto, completando a tríade com o

valor (v), (Santos; Sant'Ana, 2015) oportunidade em que uma pessoa física é identificada e o dado é alçado à categoria de dado pessoal.

Os dados pessoais sensíveis, por sua vez, são entendidos como uma subcategoria dos dados pessoais, mas em decorrência de uma interpretação, são capazes de causar maior dano lesivo aos usuários, em decorrência de seu potencial socialmente discriminatório, inerente a determinadas categorias de dados, como dados relacionados a raça, a saúde, religião, posicionamento político, dentre outros.

Assim, a figura 5, exposta a seguir, sintetiza a relação entre informação, dados, dados pessoais e dados pessoais sensíveis: a informação detém maior carga semântica, se comparada aos dados; os dados pessoais está dentro dos dados, por estarem relacionados a identificação de uma pessoa natural e os dados pessoais sensíveis, por sua vez, são uma subcategoria dentro de dados pessoais, que se destacam por seu maior potencial discriminatório. Senão vejamos:

Figura 5 - Relação entre informação e dados.



Fonte: Elaborado pela autora.

Helen Nissenbaum (2010) assevera que os dados de "acesso restrito", que incluem os dados pessoais sensíveis, exigem maiores proteções de privacidade, enquanto os dados de "acesso aberto", que incluem informações pessoais, geralmente, consideradas menos confidenciais não necessitam do mesmo nível de proteção.

2.5 A questão da privacidade e dados pessoais

A quebra da privacidade mostra-se na presente pesquisa como uma questão adjacente e não principal, uma vez que a transformação e o eventual

compartilhamento de dados sensíveis, sem a anuência do usuário acerca desse processo, pode ensejar na quebra de privacidade.

Assim, o estudo da quebra de privacidade relacionado aos casos em que dados pessoais são transformados em dados pessoais sensíveis deve ser objeto de trabalhos futuros, uma vez que o presente trabalho tem como objetivo geral um passo anterior, qual seja, verificar se existem indícios de como os dados pessoais, coletados por aplicações ou sítios eletrônicos, podem ser transformados em dados pessoais sensíveis, a partir da interferência do fator integração e não as consequências de eventual transformação.

A privacidade é um dos fatores que pode ser observado em todas as fases do CVD, sendo uma preocupação comum na maior parte das legislações mundiais (Doneda, 2021). As constituições, leis e normativas mundiais procuram proteger a privacidade dos seus cidadãos. A Declaração Universal dos Direitos Humanos das Nações Unidas de 1948, por exemplo, defende que “Ninguém sofrerá interferências arbitrárias em sua vida privada, família, lar ou correspondência, nem ataques à sua honra e reputação”. A Constituição Brasileira de 1988, em seu artigo 5º, também garante que “X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

O direito à privacidade não é sinônimo do direito à proteção de dados pessoais. Em que pese ambos estarem inseridos no âmbito dos direitos da personalidade, eles possuem diferenças, por exemplo, quanto à origem, objeto e esfera de proteção (Bioni, 2021). Trata-se o direito à privacidade da possibilidade de separar-se do ambiente público, dando ao indivíduo o direito de preservar sua identidade, não sendo obrigado a compartilhar determinadas informações, como pensamentos, sentimentos, ideias com o Estado (Autoridades) ou com terceiros que possam o coagir a agir de outra forma (Ferraz Junior, 1988). Nesse sentido, o direito à privacidade está relacionado à intimidade, à liberdade de decisão, à autonomia de cada indivíduo.

Assim, o direito à privacidade é uma liberdade negativa, uma vez que impõe-se um limite à interferência do Estado à vida privada do indivíduo. É gerado, ainda, ao indivíduo o poder de reivindicar ao Estado a proteção contra a violação deste direito, caso pertubado por terceiros ou por Autoridades (Ferraz Junior, 1988).

O direito à proteção de dados pessoais, a seu turno, é posterior ao direito à privacidade, por ser produto da Sociedade em Rede. A partir do surgimento de banco de dados e, consequentemente, o controle sobre dados e informações relacionados a indivíduos, nasce a preocupação acerca do uso responsável sobre dados, pois percebeu-se que os dados teriam o potencial de serem controlados e manipulados pelo Estados e pelo mercado (Doneda, 2021).

Nesse contexto, o direito à proteção de dados pessoais relaciona-se com a proteção na forma como os dados pessoais são tratados, visando manter a autodeterminação informativa desses indivíduos. Com efeito, o direito à proteção de dados compõe uma esfera positiva de proteção, pois é relacionado à atuação regulatória e fiscalizadora do Estado (Doneda, 2021).

Contudo, caso o direito à proteção de dados não seja devidamente respeitado, é possível que a privacidade do indivíduo seja quebrada, pois informações de sua esfera íntima, tornam-se públicas, sem a anuência ou conhecimento do indivíduo.

Daniel Solove, estudioso do tema privacidade, assevera que “A privacidade é um conceito muito complicado para ser resumido a uma única essência. As tentativas de encontrar tal essência muitas vezes acabam sendo muito amplas e vagas, com pouca utilidade para abordar questões concretas” (Solove, 2006, p. 485). Na tentativa de explicar a (quebra de) privacidade, o autor desenvolve a chamada Taxonomia da Privacidade (Solove, 2006), afirmando que a quebra de privacidade não ocorre a partir de um único critério.

O professor Daniel Solove (2008) atestou que quando iniciou seus estudos sobre o tema, procurou uma definição para o termo “privacidade”, mas quando se aprofundou na questão, não encontrou nenhum conceito satisfatório.

Nesse sentido, indaga-se: por que a definição de privacidade parece tão comum e ao mesmo tempo tão complexa? Ainda segundo Solove (2008), “[...] Freqüentemente, os problemas de privacidade são meramente declarados de forma instintiva. Não é raro ouvirmos ou até mesmo falarmos: “Isso viola minha privacidade!” (Solove, 2008, p. 7, tradução nossa). É comum, por exemplo, quando os pais entram no quarto dos filhos, sem bater à porta, ouvirem “vocês não respeitam minha privacidade”.

Assim, instintivamente, segundo Solove (2008), sabemos que certas situações são capazes de quebrar nossa privacidade, por exemplo: quando nossos

dados pessoais coletadas por empresas, sem nossa autorização ou no mínimo ciência, nós instintivamente sabemos que ali houve uma quebra de privacidade (Solove, 2008, p. 7). Mas como apresentar, tecnicamente, o conceito de privacidade?

O próprio Solove (2008) reflete que a “A privacidade parece abranger tudo e, portanto, parece não ser nada em si mesma" (Solove, 2008 p. 7) e, assim, o autor traz a percepção de que “O termo *privacidade* é um termo guarda-chuva, referindo-se a um grupo amplo e díspar de coisas relacionadas. O uso de um termo tão amplo é útil em alguns contextos, mas bastante inútil em outros” (Solove, 2006, p. 485, tradução nossa). Com efeito, são várias as situações que podem representar a quebra de privacidade e são trazidas como exemplo por Solove (2006), tais como:

> • Um jornal noticia o nome de uma vítima de estupro.
> • Repórteres conseguem entrar na casa de uma pessoa e secretamente fotografam e gravam a pessoa.
> • Novos dispositivos de raios-X podem ver através da roupa das pessoas, totalizando o que alguns chamam de “revista virtual”.
> • O governo usa um dispositivo de sensor térmico para detectar padrões de calor em a casa de uma pessoa.
> • Uma empresa comercializa uma lista de cinco milhões de mulheres idosas incontinentes.
> • Apesar de prometer não vender as informações pessoais de seus membros para outros, uma empresa faz isso de qualquer maneira (Solove, 2006, p. 481).

Warren e Brandeis (1890) foram os autores do artigo "*The right to Privacy*”, na *Harvard Law Review,* oportunidade em que os autores alertavam sobre as novas tecnologias, como a fotografia instantânea, que eram capazes de invadir os recintos sagrados da vida privada e doméstica, quando divulgadas na imprensa, por exemplo. Assim, a quebra de privacidade passou a ser vista também como um dano, mas incorpóreo e não físico, como até então os danos eram vistos. Eles notaram que a lei e normativas deveriam reconhecer os danos não-físicos, na mesma proporção em que se reconhecia os danos físicos.

No caso da privacidade, afirmaram os autores, envolve o “ferimento aos sentimentos”. A privacidade, portanto, está relacionada à proteção concedida a pensamentos, sentimentos e emoções, expressados por qualquer meio é uma das instâncias de aplicação do direito a estar só, do direito a ser deixado em paz, conforme defendido pela primeira vez pelo juiz Thomas Cooley, da Suprema Corte Norte Americana (1888).

Warren e Brandeis (1890) já argumentavam que ninguém tem o direito de publicar material sem o consentimento do titular interessado, independentemente do que seja. Assim, afirmaram que

> Nenhum outro tem o direito de publicar suas produções sob qualquer forma, sem o seu consentimento. Este direito é totalmente independente do material sobre o qual, ou os meios pelos quais, o pensamento, o sentimento ou a emoção são expressos (Warren; Brandeis, 1890, p. 99, tradução nossa)[17].

William Prosser (1960) também destinou parte de seus estudos à compreensão da privacidade. O autor defende que o direito à privacidade compreende quatro distintos tipos de quebra a diferentes interesses do indivíduo, os quais são reunidos por um mesmo nome (privacidade), mas que não têm quase nada em comum. Assim, cada um representa uma interferência contra o direito do demandante de ser deixado em paz. Estes quatro delitos foram descritos por Prosser (1960) como sendo: (1) intrusão na reclusão ou solidão, ou na sua vida privada (*intrusion*); (2) divulgação pública de fatos privados embaraçosos sobre o demandante (*public disclosure of private fact*s); (3) publicidade na qual o demandante é apresentado de modo equivocado para o público *(false light in the public eye*); e (4) apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (*apropriation*).

Alan Westin (1967), no mesmo sentido, identificou quatro estados básicos de privacidade individual: (1) solidão: indivíduo é separado do grupo e se encontra livre da observação ou interação com outras pessoas; (2) intimidade: a pessoa tem a opção de escolher com quem quer se relacionar de maneira reservada, íntima; (3) anonimato: o indivíduo se expressa publicamente (através de atos ou outra manifestação), porém, sua identidade permanece oculta; e (4) reserva ("a criação de uma barreira psicológica contra intrusão indesejada)".

Para Westin (1967), a privacidade está relacionada à alegação de indivíduos, grupos ou instituições para determinar por si mesmo quando, como e em que medida as informações sobre eles são comunicadas aos outros. Westin (1967) também apresentou sua preocupação com a preservação da privacidade diante das novas tecnologias de vigilância. Westin afirmava, contudo,

---

[17] No original, *"No other has the right to publish his productions in any form, without his consent. This right is wholly independent of the material on which, or the means by which, the thought, sentiment, or emotion is expressed".*

> O desejo do indivíduo por privacidade nunca é absoluto, uma vez que a participação em sociedade é igualmente importante. Assim, cada indivíduo está continuamente envolvido em um processo pessoal de equilíbrio entre o desejo de privacidade e o desejo de exposição e comunicação com os outros, à luz de condições do ambiente e de normas sociais na sociedade em que vive. O indivíduo o faz em face das pressões da curiosidade dos outros e dos processos de vigilância que toda sociedade necessita para a implementação de normas sociais (Westin 1967, p. 7).

Para Smitis (1987), a privacidade é um elemento constitutivo de uma sociedade civil; “as considerações de privacidade não surgem mais de problemas individuais específicos; ao contrário, eles expressam conflitos que afetam a todos” (Smitis , 1987, p. 135).

Nesse sentido, é necessário entender quem são os atores envolvidos nos processos de tratamento de dados pessoais e sensíveis, bem como os requisitos legais impostos para as operações relacionadas a cada uma das categorias, conforme apresentado na seção 3 a seguir.

3 OS ATORES E REQUISITOS LEGAIS ENVOLVIDOS NO TRATAMENTO DE DADOS PESSOAIS

A partir da promulgação das legislações de proteção de dados pessoais, requisitos foram exigidos aos atores envolvidos no processo de tratamento de dados pessoais e dados pessoais sensíveis. A presente seção busca identificar os atores e requisitos envolvidos nesse processo.

3.1 O tratamento de dados pessoais e os atores envolvidos

A LGPD, legislação brasileira responsável por regular o tratamento de dados pessoais e dados pessoais sensíveis, no Brasil, relaciona uma série de atividades que são tidas por tratamento de dados, tais como as previstas no artigo 5º, inciso X, senão vejamos:

> X- tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018).

A legislação europeia, por sua vez, em seu artigo 4º, relaciona como tratamento de dados pessoais:

> uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

Observa-se que os núcleos em questão são meramente exemplificativos, posto que a legislação trouxe como tratamento toda operação realizada com dados pessoais, trazendo de forma exemplificativa as ações que se seguiram (DONEDA, 2021).

Nesse sentido, os estudos de Sant'Ana (2016) e o conceito de Ciclo de Vida dos Dados (CVD) contribuem para o entendimento do caminho percorrido pelos dados pessoais coletados, armazenados, recuperados e, porventura, descartados, bem como visa reduzir a assimetria informacional entre detentores e usuários, uma vez que o tratamento de dados em larga escala pelos detentores e com o auxílio de

TIC pode ensejar no desconhecimento, por parte dos indivíduos, acerca dos fluxos de seus dados ante as camadas de abstração envolvidas nesse processo (Milagre, 2021).

O CVD possui as seguintes fases: coleta, armazenamento, recuperação e descarte. Nesse sentido, é possível relacionar os núcleos verbais dispostos, de forma exemplificativa, na legislação brasileira, com as fases do CVD, conforme adaptado de Milagre (2021), no Quadro 4, a seguir. Vejamos:

Quadro 4 - Comparativo das atividades de tratamento de dados pessoais e fases do Ciclo de Vida dos Dados

LGPD (art. 5º, X)	**CVD**
Coleta	Coleta
Recepção	
Produção	Recuperação
Classificação	
Utilização	
Acesso	
Reprodução	
Transmissão	
Distribuição	
Processamento	
Arquivamento	Armazenamento
Armazenamento	
Eliminação	Descarte
Avaliação	Recuperação
Controle	
Modificação	
Comunicação	
Transferência	
Difusão	
Extração	

Fonte: Adaptado de Milagre (2021).

Observa-se, assim, que mesmo havendo diversos núcleos verbais expostos na legislação brasileira, todos podem ser relacionados às fases do CVD. A fase de coleta, por exemplo, aborda também a recepção de dados pessoais pelos detentores. A fase de recuperação é a que possui maior variedade de núcleos verbais, tais como: utilização, acesso, processamento, transmissão, dentre outros.

A identificação de cada uma das fases que envolve o tratamento de dados pessoais auxilia a diminuir a assimetria informacional entre o usuário e os detentores dos dados pessoais, sendo papel da CI projetar recursos que seja aplicáveis pela computação, a fim de diminuir a distância entre usuários e os fluxos de seus dados pessoais, permitindo que eles alcancem a autodeterminação informativa (Milagre, 2021).

As operações de tratamento de dados pessoais e dados pessoais sensíveis são realizadas pelo que a LGPD denomina de agentes de tratamento, que são pessoas, naturais ou jurídicas, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Brasil, 2018). Na presente pesquisa, adota-se, contudo, o termo detentores para designar os agentes de tratamento, conforme Sant'Ana (2016) apresenta no CVD.

Os agentes de tratamento ou detentores são as entidades responsáveis pelo tratamento de dados pessoais, podendo ser divididos em duas categorias: operador e controlador (Brasil, 2018). Na UE, o GDPR adotou as nomenclaturas responsável pelo tratamento (controlador) e subcontratante (operador). O controlador de dados trata-se de "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", ou seja, é o detentor responsável pela tomada de decisões sobre o tratamento de dados, estabelecendo as diretrizes e finalidades ligadas ao tratamento de dados pessoais (Dias; Martins; Oliveira, 2022).

A LGPD reputa o operador como sendo a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador", nos termos do artigo 5º, inciso VII, da LGPD (Brasil, 2018). Em termos gerais, o operador pode ser identificado nas situações em que o controlador delega atividades-meio para terceiros, como empresas contratadas para realizar campanhas de publicidade e *marketing* (Dias; Martins; Oliveira, 2022). Em didático exemplo, Maldonado (2019) esclarece que:

> Por exemplo, se uma XPTO contrata outras diferentes entidades para enviar *e-mail marketing* de suas campanhas, dá instruções claras (conteúdo do material de *marketing*, destinatários, datas do envio etc.). Mesmo que as contratadas para executar tais tarefas tenham alguma autonomia para cumprir com o determinado (*software* que utilizarão, por exemplo), embora também possam oferecer consultoria (como o horário de maior abertura de *e-mail marketing*), estarão claramente vinculadas para agir de acordo com as determinações da empresa XPTO. Além disso, apenas a empresa XPTO tem o direito de utilizar os dados. **As outras entidades não podem tratá-los para qualquer outro propósito que não o determinado pela empresa XPTO**. Nesse caso, somente a empresa XPTO será a controladora, e as contratadas serão operadoras. No entanto, caso as empresas contratadas tomem a decisão – ilícita, diga-se de passagem – de utilizar os dados para outras finalidades, automaticamente elas também passam a ser controladoras, a partir desse momento (Maldonado, 2019, p. 109, grifo nosso).

A contratação de prestador de serviços, *de per si*, não provoca, automaticamente, a caracterização do contratado como operador de dados. A depender do grau de especialidade de determinado serviço ou atividade, é possível que o contratado, ante sua tamanha autonomia, seja conferido o papel de controlador e, consequentemente, a competência de tomar decisões para definir as finalidades do tratamento de dados (Dias; Martins; Oliveira, 2022). Assim, Marcel Leonardi (2019) faz importante ressalva

> [...] O simples fato de determinado agente estar tratando dados no escopo de uma prestação de serviços não significa, por si só, que ele se caracteriza como operador. Em outras palavras, como afirmado anteriormente, quem presta um serviço envolvendo o tratamento de dados pessoais a outra empresa ou entidade não necessariamente estará atuando como operador. O 'contratado' que prestará o serviço pode exercer o papel de controlador, dependendo do nível de controle exercido sobre a operação de tratamento de dados, em particular as decisões sobre as finalidades e os meios desse tratamento. A liberalidade garantida pelo controlador originário não pode ser confundida com fator determinante para a reconfiguração de um operador como controlador. O que definirá se determinado agente de tratamento será considerado controlador, concomitantemente ou não com outros, será a capacidade ou a obrigatoriedade de tomada de decisões acerca do tratamento dos dados, pelo menos de parte das etapas (Leonardi, 2019. p. 199).

A ANPD, em seu Guia Orientativo Para Definições Dos Agentes De Tratamento De Dados Pessoais e do Encarregado (ANPD, 2021) afirma que uma entidade, para ser considerada controlador de dados, basta que "[...] apenas que este mantenha sob sua influência e controle as principais decisões, isto é, aquelas relativas aos elementos essenciais para o cumprimento da finalidade do tratamento" (ANPD, 2021, p.11).

É necessário, ainda, esclarecer que as figuras do *controlador* e do *operador* não são estáticas e sim funcional. Nesse sentido, uma determinada entidade ‘X’ não será, por sua natureza, em toda e qualquer situação, controlador dos dados que detém, tampouco a entidade ‘Y’ também não será, por essência, sempre ‘operador’ (Dias; Martins; Oliveira, 2022).

As distinções entre os papéis de controlador e operador são importantes para a legislação brasileira para fins de responsabilidade e obrigações perante ao titular de dados e à própria ANPD. A LGPD designa mais obrigações ao controlador, posto ser ele quem define os elementos essenciais do tratamento de dados, tais como: a elaboração de relatório de impacto à proteção de dados pessoais e a nomeação de um encarregado pelo tratamento de dados pessoais para atuar como canal de comunicação entre o controlador, ANPD e titulares (Leonardi, 2019).

