UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE CIÊNCIAS JURÍDICAS

FACULDADE DE DIREITO DO RECIFE

NÁDIA DE FRANÇA BORDONI

LEI GERAL DE PROTEÇÃO DE DADOS: uma reflexão sobre a proteção dos dados

RECIFE

2024

NÁDIA DE FRANÇA BORDONI

LEI GERAL DE PROTEÇÃO DE DADOS: uma reflexão sobre a proteção dos dados

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito para a obtenção do título de bacharel em Direito.

Área de Concentração: Direito Digital, Proteção de dados

Orientador(a): Prof. Leônio José Alves da Silva

RECIFE

2024

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Bordoni, Nádia de França.
Lei Geral de Proteção de Dados: uma reflexão sobre a proteção dos dados / Nádia de França Bordoni. - Recife, 2024.
44 p.

Orientador(a): Leônio José Alves da Silva
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, Direito - Bacharelado, 2024.

1. Direito Digital. 2. Proteção de dados. 3. Lei Geral de Proteção de Dados. 4. Dados sensíveis. I. da Silva, Leônio José Alves. (Orientação). II. Título.

340 CDD (22.ed.)

NÁDIA DE FRANÇA BORDONI

LEI GERAL DE PROTEÇÃO DE DADOS: uma reflexão sobre a proteção dos dados

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito para a obtenção do título de bacharel em Direito.

Aprovado em: 20/03/2024.

BANCA EXAMINADORA

_____
Profº. Dr. Leônio José Alves da Silva (Orientador)
Universidade Federal de Pernambuco

_____
Profº. Dr. Paulo Bandeira (Examinador Interno)
Universidade Federal de Pernambuco

_____
Profº. Dr. Daniel Meira (Examinador Interno)
Universidade Federal de Pernambuco

AGRADECIMENTOS

Aos meus amados pais, José Carlos e Maria Genalva, pelo amor, carinho e atenção que sempre me deram e pela oportunidade em formar-me no curso de Direito da Universidade Federal de Pernambuco;

À minha tia Jovina, pelo essencial apoio, incentivo e a quem dedico minha admiração;

Ao meu douto orientador, Leônio José Alves da Silva, pelas disponibilidade e orientações que permitiram a conclusão deste trabalho;

A Gabriel, pelo papel inestimável em minha vida;

A Lívea, Reginaldo, Dom, Bruno por participarem dessa trajetória e por terem me apoiado;

“– Não tenho nenhuma informação ainda. É um pecado capital teorizar antes de ter informações. Sem perceber, começa-se a distorcer os fatos para que caibam nas teorias (...)”

(Sir Arthur Conan Doyle, As aventuras de Sherlock Holmes: Um escândalo na boêmia e outras histórias)

RESUMO

Este trabalho tem como objetivo analisar a proteção de dados pessoais atual, introduzida pela Lei de Proteção de Dados brasileira (LGPD), e sugerir um novo fator determinante para a proteção de dados que não a categorização em dados pessoais sensíveis e não sensíveis. Partindo da evolução da proteção de dados dentro e fora do ordenamento brasileiro, foi possível perceber que tal categorização não foi criada com o Regulamento Geral sobre a Proteção de Dados (GDPR) e as leis dela derivadas; já existe há mais de 50 anos e consiste em destacar certas categorias de dados pessoais para proteção extra. No entanto, a partir de análises bibliográficas, se constata que separá-los em categorias é contraproducente; para serem realmente efetivas, as leis de privacidade deveriam ter uma proteção proporcional aos danos e riscos envolvidos na coleta, uso e transferência dos dados.

Palavras-chave: Proteção de dados pessoais; Dados sensíveis; Regulação por danos e riscos.

ABSTRACT

This work aims to analyze the current protection of personal data, introduced by the Brazilian Data Protection Law (LGPD), and suggest a new determining factor for the protection of personal data other than the categorization into sensitive and non-sensitive personal data. Based on the evolution of data protection within and outside the Brazilian system, it was possible to see that such categorization was not created with the General Data Protection Regulation (GDPR) and the laws derived from it; it has been around for over 50 years and consists of highlighting certain categories of personal data for extra protection. However, based on bibliographical analysis, it appears that separating them into categories is counterproductive; to be truly effective, privacy laws must have protection proportional to the damages and risks involved in the collection, use and transfer of data.

Keywords: Personal data protection; Sensitive data; Harm and risk regulation.

LISTA DE ABREVIAÇÕES

AIPD	Avaliação de Impacto Sobre a Proteção de Dados
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
EDPB	Comitê Europeu para a Proteção de Dados
GDPR	Regulamento Geral sobre a Proteção de Dados Europeia
LGPD	Lei Geral de Proteção de Dados Brasileira
VPPA	U.S Video Privacy Protection Act

SUMÁRIO

1 INTRODUÇÃO

Atualmente, vive-se no que se denomina Sociedade da Informação[1]. Tal termo tem como significado intrínseco que, no presente momento, faz-se possível registrar todos os atos da vida cotidiana e que a informação é elemento de influência no dia a dia face a sua possibilidade de manipulação e distorção.

Com a evolução tecnológica associada ao aprimoramento do tratamento de dados, a informação - e dá-se ênfase à informação sobre o indivíduo - tornou-se organizada e os bancos de dados multiplicaram-se ao redor do mundo, ensejando uma redefinição em relação aos poderes e direitos individuais, tal como sobre a própria pessoa. Isto porque as informações coletadas permitem o surgimento de novas concentrações de poder e, portanto, "os cidadãos têm o direito de pretender exercer um controle direto sobre aqueles sujeitos aos quais as informações fornecidas atribuíram um crescente *plus-poder"* (RODOTÀ, 2008, p.37)*;* pretensão que antes era desnecessária.

O conceito de Warren e Brandeis (1890), que definiu a privacidade como o "direito de ficar só", tornou-se obsoleto. Como se falar de direito à vida privada quando se tornou tão tênue a linha que separa o público e o privado? Como se sentir protegido quando passamos a ser a maneira como nossas informações são coletadas, definidas, classificadas e etiquetadas, de forma que a difusão das mesmas afeta diretamente, como um ato reflexo, nossa privacidade?

Surgiu a necessidade da evolução do conceito de privacidade, definido hoje como o direito de manter o controle sobre as próprias informações; assim como a necessidade de que o sistema jurídico evoluísse, pois, com o desdobramento da tutela dos direitos à privacidade, as informações pessoais encontrariam guarida nos ordenamentos jurídicos.

Com o tempo, percebeu-se que se fazia necessário leis que defendem com mais afinco os dados e a privacidade do indivíduo. A Lei Geral de Proteção de Dados Brasileira, LGPD, preocupa-se com o tratamento dos dados pessoais desses

---

[1] O termo foi amplamente divulgado por Castells (1999). Para o sociólogo, uma revolução tecnológica concentrada nas tecnologias da informação tem remodelado a sociedade em ritmo recorde. O informacionalismo, era pós capitalista em que encontra-se a sociedade, tem como fonte de produtividade a tecnologia de geração de conhecimento, de processamento de informações e de comunicação de símbolos. "O conhecimento e a informação tornaram-se elementos cruciais em todos os modos de desenvolvimento, visto que o processo produtivo sempre se baseia em algum grau de conhecimento e no processamento da informação." (CASTELLS, 1999, p. 35).

indivíduos, reconhecendo-os como vulneráveis em comparação com o controlador e o operador destes dados.