Assim, passa-se a dissertar acerca dos requisitos e diretrizes gerais exigidos, na LGPD, para que o tratamento de dados pessoais seja considerado lícito, isto é, destaca-se os mecanismos básicos que a legislação exige para que as operações que envolvam dados pessoais estejam de acordo com a lei, sob pena de sanções, a serem abordadas no item 3.3, a seguir.

3.2 Os princípios e as hipóteses de tratamento

Newton de Lucca (2015) esclarece que os princípios, derivado do latim *principium* (origem, começo), emanam orientações gerais, advindos das exigências de equidade, moralidade ou justiça. Nesse sentido, os princípios são normas fundamentais ou generalíssimas em um sistema, podendo ser entendidas como normas jurídicas que são determinantes de outra ou outras que lhe são subordinadas, que a pressupõem.

Para Dworkin (2002, p. 41), “um princípio [...] enuncia uma razão que conduz o argumento em uma certa direção”, ou seja, os princípios “inclinam a decisão em uma direção, embora de maneira não conclusiva”. Apesar de não possuírem definição legal, a doutrina jurídica entende os princípios como:

> [...] verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade. Às vezes também se denominam princípios certas proposições, que apesar de não serem evidentes ou resultantes de evidências, são assumidas como fundantes da validez de um sistema particular de

> conhecimentos, como seus pressupostos necessários (Reale, 1986, p 60).

Assim, os princípios jurídicos podem ser entendidos como mandamentos nucleares, pontos básicos e fundamentais de um sistema, são a base fundamental do ordenamento jurídico e atuam como critérios de direção na elaboração e aplicação das outras normas jurídicas (Silva, 2003).

O direito à proteção de dados possui princípios próprios. Em 1972, o Departamento de Saúde, Educação e Bem-estar Social dos EUA (1996) formulou princípios que visavam evitar abusos na utilização de dados pessoais por parte do Estado, os chamados *Fair Information Practice Principles* (FIPP), que são alicerces para as leis gerais de proteção de dados ao redor do mundo (Bioni, 2019), sendo eles:, Acesso e alteração; responsabilidade; competência; minimização; qualidade e integridade; participação individual; especificação de finalidade e limitação de uso; segurança e transparência[18].

A Organização para a Cooperação de Desenvolvimento Socioeconômico (OCDE) e o Conselho da Europa, na década de 80, também formularam diretrizes para privacidade e a Convenção Internacional de Proteção de Dados Pessoais, ambos documentos baseados nos FIPP, quais sejam, Princípio de Limitação de Coleta, Princípio de Qualidade de Dados, Princípio de Especificação de Propósito, Princípio de Limitação de Uso, Princípio de Salvaguardas de Segurança, Princípio de Abertura, Princípio de Participação Individual e Princípio de Responsabilidade[19].

Assim, passou a haver um alto nível de convergência dos princípios sobre proteção de dados pessoais em todo o mundo (Bioni, 2019). O GDPR (2018) adotou semelhantes princípios em sua legislação, senão vejamos:

> Artigo 5.o Princípios relativos ao tratamento de dados pessoais
> 1. Os dados pessoais são:
> a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as

[18] U.S. department of health, education and welfare. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: https://www.fpc.gov/resources/fipps/. Acesso em: 08 out. 2023.
[19] ORGANIZATION For Economic Cooperation And Development (OECD). OECD Privacy Framework, 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

> finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»);
> c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);
> d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);
> e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, nº 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);
> f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);
> 2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no nº 1 e tem de poder comprová-lo («responsabilidade»).

No Brasil, a LGPD (Brasil, 2018) trouxe como princípios semelhantes aos europeus, sendo os seguintes mandamentos alçados à condição de princípios e expressos no artigo 6º da legislação em comento:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boafé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações

> acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O estudo dos princípios é relevante à presente pesquisa, uma vez que o tratamento de dados pessoais, em qualquer fase do CVD, deve observar a aplicação dos princípios expressos na legislação, aprimorando a governança dos dados pessoais e sensíveis, sob responsabilidade do detentor. A governança de dados tem por escopo estabelecer e efetivar estratégias no tratamento de dados, a partir da implementação de políticas, normas, padrões, processos e métricas, aprimorando a eficiência dos processos (Brandt; Vidotti, 2019).

A Escola Nacional de Administração Pública - ENAP (ENAP, 2019) esclarece que “As atividades de governança ajudam a controlar o desenvolvimento de dados e reduzem os riscos associados ao seu uso, ao mesmo tempo em que permitem que uma organização aproveite-os estrategicamente” (ENAP, 2019, p.7). O Código de Melhores Práticas do Instituto Brasileiro de Governança Corporativa (2015, p. 20) define a governança como sendo:

> [...] o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.

Os primeiros princípios expressos nos três primeiros incisos da lei, quais sejam, finalidade, adequação e necessidade, parecem ser complementares entre si, bem como de aplicação prática concomitante. No contexto dos dados pessoais, a aplicação do princípio da finalidade, expresso no inciso I, contribui para que o detentor selecione apenas os dados que tenham razão de ser, isto é, utilidade de fato para a instituição, evitando a aglomeração de dados e a consequente formação de robustos bancos de dados.

Nesse sentido, Ghisleni (2022, p. 110) explica que “Como reflexo desse princípio, concebe-se uma limitação imposta à atuação do controlador, permitindo o tratamento de dados em proporção limitada àquele propósito que foi informado”. Dessa forma, cabe ao detentor que, desde a fase de coleta, selecionar os dados relacionados a um propósito específico e anteriormente proposto.

O princípio da adequação, por sua vez, expresso no inciso II, ensina a verificar a compatibilidade dos dados coletados com a finalidade proposta e informada ao titular. Assim, estabelecidas as finalidades de coleta dos metadados de negócio, caberá ao gestor coletar dados coerentes com os propósitos propostos, de acordo com o contexto (Ghisleni, 2022).

A aplicação do princípio da necessidade (inciso III) auxilia ao detentor a limitar o tratamento dos dados pessoais e dados pessoais sensíveis estritamente necessários e proporcionais para alcançar as finalidades propostas, ou seja, o detentor deve realizar a coleta dos dados pessoais e dados pessoais sensíveis imprescindíveis aos propósitos elencados, nem mais, nem menos. Percebe-se, portanto, que caberá ao detentor conhecer e estabelecer os propósitos do tratamento de dados, bem como coletar somente aqueles que sejam coerentes e imprescindíveis aos objetivos delimitados.

O princípio do livre acesso, expresso no inciso IV, também contribui para a governança de dados pessoais e dados pessoais sensíveis, haja vista que é necessário efetivar o armazenamento dos dados pessoais de forma estruturada, a fim de garantir a consulta facilitada aos titulares que tenham interesse em conhecer qual a forma e duração de tratamento de seus dados pessoais.

A qualidade dos dados (inciso V) também foi elencada como princípio na LGPD e pode contribuir para gestão de dados pessoais e dados pessoais sensíveis, posto que o detentor deve garantir que os dados tratados estejam constantemente atualizados e exatos.

Considerando que o escopo da LGPD, expresso em seu artigo 1º é “(...) proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Brasil, 2018), o princípio da da transparência, conceituado no inciso VI do artigo 6º, da LGPD, é de observância obrigatória para o detentor de dados pessoais e dados sensíveis, posto que passará a ser sua função garantir que o titular tenha ciência do tratamento de seus dados pessoais por determinada instituição.

Além disso, os dados pessoais e dados sensíveis deverão estar estruturados para que o titular seja capaz de compreender quais dados estão sendo tratados, para quais finalidades, por quais agentes de tratamento e por quanto tempo, sendo evitado o tratamento de dados forma discriminatória ou abusiva, conforme inteligência do inciso IX, do artigo 6º, da LGPD.

Outrossim, a partir dos princípios da segurança e prevenção, descritos nos incisos VII e VIII, do artigo 6º, da LGPD, respectivamente, caberá ao detentor resguardar os dados que estão sob sua guarda, fase de armazenamento, a partir de medidas técnicas e administrativas capazes de protegê-los de eventuais incidentes e, sobretudo, evitá-los, isto é, os eventos que comprometam a confidencialidade, integridade e disponibilidade dos dados de negócio deverão ser prevenidos.

Dessa forma, é notório o interesse do detentor em adotar mecanismos que antevejam os danos causados por incidente de segurança e proporcionem uma maior proteção ao titular de dados (Flumignan; Flumignan, 2020).

O princípio da responsabilização e prestação de contas, por fim, auxilia o detentor em preocupar-se com a capacidade de demonstrar a adoção de medidas técnicas eficazes em proteger os dados pessoais e dados pessoais sensíveis às autoridades, quando necessário. Assim, Teixeira e Armelin (2020) alertam que:

> [...] não basta o agente ter cumprido todas as regras e determinações legais, é preciso que ele a todo tempo registre que cumpriu a lei, utilizando-se das mais diversas formas para que consiga comprovar o atendimento aos preceitos da lei caso algum incidente ocorra. É de se mencionar a obrigatoriedade da prestação de contas por parte do agente até mesmo quando não houver qualquer descumprimento ou irregularidade.

Dessa forma, percebe-se que a aplicação dos princípios da LGPD contribuem sobremaneira a governança de dados pessoais e dados pessoais sensíveis e o descumprimento dos princípios pode ensejar em sanções, pois o cumprimento dos princípios.

Além disso, a LGPD também propôs um rol taxativo de hipóteses legais que autorizam o tratamento de dados pessoais e dados pessoais sensíveis, isto é, a legislação entende que as operações de tratamento tornam-se legítimas, caso a operação se encaixe em, pelo menos, uma das hipóteses legais de tratamento arroladas, devendo essas hipóteses serem cumpridas junto aos princípios ora debatidos (Lima, 2019).

Nesse sentido, tanto o legislador brasileiro, quanto o legislador europeu, apresentam duas possibilidades: i. o enquadramento legal de dados pessoais e suas respectivas bases legais, expostas no artigo 7º, da LGPD e no artigo 6º, da GDPR; ii. enquadramento legal de dados pessoais sensíveis e suas respectivas bases legais, expostas no artigo 11, da LGPD e no artigo 9º da GDPR, conforme exposto no Quadro 5, a seguir:

Quadro 5 - Hipóteses legais expostas da LGPD e no GDPR.

Hipóteses legais - LGPD		**Hipóteses legais - GDPR**	
Dados pessoais LGPD (art. 7º)	**Dados sensíveis LGPD (art. 11)**	**Dados pessoais GDPR (art. 6º)**	**Dados sensíveis GDPR (art. 9)**
Consentimento	Consentimento	Consentimento	Consentimento
Cumprimento de obrigação legal ou regulatória	Cumprimento de obrigação legal ou regulatória	Execução de Contrato	Cumprimento de obrigação legal e do exercício de direitos específicos do titular ou do detentor
Execução de políticas públicas	Execução de políticas públicas	Cumprimento de obrigação legal	Defesa de interesses vitais de pessoas físicas
Estudos por órgão de pesquisa	Estudos por órgão de pesquisa	Defesa de interesses vitais de pessoas físicas	No âmbito das suas atividades legítimas (ex. sindicato, igrejas)
Execução de contrato	Exercício regular de direitos	Funções de interesse público ou ao exercício da autoridade pública	Dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular
Exercício regular de direitos	Proteção da vida	Legítimo Interesse	Exercício ou à defesa de um direito num processo judicial
Proteção da vida	Tutela da saúde	-	Interesse público importante
Tutela da saúde	Prevenção à fraude	-	Para fins médicos
Legítimo Interesse	-	-	Interesse público no domínio da saúde pública
Proteção do crédito	-	-	Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para

			fins estatísticos

Fonte: Elaborado pela autora.

Assim, tanto o legislador europeu (GDPR, 2016), quanto o legislador brasileiro (Brasil, 2018) preveem uma série de situações que tornam o tratamento de dados lícito, se também respeitadas as demais exigências legais, como os princípios. Para o tratamento de dados pessoais, em comum, ambas as legislações preveem o tratamento de dados para fins consentimento, cumprimento de obrigação legal, execução de contrato, proteção da vida (defesa de interesses vitais, na Europa), e execução de políticas públicas (Funções de interesse público ou ao exercício da autoridade pública) e legítimo interesse, não sendo mencionados na legislação europeia para o tratamento de dados pessoais a tutela da saúde, estudos por órgão de pesquisa, exercício regular de direitos e proteção ao crédito.

Para o tratamento de dados pessoais sensíveis, por sua vez, são comuns as seguintes bases legais: consentimento, cumprimento de obrigação legal, tutela da saúde (fins médicos, na Europa), exercício regular de direitos (exercício ou defesa de um direito em processo judicial, na Europa), estudos por órgão de pesquisa (Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, na Europa) e proteção da vida (defesa de interesses vitais, na Europa).

Na legislação europeia percebe-se que as seguintes hipóteses não foram mencionadas na LGPD: No âmbito das suas atividades legítimas (ex. sindicato, igrejas), Dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular, interesse público importante e Interesse público no domínio da saúde pública, enquanto a LGPD trouxe a possibilidade de tratamento de dados para fins de prevenção à fraude, que não é expressamente prevista na legislação Europeia.

Com efeito, tanto a LGPD, quanto a GDPR prevêem possibilidades para o tratamento de dados pessoais e dados pessoais sensíveis, além do consentimento do titular dos dados (Milagre, 2021). No entanto, em que pese o consentimento do titular não ser necessário em todo e qualquer tipo de operação de tratamento, é imprescindível que o princípio da transparência seja cumprido, isto é, os detentores devem ser capazes de prestar informações claras, precisas e facilmente acessíveis sobre a realização do tratamento que estão realizando (Bioni, 2019).

Como debatido na seção 2, os dados pessoais sensíveis, por estarem associados às características basilares do indivíduo, são aptos a gerar situações de discriminação, tanto por parte de particulares, quanto por parte do Estado, podendo haver violações de direitos fundamentais (Rodotà, 2008).

Assim, ante os riscos associados ao tratamento de dados pessoais sensíveis, percebe-se que tanto a legislação brasileira, quanto a europeia estabeleceram um regime jurídico diferenciado, com hipóteses legais de tratamento próprias e diferentes das situações previstas para o tratamento de dados pessoais (Mulholland, 2018).

Destaca-se que um rol mais restrito de hipóteses autorizativas é prevista para o tratamento de dados pessoais sensíveis, não sendo permitido o tratamento de pessoais sensíveis para fins de legítimo interesse, proteção ao crédito ou para fins contratuais, por exemplo (Negri; Korkmaz, 2019).

Observa-se que as hipóteses de tratamento que autorizam o tratamento de dados pessoais sensíveis são voltadas, em geral, para interesses mais coletivos, como o cumprimento de obrigações legais, efetivação de direitos, interesse público, proteger a vida do titular ou de terceiros ou, no caso expresso pelo GDPR, é possível o tratamento de dados pessoais sensíveis, caso o próprio titular tenha tornado aquele dado público, não sendo desvirtuada a finalidade.

Nesse sentido, Mulholland, a respeito dos dados pessoais sensíveis, alerta que “deve-se visar a um tratamento limitado desses dados, para evitar o seu eventual uso para propósitos que não atendam aos fundamentos republicanos do Estado Democrático de Direito” (Mulholland, 2018, p. 163).

A LGPD estabelece, ainda, a necessidade do detentor estabelecer padrões técnicos voltados à natureza dos dados pessoais tratados, visando adotar medidas de segurança, técnicas e administrativas, para prevenir acessos não autorizados e situações acidentais ou ilícitas, conforme estabelecido no artigo 46, parágrafo 1º (Negri; Korkmaz, 2019). Negri e Korkmaz (2019) afirma que

> Em síntese, é possível identificar um *standard* de proteção mais rigoroso para os dados pessoais sensíveis em razão da sua natureza. É relevante considerar que a normatividade das regras jurídicas, enquanto geradoras de práticas protetivas, pode avançar para outras esferas, inclusive a interna dos controladores e operadores de tratamento de dados, como é caso, por exemplo, das práticas de compliance e dos conceitos de *privacy by design* e *privacy by default*, em que a proteção de dados é pensada desde a

> concepção das operações, de forma estrutural, bem como estabelecendo-se um padrão de alto nível de proteção (Negri; Korkmaz, 2019, p.75).

Contudo, o avanço da tecnologia permite que um dado que, em tese, não pertença à subcategoria de dados pessoais sensíveis em sua gênese, a partir do cruzamento ou correlação de dados pode ser transmudado para dado sensível (Bioni, 2020).

3.3 As autoridades de proteção de dados pessoais

Conforme abordado na seção 2, as legislações voltadas à proteção de dados pessoais, na União Europeia, são datadas desde a década de 1970, observando uma constante consolidação de normas protetivas de dados pessoais em todo o mundo.

Em 2022, segundo um levantamento feito pelo *World Privacy Assembly* 2022, dos 193 (cento e noventa e três) Estados-Membros da ONU, 128 (cento e vinte e oito) já adotaram leis protetivas de dados pessoais, o que corresponde a dois terços do total. Nesse sentido, apurou-se que cerca de 57% (cinquenta e sete por cento) da população e entidades mundiais está submetida à jurisdição que possui normas de proteção de dados.

Visando a efetivação das normas impostas pelas legislações protetivas de dados, é possível que as próprias normas prevejam a criação de Autoridades Nacionais (autoridades de controlo, na UE) de proteção de dados. As autoridades são estruturas administrativas governamentais que representam entidades de controle responsáveis, sobretudo, por zelar e fiscalizar o cumprimento das diretrizes e obrigações impostas pelas leis de proteção de dados pessoais, sendo, portanto, elementos-chave das estratégias regulatórias para a efetivação das normas de proteção de dados. Francesco Caringella e Roberto Garofoli (2000) explicam que as Autoridades Nacionais são

> entes ou órgãos públicos dotados de substancial independência do governo, caracterizados pela sua autonomia de organização, financiamento e contabilidade; da falta de controle e sujeição ao poder Executivo, dotadas de garantias de autonomia através da nomeação de seus membros, dos requisitos para esta nomeação e da duração de seus mandatos; e tendo função de tutela de interesses constitucionais em campos socialmente relevantes (Carimgella; Garofoli, 2000, p. 10).

As Autoridades Nacionais possuem, entre suas principais funções, as de “ouvidores (*ombudsman*), auditores, consultores, educadores, orientadores de política pública e negociadores” (Mendes, 2014, P. 49). Bennett e Raab esclarecem que:

> A existência de autoridades supervisoras robustas tem sido considerada como condição *sine qua non* para a adequada proteção à privacidade, pois as leis não são auto implementáveis e a cultura da privacidade não pode se estabelecer sem uma autoridade que a patrocine (Bennett; Raab, 2014, p. 49).

A criação de autoridades dessa natureza mostra-se um mecanismo habitualmente utilizado pelas legislações de protetivas de dados pessoais. Segundo Greenleaf (2019), 90% (noventa por cento) dos países que possuem leis de proteção de dados, promoveram a criação de autoridades estatais especializadas em proteção de dados pessoais, garantido o *enforcement* da legislação. Para Danilo Doneda (2019), as autoridades de proteção de dados representam um papel fundamental na tutela do direito à proteção de dados pessoais, sendo

> [...] parte fundamental da estrutura administrativa e jurídica estatal, realizando a aproximação entre as esferas do Estado, do mercado e da pessoa em contextos por demais complexos e especializados para serem efetivamente regulados pelas instituições tradicionais (Doneda, 2019, p. 387).