Com o objetivo de regular das atividades de tratamento[2], a Lei 13.709/18 categoriza e tutela de forma diferenciada os dados pessoais e os dados pessoais sensíveis. Assim, o presente estudo tem por objetivo geral demonstrar que tal categorização se apresenta contra produtiva, pois a natureza dos dados não aparenta ser o problema, mas, sim, a finalidade da sua utilização. Bem como, especificamente, apresentar, sob a perspectiva histórica, a evolução da proteção de dados pessoais, assim como verificar a diferença entre dados pessoais e dados pessoais sensíveis.

Apesar da temática de tratamento dos dados pessoais ser atual, o ordenamento brasileiro sempre apresentou interesse quanto ao tema. Assim, o primeiro capítulo abordará a evolução na legislação brasileira, dando ênfase a forma como foi feita a melhora na proteção de dados no Brasil e a importância da Lei de Proteção de Dados (LGPD) para proteger a privacidade e a segurança dos dados pessoais dos brasileiros.

O segundo capítulo é dedicado à compreensão e distinção dos dados pessoais e os dados pessoais sensíveis, sua conceituação e dispositivos de proteção.

Por fim, o terceiro capítulo trata da capacidade de inferência das tecnologias atuais, demonstrando que é possível com dados não sensíveis se chegar a dados sensíveis; assim como demonstra que tais dados podem ser tão danosos quanto os categorizados como sensíveis. Portanto, a hipótese que se levanta é a de que a regulação deveria ocorrer pelos danos e riscos que o tratamento dos dados pode causar e não pelo tipo de dado.

Para o desenvolvimento da pesquisa será realizado levantamento bibliográfico em especial em *site*s, artigos, doutrinas, jurisprudência e legislação. Nesse sentido esta pesquisa caracteriza-se como qualitativa e bibliográfica.

---

[2] A Lei Geral de Proteção de Dados (LGPD) define tratamento em seu artigo 5º, inciso X. Tal inciso afirma que tratamento é "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".

2 A EVOLUÇÃO DA PROTEÇÃO DE DADOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Com o advento das leis de privacidade e proteção de dados, tem-se aumentado a consciência em relação à necessidade de tutela-los, não só pela necessidade de se proteger a vida privada dos indivíduos, mas também a própria liberdade destes. Sendo importante ressaltar que com o passar dos anos, a privacidade, que antes era o "direito de ser deixado só" cunhado por Warren e Brandeis (1890), passou a ser o direito de manter controle sobre as próprias informações.

A privacidade era vista como um direito negativo até as décadas de 60 e 70, ou seja, estaria garantida contanto que o Estado se abstivesse de adentrar na esfera individual do cidadão. Entretanto, com avanço tecnológico e o tratamento de dados crescente, o conceito de privacidade toma novas conotações, passando a prevalecer definições funcionais que fazem referência à possibilidade de a pessoa conhecer, controlar e até interromper o fluxo das informações a ela relacionadas. "Assim a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações". (RODOTÀ, 2018, p. 92).

Já em 1970, o Estado Alemão de Hesse e a Suécia incluíam em sua lei de privacidade a proteção de dados, como afirma Rodotà (2008). Tal tendência prosseguiu nos anos seguintes, inclusive na jurisprudência brasileira.

2.1 Evolução histórica antes da LGPD

Segundo Lugati e Almeida (2020), no Brasil, a regulação da proteção de dados construiu-se de forma lenta e descentralizada. Porém, é possível afirmar que se iniciou, de forma tácita, com a Constituição Federal de 1988.

O artigo 5º, responsável por listar os direitos e garantias fundamentais invioláveis, traz vários incisos que baseiam a proteção de dados, como o inciso X o qual literalmente afirma que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação". Além disso, a garantia da livre expressão, não só intelectual, mas artística, a científica e a de comunicação, além da garantia de

acesso à informação, estão defendidas no artigo 5º, incisos IX e XIV da CF/88.

Nesse sentido, Doneda (2017) chama a atenção que a Constituição Federal considera que não podem ser violados a vida privada e a intimidade, nos termos do art. 5º, X, especialmente relacionadas a interceptação de comunicações telefônicas, telegráficas ou de dados, como dispõe o art. 5º, XII, além de ter sido instituída a ação de *Habeas Data,* disposta no art. 5º, LXXII, que tem por objetivo a previsão de direito genérico de acesso e retificação dos dados pessoais.

Inclusive, afirma que o *Habeas Data* deve ser observado com atenção, não só pela sua importância na formação da democracia ou por ter sido inserido em várias das legislações latino-americanas, mas também por ser o primeiro instrumento voltado à proteção de dados pessoais, pois trata-se de um remédio constitucional que tem por finalidade garantir à pessoa física ou jurídica o acesso ou a promoção de retificação de suas informações constantes em bancos de dados de órgãos públicos ou instituições similares.

É importante ressaltar que tal instituto surgiu como ruptura para com o regime militar e tinha, a princípio, o objetivo de assegurar ao cidadão o direito ao conhecimento das informações sobre si mesmo que o regime autoritário poderia ter. O *Habeas Data* "teve o mérito de chamar a atenção do operador e da sociedade para um direito que vinha sendo negligenciado". (DONEDA, 2017, p.23)

Com o Código de Defesa do Consumidor (CDC) em 1990, o qual disciplina a proteção frente a cadastros e bancos de dados. O artigo 43 dispõe: "o consumidor, sem prejuízo no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como suas respectivas fontes".

Tal artigo contém relação com o *Habeas Data* supracitado, pois dentre as proteções enunciadas chama atenção a exigência que os cadastros e dados dos consumidores sejam objetivos, claros, verdadeiros, dando a possibilidade de exigência pelo consumidor sua imediata correção caso não o sejam.

Ademais, ressalta-se a importância do § 2° do artigo 43, do CDC, no qual determina-se que qualquer abertura de cadastro, ficha, registro e dados pessoais e de consumo deve ser comunicada por escrito ao consumidor. De tal maneira, é possível afirmar-se que o CDC tentou garantir ao titular dos dados o controle sobre suas informações, sendo este um princípio de autodeterminação informativa.

> O artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em “bancos de dados e cadastros”, implementando uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro. (DONEDA, 2011, p.103)

Já no ano de 2011, surge a Lei 12.414/2011, denominada Lei do Cadastro Positivo, a qual disciplina acerca dos dados de adimplemento utilizados para a formação de histórico de crédito.

É um avanço em relação à legislação infraconstitucional anterior, pois além de trazer os conceitos de banco de dados e das informações que este pode conter, também segue a interpretação de que o compartilhamento de dados só é lícito se houver o consentimento do cadastrado. Desta forma, consolida a "evolução do conceito de autodeterminação informativa no nosso ordenamento”. (MENDES, 2014, p. 146).