Contudo, é importante ressaltar que as Autoridades de Proteção não possuem uma estrutura ou forma de atuação única. Em 2017, o censo de Autoridades de Proteção de Dados Pessoais, realizado pelo *International Conference of Data Protection & Privacy Commissioners - ICDPPC* apontava para uma diversidade de estrutura e funcionamento entre as autoridades mundiais. Dentre essas diversidades, por exemplo, está relacionada à escolha de um comissário único ou a criação de uma autoridade colegiada (Lloyd, 2011).

Além disso, o censo apontou diferenças em outros elementos estruturantes, como: estrutura decisória, forma de nomeação dos dirigentes, disponibilidade de recursos financeiros, corpo de membros, dentre outras (Wimmer, 2020). É possível, ainda, verificar diferenças nas competências legais atribuídas a essas instituições: i. atividades de *advocacy*; ii. atividades de repressão de infrações e aplicação de sanções. Contudo, é possível que o mesmo órgão acumule uma caráter híbrido, isto é, assuma tanto a competência de regulação do ambiente institucional, a partir de competências normativas e da defesa de direitos (*advocacy*), quanto a aplicação de

normas e repressão de infrações, seja por meio de *enforcement* ou por mediação (Wimmer, 2020).

Ressalta-se que as autoridades em questão possuem suas particularidades, conforme o contexto social, político e jurídico nas quais estão inseridas. Reidenberg (1999) destaca que as diferenças e semelhanças encontradas entre países, no que tange às normas protetivas de dados pessoais, são reflexo das escolhas políticas, do regime de governo, do mercado e da sociedade, ensejando em diferentes interpretações e formas de implementação, sendo esse estudo comparativo enriquecedor. Nesse sentido, Wimmer (2020) salienta que

> Tais reflexões são úteis para que possa compreender as profundas variações encontradas não apenas na estrutura e no tamanho das autoridades de proteção de dados em diferentes países do mundo, mas também para justificar as significativas divergências quanto à própria concepção sobre a finalidade de tais estruturas e seu modo de atuação, assim como os desafios existentes em termos de harmonização e interoperabilidade de marcos jurídicos (Wimmer, 2020).

Norberto Bobbio (2014) alerta que o legislador pode esperar a transgressão das disposições previstas em leis e atos normativos, em um ordenamento jurídico, posto que a norma é um “dever ser” e não expressa, necessariamente, a realidade como é. Assim, visando evitar condutas transgressoras, é imprescindível a criação de um mecanismo que elimine ou atenue os efeitos danosos da violação. Esse mecanismo é a chamada sanção, isto é, a penalidade ou recompensa atrelada à violação ou execução de uma lei. As leis de proteção de dados, nesse sentido, possuem sanções previstas, em caso de descumprimento, havendo variações por legislação. Em geral, as sanções previstas são advertência, multas, proibição de tratar dados pessoais, dentre outras.

A presente seção, a seguir, busca descrever um breve panorama das autoridades de proteção de dados europeias e latino americanas, evidenciando suas funções e formas de atuação, bem como as características em comum dessas entidades administrativas governamentais. A importância dessa seção está relacionada à seção 7, que visa apurar sanções impostas pelas autoridades de proteção de dados da UE, entre os anos de 2019-2023, relacionando-se o objetivo da presente pesquisa, qual seja, o de investigar como os dados pessoais, coletados por aplicações e sítios eletrônicos, podem ser transformados em dados pessoais sensíveis.

3.3.1 As autoridades europeias de proteção de dados

Na Europa, em 28 de janeiro de 1981, foi criado o primeiro instrumento internacional juridicamente vinculativo, isto é, o primeiro e, ainda, único tratado internacional referente à proteção de dados pessoais, a Convenção Convenção 108 do Conselho da Europa. O documento foi ratificado pelos Estados-Membros da UE e visa garantir “a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal”.

Ainda em solo europeu, em meados dos anos de 1990, foi aprovada a primeira norma da Comissão Europeia, a chamada Diretiva 95/46, de 24 de outubro de 1995, a qual instituiu a obrigatoriedade da criação de autoridades em proteção de dados independentes aos membros da União Europeia, estabelecendo de forma detalhada as funções, competências e responsabilidades dessas instituições.

A Diretiva era aplicável aos então 28 (vinte e oito) Estados-Membros da UE, bem como aos membros do Espaço Econômico Europeu (EEE): Islândia, Listenstaine e Noruega e também determinou critérios e padrões de transferência internacional de dados.

Hijmans (2016) destaca que o fluxo de dados pessoais foi o contexto que tornou necessário a necessidade de uniformização das normas europeias, harmonizando as práticas recorrentes em cada Estado-membro. Todavia, por ter natureza de Diretiva e não de Regulamento, a transposição da exigência de criação de autoridades de proteção de dados ficou a cargo dos Estados-membros da União Europeia. Contudo, como o tema da proteção de dados pessoais, enquanto política pública, já datava da década de 1970 (período a partir do qual percebe-se a promulgação de legislações atinentes à proteção de dados pessoais), quando foi instituída a obrigatoriedade da criação, muitos países já possuíam suas próprias autoridade devidamente instituídas e em funcionamento (Hijmans, 2016).

Em 2000, a Carta de Direitos Fundamentais garantiu a instituição de Autoridades Nacionais independentes, enfatizando o papel fiscalizador dessa identidades:

> Artigo 8. Proteção de dados pessoais :1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas

> têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. **3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente**. (grifo nosso)

Nesse contexto, foi necessário a criação de um Regulamento, instrumento jurídico que torna imediatamente vinculante todos os Estados-Membros da UE, trazendo maior harmonia e uniformidade ao sistema. Em 2016, foi aprovado o Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* - GDPR), que entrou em vigor em maio de 2018 e trouxe o capítulo 6 dedicado às características e funções das autoridades de proteção de dados europeias.

Nos termos da legislação em comento, cabe a cada Estados-Membros da UE estabelecer uma ou mais autoridades públicas independentes, as chamadas autoridades de controle, a quem são atribuídas a responsabilidade pela fiscalização da aplicação do GDPR, bem como as seguintes funções, em seus respectivos territórios:

> a) Controla e executa a aplicação do presente regulamento;
> b) Promove a sensibilização e a compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser alvo de uma atenção especial;
> c) Aconselha, em conformidade com o direito do Estado-Membro, o Parlamento nacional, o Governo e outras instituições e organismos a respeito das medidas legislativas e administrativas relacionadas com a defesa dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento;
> d) Promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento;
> e) Se lhe for solicitado, presta informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, coopera com as autoridades de controlo de outros Estados-Membros para esse efeito;
> f) Trata as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80.o, e investigar, na medida do necessário, o conteúdo da reclamação e informar o autor da reclamação do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo;
> g) Coopera, incluindo partilhando informações e prestando assistência mútua a outras autoridades de controlo, tendo em vista assegurar a coerência da aplicação e da execução do presente regulamento;

> **h) Conduz investigações sobre a aplicação do presente regulamento, incluindo com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública;**
> i) Acompanha factos novos relevantes, na medida em que tenham incidência na proteção de dados pessoais, nomeadamente a evolução a nível das tecnologias da informação e das comunicações e das práticas comerciais;
> j) Adota as cláusulas contratuais-tipo previstas no artigo 28.o, n.o 8, e no artigo 46.o, n.o 2, alínea d);
> k) Elabora e conserva uma lista associada à exigência de realizar uma avaliação do impacto sobre a proteção de dados, nos termos do artigo 35.o, n.o 4;
> l) Dá orientações sobre as operações de tratamento previstas no artigo 36.o, n.o 2;
> m) Incentiva a elaboração de códigos de conduta nos termos do artigo 40.o, n.o 1, dá parecer sobre eles e aprova os que preveem garantias suficientes, nos termos do artigo 40.o, n.o 5;
> n) Incentiva o estabelecimento de procedimentos de certificação de proteção de dados, e de selos e marcas de proteção de dados, nos termos do artigo 42.o, n.o 1, e aprova os critérios de certificação nos termos do artigo 42.o, n.o 5;
> o) Se necessário, procede a uma revisão periódica das certificações emitidas, nos termos do artigo 42.o, n.o 7;
> p) Redige e publica os critérios de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.o e de um organismo de certificação nos termos do artigo 43.o;
> q) Conduz o processo de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.o e de um organismo de certificação nos termos do artigo 43.o;
> r) Autoriza as cláusulas contratuais e disposições previstas no artigo 46.o, n.o 3;
> s) Aprova as regras vinculativas aplicáveis às empresas nos termos do artigo 47.o;
> t) Contribui para as atividades do Comité; u) Conserva registos internos de violações do presente regulamento e das medidas tomadas nos termos do artigo 58.o, n.o 2; e v) Desempenha quaisquer outras tarefas relacionadas com a proteção de dados pessoais.

A legislação prevê, ainda, penas pecuniárias, em caso de descumprimento ou violação das normas previstas. As sanções mais elevadas chegam ao montante de até 20.000.000 EUR (vinte milhões de euros) ou, no caso de uma empresa, até 4% (quatro por cento) do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

Os mecanismos de aplicação das sanções pecuniárias também são devidamente dispostos no GDPR, sendo levados em consideração: a natureza, a gravidade e a duração da infração; o número de titulares de dados afetados; o nível de danos por eles sofridos; o caráter intencional ou negligente da infração; as

medidas tomadas para atenuar os danos sofridos pelos titulares; o grau de responsabilidade, levando em consideração as medidas técnicas ou organizativas por eles implementadas; grau de cooperação com as autoridades; as categorias específicas de dados pessoais afetadas pela infração; dentre outros critérios.

Destaca-se que antes da aprovação e vigência do GDPR, as Autoridades Nacionais de proteção de dados possuíam grandes diferenças não apenas na interpretação da Diretiva 95/46, mas também com relação à estrutura, postura e comportamento adotados (Jóri, 2015). Nesse sentido, o GDPR mostrou-se um relevante instrumento de promoção da uniformização de padrões e práticas, no que tange à aplicação da proteção de dados pessoais (Wimmer, 2020).

3.3.2 As autoridades de proteção de dados na américa latina

Na América Latina, o surgimento e consolidação das autoridades responsáveis pela proteção de dados é comumente relacionada ao Direito Europeu. Segundo Wimmer (2020), os sistemas jurídicos da América Latina, à semelhança do sistema jurídico europeu, preocupam-se com a questão da privacidade e da vida privada, incorporando-a às Constituições nacionais e, mais recentemente, consolidam o direito à proteção de dados pessoais.

Dos 12 (doze) países que constituem a América do Sul, por exemplo, Argentina, Chile, Colômbia, Peru, Uruguai, Paraguai, Guiana Francesa [20] e Brasil possuem leis gerais para a proteção dos dados. Apesar de não possuírem leis gerais, Equador[21], Bolívia[22], Venezuela[23] e Guiana[24] possuem leis setoriais sobre proteção de dados. O Suriname, por sua vez, é o único país do continente que ainda não possui leis sobre o tema.

---

[20] Disponível em: BATISTA LUZ ADVOGADOS. Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos. Disponível em: en.baptistaluz.com.br. Acesso em: 20 de set. 2023.
[21] Disponível em: OEA. Desarrollos Normativos por País – Equador. Disponível em: http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn_ecuador.asp. Acesso em: 20 de set. 2023.
[22]Disponível em: RED IBEROAMERICANA DE PROTECCION DE DATOS. Legislación-Bolívia. Disponível em http://www.redipd.org/legislacion/bolivia-ides-idphp.php. . Acesso em: 20 de set. 2023.
[23] Disponível em: RED IBEROAMERICANA DE PROTECCION DE DATOS. Legislación-Venezuela. Disponível em: http://www.redipd.org/legislacion/venezuela-ides-idphp.php. Acesso em: 20 de set. 2023.
[24] Disponível em: A Guiana possui leis setoriais de proteção de dados como o Statistics Act 1965 e o Access to Information Act 2011. BATISTA LUZ ADVOGADOS. Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos. Disponível em: en.baptistaluz.com.br. Acesso em: 20 de set. 2023.

Países como a Argentina e o Uruguai, por exemplo, são considerados, pela Comissão Europeia, como detentores de níveis adequados de proteção de dados pessoais, o que evidencia uma maturidade de ambos. Contudo, Lehuedé (2019) ressalta que uma característica peculiar às leis da América Latina é relacionar normas de transparência com leis voltadas à proteção de dados. Países como México, Peru, Uruguai e Argentina designam os órgãos como responsáveis por assegurar a transparência e o acesso à informação, o que pode ensejar em consequências, como a ênfase com a qual a autoridade irá destinar seus trabalhos, podendo gerar conflitos entre privacidade e transparência (Lehuedé, 2019).

3.3.2.1 A Autoridade Nacional de Proteção de Dados brasileira

A Autoridade Nacional de Proteção de Dados brasileira (ANPD) está disposta na LGPD, sendo criada pela Medida Provisória nº 869, de 2018, convertida na Lei nº 13.853, de 08 de julho de 2019, passando a funcionar efetivamente a partir da nomeação de seu primeiro Diretor-Presidente, em 05 de novembro de 2020.

A ANPD é o órgão central de interpretação da LGPD, dotada de autonomia técnico-decisória, possuindo patrimônio próprio e, ainda, sendo responsável por zelar pela proteção dos dados pessoais, bem como por orientar, regulamentar e fiscalizar o cumprimento da LGPD, no Brasil.

As competências da ANPD estão descritas na LGPD e, conforme estabelecido no art. 55-J, cabe a Autoridade:

> I - zelar pela proteção dos dados pessoais, nos termos da legislação;
>
> II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
>
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
>
> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

> XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;
>
> XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;
>
> XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);
>
> XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;
>
> XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;
>
> XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;
>
> XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e
>
> XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

No que tange às possíveis sanções que podem ser aplicadas aos agentes de tratamento de dados, em decorrência de eventuais infrações cometidas às normas da LGPD, o artigo 52 da supracitada norma prevê as seguintes sanções:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (Brasil, 2018).

A partir da publicação da Resolução CD/ANPD Nº 1, de 28 de outubro de 2021, que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados é possível afirmar que a ANPD adotou o modelo regulatório chamado de Regulação Responsiva, destacando em seu artigo 15, intitulado “Objeto da atuação responsiva” que “A ANPD adotará atividades de monitoramento, de orientação e de prevenção no processo de fiscalização e poderá iniciar a atividade repressiva”.

O modelo em estudo propõe uma maior inteligência regulatória, isto é, busca o equilíbrio entre a punição e a persuasão. Assim, o regulador deve trabalhar em conjunto com seus regulados e não apenas impor regulamentos, posto que visa-se a conformidade das instituições, o fomento à cultura de proteção de dados e garantia dos direitos dos titulares e não a mera punição (Santos, 2023).

Contudo, a regulação responsiva não prevê somente a orientação (persuasão), pois à medida em que as instituições resistem o cumprimento da norma por boa fé, deve ocorrer a intervenção estatal, aplicando as sanções mais severas previstas, caso haja falha na persuasão (Braithwaite, 2011).

Em 2023, a ANPD publicou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas, que tem por objetivo estabelecer parâmetros e critérios para aplicação de sanções administrativas pela ANPD, bem como as formas e dosimetrias para o cálculo do valor-base das sanções de multa para os casos, por exemplo, em que a orientação não são mais suficientes.

3.3.2.2 A primeira multa aplicada pela ANPD

A Coordenação-Geral de Fiscalização da ANPD (CGF/ANPD), em 2023, publicou no Diário Oficial da União a primeira sanção pecuniária decorrente da conclusão de processo administrativo sancionador contra a empresa Telekall Infoservice, no valor de R$14.400,00 (quatorze mil e quatrocentos reais).

A fiscalização do caso foi iniciada após denúncia de que a empresa em questão estaria ofertando uma listagem de números de telefones de eleitores para fins de disseminação de material de campanha eleitoral municipal.

Segundo a CGF/ANPD, após o deslinde do processo administrativo, foi possível concluir que a empresa infringiu os arts. 7º e o 41 da LGPD, além do art. 5º do Regulamento de Fiscalização da ANPD, não sendo aplicadas hipóteses lícitas de tratamento de dados (artigo 7º), tampouco sendo nomeado encarregado de dados (artigo 41). Para a infração ao art. 7º da LGPD e ao art. 5º do Regulamento de Fiscalização foram aplicadas sanções de multa simples. O descumprimento ao art. 41, por sua vez, enseja sanção de advertência.

Assim, ante essa ter sido a única sanção pecuniária aplicada pela ANPD, até o fechamento da presente pesquisa, não houve possibilidade de catalogar os eventuais casos brasileiros para alcançar o objeto proposto neste trabalho, o que poderá ser objeto de trabalhos futuros.

4 A FASE DE COLETA DE DADOS PESSOAIS E O FATOR INTEGRAÇÃO NO CVD

Conforme explanado em seções anteriores, a CI deve contribuir para que o acesso e uso intenso de dados se desenvolva da mais forma mais equilibrada possível, a partir da delimitação das fases envolvidas no acesso e uso dos dados, bem como os atores envolvidos (Sant'Ana, 2016).

O CVD, segundo os estudos de Sant'ana (2016), é composto das seguintes fases: coleta, armazenamento, recuperação e descarte. Na fase de coleta, fase a qual a presente pesquisa é voltada, é necessário que o detentor dos dados conheça quais são os dados coletados em determinada atividade? Os dados que não serão coletados, serão descartados? De que forma? Os que foram coletados, atenderão qual finalidade? Qual o volume de dados envolvidos nessa operação? Na fase de armazenamento, por sua vez, quais são os dados que serão armazenados? Com qual finalidade? Quais dados são descartados após a coleta? Por qual razão? Por quanto tempo são armazenados? Em que local? São compartilhados com operadores ou pelo próprio detentor? Na fase de recuperação, como tais dados são recuperados? Eles são descartados definitivamente?

Cada uma dessas fases é permeada por fatores transversais, quais sejam: Privacidade, Integração, Qualidade, Direitos Autorais, Disseminação e Preservação. Um desses fatores, objeto do presente estudo, é a Integração que ocorre em diferentes bases de dados, isto é, a partir da relação entre os diversos ciclos de dados que ocorrem, é possível que esses dados sejam agrupados, sendo organizados e gerados novos dados.

Cianconi (1987) destaca que há desalinhamento no que se refere aos banco de dados e bases de dados, muitas vezes são tratados como sinônimos. Para o estudioso, tratam-se as bases de dados de um conjunto de dados interrelacionados, organizados de forma a permitir recuperação de informações, enquanto banco de dados refere-se a um conjunto de bases de dados.

Guinchat e Menou (1994, p. 295), defendem bases de dados como sendo um conceito diferente de bancos de dados, sendo "uma base de dados é um conjunto organizado de referências bibliográficas de documentos que se encontram armazenados, fisicamente em vários locais [...] ". Os bancos de dados, por sua vez, "[...] tratam das informações factuais, numéricas ou textuais diretamente utilizáveis".

Heemann (1997, p. 2) destaca que a Ciência da Informação, de maneira geral, trata as bases de dados atuais "como um arquivo ou um conjunto de arquivos computacionais no qual são armazenados dados, permitindo a recuperação e atualização de informações", conceito que passa a ser adotado na presente pesquisa.

Assim, Albrecht e Ohira (2000, p. 133) esclarecem que a função de uma base de dados é proporcionar “(...) informação atualizada (recursos estruturais), precisa e confiável (não dar a informação pela metade) e de acordo com a demanda (oferecer o que o usuário necessita)”, sendo imprescindível que a base de dados forneça mais do que uma armazenagem eficiente de dados, mas o fornecimento de mecanismos eficazes de recuperação.

Nesse sentido, passa-se a seguir a esclarecer a fase de coleta do CVD, bem como essa fase contribui para o presente estudo.