Enquanto o Código de Defesa do Consumidor exige apenas a notificação do titular quanto a abertura de cadastros e bancos, a Lei de Cadastro Positivo avança mais um passo e exige o consentimento deste. Ademais, cria o dever para o controlador de não utilizar os dados fora da finalidade para o qual foram coletados e proíbe as anotações de informações excessivas.

Também foi inovadora em seu artigo 17:

> Nas situações em que o cadastrado for consumidor, caracterizado conforme a Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor, aplicam-se às sanções e penas nela previstas e o disposto no § 2º .
> § 1º Nos casos previstos no caput , a fiscalização e a aplicação das sanções serão exercidas concorrentemente pelos órgãos de proteção e defesa do consumidor da União, dos Estados, do Distrito Federal e dos Municípios, nas respectivas áreas de atuação administrativa.
> § 2º Sem prejuízo do disposto no caput e no § 1º deste artigo, os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas e estabelecer aos bancos de dados que descumprirem o previsto nesta Lei a obrigação de excluir do cadastro informações incorretas, no prazo de 10 (dez) dias, bem como de cancelar os cadastros de pessoas que solicitaram o cancelamento, conforme disposto no inciso I do caput do art. 5º desta Lei.

Para Mendes (2014), tal previsão expressa o controle da atividade de processamento por autoridade administrativa, possibilitada a aplicar medidas e sanções em conjunto com um sistema clássico judicial de resolução de lides.

Por fim, o referido diploma é responsável, segundo Doneda (2006), por refletir com maior intensidade um modelo de proteção de dados pessoais, menos que em âmbito restrito. Sendo de grande importância para integrar alguns princípios relativos

à proteção de dados ao nosso ordenamento jurídico.

No ano de 2011, a atriz Carolina Dieckmann teve o computador invadido por hackers e sua intimidade violada após 36 de suas imagens íntimas serem divulgadas sem autorização nas redes sociais. Devido a este fato, menos de um ano depois, a Lei 12.737/2012 foi sancionada, pois a justiça percebeu que não havia uma legislação específica para a devida penalização dos envolvidos.

A lei tem como objetivo garantir a segurança no ambiente virtual, tornando crime a invasão de dispositivo informático alheio com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, bem como obter vantagem ilícita com os dados obtidos. A lei acrescentou ao Código Penal os artigos 154-A, 154-B, 266 e 298.

Apesar de obter falhas e de não dispor de meios processuais que garantam sua eficácia, como afirma Beretta (2014), a Lei Carolina Dieckmann entra na trajetória da proteção de dados pessoais do Brasil por também tentar devolver ao cidadão o controle de seus dados, já que mais uma vez se fala de autorização do titular para ter acesso aos dados pessoais.

Seguindo a linha cronológica brasileira sobre proteção de dados, o Marco Civil da Internet, Lei 12.965 de 23 de abril de 2014, foi o primeiro documento legislativo a reconhecer a internet como serviço essencial para o exercício da cidadania e, por isso, se preocupou em estabelecer princípios, garantias, deveres para o uso da Internet no Brasil. Tal regulamentação teve seu trâmite legislativo acelerado após ser comprovado que a espionagem feita pela Agência de Segurança dos Estados Unidos teve repercussão dentro do âmbito brasileiro.

A lei tem como inovação a tentativa de assegurar o direito à privacidade e a proteção de dados pessoais, entre outros, com o disposto no artigo 7º:

> O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Desta forma, é possível perceber que por mais que o diploma não possua um regramento detalhado, já é possível encontrar a base dos direitos assegurados aos usuários que seriam, posteriormente, melhor elucidados com a Lei Geral de Proteção de Dados.

O Marco Civil da Internet já considera indispensável o consentimento do titular, de maneira livre, expressa e informada, para o fornecimento de dados pessoais a terceiros. Inclusive, Masso e Abrusio (2014) afirmam, em relação ao adjetivo "livre", que o titular deveria ter a possibilidade de optar sobre cláusulas ou contratos de forma parcial, e não somente pelo todo, para realmente se seguir o disposto no inciso VII do artigo 7º, acima supracitado. Faz-se necessário, no entanto, que seja informado das possibilidades e consequências de tal escolha.

Também é possível perceber que o texto já inclui em seus dispositivos alguns dos princípios presentes em diversas leis de proteção de dados, como o princípio da finalidade, da adequação e da transparência. Bem como já atribui ao titular a possibilidade de requerer a exclusão de suas informações, após o término da relação entre titular e responsável pela coleta dos dados.

Apesar de o Marco Civil da internet ter sido um grande avanço se comparado às tentativas anteriores, as quais se utilizavam, segundo Bioni (2020), de uma técnica prescritiva e restritiva, o Brasil ainda necessitava de uma legislação mais

abrangente. Principalmente após o surgimento do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), cujo artigo 46 afirmava que as transferências de dados entre os responsáveis pelo tratamento só poderiam ocorrer para um país terceiro ou organização internacional se houvesse leis que gerassem garantias adequadas. Portanto, a GDPR exerceu influência na criação da legislação de proteção de dados em diversos países.

> Na ausência de uma decisão nos termos do artigo 45.º, 3, um responsável pelo tratamento ou subcontratante só pode transferir dados pessoais para um país terceiro ou para uma organização internacional se o responsável pelo tratamento ou subcontratante tiver fornecido garantias adequadas, e desde que estejam disponíveis direitos aplicáveis e soluções legais eficazes para os titulares dos dados.[3] (tradução nossa).

Desta forma, dadas às restrições criadas pela GDPR, surgiu a necessidade de criar uma lei específica para a tratamento, proteção e sigilo de dados, que veio a ser a Lei Geral de Proteção de Dados (LGPD); trazendo em seu cerne grandes avanços para a privacidade e segurança dos dados pessoais dos brasileiros, ainda que incite debates sobre sua revisão e aprimoramento.

2.2 A Lei Geral de Proteção de Dados brasileira

De acordo com o exposto por Bioni (2020), desde 2010 havia um debate em relação a uma legislação de proteção de dados, inclusive a primeira versão do anteprojeto de lei sobre o assunto foi colocada para consulta no mesmo ano. Porém, foi somente em 2018 que o Projeto de Lei 53/2018 tornou-se a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD).

A LGPD, então, baseada fortemente nos dispositivos da GDPR, tem como fundamento a proteção de dados de uma pessoa natural identificada ou identificável e versa sobre os mecanismos pelos quais entidades públicas e privadas podem coletar e tratar tais dados. Trata-se de uma legislação extremamente técnica que visa assegurar, em seu âmago, os direitos humanos, em principal os da liberdade, da privacidade e o livre desenvolvimento da personalidade da pessoa natural, como afirma seu primeiro artigo.

---

[3] "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

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

De acordo com Mendes e Doneda (2018), é possível identificar cinco eixos principais da LGPD em torno dos quais a proteção de dados se articula. O primeiro eixo seria a unidade e generalidade da aplicação da Lei, pois concentra-se na proteção de dados do cidadão, independentemente de quem realiza seu tratamento. Os pressupostos da LGPD serão aplicados tanto para os setores privados quanto os públicos, recaindo sobre dados tratados na internet e fora dela.