4.1 A fase de Coleta do CVD

A coleta, primeira fase do CVD, permeia a definição das necessidades informacionais por parte dos detentores ou o que a legislação chama de princípio da finalidade. Nesse sentido, caberá aos detentores, a partir da finalidade proposta, definir quais são os dados pessoais necessários para o atingimento do objetivo do tratamento, bem como escolher os mecanismos que serão utilizados para obtenção dos dados (Sant’Ana, 2016).

Os detentores utilizam a fase da coleta de dados pessoais como um processo ou um projeto. No caso de processo, a coleta será constante, ocorrendo a partir da fonte de dados que permite a aquisição de novos dados, podendo ser estabelecida a cadência da coleta. É possível, contudo, que a fase de coleta seja algo pontual, com definição clara de início e término, tendo cada procedimento de coleta suas próprias configurações e estabelecimento de metadados, o que caracteriza a fase de coleta como projeto (Sant’Ana, 2016).

Affonso (2018, p. 198) alerta para o fato de que “No momento da coleta, o usuário transfere para os detentores a tutela dos seus dados; assim, o uso desses dados não está mais sob controle do usuário”, que passa a estar na posse dos detentores.

As TIC permitem uma coleta constante de dados, inclusive dados pessoais, enquanto os usuários fazem uso delas, o que já é naturalizado pelos usuários, não gerando questionamentos ou preocupações (Affonso, 2018), mesmo que o princípio da transparência não esteja sendo diretamente respeitado, ou seja, os usuários não são claramente informados acerca da coleta de seus, enquanto interage com aplicações ou sítios eletrônicos, por exemplo.

Os ambientes digitais são essenciais para efetivar esse processo, sobretudo a Internet, pois por meio da World Wide Web (WWW), também conhecida como ambiente Web, é possível a configuração amigável de diversas páginas, com textos, figuras, sons e vídeos, atraindo milhões de usuários, que podem utilizar serviços sem nenhuma complexidade aparente para o usuário (Tanenbaum, 2003), uma vez que detalhes técnicos são abstraídos.

Mayer-Schönberger (2011) ressalta que os detentores afirmam que por meio dessa coleta de dados é possível prestar melhores serviços e experiências personalizadas aos usuários, o que torna uma moeda de troca. Affonso (2018, p.197) afirma que “Essa situação pode ser vista, por exemplo, durante o uso de aplicativos para dispositivos móveis, que solicitam permissão de acesso aos dados do usuário para que a instalação seja concluída”. Assim, ante o desejo do usuário em acessar o serviço disponível, ele aceita remunerar indiretamente esses serviços, permitindo com que seus dados sejam acessados pelos detentores.

Affonso, Monteiro e Camargo (2016) confirmaram, em estudo realizado, que dados são coletados durante a instalação de aplicativos em dispositivos móveis. Dentre os aplicativos levantados, 98.75% solicitam acesso aos dados do usuário durante a instalação, tais como: dados de localização; informação de conexão Wi-Fi; acesso à câmera; identidade; dados de contato; entre outros.

Com efeito, essa coleta expressiva de dados pode ensejar em problemas, por exemplo, relacionados à privacidade dos usuários, posto que as interações são constantemente medidas (Floridi, 2005; Bergström, 2015) e os usuários parecem não ter o exato conhecimento de como esses dados são coletados ou quais dados exatamente estão sendo recepcionados.

Affonso (2018) afirma que existem dados perceptíveis para usuário na fase de coleta de dados. Contudo, existe uma abstração entre o momento em que o dado é solicitado até a resposta do servidor, o que pode envolver outros dados. Assim, “Essa abstração se dá em relação aos dados de tráfego que são coletados e aos

valores semânticos que eles carregam, podendo resultar em algum tipo de brecha de privacidade aos sujeitos que interagem com ambientes Web" (Affonso, 2018, p. 199).

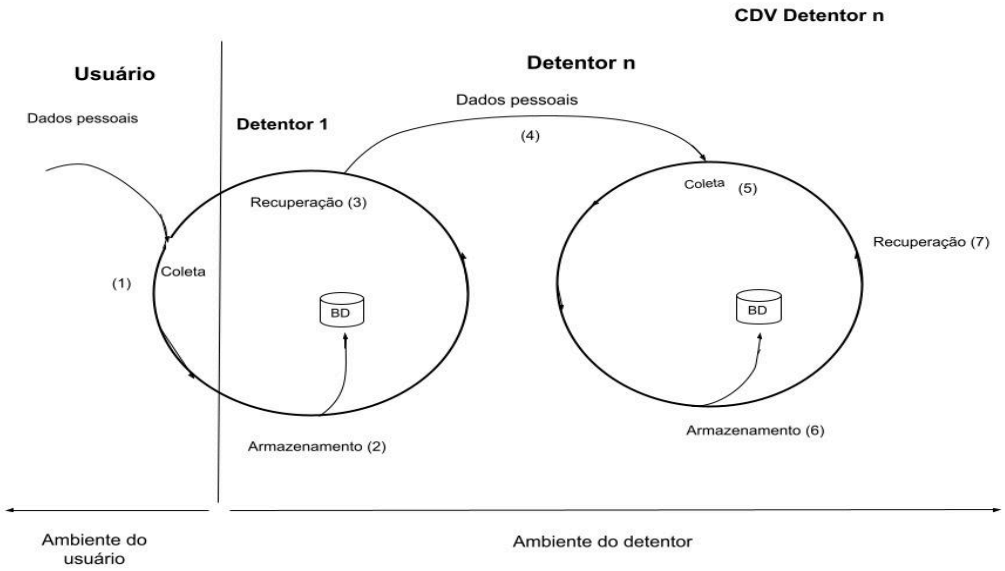
Nesse sentido, Mayer-Schönberger (2011) destaca que os detentores ampliam seu poder sobre os usuários, ao terem acesso às suas informações, ensejando em assimetria informacional, pois o usuário não tem consciência sobre o que está sendo coletado, tampouco integrado, perdendo o controle sobre seus próprios dados. Assim, é necessário destacar que

> Já com relação às fases de coleta, a insciência dos usuários acentua-se, chegando mesmo ao extremo de não lhe ser possível, muitas das vezes, nem mesmo ter ciência de que o processo está ocorrendo. Quando se trata de formas mais diretas de obtenção de dados, tais como formulários ou mesmo por meio de registro de interações com mídias sociais por exemplo, os usuários são convencidos de que os dados coletados terão como finalidade sua comodidade e podem até ser alvo de legislações, como as que prevêem garantias em relação aos dados pessoais (BRASIL, 2018). No entanto, muitas das coletas, que são realizadas por meio de dispositivos que podem atuar sem a participação ativa do usuário, podem coletar dados, inicialmente considerados como não identificadores, e que, portanto, ficam livres de controle ou de desconfianças mais diretas. No entanto, quando esses dados são integrados com outros dados, para subsequente tratamento, eles podem gerar o que se denomina de efeito mosaico e levar à identificação e violação de privacidade, que não poderiam ser previstas sem o acesso às camadas mais internas do ciclo de vida dos dados (Sant'Ana, 2019, p. 125-6).

A coleta de dados pode ocorrer, ainda, diretamente do usuário ou indiretamente. Na forma direta, o detentor indaga os usuários sobre seus dados, como ocorre no preenchimento de formulários, necessários para o ingresso em plataformas digitais. É possível, contudo, que a coleta ocorra durante a interação do usuário com a aplicação ou sítio eletrônico e a partir da integração de bases de dados. Nesse caso, o detentor coleta logs do servidor, que podem incluir informações como endereço IP do aparelho, por exemplo, sem que o usuário seja diretamente indagado sobre essa coleta (Sant'Ana, 2019).

A coleta de dados pode ocorrer, ainda, a partir de dados compartilhados entre detentores parceiros, a partir da integração de duas bases de dados, conforme figura 6 abaixo:

Figura 6 - A coleta de dados a partir de detentores parceiros



Fonte: Elaborado pela autora.

Com a contextualização propiciada pelo CVD (Sant'Ana, 2016), percebe-se que o usuário tem (possível) ciência da coleta dos dados que são transferidos ao detentor 1 (1), pois ocorrem no ambiente do usuário e é feita diretamente. Assim, o próprio usuário pode, por exemplo, responder a formulários que solicitam seus dados para que possa acessar o serviço disponibilizado pelo detentor 1.

No ambiente do detentor, contudo, percebe-se uma maior complexidade do CVD. A análise do contexto do acesso aos dados demonstra que ao acessar o sítio eletrônico ou aplicação, o usuário, ciente ou não, permite que o detentor realize uma coleta de dados (fase de coleta - 1), que são enviados para serem armazenados na base de dados do detentor 1 (fase de armazenamento - 2). Os dados ficam armazenados na base de dados do detentor 1 (2), processo que não é objeto de estudo da presente pesquisa, sendo o acesso a forma de armazenamento dificultoso aos pesquisadores por tratar-se de procedimento interno dos detentores e pouco expostos.

Seguindo o CVD, o detentor 1 pode disponibilizar os dados armazenados a terceiros, como parceiros comerciais, por exemplo (fase de recuperação - 3). O processo de recuperação destes dados ocorre em um subciclo do detentor 1, relacionando-se com detetores N, permitindo que parceiros (detentores N) tenham acesso aos dados coletados em 1, oportunidade em que o detentor N coleta esses dados, a partir da fase de recuperação do detentor 1 e da fase de coleta do detentor

N (5). Todo esse processo ocorre no ambiente dos detentores, não sendo, necessariamente, disponibilizado aos usuários, que possivelmente desconhecem o fluxo pelo qual seus dados percorrem, isto é, são compartilhados com terceiros com quem, em tese, não possuem relação.

O encapsulamento próprio do funcionamento maquínico, necessário para que o acesso a tais dados ocorra de forma eficiente, pode levar a uma insciência do usuário sobre eventual compartilhamento (fase de recuperação para o detentor 1) dos dados armazenados com detentores N.

Exemplo disso foi detectado pela Fundação Procon-SP, que, em 2019, multou as empresas Google e Apple, no Brasil, na quantia de R$ 9.964.615,77 e R$ 7.744.320,00, respectivamente, por não seguirem as diretrizes previstas no Código de Defesa do Consumidor (CDC)[25]. Ambas as empresas disponibilizaram em suas plataformas o aplicativo FaceApp, serviço que permitia ao usuário visualizar seus rostos envelhecidos.

A Fundação Procon-SP sustentou que além de não disponibilizar cláusulas contratuais em português, somente em inglês, por meio de seus “Termos de uso”, uma das cláusulas previa a possibilidade de compartilhamento dos dados dos usuários com as empresas que fazem parte do mesmo grupo, prestadoras de serviços e organizações terceirizadas. Segundo o apurado, uma cláusula previa que “os dados do consumidor podem ser transferidos para outros países que não tenham as mesmas leis de proteção de dados que as do país de origem, o que implica em renúncia de direitos dos consumidores”.

Nesse sentido, observa-se que ao instalar o aplicativo, o usuário tinha seus dados coletados, dentro de seu ambiente, conforme (1) na Figura 6. Contudo, o aplicativo, após armazenar dados de seus usuários (2), recuperava tais dados (3), oportunidade em que terceiros (parceiros comerciais), coletam os dados dos usuários (dados pessoais 4), mas não sendo disponibilizados diretamente por eles e sim pela aplicação (3 e 5). Assim, um CVD passa a ser observado, pois o detentor N passa a armazenar (6) e poder recuperar (7) os dados coletados em 5.

Assim, percebe-se que a fase de coleta pode ocorrer tanto de forma direta, a partir da coleta de dados pessoais diretamente com o usuário, quanto indiretamente.

---

[25] Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2019/08/30/procon-sp-aplica-multas-milionarias-em-google-a-apple-por-aplicativo-que-envelhece-rostos.ghtml

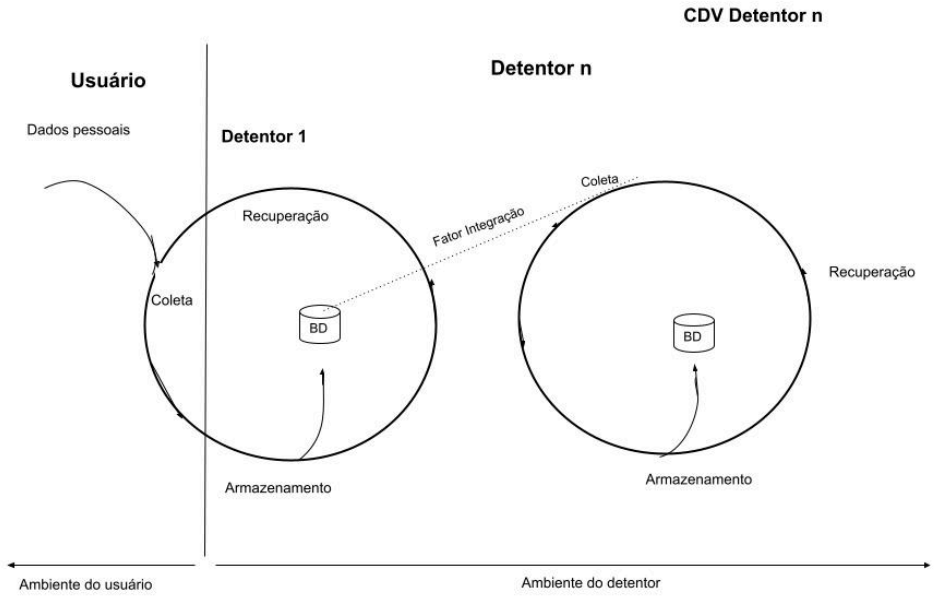
Nesse contexto, é possível que os detentores N coletem dados pessoais, a partir do compartilhamento (fase de recuperação do detentor 1) de dados pessoais disponibilizados por parceiros comerciais (detentor 1), que tiveram acesso a esses dados diretamente ao usuário. No próximo item, busca-se dissertar acerca da interferência do fator integração nesse processo, tornando-o ainda mais complexo.

4.2 O fator integração do CVD

O desenvolvimento das TIC proporcionou transformações nas geração de dados coletados por diversos aparatos tecnológicos (Monteiro *et al*, 2016), propiciando também a integração de bases dados, a partir de tecnologias interoperáveis e infraestrutura que possibilita aos computadores integrarem e processarem informações de acordo com seu significado, como a Web Semântica (Chowdhury, G.; Chowdhury, S., 2007).

Assim, a figura 7 representa a integração de bases de dados, por meio do fator integração, a partir do CVD do detentor 1, que interage com a base de dados de n detentores.

Figura 7 - O fator integração em bases de dados.



Fonte: Elaborado pela autora.

A integração é um fator que permeia todas as fases do CVD. Em que pese não ser objeto da presente pesquisa dissertar acerca das técnicas de integração de bases de dados, destaca-se que na coleta, inicialmente, percebe-se que os dados

podem não ser adquiridos diretamente do usuário, mas sim, a partir de outra base de dados que, de alguma forma, já possuía aqueles dados, não sendo necessário indagá-lo novamente.

Nesse sentido, é necessário que, na fase de coleta, o detentor tenha a definição dos requisitos sobre a base de dados que se pretende adquirir como um todo, bem como os relacionamentos necessários para que uma base esteja integrada a outras bases, pois, assim, é possível proporcionar “um resultado que remete à questão do valor do todo que tende a ser maior que a soma das partes quando estas partes estão devidamente integrada” (Sant’Ana, 2016, p. 125).

Observa-se, também, a partir da Figura 7 que os dados são, para os usuários, coletados apenas pelo detentor 1. Contudo, a partir da integração da base de dados do detentor 1 e dos detentores n, os detentores n passam a também ter acesso aos dados coletados, sem, necessariamente, haver a ciência do usuário sobre esse processo. Nesse sentido, os CVD possuem constantes interações.

A integração passa a ser um fator na fase de coleta a partir da identificação e validação dos atributos que serão responsáveis pela identificação unívoca de cada registro e seus correspondentes estrangeiros, visando a garantia da integração (Sant’Ana, 2016).

Na fase de armazenamento, fase que tem um enfoque mais tecnológico e são definidos requisitos que possibilitam a reutilização destes dados, a possibilidade de integração dos dados depende, sobretudo: i. da forma de acesso; ii. do formato ou padrão. Sant’Ana (2016) esclarece, no que tange a forma de acesso, que os dados podem ser acessados diretamente por meio de um Sistema Gerenciador de Banco de Dados (SGBD). Caso seja adotado um SGBD, indica-se que o próprio formato utilizado pelo sistema seja mantido, pois, assim os dados ficam sob a gestão destes, ensejando na redução da interação mais direta, mas amplia a segurança tanto física quanto lógica. Caso opte-se por uma forma de acesso direta, o detentor poderá adotar tanto o padrão de formatação baseada em semântica posicional quanto formatos mais elaborados, buscando incluir a semântica que define as entidades e os atributos “por meio de metadados incorporados aos conteúdos o que pode propiciar a interpretação e uso destes dados, inclusive, de forma automatizada” (Sant’Ana, 2016, p.128).

No que diz respeito ao formato ou padrão, é necessário que a semântica tanto das entidades, quanto dos atributos sejam disponibilizados em conjunto aos conteúdos. Nesse sentido,

> (...) Como exemplos desta definição pode-se citar escolhas como a do formato Comma Separated Values ou CSV que é muito simples e permite acesso facilitado por meio de uma simples planilha. Seu formato é baseado em uma planilha em que cada linha do arquivo, delimitada por uma quebra de linha (*carriege return e line feed - CRLF*), representa uma linha da planilha e o conteúdo de cada coluna é separado por um caractere escolhido, na maioria das vezes opta-se pelo uso da vírgula como o próprio nome indica (...) (Sant'Ana, 2016, p.128-9).

Ressalta-se que uma vez acessados, os dados também devem estar articulados entre si, por meio de relacionamentos possíveis de serem identificados pelos próprios algoritmos, a partir da viabilidade com outras entidades (SANT'ANA, 2016). Sant'ana (2016) destaca, ainda, que

> Quando se trata de dados sensíveis a questão se agrava já que a definição bem feita de identificadores e até semi-identificadores pode ampliar, e muito, as possibilidades de uma ação e ataque, que, por meio da integração de bases que não ferem diretamente a privacidade formando novas bases de dados com grande potencial de quebra da privacidade (Sant'Ana, 2016, p.130-1).

Na fase de recuperação, qual seja, após a coleta e armazenamento dos dados, propicia-se uma nova fase que torna esses dados disponíveis para acesso e uso, a integração também é um fator a ser considerado. Santarém Segundo (2014, p. 3.866) destaca que:

> Utilizar ontologias e suas relações é uma das maneiras de se construir uma relação entre termos dentro de um domínio, favorecendo a possibilidade de contextualizar os dados, tornando mais eficiente e facilitando o processo de interpretação dos dados pelas ferramentas de recuperação da informação.

Visando obter um nível satisfatório dos dados coletados e armazenados, é importante que eles apresentem um grau de interação que análises de entidades diferentes, mas integradas, a fim de compor um todo que representa um valor de uso maior do que se comparado a soma dos valores de uso das entidades individualmente (Sant'Ana, 2016).

Em São Paulo, uma mulher foi indenizada em 10 (dez) mil reais pelo Tribunal de Justiça de São Paulo. No caso, a autora afirmou que descobriu, em dezembro de 2020, uma gestação, mas perdeu o bebê em fevereiro de 2021. Após poucos dias do aborto espontâneo, a autora passou a receber mensagens de

aplicativos de mensagem instantânea de um laboratório de criobiologia com uma oferta de coleta e armazenamento de cordão umbilical[26].