O segundo eixo é a legitimação para o tratamento de dados, que só poderá ser realizado se uma base normativa autorizar, havendo um exame quanto à sua legitimidade. "Somente serão legítimos aqueles tratamentos que se enquadrem em ao menos uma das hipóteses previstas no art. 7º ou no art. 23 da LGPD, totalizando 11 hipóteses autorizativas para o tratamento de dados pessoais". (MENDES e DONEDA, 2018, p. 472)

O terceiro eixo da LGPD são os princípios e direitos do titular. A Lei cita uma série de princípios e direitos que buscam garantir meios efetivos de controle, por parte do titular, dos dados utilizados por terceiros, além de conferir unidade sistêmica à disciplina de dados pessoais.

Os princípios, elencados no artigo 6º da LGPD, são:

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

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

O quarto eixo da Lei é o estabelecimento de obrigações para os agentes de tratamento. Além dos limites, prevê uma série de procedimentos que reforçam a segurança e as garantias dos titulares de dados. Um exemplo é a obrigação, por parte do controlador, de instituir um encarregado para o tratamento de dados, como dispõe o artigo 41 da LGPD.

Já o quinto eixo é a responsabilidade dos agentes quando houver danos decorrentes do tratamento de dados. A LGPD considera que a natureza da atividade de tratamento de dados encerra um risco intrínseco e, portanto, só deve compreender os dados estritamente necessários. Desta forma, como observado no artigo 42, o legislador optou por um regime de responsabilidade objetiva.

A LGPD está dividida em 10 capítulos e possui um total de 65 artigos, sendo, portanto, menor e mais enxuta que a Lei que utilizou como referência (GDPR), que possui 11 capítulos e 99 artigos. Assim, é possível afirmar que deixou margem para uma interpretação mais ampla em determinados assuntos, como é o exemplo dos prazos, "trazendo alguns pontos de insegurança jurídica por permitir espaço para a subjetividade onde deveria ter sido mais assertiva." (PINHEIRO, 2020, p.14)

Também é importante lembrar que, por ser um marco de grande impacto tanto para instituições públicas quanto privadas, foi estabelecido o prazo de dezoito meses para que estas instituições se adaptassem às novas regras. Após este período, as penalidades previstas poderiam ser aplicadas.

A Lei 13.709/18 inova não só ao trazer uma legislação própria no tocante ao tratamento e uso de dados pessoais, mas ao apresentar definições mais precisas sobre titular, tratamento de dados, dados pessoais e consentimento, por exemplo, do que qualquer legislação anterior supracitada. Ademais, o instituto do consentimento passou a ser uma das hipóteses de permissão de tratamento, o que para Bioni (2020) demonstra que o instituto não só deixou de ser a única base legal, como não mais possui uma hierarquia superior às demais bases legais trazidas pelos incisos do artigo 7º da LGPD.

Porém, não significa que o instituto perdeu sua importância. Pois segundo o artigo publicado pelo SERPRO intitulado "Seu consentimento é lei!”, traz essa noção:

> Se a gente fosse eleger a principal palavra da Lei Geral de Proteção de Dados Pessoais (LGPD), a escolhida seria, sem dúvidas, CONSENTIMENTO. É o titular, ou seja, a pessoa a quem se referem os dados que deve, se quiser - ao ser questionada, de forma explícita e inequívoca - autorizar que suas informações sejam usadas, por empresas e órgãos públicos, na hora da oferta de produtos e serviços, gratuitos ou não.

Por fim, como a maioria das leis de proteção de dados, podemos perceber que a LGPD possui dois graus de proteção para estes: uma para dados pessoais e outra para dados pessoais sensíveis. Significa afirmar que reconhece a diferença entre as situações envolvendo tratamento e vazamento de dados; enquanto algumas podem causar leve aborrecimento, outras podem trazer ameaça contra a integridade física, discriminação, estresse emocional, danos morais e fraude.

3 TIPOS DE DADOS E COMO DEVEM SER TRATADOS

Para o melhor entendimento do escopo das leis de proteção de dados, faz-se necessário, a princípio, que se distinga dados e informações. O primeiro é uma entidade básica, o conhecimento bruto, que por não ter sido tratado ainda não consegue transmitir uma mensagem clara. Segundo Setzer (1999), dado é uma sequência de símbolos quantificados ou quantificáveis, podendo ser um texto, imagens, sons, cliques, interações, compartilhamentos.

Na realidade em que vivemos, a chamada sociedade da informação, os dados são onipresentes, gerados a todo instante, tendo se tornado verdadeiras *commodities*[4]. Com a maioria das pessoas conectadas *online,* seja em redes sociais ou em sites variados, é gerado um imenso volume de dados a cada segundo por atividade realizada; até o tempo em que um usuário passa parado em determinada página de um site é contabilizado, por exemplo.

Quando os dados passam pelo processo de captação, tratamento e análise transformam-se em informação. É atualmente o insumo mais importante da produção humana e trata-se de uma constatação concreta, a partir dos dados analisados, dentro de um contexto real. A informação tem seu conteúdo entendível e possui propósito, significado e relevância.

Desta forma, é fácil compreender que, sendo dado uma partícula de um registro qualquer, não faz-se possível que uma lei se habilite a protegê-los em sua integridade. "As leis de privacidade não podem abranger todos os dados, caso contrário seriam ilimitadas, então limitam-se a abranger dados relativos às pessoas". (SOLOVE, 2023, p.6, tradução nossa).

3.1 O que são dados pessoais

Com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural, a maioria das leis baseia-se na definição de dados pessoais, sendo 70% de 194

[4] *Commodities* significa mercadoria. Segundo o site da XP Investimentos (2019), o termo se refere a uma determinada matéria-prima ou produto que é facilmente intercambiável e amplamente negociado, como milho, dólar, carne, café, petróleo. Trata-se de insumos pouco processados ou em estado bruto.
Os dados, por na era da informação, terem se tornado cruciais para o desenvolvimento econômico de empresas ou Estado e por não serem um produto "processado", são vistos como *commodities*.

países, segundo Solove (2023). Portanto, para a Lei Geral de Proteção de Dados (LGPD), tal como para o Regulamento Geral sobre a Proteção de Dados (GDPR), dado pessoal é a informação relacionada à pessoa natural identificada ou identificável. Sendo informação identificada quando vinculada a uma pessoa e identificável se tem o potencial de ser vinculada a alguém, mesmo que no momento não o seja.

> É imprescindível, assim, seja diretamente, seja indiretamente, mesmo que em um segundo momento, ter o componente da identidade de uma pessoa natural como característica fundamental do dado pessoal. Lembrando, na lição de Lawrence Lessig, que a identidade vai além do que a pessoa realmente é, envolvendo também atributos, fatos, comportamentos e padrões, os quais são usados como formas de comunicação automática. (MALDONADO e BLUM, 2022, p. RL-1.2)

Nem todas as leis definem dados pessoais da mesma forma, afirma Schwartz e Solove (2011), boa parte das leis dos Estados Unidos define como informação aquela que efetivamente identifica uma pessoa. A *U.S Video Privacy Protection Act (VPPA),* por exemplo, define informação pessoal como "informação que identifica uma pessoa"[5]. De tal forma que os dados identificáveis acabam por não serem considerados e geram lacunas na proteção por parte dessas leis.