A autora alegou não ter fornecido seus dados pessoais, como nome e telefone, nem informações sobre seu estado gravídico para o laboratório, com o qual não tinha relação. Em contestação, o laboratório afirmou que só teria utilizado dados não sensíveis e não sigilosos, referentes apenas ao nome e número de telefone da autora. Não foi esse o entendimento da Justiça ao condenar o laboratório, que afirmou:

> Embora a ré afirme que se utilizou de dados não sensíveis e não sigilosos, referentes apenas ao nome e telefone celular da autora, não é o que se depreende dos fatos narrados. A autora estava grávida. Esta informação é um dado, que foi utilizado pela ré em sua atividade empresarial: angariação de novos clientes. [...] Não há verossimilhança na alegação da ré de que não tinha conhecimento da gravidez da autora. A própria ré confirma que trabalha com coleta e armazenamento de cordão umbilical de bebês recém-nascidos. Seria natural que dirigisse sua atividade de prospecção de novos clientes a mulheres grávidas. Daí a razão pela qual não convence a argumentação da ré de que não teria se utilizado de dado sensível pertencente à autora. (TJ-SP. Apelação Cível 1041607-35.2021.8.26.0100, rel. Des. Alexandre Marcondes, DJ 17/05/2022).

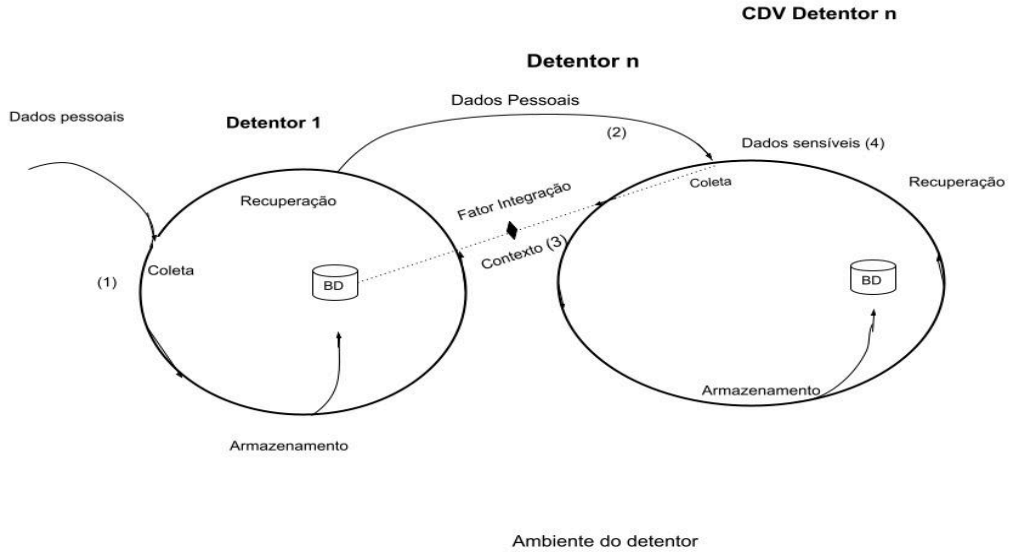
Segundo o Tribunal, a gravidez da autora é considerada um dado de saúde e, consequentemente, dado pessoal sensível, que foi compartilhado pelo detentor 1 com o detentor n (o laboratório). A autora indagou ao laboratório como havia conseguido seus dados e obteve a seguinte resposta: “Seu contato chegou até nós através de parcerias com parcerias com obstetras, clínicas ou cursos de gestantes”. Como não houve a identificação exata, a presente pesquisa irá identificar como detentor 1, isto é, possivelmente o detentor quem coletou os dados pela primeira vez, mas não podemos afirmar se o detentor 1 é o detentor inicial, pois existem múltiplos ciclos dos quais não temos acesso.

Nesse sentido, é possível que mais dados pessoais sejam coletados pelos detentores N, se comparado ao que foi coletado pelo detentor 1, diretamente com o usuário. É possível, inclusive, que dados pessoais sensíveis sejam coletados pelos detentores N, a partir do contexto em que os dados pessoais estão inseridos, mesmo que apenas dados pessoais sejam de fato compartilhados, conforme apresenta-se a Figura 8:

---

[26] Disponível em: https://olhardigital.com.br/2022/07/22/seguranca/mulher-informacoes-dados-vazados-indenizacao/

Figura 8 - A coleta de dados pessoais sensíveis a partir de detentores parceiros



Fonte: Elaborado pela autora.

Observa-se que como a autora da ação desconhecia o tratamento de dados por parte do detentor n (laboratório), os dados pessoais (nome e telefone) foram coletados diretamente pelo detentor 1 (1). Segundo o detentor n (laboratório), foram acessados da autora apenas nome e contato telefônico. Esse acesso decorre da recuperação dos dados da autora (2) pelo detentor 1, todavia o fato desses dados terem um contexto específico, qual seja, estarem sendo compartilhados por estabelecimentos de saúde (3), o fator integração é observado, oportunidade em que são coletados pelo detentor n dados pessoais sensíveis(4) e, posteriormente, armazenados em seu banco de dados. Nesse sentido,

> Posso autorizar uma instituição a coletar informações “A” sobre mim e outra instituição a coletar informações “B” sobre mim; mas eu não quero que ninguém possua “A” e “B” sobre mim ao mesmo tempo. Quando “C” é adicionado à lista de conjunções, o dono da nova informação saberá ainda mais sobre mim. E então “D” é adicionado e assim por diante. Cada atributo que vai adicionando na minha tecelagem revela cada vez mais sobre mim. No processo, o tecido criado é uma ameaça à minha privacidade (Mason, 1986, p. 2, tradução nossa)[27].

[27] No original, “*I may authorize one institution to collect information "A" about me, and another institution to collect information "B" about me; but I might not want anyone to possess "A and B" about me at the same time. When "C" is added to the list of conjunctions, the possessor of the new information will know even more about me. And then "D" is added and so forth. Each additional weaving together of my attributes reveals more and more about me. In the process, the fabric that is created poses a threat to my privacy*”.

Nesse contexto, percebe-se que a integração de bases de dados por diversos detentores de dados pode ensejar na disponibilização de mais dados que o usuário permitiu, uma vez que os dados disponibilizados não foram os necessariamente apresentados ao usuário como sendo os que seriam coletados.

Assim, em que pese terem sido coletados pelo detentor n apenas dados pessoais (3), em decorrência do serviço prestado pelo detentor 1, infere-se que, a partir do contexto em que esses dados pessoais estavam inseridos, qual seja, possivelmente armazenados por uma clínica especializada, os dados que então eram estritamente pessoais, se transformaram em pessoais sensíveis.

No caso do tratamento de dados ocorridos por computadores, é possível que além do contexto, haja também inferências, a partir da interferência de tecnologias. De acordo com Segundo e Coneglian (2016), as inferências têm por base a dedução ou tomada de decisão a partir de determinadas lógicas chamadas de Axiomas.

No contexto computacional, existem inúmeras formas tanto matemáticas, quanto algorítmicas, a partir de motores, que permitem que as inferências sejam aplicadas e gerem a tomada de decisão. Nesse sentido,

> Os motores de inferência são mecanismos capazes de atuarem seguindo lógicas pré-definidas. Inicialmente, os motores de inferência foram criados dentro dos estudos de Inteligência Artificial, sendo uma ferramenta com atuação em Sistemas Especialistas. (...) Neste sentido, os motores de inferência são responsáveis por possibilitar que as expressões lógicas definidas possam gerar novos conhecimentos, visto que, são estes mecanismos que possibilitarão a deduções e a tomadas de decisões. Estes mecanismos necessitam de regras (axiomas) para realizar a inferência, sendo que existem diversas linguagens para a criação das regras (Segundo; Coneglian, 2016, p. 9).

Não é objeto do presente trabalho analisar os tipos, características, as regras adotadas, protocolos ou as formas em que as inferências ocorrem, mas sim destacar que a partir delas é possível que dados pessoais sejam transformados em dados pessoais sensíveis, que não foram coletados diretamente do usuário.

O caso Target, contudo, ilustra a questão: em 2012, nos Estados Unidos, a empresa varejista Target, visando aumentar o número de vendas direcionadas ao público propenso ao consumo, separou uma lista de 25 (vinte e cinco) produtos que mulheres grávidas costumam comprar, tais como: loções sem essência, sabonetes sem cheiro, suplementos alimentares com cálcio, zinco, dentre outros. A equipe de

estatística conseguia estimar a probabilidade de gravidez (de 0 a 100%), bem como o estágio em que a mulher se encontrava, a partir do consumo dos produtos[28].

A partir desses dados, a Target enviava às “potenciais” mães cupons de descontos e ofertas relacionadas à gravidez, aumentando a chance de consumo daquela mulher na varejista. A Target, contudo, recebeu a ligação de um homem indagando o porquê sua filha adolescente estava recebendo cupons de desconto relacionados à gravidez da loja, uma vez que sua filha ainda estava no ensino médio. O gerente se desculpou em nome da varejista. Contudo, pouco tempo depois, o mesmo pai ligou novamente para a Target, confirmando a gravidez da filha.

A acurácia do protocolo adotado era tão precisa que dados pessoais sensíveis, qual seja, o estado gravídico de uma adolescente foi inferido, a partir dos produtos adquiridos por ela, sofrendo a interferência da integração de bases de dados.

Nesse sentido, a privacidade da adolescente foi quebrada e, mesmo que essa questão não esteja relacionada ao objeto do presente trabalho, percebe-se que um grande prejuízo da transformação de dados pessoais em dados pessoais sensíveis é a quebra de privacidade do usuário, que pode não conhecer que outros dados estão sendo coletados para além dos que foram diretamente coletados.

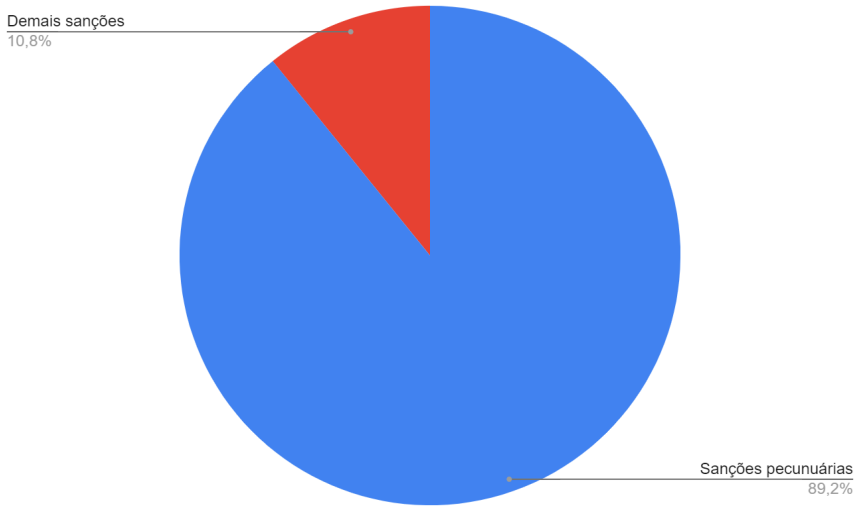
[28] Disponível em: https://www.estadao.com.br/politica/eleicoes/dados-gravidos-imp-/

5 RESULTADOS E DISCUSSÃO

A lista de sanções impostas por Autoridades de Proteção de Dados Europeias às instituições que operam na União Europeia, disponibilizada pelo *CMS.Law GDPR Enforcement Tracker*, entre os anos de 2019-2023, apresentou um total de 2.038 (duas mil e trinta e oito) sanções, no geral.

Desse número total, foram aplicadas pelas Autoridades 1.824 (mil oitocentos e vinte e quatro) sanções pecuniárias na UE, representando um montante de 4 bilhões de euros. Nesse sentido, o gráfico 1 demonstra a proporção entre sanções gerais e sanções pecuniárias, qual seja, as sanções pecuniárias representam proporção superior a 89% (oitenta e nove por cento) das demais sanções, senão vejamos:

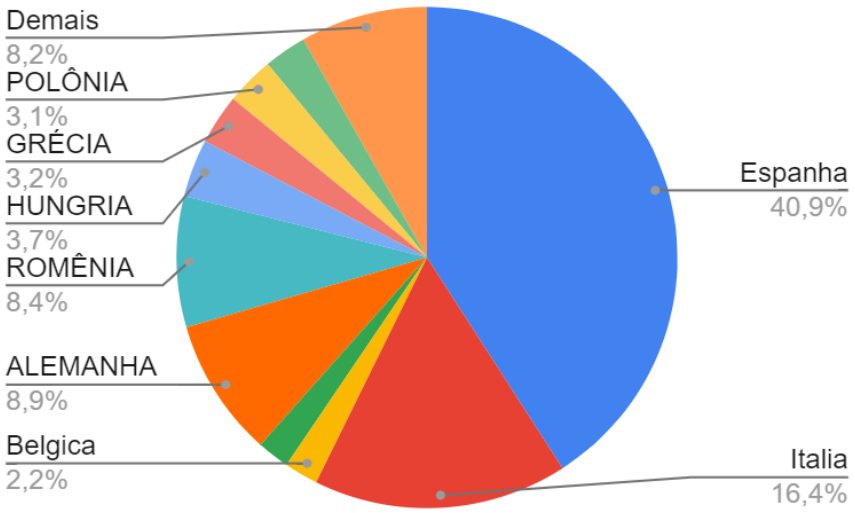
Gráfico 1 - Sanções das Autoridades de Proteção de Dados da UE: 2019-2023



Fonte: Elaborado pela autora.

Nesse contexto, é possível afirmar que a maior parte das sanções aplicadas envolve sanções pecuniárias. Em relação às Autoridades, a Autoridade Espanhola foi a que teve, até o fechamento desta pesquisa, o maior número de sanções pecuniárias aplicadas, no total de 746 (setecentos e quarenta e seis), representando 40,9% das sanções pecuniárias aplicadas; seguida da Itália, que aplicou 299 (duzentas e noventa e nove). As Autoridades francesa e belga foram as que aplicaram o menor número: 38 (trinta e oito) e 40 (quarenta), respectivamente.

Gráfico 2 - Sanções pecuniárias aplicadas por Autoridade



Fonte: Adaptado de *CMS.Law GDPR Enforcement Tracker* (2023).

A partir do filtro disponibilizado pelo próprio sítio eletrônico, observou-se que a base de dados ora estudada, qual seja, 2.039 (dois mil e trinta e nove) casos de infrações ao GDPR, 129 (cento e vinte e nove) estão relacionados ao artigo 9º da GDPR, isto é, estão relacionados ao tratamento incorreto de dados pessoais sensíveis, posto que é o artigo 9º o responsável por dispor como os dados de categorias especiais (dados sensíveis) devem ter tratados pelos detentores. Inicialmente, o artigo impõe que

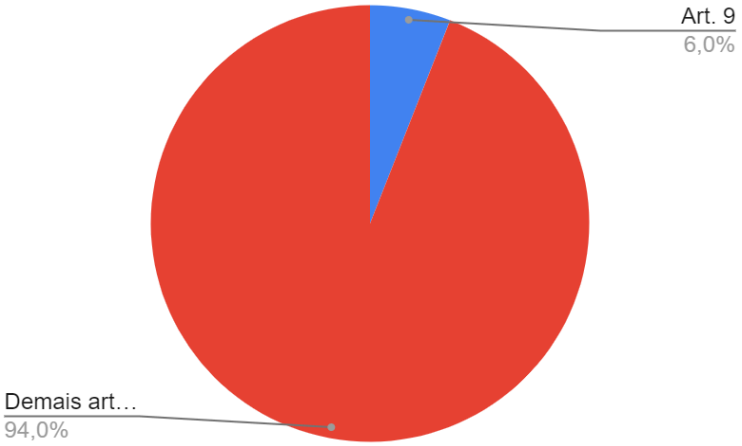
> É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (UE, 2018).

Todavia, o mesmo dispositivo traz as ações em que é possível o tratamento de dados pessoais sensíveis, tais como: a partir do consentimento do titular; por cumprimento de obrigações legais; exercício de direitos, seja do detentor ou do titular; para proteção de interesses vitais do titular ou de outra pessoa física; por associações políticas, filosóficas, religiosas ou sindicais, no exercício de suas atividades; quando o próprio titular torna o dado público; interesse público importante; para fins de saúde do titular ou pública; fins científicos, históricos ou estatísticos.

Assim, a presente pesquisa filtrou o total de 2.038 (duas mil e trinta e oito) sanções, chegando ao número de 129 (cento e vinte e nove) casos para serem

analisados o conteúdo, pois restringiu-se apenas aos casos relacionados ao artigo 9º do GDPR. O Gráfico 3 apresenta a proporção entre o número de sanções relacionadas ao artigo 9º do GDPR (129 casos) e os demais artigos do Regulamento, sendo constatado um total de 6% (seis por cento) das sanções aplicadas relacionadas ao descumprimento do artigo 9º, senão vejamos:

Gráfico 3 - Proporção de sanções totais aplicadas relacionadas ao artigo 9º do GDPR.



Fonte: Adaptado de *CMS.Law GDPR Enforcement Tracker* (2023).

Nesse cenário, caso quaisquer Autoridades tenham entendido que dados pessoais sensíveis foram tratados de forma incorreta, isto é, que não foram coletados diretamente com o titular ou foram coletados dados pessoais sensíveis por inferência, o artigo 9º do GDPR teria sido descumprido, uma vez que é esse artigo que trata dos dados sensíveis.

Com efeito, foram avaliadas 129 (cento e vinte e nove) decisões de Autoridades de Proteção de Dados europeias, disponibilizadas pelo sítio eletrônico *Enforcement Tracker,* sendo, ainda, 12 (doze) catalogados casos em que houve indícios da transformação de dados pessoais em dados pessoais sensível, isto é, casos em que dados pessoais sensíveis foram coletados, a partir do contexto em que meros dados pessoais foram coletados ou recuperados, conforme resultados apresentados a seguir.

5. 1 A transformação de dados pessoais em dados pessoais sensíveis a partir de dados de contato

Os dados de contato, como e-mail, telefone residencial e telefone celular são considerados dados pessoais e não sensíveis, uma vez que, em tese, não estou relacionados à 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, e vinculado a uma pessoa natural.

Contudo, a presente pesquisa detectou quatro casos, investigados por Autoridades de Proteção de Dados, na UE, em que os dados de contato transformaram-se em dados pessoais sensíveis, senão vejamos:

5.1.1 O caso Senseonics Inc

A Autoridade de Proteção de Dados italiana impôs uma multa de 45.000 euros à Senseonics Inc. A detentora informou à Autoridade uma violação de dados, nos termos do Art. 33 do GDPR. No caso em questão, dentre outras violações apuradas e desconsideradas por ausência de pertinência à presente pesquisa, um funcionário da detentora enviou, acidentalmente, uma campanha informativa por e-mail para cerca de 2.000 (dois mil) destinatários, em uma lista aberta, ou seja, todos os destinatários tinham acesso aos endereços de e-mails um dos outros. Contudo, os destinatários dos e-mails eram pacientes diabéticos, possibilitando a obtenção de informações sobre o estado de saúde dos titulares dos dados através dos e-mails, uma vez que apenas diabéticos teriam interesse na mensagem eletrônica enviada. Assim, a Autoridade estabeleceu que:

> [...] O incidente notificado envolve a possibilidade de terceiros não autorizados acederem aos endereços de e-mail de pessoas potencialmente interessadas em produtos para a diabetes, ou aos endereços de e-mail dos seus cuidadores. Estes endereços de correio eletrónico são, em alguns casos, constituídos por uma combinação de nome e apelido, o que permite identificar o titular em questão, divulgando indiretamente dados relativos à sua saúde, ou seja, uma determinada categoria de dados pessoais nos termos do art. 9º do GDPR (tradução livre). [29]

[29] No original, "(...) *L'incidente notificato comporta la possibilità per terzi non autorizzati di accedere a indirizzi email di persone potenzialmente interessate a prodotti per il diabete, ovvero agli indirizzi email dei loro caretaker. Tali indirizzi email sono in alcuni casi costituiti da una combinazione di nome e cognome che rende così possibile l'identificazione del soggetto in questione, divulgando*

Nesse sentido, a própria Autoridade reconheceu que o contexto em que a mensagem eletrônica estava inserida, qual seja envolvendo produtos para diabetes, gerava dados pessoais sensíveis, uma vez que a combinação de dados (nome, e-mail e motivo de contato) divulgava dados pessoais sensíveis, sem o consentimento dos titulares.

A partir do CVD, em que pese na fase de recuperação, o detentor 1 apenas disponibilizar dados pessoais de contato, os detentores n, que receberam a mensagem eletrônica, coletaram mais do que os dados disponibilizados: foram coletados tanto dados pessoais, quanto dados pessoais sensíveis, relacionados à saúde de quem estava na lista de transmissão.

5.1.2 O caso do Hospital San Raffaele srl

A Autoridade de Proteção de Dados italiana aplicou uma multa de 70.000 euros à unidade de saúde Hospital San Raffaele srl. Segundo a Autoridade, o hospital relatou duas violações de dados: No primeiro caso, o departamento de neurologia do hospital enviou uma *newsletter* em uma lista de distribuição aberta, resultando na visibilidade dos endereços de e-mail dos destinatários a todos que estavam dentro da lista. Assim, dos 499 (quatrocentos e noventa e nove) endereços de e-mail afetados, 321 (trezentos e vinte e um) endereços de e-mail eram relacionados a pacientes e 46 (quarenta e seis) eram referentes à familiares/cuidadores de pacientes, o que permitiu identificar estes indivíduos pelo nome.

No segundo caso, o departamento de cirurgia também enviou um boletim informativo a lista de distribuição aberta, deixando os endereços de e-mail dos destinatários visíveis para todos os destinatários. Dos 90 (noventa) endereços de e-mail afetados, 75 (setenta e cinco) endereços de e-mail referiam-se a pacientes e/ou familiares/cuidadores dos pacientes, o que possibilitou a identificação desses indivíduos pelo nome, bem como dados de saúde.

Em sua defesa, o Hospital afirmou que o mero envio das mensagens eletrônicas não tornava de forma alguma possível a identificação de dados de saúde dos destinatários da *newsletter*, uma vez não ser possível realizar uma distinção

---

indirettamente dati relativi alla sua salute, ovverosia una categoria particolare di dati personali ai sensi dell'Art. 9 del RGPD".

concreta, apenas potencial ou casual. Contudo, após realizar a investigação, a Autoridade de Proteção de Dados italiana entendeu que:

> [...] Portanto, mesmo que parte dos endereços de e-mail não contenham referências ao nome e sobrenome ou, em qualquer caso, a outros dados de identificação direta dos interessados, trata-se de informação pessoal, sujeita, como as demais, à aplicação da regulamentação, relativamente à proteção de dados pessoais. Além disso, a circunstância do contexto das comunicações se pode deduzir que os destinatários das mesmas eram utentes, num caso, da Unidade Operativa de Neurologia e, no outro, da Unidade de Transplantação e Cirurgia Metabólico-Bariátrica e, portanto, pacientes em tratamento nas referidas Unidades, (tradução livre)[30].

A Autoridade considerou, assim, que o envio de mensagens eletrônicas constituiu uma violação ao princípio da confidencialidade, que exige que os dados pessoais sejam tratados de uma forma que garanta a segurança adequada, incluindo a protecção contra o tratamento não autorizado ou ilegal e contra a perda, destruição ou danos acidentais por meios apropriados. medidas técnicas e organizacionais.

No mesmo sentido do caso anterior, o detentor 1 disponibilizou dados pessoais de contato (fase de recuperação). Contudo, os detentores n, que receberam a mensagem eletrônica, coletaram tanto dados pessoais, quanto dados pessoais sensíveis, relacionados à saúde de quem estava na lista de transmissão.

5.1.3 O caso Azienda USL della Romagna

A Autoridade de Proteção de Dados italiana impôs uma multa de 50.000 euros à Azienda USL della Romagna. Uma paciente, após sofrer um aborto espontâneo na instituição, solicitou explicitamente ao responsável pelo tratamento que não partilhasse os seus dados de saúde com terceiros. Além disso, ela havia deixado separadamente um número de telefone para ser contatada, caso necessário. Após a alta hospitalar da paciente, uma enfermeira tentou contatá-la, a fim de informá-la sobre a continuação da terapia.

---

[30] No original: "*Pertanto, anche se una parte degli indirizzi e-mail erano privi di riferimenti al nome e al cognome o comunque ad altri dati direttamente identificativi degli interessati, si tratta di informazioni personali, soggette, come le altre, all'applicazione della disciplina in materia di protezione dei dati personali. Inoltre, la circostanza che dal contesto delle comunicazioni poteva desumersi che i destinatari della stessa erano utenti, in un caso, dell'Unità Operativa di Neurologia e, nell'altro, dell'Unità Chirurgia Trapianti e Metabolico-Bariatrica e, quindi, pazienti in cura presso le predette Unità*".

No entanto, a enfermeira não utilizou o número de telefone fornecido pela paciente especificamente para esse fim, mas sim o telefone residencial, obtido por meio de seu prontuário. Na ocasião, o marido da paciente atendeu e foi informado sobre o tipo de serviço onde a paciente esteve internada, não sendo fornecidas mais informações sobre o seu estado de saúde.

Apesar da enfermeira não ter revelado detalhes acerca do estado de saúde da paciente, a Autoridade entendeu que a privacidade da paciente foi quebrada, uma vez que a identificação da profissional como uma enfermeira ginecológica do Hospital em questão, já permitiu ao marido, terceiro, supor que houve alguma alteração no estado de saúde de sua esposa. Nesse sentido, a partir do telefone de contato da paciente e a identificação da enfermeira, foi coletado um dado sensível, qual seja, a presença da paciente em um hospital ginecológico.

O presente caso, contudo, em que pese sua gravidade, não será considerado na presente pesquisa, uma vez que não foram coletados dados pessoais a partir de aplicações ou sítios eletrônicos e sim por interferência humana.

5.1.4 O caso Azienda Ospedale-Università Padova

A Autoridade de Proteção de Dados italiana aplicou uma multa de 5.000 euros à Azienda Ospedale-Università Padova. No caso, o detentor enviou um e-mail contendo formulários de consentimento para participação em um ensaio clínico a vários destinatários numa lista de distribuição aberta. A atitude permitiu com que os destinatários visualizassem os endereços de e-mail de todos os outros destinatários.

Em que pese a defesa ter alegado, que não havia dados de saúde envolvidos diretamente, a Autoridade de Proteção de Dados Italiana considerou que:

> Assim, o envio da referida comunicação através de uma única mensagem de correio eletrónico dirigida a um número múltiplo de destinatários, cujos endereços foram indicados de forma clara no campo cópia carbono (cc), tem, de facto, sem motivo justificado e na ausência de base legal, divulgados mutuamente aos destinatários da mesma comunicação, o estado de saúde dos demais pacientes (tradução livre)[31] .

[31] No original, "*Pertanto, l'invio della citata comunicazione mediante un unico messaggio di posta elettronica indirizzato a un numero plurimo di destinatari, i cui indirizzi sono stati inseriti in chiaro nel campo copia conoscenza (c.c.), ha, di fatto, senza giustificato motivo e in assenza di presupposto giuridico, rivelato reciprocamente, ai destinatari della medesima comunicazione, lo stato di salute degli altri pazienti*".

Nesse sentido, os dados compartilhados (fase de recuperação do detentor 1), de forma direta, foram os e-mails dos pacientes. Contudo, o conteúdo da mensagem eletrônica, isto é, o endereço em que ela está inserida, permitiu que dados pessoais sensíveis, quais sejam, dados de saúde, fossem coletados (fase de coleta por detentores n), podendo ser inferidos pelos destinatários.

5.2 A transformação de dados pessoais em dados pessoais sensíveis a partir de benefícios previdenciários

A presente pesquisa identificou, ainda, que Autoridades de Proteção de Dados europeias reconheceram que dados pessoais foram transformados em dados pessoais sensíveis, a partir de um contexto específico, qual seja, benefícios previdenciários ligados à saúde. Em que pese não ter ocorrido a divulgação direta do diagnóstico dos beneficiários, o afastamento por determinados tipos de benefícios previdenciários, como auxílio doença, indicam problemas de saúde dos titulares, senão vejamos:

5.2.1 O caso da Escola Isabella Gonzaga

A Autoridade de Proteção de Dados italiana impôs uma multa de 2.500 euros à escola secundária 'Isabella Gonzaga'. A escola em estudo publicou, em plataforma *online*, um documento, que continha também dados pessoais relacionados à benefícios previdenciários de professores. Em sua defesa, a escola afirmou que:

> [...] não foi divulgado o motivo que levou o trabalhador a obter os benefícios previstos na Lei 104/92. Não houve, portanto, publicação de dados reais de saúde, mas apenas de um índice a partir do qual se deduzisse uma certa deficiência de uma pessoa (tradução livre) [32].

Contudo, a Autoridade entendeu que são dados relativos à saúde os “dados pessoais relativos à saúde física e mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde” e, em que pese não ter sido detalhado o estado clínico de nenhum dos professores, a concessão de benefícios previdenciários permite inferir informações sobre o estado de saúde de uma pessoa.

---

[32] No original: “*non [è] stato divulgato il motivo che ha portato il dipendente ad avere riconosciuti i benefici ex L. 104/92. Non c’è stata quindi la pubblicazione di un dato sanitario vero e proprio ma solo di un indice da cui dedurre una certa invalidità di una persona*”.

Nesse sentido, a escola (detentora 1) recuperou (fase de recuperação) dados pessoais dos professores, a partir da disponibilização em seu sítio eletrônico. Contudo, os dados que foram coletados pelos detentores n, que passaram a ter acesso aos dados do sítio eletrônico, foram além do recuperado pela detentora 1, uma vez que foi possível inferir, a partir da coleta, que as pessoas que detinham benefícios previdenciários possuíam alguma questão de saúde, sendo, portanto, coletados dados pessoais sensíveis.

5.2.2 O caso Escola Edoardo Amaldi

Caso semelhante ocorreu na Escola Edoardo Amaldi, também na Itália. A Autoridade de Proteção de Dados italiana impôs uma multa de 4.000 euros à escola 'Edoardo Amaldi'. A escola publicou uma circular no sítio eletrônico da escola sobre as férias de verão que continha as datas exatas das férias dos funcionários da escola, bem como uma declaração do plano de férias que continha o nome de todos os funcionários e a referência à utilização dos benefícios previdenciários, inclusive relacionados a afastamentos por COVID-19.

No mesmo sentido, a Autoridade Italiana entendeu que o fato do detentor 1 informar a utilização (ou não) de benefícios previdenciários, em seu sítio eletrônico, permite que detentores n infiram informações relacionadas à saúde de uma pessoa física, quebrando a privacidade dos colegas de trabalho.

5.2.3 O caso Istituto Comprensivo - IC Cosenza III “V. Negroni”

A Autoridade de Proteção de Dados italiana impôs uma multa de 2.000 euros ao Istituto Comprensivo - IC Cosenza III “V. Negroni”. A instituição de ensino publicou, em uma plataforma *online* destinada ao corpo docente, um documento que continha o nome do professor, sendo assinalado dois asteriscos, junto ao nome do professor, com a especificação: “Beneficiário da Lei 104/92. A supracitada legislação prevê uma série de benefícios destinados a quem presta assistência a pais idosos, desde autorizações até licenças.

No decurso da sua investigação, a Autoridade de Proteção de Dados italiana concluiu que a identificação do uso de benefícios previdenciários detonam dados pessoais sensíveis, uma vez que passa a ser possível ter informações, mesmo que inferidas, acerca da saúde dos professores.

5.3 A transformação de dados pessoais em dados pessoais sensíveis a partir dos serviços oferecidos pelo detentor

Os dados pessoais também podem ser transformados em dados sensíveis, a partir dos serviços oferecidos pelo detentor. Em alguns casos, os serviços oferecidos são específicos e consumidos apenas por determinados tipos de público, o que nos possibilita a obter informações (fase de recuperação) diferentes daquelas coletadas (fase de coleta), isto é, o detentor ou mesmo seus parceiros comerciais com quem os dados são compartilhados coletam mais dados, se comparados aos dados coletados diretamente do usuário, os quais o usuário tinha ciência, senão vejamos:

5.3.1 O caso Miropass Srl

A Autoridade de Proteção de Dados Italiana também multou a Miropass Srl em 40.000 euros. A Miropass é uma empresa fornecedora do sistema de reservas TuPassi, que, entre outros, é utilizado pelo Município de Roma desde 2015. O sistema de reservas permite a marcação de consultas e exames, tanto no site do controlador (www.tupassi.it), como através do aplicativo correspondente.

A empresa é responsável por coletar os dados dos usuários que desejam marcar suas consultas. No decurso da sua investigação, a Autoridade de Proteção de Dados concluiu que a Miropass, tinha acesso à dados de saúde dos usuários, mesmo que de forma indireta, posto que a depender do tipo de consulta marcada, é possível pressupor dados de saúde dos usuários, sem o necessário consentimento.

Os dados coletados eram: nome, apelido, código fiscal, número de telefone e endereço de e-mail e um segundo número de telefone opcional), e no momento da marcação da consulta (estrutura escolhida, data, hora, tipo de serviço). Em tese, todos os dados coletados eram pessoais. Contudo, a empresa tinha acesso a mais informações, pois era capaz de coletar dados de saúde, a partir do tipo de consulta marcada, isto é, poderia inferir dados relacionados à saúde do usuário a partir do tipo de consulta marcada na aplicação.

5.3.2 O caso de um médico particular

A Autoridade de Proteção de Dados Italiana aplicou multa a um médico em 2.000 euros. Um paciente queixou-se à Autoridade de que o médico tinha divulgado

os seus dados pessoais a terceiros sem autorização. Segundo o denunciante, o médico recomendou produtos médicos ao titular dos dados como parte do seu tratamento. Poucos dias depois, o titular dos dados recebeu uma ligação do consultor de *marketing* responsável pelos produtos recomendados. O titular dos dados salientou que nunca deu o seu consentimento para a divulgação dos seus dados.

Em sua defesa, o médico afirmou que nenhum dado clínico do paciente havia sido compartilhado com o parceiro comercial, apenas dados de contato. A Autoridade de Proteção de Dados afirma que não é necessário consentimento específico para o tratamento de dados pessoais necessários ao tratamento médico. Contudo, apesar de apenas dados de contato terem sido compartilhados (fase de recuperação) com parceiros comerciais, a partir do contexto em que estavam inseridos (indicação de médico de especialidade específica), percebe-se a transformação de dados pessoais em dados pessoais sensíveis, posto que os dados foram processados para fins de promoção de produtos relacionados à saúde e, portanto, o consentimento explícito deveria ter sido exigido.

5.3.3 O caso Camedi srl Medical Center

A Autoridade de Proteção de Dados italiana impôs uma multa de 10.000 euros ao Camedi srl Medical Center. Nesse caso, um usuário apresentou queixa à Autoridade de Proteção de Dados porque recebeu faturas e lembretes de consultas de outro paciente com o mesmo nome que o seu. Em pesquisas realizadas, o usuário descobriu que o centro médico estava cuidando de um paciente com o seu mesmo nome e que tudo o que diz respeito aos seus serviços era comunicado por meio de mensagens, sendo, ainda, emitidas faturas atribuídas ao seu código fiscal.

Em defesa, o centro médico afirmou que as faturas não continham dados relativos ao estado de saúde do terceiro. A Autoridade, no entanto, entendeu que “a prestação de um serviço de saúde referente a uma pessoa especificamente indicada constitui informação atribuível à noção de dado de saúde (...)”[33].

Nesse sentido, ante ao serviço prestado pelo centro médico, mesmo que não tenha sido compartilhado (fase de recuperação) o estado clínico do paciente

---

[33] No original, *“l’avvenuta prestazione di un servizio di assistenza sanitaria riferita ad una persona specificatamente indicata costituisce un’informazione riconducibile alla nozione di dato sulla salut (...)”*

internado, a partir do contexto em que o paciente estava inserido, foi possível a coleta de dados de saúde por parte do indivíduo que recebia as notificações.

5.3.4 O caso Grindr

A Autoridade de Proteção de Dados norueguesa multou a Grindr LLC em 6,3 milhões de euros. O Grindr é um aplicativo de relacionamento baseado em localização projetado para pessoas LGBTQIAPN+. Em 2020, a Autoridade Norueguesa de Proteção ao Consumidor (*Norwegian Consumer Council* - NCC), apresentou à Autoridade de Proteção de Dados uma queixa contra o Grindr, afirmando que a aplicação havia compartilhado informações (fase de recuperação) sobre a localização GPS dos usuários, endereço IP, ID de publicidade do telefone celular, idade e sexo (dados pessoais) com vários terceiros para fins de *marketing*, que coletaram esses dados, a partir do compartilhamento feito pelo Grindr e não diretamente dos usuários.

De acordo com o GDPR, é necessário consentimento para o compartilhamento desses dados pessoais com parceiros comerciais. No entanto, durante a sua investigação, a Autoridade concluiu que o consentimento recolhido pelo Grindr não era válido, pois os usuários eram obrigados a aceitar a política de privacidade para usar a aplicação, não sendo livres para a escolha do compartilhamento. Além disso, a Autoridade entendeu que os usuários não foram explicitamente questionados se consentiam que seus dados fossem compartilhados com terceiros para fins de *marketing*. Além disso, as informações sobre a divulgação de dados pessoais não eram suficientemente claras ou acessíveis aos utilizadores.

Apesar de não estar listado como dados compartilhados oficialmente, a Autoridade entendeu, ainda, que dados pessoais sensíveis estavam sendo compartilhados (fase de recuperação) pelo Grindr (detentor 1) com parceiros comerciais (detentores n), posto que o contexto em que os usuários estavam inseridos, qual seja, usuários de um aplicativo especificamente voltado às pessoas LGBTQIAPN+, poderia-se inferir que esses indivíduos como membro de uma minoria sexual.

A Autoridade considerou a infração um caso particularmente grave que justifica uma multa dissuasiva elevada. Os modelos de negócios baseados no *marketing* de comportamento são difundidos na economia digital, tornando

importante que as multas por violações do GDPR sejam dissuasoras, segundo a Autoridade.

5.4 A transformação de dados pessoais em dados pessoais sensíveis a partir de dados comportamentais e de consumo

Os dados pessoais também podem ser transformados em dados sensíveis, a partir de dados pessoais relacionados ao comportamento ou aos produtos consumidos pelo usuário. Em teoria, o registro (fase de coleta) de dados relacionados ao comportamento ou ao consumo dos usuários, são pessoais. Contudo, o compartilhamento (fase de recuperação) de tais pode ensejar em dados de natureza sensível, mesmo que não tenha ocorrido a coleta de dados pessoais sensíveis de forma direta, senão vejamos:

5.4.1 O caso Easylife

A Autoridade de Proteção de Dados do Reino Unido aplicou uma multa de 1.547.000 euros à Easylife Ltd. A Easylife é uma rede de lojas que vende utensílios domésticos, bem como produtos diversos, como saúde, motor, supercard e jardinagem e clubes de fidelidade. Durante a investigação, a Autoridade percebeu que, ao adquirir determinados produtos (dados pessoais de consumo coletados), a empresa fazia suposições sobre o estado de saúde do cliente (fase de recuperação com dados pessoais sensíveis), sendo então oferecidos ao cliente outros produtos para compra por telefone ou SMS relacionados ao seu estado de saúde. Dos 122 produtos do catálogo do *Health Club* da Easylife, 80 itens foram classificados como 'produtos desencadeadores'.