Porém, as leis de privacidade ao redor do globo têm seguido a tendência, segundo Graham Greenleaf (2020), de incluírem, ao se falar de informação pessoal, incluem o termo "identificável", possuindo assim um caráter expansionista em seu conceito de dados pessoais, como é o caso do Brasil.

> Na definição mais comum de dados pessoais, que envolve dados identificados e identificáveis, a existência do elemento de identificabilidade confere aos dados pessoais um âmbito amplo, aberto e dinâmico. Os dados que podem ser utilizados em combinação com outros dados para identificar uma pessoa se tornam dados pessoais, mesmo que isoladamente não possam ser associados a um indivíduo específico.[6] (SOLOVE, 2023, p.7, tradução nossa).

Inclusive, faz-se importante ressaltar que a inclusão dos dados identificáveis no conceito de dados pessoais se mostra um avanço para as leis de proteção de dados. O conceito de privacidade conhecido desde 1980, criado por Samuel Warren

---

[5] Trata-se de uma tradução nossa. A Video Privacy Protection Act afirma está escrita nos seguintes termos: "the term “personally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider;"

[6] "Under the more common definition of personal data, which involves identified and identifiable data, the existence of the identifiability prong gives personal data a broad, open-ended, and dynamic scope. Data that can reasonably be used in combination with other data to identify a person is personal data, even if in isolation it cannot be linked to a specific individual."

e Louis Brandeis, assumia ser um direito da personalidade, se preocupando apenas com as informações que identificassem a pessoa, como afirma Rodotà (2008).

Porém, na era da *Big Data*[7], tal conceito se torna obsoleto. Isso porque, com os algoritmos, as análises de dados são relativamente fáceis de serem feitas com dados que não são diretamente associados a alguém. De acordo com Latanya Sweeney (2000), é possível identificar 87% das pessoas com uma combinação de CEP, data de nascimento e gênero.

Dito isso, são exemplos de dados pessoais os dados cadastrais, como: o nome, pronome, RG, CPF, endereço, gênero, estado civil, data e local de nascimento, filiação, título de eleitor, número de passaporte, números de telefone, registro de ligações, cartão ou dados bancários, registros de conexão, *cookies*[8], contas de e-mail, endereço de IP[9], assim como dados mais intrínsecos, orientação sexual, dados biométricos, raça, saúde, entre outros. Estes últimos fazem parte de uma característica específica denominada dados sensíveis.

3.2 Dados sensíveis na LGPD

O conceito de dados sensíveis não foi criado com a GDPR ou as leis que dela derivaram. Na verdade, tem-se uma evolução legislativa sobre essa subespécie de dados por mais de 50 anos, já que a primeira lei surgiu em Hesse, Estado Alemão, em 1970.

3.2.1 A presença dos dados sensíveis nas legislações ao longo dos anos

Porém, foi em 1980, com a recomendação da Organização para a Cooperação e Desenvolvimento Econômico (OECD), cujas diretrizes eram relativas

---

[7] *Big Data* está relacionado a grandes conjuntos de dados que precisam ser processados e armazenados. *Big Data* está relacionado "à capacidade de processar e analisar grandes volumes de informação, permitindo a extração de conhecimentos úteis para melhorar o processo de tomada de decisão". (SCAICO, DE QUEIROZ, SCAICO, 2014, p.329).

[8] Segundo Pessôa (2023), *cookies* são pequenos pacotes de arquivos de texto que informam ao navegador se o usuário já acessou determinado link. Também podem guardar a navegação na web, vídeos assistidos, o tempo passado em determinada página, o idioma de preferência e até mesmo as buscas feitas em um site por determinada pessoa.

[9] Endereço de IP é a representação numérica de uma rede ou de um dispositivo na internet. Pode servir como geolocalização do aparelho e também como identificação do tipo de dispositivo usado, assim como é possível entender que informações esses dispositivos estão enviando, solicitando e recebendo.

à proteção da vida privada e à circulação transnacional dos dados de caráter pessoal, que foram reconhecidos os dados sensíveis. No entanto, ainda com uma abordagem básica, pois não especificava como tais dados deveriam ser protegidos ou que tipo de dados fariam parte da categoria.

Em 1981, a Convenção do Conselho da Europa n. 108, voltada para proteção das pessoas em relação à coleta automática de dados de caráter pessoal, deu um passo adiante. Reconheceu a categoria de dados sensíveis e incluiu nesta os dados que incluíssem origem racial, opiniões políticas, crenças religiosas, saúde e vida sexual. Segundo McCullagh (2007), estas categorias listadas no artigo 6 relatório n. 108 não são exaustivas. Na verdade, os Estados-Membros eram livres para incluir outras categorias de dados sensíveis.

Em seguida veio a diretiva da União Europeia sobre Proteção de Dados 95/46/EC. Nela havia uma especificação clara sobre as categorias a serem consideradas sensíveis, sendo sete categorias que necessitavam proteção extra. O artigo desta diretiva afirmava:

> Os Estados Membros devem proibir o processamento de dados pessoais relevando origem racial ou étnica, opinião política, crenças religiosas ou filosóficas, filiação partidária e o processamento de dados relativos à saúde e vida sexual. (tradução nossa)

Portanto, pode-se perceber que a abordagem geral da diretiva consistia em estabelecer uma regra de proibição para o tratamento de dados sensíveis, a não ser que houvesse uma razão específica para o tratamento autorizada em lei.

É importante mencionar que antes da GDPR, que influenciou fortemente a Lei de Proteção de Dados Brasileira, já havia no Brasil tratamento - mesmo que mais restrito - para os dados sensíveis na Lei de Cadastro Positivo, em inciso II, § 3º, do artigo 3º:

> Ficam proibidas as anotações de:
>
> [...]
>
> II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

O que significa afirmar que, em se tratando de análise de concessão de crédito, é proibido anotar informações personalíssimas e cuja finalidade não esteja relacionada à análise de crédito, a fim de evitar o tratamento discriminatório.

Já em 2016, houve a criação da GDPR, na qual diversas categorias foram adicionadas àquela lista da Diretiva 95/46/EC, como dados genéticos, dados biométricos e orientação sexual. No entanto, como afirmado por Solove (2023), a GDPR se diferencia da diretiva por ser uma lista exclusiva, ou seja, os Estados-Membros não podem reconhecer categorias adicionais de dados sensíveis.

A listagem da Regulamento Geral sobre a Proteção de Dados (GDPR) é bem parecida com a disposta pela Lei Geral de Proteção de Dados (LGPD), tendo ambas as mesmas categorias sob proteção extra.

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Faz-se necessário apontar que, assim como a GDPR, tal inciso traz um rol taxativo, não podendo ser ampliado suas previsões quando interpretada pelo julgador, como é o afirmado pelo Ministro do STJ Francisco Falcão no Agravo em Recurso Especial nº 2.130.619.