Após a compra dos produtos, a Easlylife criou um perfil deles para direcioná-los a um item relacionado à saúde. Durante a sua investigação, a Autoridade descobriu que a empresa recolheu e utilizou dados pessoais de um total de mais de 140.000 titulares de dados sem o seu consentimento ou mesmo conhecimento deles. A Autoridade concluiu que este tratamento “invisível” dos dados pessoais constituía uma violação grave dos direitos dos titulares dos dados, uma vez que estes não foram capazes de exercer os seus direitos de privacidade e proteção de dados devido à falta de conhecimento do tratamento.

Além disso, a empresa fez 1.345.732 ligações de *marketing* não solicitadas a indivíduos sem o seu consentimento para as ligações.

5.4.2 O caso Desinfolab

A Autoridade de Proteção de Dados belga multou a ONG EU DisinfoLab em 2.700 euros. Em 2018, a ONG publicou uma análise para identificar a possível origem política dos tweets que circulavam sobre um determinado caso polêmico, ocorrido na França, o “caso Benalla”. Para realizar a análise, a organização processou os dados de 55 mil contas do Twitter, das quais mais de 3.300 foram classificadas como políticas, isto é, dados pessoais sensíveis.

Os dados brutos obtidos foram então publicados sem tomar precauções mínimas de segurança, como pseudonimizar os dados. A Autoridade de Proteção de Dados observou que a publicação dos dados poderia potencialmente expor os titulares dos dados ao risco de discriminação ou descrédito devido ao perfil político não anonimizado. Além disso, os arquivos também continham informações sobre crenças religiosas, origem étnica ou orientação sexual dos indivíduos cujos relatos foram analisados.

Nesse sentido, ao compartilhar dados comportamentais, como as curtidas de uma rede social, o detentor 1 deixou exposto aos detentores n que puderam coletar dados pessoais sensíveis, qual seja, a opinião política dos usuários das redes sociais. Assim, foi possível inferir dados pessoais sensíveis, a partir do comportamento dos usuários em determinada rede social.

5.4.3 O caso Call Center Concentrix Cvg Italy srl

O sindicato UILCOM Sardegna apresentou queixa à Autoridade de Proteção de Dados italina contra a operadora de call center Concentrix Cvg Italy srl, a respeito de um regulamento interno do controlador.

A “política de mesa limpa” da empresa proibia os funcionários de manterem determinados itens, como smartphones, nas suas mesas, o que se destinava a garantir a confidencialidade no tratamento dos dados pessoais dos clientes. Contudo, foram abertas exceções para medicamentos que os funcionários comprovaram necessitar tomar durante o seu turno de trabalho. Estes deviam ser colocados de forma visível sobre a secretária, possibilitando indiretamente a outros

funcionários a obtenção de informações sobre o estado de saúde dos titulares dos dados.

O caso em questão, apesar de também ser um exemplo de indícios de transformação de dados pessoais em dados pessoais sensíveis, uma vez que era possível inferir dados pessoais sensíveis de saúde, não deverá ser computado na presente pesquisa, por não envolver aplicações ou sítios eletrônicos.

5.5 Indícios de transformação de dados pessoais em sensíveis

A partir do levantamento das sanções estabelecidas pelas Autoridades de Proteção de Dados europeias, no sítio eletrônico é possível sintetizar os casos que apresentam indícios de transformação de dados pessoais em dados pessoais sensíveis, conforme o Quadro 6, senão vejamos:

Quadro 6 - Síntese de indícios de transformação de dados pessoais em sensíveis.

Caso	País	Ano	Dados coletados	Dados transformados
Senseonics Inc	Itália	2022	E-mail	Dados de saúde
Hospital San Raffaele srl	Itália	2022	E-mail	Dados de saúde
Azienda Ospedale-Università Padova	Itália	2023	E-mail	Dados de saúde
Escola Isabella Gonzaga	Itália	2022	Dados de Identificação	Dados de saúde
Escola Edoardo Amaldi	Itália	2022	Dados de Identificação	Dados de saúde
Istituto Comprensivo - IC Cosenza III “V. Negroni”	Itália	2021	Nome	Dados de saúde
Miropass Srl	Itália	2020	Nome, apelido, código fiscal, número de telefone e endereço de e-mail	Dados de saúde
Médico particular	Itália	2021	Nome e telefone	Dados de saúde
Camedi srl Medical Center	Itália	2023	Nome e dados de consumo	Dados de saúde
Grindr	Noruega	2021	Localização GPS dos usuários, endereço IP, ID de publicidade do telefone celular, idade e sexo	Dados referente à vida sexual
Easylife	Reino Unido	2022	Dados de consumo	Dados de saúde
Desinfolab	Bélgica	2023	Curtidas em redes sociais	Opinião política

Fonte: Elaborado pela autora.

A partir dos casos levantados e os estudos do Ciclo de Vida dos Dados, é possível averiguar 12 (doze) casos que apresentam indícios de que dados pessoais foram coletados por detentores 1, mas foram transformados em dados pessoais sensíveis, oportunidade em que outros detentores coletaram dados pessoais sensíveis que, em tese, não foram coletados diretamente do usuário, pelo detentor 1.

Nos casos Senseonics Inc, Hospital San Raffaele srl e Azienda Ospedale-Università Padova, provavelmente, uma série de dados foram coletados diretamente dos indivíduos por esses detentores, sendo armazenados em banco de dados. Contudo, ao permitirem que os endereços de e-mail desses indivíduos estivessem públicos (fase de recuperação), somado ao contexto em que esses e-mails foram enviados, qual seja, por entidades de saúde, foi possível que os novos detentores coletassem (fase de coleta) dados pessoais sensíveis, pois foi possível a inferir que os indivíduos que estavam na lista de e-mails tinham determinado quadro clínico. Repisa-se: nenhum dado de saúde foi diretamente exposto, uma vez que apenas os endereços de e-mail foram visíveis, mas os novos detentores dos dados conseguiram fazer suposições, ante o contexto em que o e-mail foi enviado, isto é, a partir da interferência do fator integração.

O caso do médico particular é bem semelhante, posto que os dados compartilhados com os parceiros comerciais eram dados de contato. Contudo, no contexto em que esse indivíduo estava inserido, qual seja, paciente de médico de determinada especialidade, é possível inferir que dados pessoais sensíveis relacionados à saúde do paciente.

O caso da Escola Isabella Gonzaga, Escola Edoardo Amaldi e Istituto Comprensivo - IC Cosenza III “V. Negroni”, foram expostos (fase de recuperação) apenas dados de identificação, como nome dos professores, em uma plataforma online. Contudo, o fato de identificar os professores que recebiam benefícios previdenciários, mesmo que não expondo diretamente o motivo, é possível considerar que dados de saúde também foram expostos. Assim, dados pessoais foram disponibilizados (fase de recuperação) a novos detentores, mas que a partir do contexto que esses usuários estavam inseridos, enquanto beneficiários previdenciários, foi possível inferir que essas pessoas estavam vivenciando questões de saúde.

A aplicação Miropass coletava uma série de dados pessoais dos usuários. Contudo, a aplicação também tinha acesso a dados pessoais sensíveis que, apesar de não serem coletados diretamente dos usuários, também estavam na base de dados dessa aplicação. Ao marcarem determinados tipos de consultas, a aplicação poderia integrar com outras bases de dados, fazendo inferências de que os usuários teriam determinado estado clínico, a partir das consultas marcadas. Nesse sentido, dados pessoais sensíveis eram coletados, mesmo que indiretamente.

No caso da aplicação Camedi, os dados pessoais compartilhados (fase de recuperação) estavam relacionados a dados de identificação e dados de consumo. Contudo, a partir do serviço prestado pelo detentor, mesmo que a aplicação tenha recuperado apenas dados pessoais, o novo detentor, que passou a receber os dados pessoais, pode pressupor dados pessoais de saúde, mesmo que nenhum dado de saúde tenha sido exposto diretamente.

Os casos Grindr, Easylife e Desinfolab são os mais complexos. No caso do Grindr, uma série de dados pessoais de seus usuários foram compartilhados com parceiros comerciais sem a devida anuência desses usuários. Contudo, mesmo que apenas um único dado pessoal fosse compartilhado (fase de recuperação), ainda sim haveria a transformação de dados pessoais em dados pessoais sensíveis.

A origem da coleta dos dados compartilhados com os parceiros comerciais (fase de coleta) foi o detentor 1, qual seja, o Grindr, uma aplicação com serviço específico, qual seja, aproximação e relacionamento entre pessoas LGBTQIAPN+. Ao coletar esses dados, os parceiros comerciais (detentores n) também estavam coletando dados pessoais sensíveis, no caso a orientação sexual desses usuários, mesmo que esses dados não tenham sido compartilhados diretamente.

A Easylife e a Desinfolab usaram mecanismos semelhantes, apesar de visar finalidades diferentes. Em ambos os casos, as entidades perceberam o consumo dos usuários, seja em forma de produtos (Easylife), seja em forma de curtidas (redes sociais) que, em princípio, não eram dados pessoais sensíveis. Contudo, ao integrarem os dados pessoais, ambos puderam inferir dados pessoais sensíveis. No caso da Desinfolab, a rede social disponibiliza de forma pública (fase de recuperação) as interações dos usuários ao utilizarem a rede social, como comentários e curtidas. Nesse sentido, foi possível classificar determinadas contas como políticas, a partir da integração das interações, sendo coletados dados

pessoais sensíveis, em decorrência de curtidas e comentários que, em tese, não pertencem a essa categoria.

Por fim, foi possível concluir que as Autoridades de Proteção de Dados europeias têm se preocupado em punir entidades que não cumprem devidamente a legislação relacionada a dados pessoais sensíveis de saúde. Nesse cenário, o objetivo geral do presente estudo foi alcançado, pois das 129 (cento e vinte nove) decisões avaliadas, observou-se que 12 (doze) casos em que houve indícios de transformação de dados pessoais em dados pessoais sensíveis, sendo 10 (dez) desses casos estavam relacionados a dados de saúde.

6 CONSIDERAÇÕES FINAIS

O levantamento histórico, a partir de gerações de leis de proteção de dados pessoais, permite a percepção de que a definição de dados pessoais não foi muito alterada ao longo dos anos. Conforme explanado na seção 2, as legislações pertinentes ao assunto, contudo, tiveram um alargamento de sua abrangência de atuação, visto que tiveram como preocupação inicial a criação e controle de banco de dados pelos governos e Estados, passando a focar no tratamento de dados por entes e organizações de natureza privada, que passaram a ter seus próprios banco de dados com o avanço da tecnologia da informação.

Além disso, as legislações tiveram uma mudança de foco, preocupando-se com a efetiva participação do cidadão, seja pelo seu consentimento, seja por sua ciência, que de forma acessível deve atingir a sua autodeterminação informativa.

Apesar das legislações não utilizarem o termo informação de forma técnica, colocando-a como sinônimo de dado, é importante entender que as legislações protetivas de dados se preocupam com a eventual identificação de uma pessoa física, a partir do tratamento de dados. Os legisladores, portanto, têm se preocupado com a diferenciação entre dados pessoais e sensíveis, que são uma subcategoria de dados pessoais capazes de causar discriminação aos usuários, e, a partir disso, as legislações conferem maior proteção aos dados de natureza sensível, posto que o tratamento desses dados podem gerar discriminação aos seus titulares e danos relevantes.

A maior preocupação da legislação é evitar o tratamento discriminatório, que está expresso na LGPD, artigo 6º, inciso IX, como a “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos” (Brasil, 2018). Ante o

potencial lesivo do tratamento de dados pessoais sensíveis, operações que envolvam essa categoria de dados, seja por entes privados ou públicos, pode ensejar em flagrante discriminação aos indivíduos (Mulholland, 2021).

Nesse sentido, a partir das explanações trazidas na seção 2, o primeiro objetivo específico da presente pesquisa foi alcançado, qual seja, identificar aspectos relacionados a dados pessoais e dados pessoais sensíveis.

Em decorrência do tratamento massivo de dados pessoais, foi necessário a promulgação das legislações de proteção de dados pessoais que trouxeram requisitos para que os atores envolvidos no processo de tratamento de dados pessoais e dados pessoais sensíveis pudessem seguir. Nesse cenário, a seção 3 alcançou o segundo objetivo específico do presente trabalho, uma vez que indicou os requisitos legais envolvidos no tratamento de dados, tais como os princípios arrolados e hipóteses legais de tratamento.

Além disso, a seção 3 também foi responsável pelo êxito do terceiro objetivo específico, qual seja, estudar o papel das Autoridades de Proteção de Dados em caso de descumprimento dos requisitos legais, uma vez que descreveu-se o papel exercidos pelas Autoridades de Proteção de dados, tanto europeias, quanto latino americanas, em especial a brasileira, a fim de destacar suas principais atribuições, sobretudo a aplicação de sanções para os casos em que entidades, públicas ou privadas, não cumprem os requisitos determinados pelas respectivas leis de proteção de dados.

Em decorrência do tipo de informação que podem gerar, os dados sensíveis apresentam maior potencial de causar danos relevantes, como discriminação ou outras consequências negativas ao indivíduo. Ciente do potencial lesivo, às legislações protetivas de dados, em geral, apresentam mecanismos restritivos para o tratamento de dados sensíveis, conforme expresso na seção 3 e relacionado no segundo objetivo específico.

No caso da legislação brasileira, por exemplo, ao contrário de dados apenas pessoais, o tratamento de dados sensíveis não pode ser realizado com base no legítimo interesse dos detentores, isto é, dados sensíveis não podem ser utilizados para fins de promoção da atividade empresarial, cabendo às Autoridades de Proteção de Dados a devida punição, conforme destacado na seção 3 e relacionado ao terceiro objetivo específico.

O avanço da TIC permitiu que os dados pessoais coletados sejam integrados em diversas bases de dados, tornando possíveis inferências sobre os indivíduos, conforme abordado na seção 4. Dessa forma, mesmo que um dado coletado por determinado detentor não pertença à subcategoria de dados pessoais sensíveis, sendo, em sua gênese, um dado pessoal, a partir do cruzamento ou inferências dos dados coletados pode ser transformado para dado sensível (BIONI, 2020).

Assim, o quarto objetivo específico, qual seja, descrever o papel do fator integração na fase de coleta de dados, foi alcançado a partir dos estudos expressados na seção 4. Conforme estudado, o fator integração pode, por exemplo, permitir a formação de perfis que contenham dados pessoais sensíveis, o que pode ensejar na discriminação ou exclusões indejadas dos indivíduos,

> (…) seja porque dados pessoais, aparentemente não “sensíveis”, podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas (Rodotà, 2008, p. 56).

Rodotà (2008), contudo, alertou que os dados pessoais sensíveis, sobretudo os relacionados à vida sexual e a opinião política, não devem, necessariamente, ser mantidos na intimidade do indivíduo. Ao contrário, devem poder ser expressados livremente, em público, oferecendo a cada um de nós o direito de participação da vida civil e política.

A LGPD, considerando a real possibilidade de transformação de dados pessoais em dados pessoais sensíveis, pois, em seu parágrafo primeiro, do artigo 11, afirma que será aplicado o regime jurídico específico conferido aos dados sensíveis para o tratamento de dados pessoais que seja capaz de revelar dados pessoais sensíveis e que possa causar dano ao titular, mesmo que não tenha sido coletado dados pessoais sensíveis diretamente (Negri; Korkmaz, 2019), isto é, mesmo que tenha ocorrido a interferência do fator integração e, consequentemente, dados pessoais sensíveis tenham sido coletados indiretamente, a partir da coleta direta de dados pessoais.

Assim, a tutela mais robusta aos dados pessoais sensíveis não está relacionada ao direito de “esconder” essas informações, mas sim ao direito de autodeterminação informativa, isto é, do próprio titular exercer o direito de tornar essas informações públicas no tempo que desejar e a quem desejar.

Cohen (2000) destaca que o tratamento inadequado de dados pessoais sensíveis, especialmente sem a ciência do indivíduo, pode gerar a discriminação e segregação abusiva. Nesse sentido,

> os dados dos consumidores podem ser utilizados para muitos fins com os quais os consumidores podem não concordar tão alegremente: decisões de emprego e classificações por parte dos prestadores de seguros de saúde que excluem ou prejudicam os "pobres" genéticos ou médicos; decisões de emprego ou habitação baseadas em riscos de personalidade percebidos; decisões de emprego ou habitação baseadas em preferências sexuais ou religiosas; e assim por diante (Cohen, 2000, p. 27, tradução livre)[34].

O quinto objetivo específico, qual seja, analisar casos em que organizações foram punidas por Autoridades de Proteção de Dados por tratar dados pessoais sensíveis sem os requisitos legais necessários, foi alcançado a partir do levantamento das sanções aplicadas pelas Autoridades de Proteção de Dados europeias, compiladas na seção 5.

Assim, o objetivo geral do presente trabalho foi alcançado, uma vez que apurou-se que de 129 (cento e vinte e nove) decisões de Autoridades de Proteção de Dados europeias, relacionadas ao artigo 9º do GDPR, disponibilizadas pelo sítio eletrônico *Enforcement Tracker,* 12 (doze) casos apresentaram indícios de que dados pessoais, coletados por aplicações ou sítios eletrônicos, foram transformados em dados pessoais sensíveis, a partir da interferência do fator integração.

Ante todo o exposto, o presente trabalhou buscou demonstrar indícios de transformação de dados pessoais em dados pessoais sensíveis, a partir do fator integração, o que ficou comprovado com a avaliação das sanções aplicadas pelas Autoridades de Proteção de Dados europeias. As Autoridades em questão já têm reconhecido a complexidade do ciclo de vida dos dados coletados por detentores, uma vez que, em decorrência da integração de bases de dados, é possível que novos dados surjam.

Assim, é possível também observar a relação do presente estudo com a ODS 16.10, uma vez que pretendeu-se contribuir com o acesso público à informação, visando garantir aos cidadãos, especialmente os usuários de aplicações

---

[34] No original "*consumer data can be used for many purposes to which consumers might not so blithely agree: employment decisions and classifications by health insurance providers that exclude or disadvantage genetic or medical "have- -nots"; employment or housing decisions based on perceived personality risks; employment or housing decisions based on sexual or religious preferences; and so on*" (COHEN, 2000, p. 27).

e sítios eletrônicos, o conhecimento de que os detentores de dados podem coletar mais dados dos que àqueles diretamente solicitados aos usuários.

A CI, enquanto área do conhecimento responsável pelo estudo da informação, pode, portanto, contribuir para que os usuários tenham acesso a como seus dados são tratados pelos detentores de dados. Nesse sentido, pesquisadores da CI também podem realizar estudos futuros que estejam focados no impacto que a coleta indireta de dados pessoais sensíveis pode causar, por exemplo, a privacidade do indivíduo, bem como o nível de conhecimento dos usuários sobre o processo de compartilhamento de dados entre os detentores.

REFERÊNCIAS

AFFONSO, E. P.; MONTEIRO, E. C. S. A.; CAMARGO, F. B. Aplicativos móveis na agricultura e as implicações nas questões de privacidade. *In*: ENCONTRO COMPETÊNCIAS DIGITAIS PARA AGRICULTURA FAMILIAR, 3., 2016, Tupã. **Anais** [...] Tupã: CoDAF, 2016.

AFFONSO, E. P.; OLIVEIRA, S. C.; SANT'ANA, R. C. G. Análise do equilíbrio entre privacidade e utilidade no acesso a dados. **Informação & Sociedade**,v. 27, n. 1, 2017. Disponível em: https://periodicos.ufpb.br/ojs/index.php/ies/article/view/29422. Acesso em: 05 jun. 2023.

AFFONSO, E. P.; SANT'ANA, R. C. G. Preservação da privacidade no acesso a dados por meio do modelo k-anonimato. **Ponto de Acesso**, v. 11, n. 1, 2017. Disponível em: https://periodicos.ufba.br/index.php/revistaici/article/view/13754. Acesso em: 18 fev. 2024.

AFFONSO, E. P. **A insciência do usuário na fase de coleta de dados**: privacidade em foco. 2018. Tese (Doutorado em Ciência da Informação) - Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2018. Disponível em: https://repositorio.unesp.br/handle/11449/154737. Acesso em 16 set. 2023.

ALBRECHT, R. F.; OHIRA, M. L. B.; OHIRA, M. L. B. Bases de dados: metodologia para seleção e coleta de documentos. **Revista ACB**: Biblioteconomia em Santa Catarina, v. 5, n. 5, p. 131-144, 2000. Disponível em: http://hdl.handle.net/20.500.11959/brapci/71931. Acesso em: 29 set. 2023.

ALEMANHA. Lei Hessisches Datenschutzgesetz de 7 de outubro de 1970. Dispõe sobre a lei de dados no estado alemão. 1970.

ANPD. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 18 jan. 2024.

AUSTRÁLIA, **Privacy Act**, de 1 de janeiro de 1988. Disponível em: https://www.legislation.gov.au/Details/C2021C00139. Acesso em 02 de fev. 2023.

ARGENTINA. **Ley 25.326, de 4 de outubro de 2000**. 2000. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf. Acesso em 02 de fev. 2023.

BAGATINI, J. A.; GUIMARÃES, J. A. G.; SANT'ANA, R. C. G. Gerenciamento dos dados pessoais em arquivos: uma perspectiva centrada no indivíduo com base na LGPD. **Acervo**, v. 34, n. 3, p. 1–20, 2021. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/1749. Acesso em: 1 fev. 2023.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70; 2011.

BENNETT, C.; RAAB, C. **The governance of privacy**: policy Instruments in Global Perspective. MIT: press, 2014.

BERGSTRÖM, A. **Online privacy concerns**: a broad approach to understanding the concerns of different groups for different uses. Computers in Human Behaviour, v. 53, p. 419-426, 2015.

BIONE, B. R. Inovar pela Lei. **FGV Executivo**. Fundação Getúlio Vargas, v. 18, n. 4, jul/ago, 2019. Disponível em: https://periodicos.fgv.br/gvexecutivo/article/view/79978/76432. Acesso em: 18 jan. 2024.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

BIONI, B. R. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 191-201, jan./mar. 2020. Disponível em: ii_9_anonimização_e_dado.pdf (tjsp.jus.br). Acesso em: 23 jan. 2023.

BIONI, B. R.; SILVA, P. G. F; MARTINS, P. B. L. Interseções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Coletânea de Artigos da Pós-graduação em Ouvidoria Pública**, v.1, 2022. Disponível https://revista.cgu.gov.br/Cadernos_CGU/article/view/504. Acesso em: 11 fev. 2023.

BOBBIO, N. **Teoria do ordenamento jurídico**. 2 ed. São Paulo: EDIPRO, 2014.

BOISOT, M.H. **Knowledge Assets**. Oxford University Press, Oxford, 1998.

BORKO, H. **Information Science**: what is it? American Documentation, Washington, v. 19, p. 3-5, 1968.

BRAITHWAITE, J. **The Essence of Responsive Regulation**. U.B.C. Law. Review, v. 44, 2011.

BRANDÃO, W. C. A internet como fonte de informações para negócio: um ensaio sobre a realidade da internet brasileira. **Perspectivas em Ciência da Informação**, v. 9, n. 1, 2004. Disponível em: http://hdl.handle.net/20.500.11959/brapci/35198. Acesso em: 25 set. 2023.

BRANDT, M. B.; VIDOTTI, S. A. B. G. Metadados de negócio: representação da informação dos processos de trabalho. **Transinformação**, v. 31, 2019. DOI: 10.1590/2318-0889201931e180006 Acesso em: 15 out. 2023.

BRASIL. **Constituição da República Federativa do Brasil,** 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 fev. 2023.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 02 fev. 2023.

CASTELLS, M. **A sociedade em rede**. 22ª ed. São Paulo: Paz e Terra, 2020.

CARINGELLA, F.; GAROFOLI, R. **Le autoritá indipendenti**. Napoli: Simoni, 2000.

CHOWDHURY, G. G.; CHOWDHURY, S. The semantic web. *In:* **Organizing information from the self to the web**. London: Facet Publishing, 2007. p. 111-129.

CIANCONI, R. Banco de Dados de acesso público. **Ciência da Informação**. Brasília, v. 16, n. J, p. 53-59,jan./jun. 1987.

COUNCIL of Europe. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,** ETS nº 108, 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=10.

COHEN, J. **Examined lives**: informational privacy and the subject as object. Stan. L. Rev. 2000.

CUNHA, M. B.; CAVALCANTI, C. R. O. **Dicionário de Biblioteconomia e Arquivologia**. Brasília, DF: Briquet de Lemos/Livros, 2008.

DE LUCCA, N. Marco Civil da Internet: uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. *In*: DE LUCCA, N. SIMÃO FILHO, A; LIMA, C. R. P. (org.). **Direito e Internet III**: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

DENZIN, N. K. Triangulation in educational research. *In*: KEEVES, J. P. (Ed.). **Educational research, methodology, and measurement**: an international handbook. Oxford: Pergamon Press, 1988.

DIAS, P. C.; MARTINS, D. O.; OLIVEIRA, H. M. Breves reflexões sobre o conceito de controlador e operador de dados em atos normativos do Poder Judiciário e do Ministério Público. **Revista CNJ**, Brasília, v. 6, n. 1, 2022. DOI: 10.54829/revistacnj.v6i1.269.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DWORKIN, R. **Levando os direitos a sério**. São Paulo: Martins Fontes, 2002.

ENAP. Escola Nacional de Administração Pública. **Governança de dados** [curso online]. Brasília, 2019. Disponível em: https://www.escolavirtual.gov.br/curso/270. Acesso em: 12 out. 2023.

ENFORCEMENT Tracker. GDPR Enforcement Tracker. 2023.Disponível em: https://www.enforcementtracker.com. Acesso em: 15 jan. 2024.

EUA. **Privacy Act Of 1974** (Lei de Privacidade de 1974). Disponível em: https://www.justice.gov/opcl/privacy-act-1974. Acesso em: 02 jun. 2023.

EUA. **Children's Online Privacy Protection Rule.** 1998. Disponível em: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312. Acesso em: 02 jun. 2023.

EUA. **Health Insurance Portability Accountability Act**. 1996. Disponível em: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996. Acesso em: 02 jun. 2023.

EUROPEAN Parliament. Council of the European Union. Regulation (EU) 2016-679. Brussel, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 02 jun. 2023.

FERRAZ JÚNIOR, T. S. **Introdução ao estudo do direito**. São Paulo: Atlas, 1988.

FIGARO, R. A triangulação metodológica em pesquisas sobre a comunicação no mundo do trabalho. Fronteiras - **Estudos Midiáticos**, v. 16, n. 2, p. 124-131, 2014.

FORBRUKERRÅDET. **Out of control: how consumers are exploited by the online advertising industry.** The Consumer Council of Norway. 2020. Disponível em: https://www.conpolicy.de/en/news-detail/out-of-control-how-consumers-are-exploited-by-the-online-advertising-industry. Acesso em: 18 jan. 2024.

FLORIDI, L. The ontological interpretation of informational privacy. **Ethics and Information Technology**, v. 7, n. 4, p. 185-200, 2005.

FLUMIGNAN, S. J. G. ; FLUMIGNAN, W. G. G. (2020). Princípios que regem o tratamento de dados no Brasil. LIMA, C. R. P.(Coord). *In:* **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina.

FRANÇA. **La Loi Informatique et Libertés**, de 06 de janeiro de 1978. Disponível em: https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006528061/2004-08-07. Acesso em: 02 jun.2023.

FORESTI, F.; VARVAKIS, G.; VIERA, A. F. G. A importância do contexto na ciência da informação. **Biblios** , p. 1-21, . DOI: 10.5195/biblios.2018.383 Acesso em: 02 nov. 2023.

GAMIZ, M. S. F. **Privacidade e intimidade**: doutrina e jurisprudência. Curitiba:Juruá, 2012.

GIL, A. C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2008.

GHISLENI , J. Z. GDPR and the risk-based approach to corporate governance: the first measure for the controller to apply the principles. **Revista de Economia, Empresas e Empreendedores na CPLP**, v. 8, n. 1, p. 103–126, 2022. DOI: 10.29073/e3.v8i1.618. Disponível em: https://revistas.ponteditora.org/index.php/e3/article/view/618. Acesso em: 16 oct. 2022.

GREENLEAF, G. Global data privacy 2019: DPAs, PEAs, and their networks (March 30, 2019). Privacy Laws & Business International Report, UNSW Law Research Paper, 2019.

GUINCHAT, C.; MENOU. **Introdução geral às ciências e técnicas da informação e documentação**. Brasília: MCT/CNPq/IBICT, 1994.

HEEMANN, V. **Avaliação ergonômica de interfaces de bases de dados por meio de "checklist" especializado**. Florianópolis, 1997. Dissertação (Mestrado em Engenharia de Produção) - Universidade Federal de Santa Catarina.

HIJMANS, H. **The European Union as Guardian of Internet Privacy**: the Story of Art 16 TFEU. Springer, 2016.

HOFFMANN-RIEM,W. Der grundrechtliche Schutz der Vertraulichkeit und Integritãt eigengenutzter informationstechnischer Systeme. In: **JuristenZeitung,** 21, p. 1010, 2008.

HOUAISS. A. **Dicionário de Língua Portuguesa**. 2001. Disponível em: https://houaiss.uol.com.br/corporativo/apps/uol_www/v6-1/html/index.php. Acesso em: 21 jan. 2024.

JÓRI, A. **Shaping vs. Applying Data Protection Law**: two core functions of data protection authorities. international data privacy law, 2015.

KURITZKES, J. **Finding the Line**: the relationship between privacy and smartphone applications, 2019. Disponível em: https://assets.pubpub.org/oqqhkwq5/11661437032683.pdf. Acesso em: 02 jun. 2023.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação com Internet**. 4.ed. Rio de Janeiro: LTC, 1999.

LE COADIC, Y. F. **A ciência da informação**. 2. ed. Brasília: Briquet de Lemos Livros, 2004.

LEHUEDÉ, H. **Corporate governance and data protection in Latin America and the Caribbean**, Production Development series, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2019.

LEONARDI, M. Controladores e operadores: papéis, distinções, mitos e equívocos. In: FRANCOSKI, D. S.; TASSO, F. A. (coord). **A Lei Geral de Proteção de Dados Pessoais LGPD** : aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Thomson Reuters Brasil, 2019.

LESSIG, L. **Code**: and other laws of Cyberspace 2.0. New York: Basic Books, 2006.

LIMA; T. C. S; MIOTO, R. C. T. Procedimento Metodológico na Construção do Conhecimento Científico: a pesquisa bibliográfica. **Rev. katálysis**, n. 10, p. 37-45, 2007.

LLOYD, I. J. **Information Technology Law.** Oxford University Press, 2011.

LUGATI, L. N.; ALMEIDA, J. E. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, Viçosa, v. 12, n. 2, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 29 jun. 2023.

MACHADO, J.; BIONI, B. R. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do "Nota Fiscal paulista". **Liinc em Revista**, v. 12, n. 2,

2016. DOI: 10.18617/liinc.v12i2.919. Disponível em: https://revista.ibict.br/liinc/article/view/3734. Acesso em: 23 set. 2023.

MALDONADO, V. B. (coord.). **LGPD**: Lei Geral de Proteção de Dados Pessoais. Manual de Implementação. São Paulo: Thomson Reuters Brasil, 2019.

MASON, R. O. **Four ethical issues of the information age**. MIS Quarterly, v. 10, n. 1, p. 5-12, 1986.

MAYER-SCÖNBERGER, V. General development of data protection in Europe. *In*: AGRE, P.; ROTENBERG, M. (orgs.). **Technology and privacy**: The new landscape. Cambridge: MIT Press, 1997.

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

MILAGRE, J. A. M. **A Blockchain como contributo à transparência e auditoria nos processos de compartilhamento de dados**. 2020. 188 f. Tese (Doutorado em Ciência da Informação) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2021.

MONTEIRO, E. C. S. A.; SEGUNDO, J. E. S.; SANT'ANA, R. C. G. E-science semântica: integração dos dados na comunicação científica. **Informação em Pauta**, v. 1, n. 1, p. 9-29, 2016. Disponível em: http://hdl.handle.net/20.500.11959/brapci/41220. Acesso em: 23 set. 2023.

MULHOLLAND, C. Dados Pessoais Sensíveis E A Tutela De Direitos Fundamentais: Uma Análise À Luz Da Lei Geral De Proteção De Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, 2018. DOI: 10.18759/rdgf.v19i3.1603. Acesso em: 14 jul. 2023.

MULHOLLAND, C. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)**. IBERC, 2021. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 29 jun. 2023.

SILVA, N.; NATHANSON, B. M. Análise da produção científica em inteligência artificial na área da ciência da informação no brasil. *In*: ENCONTRO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO (ENANCIB), 19, 2018. Marília. **Anais [...].** Disponível em: http://hdl.handle.net/20.500.11959/brapci/103730. Acesso em: 29 ago. 2023.

NEGRI, S. M. C. Á; KORKMAZ, M. R. D. C. R. A normatividade dos dados sensíveis na Lei Geral de Proteção de dados: ampliação conceitual e proteção da pessoa humana. **Rev. de Direito, Governança e Novas Tecnologias**, v. 5, n. 1, jan/jun. 2019.

NISSENBAUM, H. **Privacy in Context**: Technology, Policy, and the Integrity of Social Life. Palo Alto: Stanford University Press, 2010.

PACKARD, V. Don't tell it to the computer. **New York Times Magazine**, 8 jan. 1967.

PROSSER, W. L. **Privacy**. California Law Review, v. 48, p. 383,1960.

PASQUALE, F. **The black box society.** The secrets algorithms that control money and information. Cambridge: Harvard University Press, 2015.

REALE, M. **Filosofia do Direito**. 11. ed. São Paulo: Saraiva, 1986.

REIDENBERG, J. R. **Resolving Conflicting International Data Privacy Rules in Cyberspace**, Stanford Law Review, 1999.

RODOTÀ, S. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUN, C; KIM, H. J.; LEE, D. H; KIM ,C. G; KIM, K. J. Protecting Privacy Using K-anonymity with a Hybrid Search Scheme. **International Journal of Computer and Communication Engineering**, v.1, n. 2, jul. 2012. Disponível em: http://www.ijcce.org/papers/41-Z022.pdf, 2012. Acesso em: 10 jan de 2024.

SANT'ANA, R. C. G. Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. **Informação & Informação**, v. 21, n. 2, p. 116-142, 2016. DOI: 10.5433/1981-8920.2016v21n2p116. Acesso em: 25 set. 2022.

SANT'ANA, R. C. G. **Diagrama estrutural para teses e dissertações: uma proposta didática**. In: MOREIRA, F. M.; *et al.* (org.). Acesso a Dados e a Ciência da Informação: aplicação, tendências e reflexões. Tupã: Faculdade de Ciências e Engenharia UNESP – Campus de Tupã, 2022.

SANTOS, F. J. Você sabe no que consiste a regulação responsiva? *In:* SERPRO - Serviço Federal de Processamento de Dados. **Serpro.** Brasília, 18 ago 2023. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2023/atuacao-anpd. Acesso em: 18 fev. 2024.

SANTOS, P. L. V. A. C.; SANT'ANA, R. C. G. Transferência da informação: análise para valoração de unidades de conhecimento. **DataGramaZero:** Revista de Ciência da Informação, v. 3, n. 2, abr. 2002. Disponível em: https://cip.brapci.inf.br/download/44712. Acesso em: 25 jan. 2023.

SANTOS, P. L. V. A. C.; SANTANA, R. C. G. Dado e Granularidade na perspectiva da Informação e Tecnologia: uma interpretação pela Ciência da Informação. **Ciência da Informação**, v. 42, n. 2, 2015. DOI: 10.18225/ci.inf.v42i2.1382. Disponível em: https://revista.ibict.br/ciinf/article/view/1382. Acesso em: 12 fev. 2023.

SARACEVIC, T. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 1, n.1, p. 41-62, jan./jun., 1996. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/235. Acesso em: 5 jun. 2023.

SEGUNDO, J. E. S.; CONEGLIAN, C. S. Web semântica e ontologias: um estudo sobre construção de axiomas e uso de inferências. **Informação & Informação** , v. 21, n. 2, p. 217-244, 2016. DOI: 10.5433/1981-8920.2016v21n2p217. Acesso em: 22 out. 2023.

SEGUNDO, J. E. S. Web semântica: introdução a recuperação de dados usando sparql. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 15., 2014, Belo Horizonte. **Anais [...]** Belo Horizonte: UFMG, 2014. p. 3863-3882. Disponível em:

http://enancib2014.eci.ufmg.br/documentos/anais/anais-gt8. Acesso em: 21 de set. 2023.

SILVA, I. L. Introdução aos princípios jurídicos. **Revista de informação legislativa**, v. 40, n. 160, p. 269-289, out./dez. 2003.

SMITIS, S. **Reviewing Privacy in an Information Society**, 1987.

SOLOVE, D. J. **A Taxonomy of Privacy**. University Of Pennsylvania Law Review, v. 3, n. 154, 2006. Disponível em: http://doi.org/10.2307/40041279. Acesso em: 22 jan. 2024.

SOLOVE, D. J. **Understanding privacy**. Cambridge: Harvard University Press, 2008.

SOUZA, M.; ALMEIDA, F. G. O Comportamento do termo dado na Ciência da Informação. **Ciência da Informação em Revista**, v. 8, n. 2, p. 39–54, 2021. DOI: 10.28998/cirev.2021v8n2c. Disponível em: https://www.seer.ufal.br/index.php/cir/article/view/11764. Acesso em: 15 jun. 2023.

STJ. Supremo Tribunal de Justiça. **Recurso Especial nº 22.337/RS**, Brasília, ano 8, n. 77. 199-257, jan. 1996. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-eletronica-1996_77_capQuartaTurma.pdf. Acesso em: 18 jan. 2024.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

TANENBAUM, A. S.; WETHERALL, J. D. **Redes de computadores**. 5. ed. Rio de Janeiro: Pearson, 2011.

TEIXEIRA, T.; ARMELIM, R. M. G. F. (2020). Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC. *In:* LIMA, C. R. P. (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da lei n.13.853/2019. São Paulo: Almedina.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 24 out.1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046 . Acesso em: 5 jun. 2023.

URUGUAI. **Ley nº 18.331, de 18 de agosto de 2008.** Dispõe sobre a proteção de dados pessoais e ações de “habeas data”. Disponível em: http://www.oas.org/es/sla/ddi/docs. Acesso em 02 fev. 2023.

WARREN, S. D.; BRANDEIS, L. D. **The Right to Privacy**. Harvard Law Review, v. 6 n. 5, 1890.

WEF. World Economic Forum. **Personal data**: the emergence of a new asset class. Geneva: WEF, 2011. Disponível em:

http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf . Acesso em: 5 jun. 2023.

WESTIN, A. **Privacy and freedom.** New York: Athenaeum, 1967.

WIMMER, M. Autoridades de Proteção de Dados no mundo: Fundamentos e Evolução na Experiência Comparada. *In*: PALHARES, F. T**emas atuais de proteção de dados**. São Paulo: Revista dos Tribunais, 2022.

ZUBOFF, S. **The age of surveillance capitalism**. The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.