> O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis.

3.2.2 O conceito de dados sensíveis para além do artigo 5º da LGPD

Em análise feita em 2019, apresentada por Solove (2023), as categorias de dados sensíveis mais reconhecidas em 112 países analisados são as mesmas definidas pela GDPR; os dados que variam entre um país e outro são antecedentes criminais, idade, informação de contato, endereço residencial, educação, gênero, status social e informações de crédito.

Podemos perceber, portanto, que as leis de privacidade possuem uma sobreposição significativa nas categorias de dados sensíveis que reconhecem, porém também apresentam diferenças consideráveis. O resultado é um cenário em que a definição de dados sensíveis torna-se complicada e bastante desafiadora.

A princípio, faz-se necessário entender que, ao possuir dois níveis de

proteção, um para dados pessoais e outro para dados sensíveis, as leis reconhecem que nem todas as situações envolvendo dados é igual.

Ou seja, se o dado é sobre uma pessoa ter um cachorro chamado Marley, esse não é um dado prejudicial. No entanto, se é sobre o fato de a pessoa ter uma doença fatal a situação muda, já que muitas doenças carregam estigma e a pessoa em questão pode se sentir envergonhada, sofrer danos à reputação ou discriminação se o dado for vazado.

Assim, sendo dados sensíveis àqueles associados às características e opções inerentes à pessoa, é possível afirmar que a tipologia diferente para os dados sensíveis é justificada perante a lei porque se trata de um conteúdo que, caso conhecido e processado, trariam vulnerabilidade ao titular. Segundo Doneda (2006), os dados sensíveis são informações que possuem o potencial de utilização discriminatória ou particularmente lesiva, de tal forma que, em razão da sua natureza, poderiam causar violações aos direitos fundamentais.

Tendo o dado a natureza de sensível atribuída pela lei, então passa a ter um regime jurídico próprio, observado no artigo 11 da LGPD, o qual traz um rol mais restritivo de hipóteses que autorizam o tratamento de tais dados.

> O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Mais uma vez faz-se importante mencionar o destaque dado ao consentimento por parte do legislador, trazendo aqui também a especificação de que tal consentimento será feito de forma específica e destacada. Ou seja, o

consentimento do titular dos dados sensíveis é qualificado, como menciona Rodotà (2008), pois se trata de um contratante vulnerável.

Outro detalhe importante a se mencionar sobre os dados sensíveis é sobre o disposto no artigo 11, § 1, que afirma que se o tratamento de dados pessoais revelar dados pessoais sensíveis e potencialmente causar danos ao titular, então o regime mais restritivo acima mencionado será aplicado. Desta forma, tal parágrafo reconhece que há a possibilidade de que dados pessoais não sensíveis revelem dados sensíveis e, portanto, devem ser protegidos com o mesmo afinco.

Inclusive, tal parágrafo faz parecer que somente seria legitimada a aplicação do artigo 11 caso o tratamento dos dados pessoais que revelem dados sensíveis causasse algum dano ao titular. No entanto, Mulholland (2018, p.169) defende que o entendimento jurisprudencial é no sentido de que "o tratamento de dados pessoais sensíveis gerará sempre danos de natureza personalíssima por violação dos direitos de privacidade, liberdade ou identidade, fundamentos da proteção de dados", pois haverá dano presumido.

Por fim, por mais que a qualificação dos dados sensíveis esteja relacionada à potencialidade discriminatória, resta claro que a categorização normativa dos dados sensíveis se faz por enumeração em abstrato, como é o caso da previsão feita pela LGPD, e por muitas vezes exaustiva. Críticas ao desenvolvimento do conceito e do conteúdo de dados sensíveis existem, já que a sensibilidade advém do contexto de utilização do dado e da combinação deste com outros disponíveis. Como afirma Moraes (2010), a personalidade possui uma complexidade de situações objetivas, demandando uma normatização aberta.

4 LGPD: O TRATAMENTO DOS DADOS SENSÍVEIS

Como descrito acima, além de a LGPD definir as categorias de dados considerados sensíveis, também introduziu vários novos requerimentos que devem ser aplicados no processamento destes. Entretanto, apesar do esforço e inovação trazido pela lei, os dados sensíveis como elemento chave da nossa lei de proteção de dados é um erro, pois trata-se de um conceito falho

4.1 O poder da inferência e a inadequação da proteção atual

.

Como afirma Alicia Solow-Niederman (2022), vivemos em uma economia de inferência. Inferência é a capacidade de dedução, feita com base na lógica e na interpretação de informações que já se têm sobre os indivíduos, que que as empresas e organizações que têm e que, para a autora, é o verdadeiro poder atualmente.

O que a autora demonstra é que o procedimento de coleta e organização dos dados dos indivíduos não é tão linear quanto queremos crer. Os dados que são recolhidos sobre alguém não são tratados e armazenados somente sob o "arquivo" desta pessoa; podem ser utilizados para fazer inferência sobre outras informações que não foram fornecidas, bem como para fazer inferências sobre outras pessoas. Desta forma, não é só o indivíduo que cedeu o controle dos dados que é afetado com a coleta, o tratamento e o compartilhamento dos dados.

As inferências podem ser feitas sobre o estado das coisas no presente, mas também podem tentar predizer o futuro, o que tem o potencial mais danoso por não serem verificáveis, como afirma Hideyuki Matsumi (2018). E inferências também podem ser feitas a partir de dados não sensíveis para descobrir dados sensíveis, de forma que a raça de uma pessoa pode ser inferida pelo local que ela vive, a religião pelo padrão de alimentação, as crenças filosóficas pelos hábitos de leitura e afiliação política são passíveis de ser inferidas de milhares de formas distintas.

Segundo Joanne Hinds e Adam N. Joinson (2018), ao examinar 327 estudos sobre inferências, eles perceberam que os atributos mais comuns de se inferir são gênero, idade, política, localização, ocupação, raça e etnia, família e relacionamentos, salário, educação, saúde, orientação sexual.

Como visto, a LGPD reconhece, em seu do artigo 11, que as inferências

contam como dados sensíveis e devem ser tratadas sob o mesmo regime jurídico, o que é valorável. Porém, o problema é que as implicações são maiores do que se é reconhecido, pois se as inferências são incluídas como dados sensíveis, então quase todo dado pessoal seria abarcado por tal categoria, tornando inócua a proteção diferenciada para dados sensíveis e dados não sensíveis. De forma a ilustrar o afirmado, alguns exemplos podem ser traçados.

É possível prever a ideologia política pelo que se é escrito em fóruns não-políticos na internet. Segundo o método trazido por Angus, Kitchener, Anantharama e Raschky (2022), foi possível compilar a ideologia política de 91 mil usuários do Reddit, site para a interação com comunidades, e a taxa de acerto foi maior que 90%. Inclusive, segundo eles, a utilização frequente da palavra "sentir" em comentários online está fortemente associado a opiniões economicamente de esquerda.

Tal estudo retira qualquer dúvida que restava sobre como toda a atividade online, como *posts*, *tweets*, comentários, *likes* e subscrições, podem deixar traços individuais de diversas instâncias e o mais importante: estes traços estarão guardados de maneira indefinida e passíveis de acesso.

Outro exemplo seria a possibilidade de inferir a orientação sexual de alguém pela atividade nas redes sociais. Um estudo dizia conseguir inferir a sexualidade das pessoas somente analisando os likes no Facebook. Outro alegava ser capaz de identificar a orientação sexual da pessoa através de fotos; com cinco fotos sob análise, a taxa de acerto era de 91% quando se tratava de homens e 83% quando se tratava de mulher.

Já se falando de saúde, é reconhecido pelo Comitê Europeu para a Proteção de Dados (EDPB), em suas diretrizes sobre tomada de decisões individuais automatizadas e definição de perfis para o fim de regulamentação, que qualquer dado pode ser utilizado para inferir sobre o status de saúde atual ou o risco de saúde de uma pessoa.

> A criação de perfil pode criar dados de categorias especiais por inferência a partir de dados que não são dados de categorias especiais por direito próprio, tornando-se de categorias especiais quando combinados com outros dados. Por exemplo, pode ser possível inferir o estado de saúde de alguém a partir dos registros de suas compras de alimentos, combinados com dados sobre a qualidade e conteúdo energético dos alimentos. (EDPB,

2016, p.15, tradução nossa)[10]

Durante a pandemia de Covid-19, por exemplo, muitos países passaram a utilizar tecnologias para monitorar e controlar a propagação do vírus, no qual se fazia o mapeamento das pessoas que interagiram com indivíduos infectados, os chamados aplicativos de *contact tracing*. Tais aplicativos coletavam dados como data do diagnóstico, nacionalidade e gênero.

Porém, este é um exemplo pontual. Os estudos de Kosinski (2013) demonstram ser possível, pela análise das curtidas no Facebook, inferir o abuso de substâncias em mais de dois terços dos perfis analisados. Também se faz possível identificar a saúde mental de uma pessoa por posts em redes sociais; inclusive a atividade - ou a falta dela - nessas redes é um indicativo para os algoritmos

Até os hábitos de compra podem inferir dados sobre saúde, como é o caso trazido por Duhigg (2012) ao New York Times, no qual um algoritmo criado pela Target conseguia identificar mulheres que estavam grávidas, antes mesmo de as mesmas terem conhecimento, a partir de seus hábitos de compra. No caso relatado, o pai de uma adolescente estava recebendo muitas propagandas sobre produtos de bebe e acabou por reclamar com a loja, mais tarde ele descobriu que a filha estava realmente grávida.

Tais exemplos são para ilustrar que com dados pessoais mundanos como comprar em sites, é possível se chegar a informações consideradas sensíveis sem que as mesmas tenham sido tratadas ou compartilhadas. Além de demonstrar que a proteção atual de dados sensíveis não condiz com nossa realidade tecnológica.

4.2 O dano do dado não sensível

Sabemos que os dados sensíveis passaram por uma evolução durante mais de 50 anos e que as categorias escolhidas são aquelas que têm o maior potencial de causarem discriminação ou ferirem os direitos fundamentais. Todavia, as categorias mostram-se, de certa forma, arbitrárias.

Isto porque, se dermos uma olhada nas leis do globo, o reconhecimento das categorias de dados sensíveis é inconsistente. Várias leis dos Estados Unidos, por

[10] "Article 9 – Special categories of data. Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods"

exemplo, reconhecem a geolocalização como dado sensível, enquanto a GDPR e a LGPD não o fazem. Assim como estas últimas colocam crenças filosóficas como parte das categorias de dados sensíveis enquanto a maioria das leis dos Estados Unidos não, diz Solove (2023).

Além disso, a maioria das categorias de dados sensíveis têm uma definição vaga, de modo que é possível questionar que tipos de dados são inclusos ou não. Por exemplo, sabemos que os diagnósticos feitos por médicos são considerados dados de saúde e, portanto, são sensíveis. Porém, as pesquisas na internet sobre determinada condição de saúde ou a entrada em um grupo de apoio para uma doença também o é?

As categorias de dados sensíveis podem ser muito amplas e simplistas e nem todos os dados que estão sob este manto são igualmente sensíveis. Assim como os dados fora dessas categorias podem ser tão sensíveis ou mais, pois dados não sensíveis podem ser utilizados de forma a causar danos.

Para justificar adequadamente tal afirmação, vejamos alguns exemplos:

Endereços raramente estão nas listas de dados sensíveis e, para a maioria das pessoas, o endereço de casa ou do trabalho são bastante inócuos, porém para outras podem ser bastante prejudiciais se divulgados. Em um país em que o número de novos casos de feminicídio e violência doméstica chegam a mais de 600 mil, o endereço da casa e do trabalho dessas mulheres, se protegidos, podem salvá-las de uma situação de risco de morte.

Juízes, por exemplo, são atacados em suas casas. Tanto que no fim do ano de 2022, o congresso norte-americano aprovou o *Daniel Anderl Judicial Security And Privacy Act*, devido ao filho de um juiz - Esther Salas - que foi assassinado ao salvar seus pais dos tiros de um falso entregador que os encurralou em casa. A informação do endereço, segundo o site da USCourts.gov (2022), foi achado online.

Outro exemplo, são os dados que envolvem classe social, que levam vários fatores socioeconômicos em consideração, como a educação e a riqueza de uma pessoa. Mesmo que 30% dos brasileiros afirmem ter sofrido discriminação por causa da classe social, como mostra pesquisa do DataFolha feita pelo Jornal Folha de São Paulo em 2019, a LGPD não classifica a classe social como dado sensível.

A verdade é que as pessoas pobres são sujeitadas a discriminações significantes. A construção moral da pobreza faz com que as pessoas assumam que as pessoas pobres apresentam falhas comportamentais ou éticas (BRIDGES, 2017).

Portanto, se as categorias de dados sensíveis são inclusas nas leis de privacidade por conta da possibilidade de discriminação, então a exclusão da classe social é arbitrária.

Ademais, em muitos casos os dados não sensíveis podem ser correlacionados com dados sensíveis e trazer danos, como é o exemplo de modelos de aprendizado de máquina que têm a menor probabilidade de recomentar pacientes negros a programas de gestão de cuidado de alto risco ou são mais propensos a identificar réus negros como de alto risco sem utilizar, em momento algum, a raça como variável para sua previsões (ADAM, 2022).

Assim, as informações de gênero, idade, informações sobre a situação financeira, geolocalização e perfis pessoais não são consideradas como sensíveis pelo inciso II do artigo 5º da LGPD, apesar de frequentemente abrirem espaço para discriminação. Segundo Solove (2023), isso demonstra que "a abordagem dos dados sensíveis tem efeitos negativos porque exclui muitas situações muito importantes em que a lei deveria proporcionar uma proteção mais forte aos dados pessoais".

Para o autor, quando a lei protege alguns dados sob a sua alçada e outros não, dá-se a impressão de que algumas formas de discriminação são menos importantes que outras. O que a lei escolhe proteger e omitir tem um impacto expressivo.

4.3 Danos e riscos como fator determinante para a proteção diferenciada

Como demonstrado ao longo deste trabalho, pode-se perceber que as leis de privacidade atuais levam em consideração a natureza do dado como fator primário para determinar o tipo de proteção adequada. Tal proteção, focada em dados pessoais sensíveis e não sensíveis, pode parecer eficaz e mais simples, porém, como afirma Ohm (2015), é na verdade arbitrária e leva à subproteção ou superproteção dos dados.

Alguns estudiosos, como Daniel Solove, Danielle Citron, Paul Schwartz e Julie Cohen, reconhecem que os dados pessoais estão profundamente interligados com as pessoas e outros dados, de forma que não podem ser facilmente separados e classificados em categorias. Desta forma, trazem como sugestão que as leis de privacidade e proteção de dados tenham como foco os danos e riscos para uma

proteção mais rigorosa. Inclusive, Citron e Solove (2021), afirmam que inúmeras violações de privacidade são deixadas sem solução porque a lei falha em reconhecer os danos.

Em se tratando de dados pessoais, dano é a consequência negativa que existe devido a sua coleta, uso ou transferência, afetando o indivíduo ou a sociedade. Já o risco envolve a probabilidade e a gravidade de certos danos que ainda não ocorreram.

Com o advento do Regulamento Geral sobre a Proteção de Dados (GDPR), é possível perceber que há um gradual processo de "risquificação" presente nesta legislação europeia. Tal processo é identificável pelo reconhecimento da proteção de dados pessoais como regime de regulação de risco e pela adoção de instrumentos baseados em riscos (BERNARDES, 2022).

Tendo sido fortemente baseada na GDPR, a Lei Geral de Proteção de Dados brasileira (LGPD) possui, segundo Zanatta (2017), indícios de um modelo de regulação de risco. O primeiro elemento indicativo é o estabelecimento de padrões, objetivos e metas para definir as condições em que a atividade de tratamento é segura. O segundo elemento é a reunião de informações e cognição de riscos a fim de controlá-los. E, por fim, o terceiro elemento é o monitoramento da modificação do comportamento social (BERNARDES, 2022).

Assim, na LGPD, é possível perceber que estes elementos são satisfeitos a partir da existência de princípios que constituem um conjunto de regras de caráter procedimental (artigo 6º); nas bases legais em que o tratamento é autorizado por lei (artigos 7º e 11º); na responsabilização e prestação de contas sobre as operações desenvolvidas (artigo 50). Além da definição de responsabilidade dispostas nos artigos 52, 53 e 54, buscando a reparação dos danos resultantes dos riscos da atividade de tratamento.

No entanto, apesar de haver a inclusão do aspecto do dano e risco ao longo da Lei, pode-se perceber que ainda não possui um papel central. Para Solove (2023), as leis de proteção de dados ainda tentam abordar danos e riscos acionando requisitos sobre o processamento de dados sensíveis. Porém, tal abordagem inclui muitas situações que não são de alto risco e omite muitas situações que o são.

Danos e riscos como fator determinante para a proteção diferenciada não significa desconsiderar os avanços conquistados para a proteção de dados. O objetivo é que todas as situações possam ser consideradas por sua possível

consequência ao titular, pois, desta forma, haverá uma proteção proporcional e mais eficaz, baseada no contexto.

A proteção baseada no tipo de dados é igual independentemente das diferentes consequências que o tratamento pode trazer. Por exemplo, o endereço é considerado dado pessoal não sensível, significa, entre outras coisas, que o dano moral não é presumido a não ser que comprovado. Se o endereço de uma pessoa comum for vazado, tal procedimento é justificado. Entretanto, não fará tanto sentido em se tratando de uma mulher que sofre violência doméstica, pois dependendo da situação a proteção deste dado deve ser feita de maneira diferente e a responsabilização pelo vazamento penalizado com mais afinco, pelo prejuízo ao titular.

Para Citron e Solove (2021), a proteção focada em administrar os danos e riscos pode trazer a sensação para os indivíduos de que seu sofrimento é levado em consideração. Também declara que os responsáveis pelos danos serão responsabilizados pelas suas violações de privacidade. No entanto, é importante que não só os danos financeiros e físicos sejam considerados ou somente as situações com o risco muito alto.

As violações de privacidade podem levar a danos físicos, econômicos, reputacionais, psicológicos, de autonomia, de relacionamento. Os danos psicológicos, por exemplo, envolvem uma série de respostas mentais negativas, como ansiedade, angústia e preocupação (Citron e Solove, 2021). Faz-se importante, portanto, que os danos e riscos sejam apreciados de maneira aprofundada para que realmente se tenha uma proteção robusta em relação ao tratamento de dados pessoais.

Outra vantagem no enfoque em danos e riscos, de acordo com Solove (2023), é a possibilidade de evitar que o problema de privacidade seja utilizado como pretexto. As empresas estão utilizando a privacidade como pretexto para dificultar a concorrência, reduzir a responsabilização ou atingir outros objetivos que são desfavoráveis aos consumidores.

> A maior proteção da raça e da etnia pode minar as políticas de apoio às pessoas de cor. Em 2003, um referendo anti-ação afirmativa, a Iniciativa de Privacidade Racial, propôs proibir a recolha de dados sobre raça ou etnia para atacar políticas de ação afirmativa. O referendo foi finalmente rejeitado. Anita Allen observa que o referendo utilizou a proteção da privacidade racial como pretexto para atacar políticas que realmente beneficiavam grupos raciais. (SOLOVE, 2023, p. 48, tradução nossa).

Assim, tratar todos os dados sensíveis da mesma forma acrescenta combustível às tentativas de usar as proteções de privacidade como pretexto para atingir outros objetivos, como encobrir irregularidades governamentais ou empresariais ou, até mesmo, impedir políticas públicas, como mencionado.

Apesar de o enfoque em danos e riscos trazer maior complexidade que a proteção diferenciada baseada nos tipos de dados, também traz a vantagem de que a regulação se adapte às mudanças de tecnologia, mercados, estruturas institucionais, de políticas e obrigações legais (Black e Baldwin, 2010).

Os "novos estudiosos de privacidade", como denomina Ohm (2015), afirmam que, obviamente, nem todos os casos envolvendo riscos e danos serão claros. A lei deve fazer algumas generalizações já que não pode abordar cada situação de uma forma diferente. Para Solove (2023), uma possível solução seria focar em tipos de situação no lugar de focar em tipos de dados.

5 CONSIDERAÇÕES FINAIS

Esta monografia valeu-se de elementos teóricos e empíricos para construir uma reflexão acerca da evolução da proteção de dados no mundo, percebendo como os dados sensíveis são componente chave não só para a Lei Geral de Proteção de Dados brasileira.

Reconhece-se que a criação de leis de privacidade é um avanço para a proteção dos dados dos titulares ao buscar trazer-lhes de volta o controle acerca de suas informações. Bem como é possível afirmar que a proteção baseada em dados sensíveis foi essencial para o desenvolvimento das leis como se encontram hoje.

Não obstante, apesar de sua aparente praticidade, os dados sensíveis têm sua eficácia limitada frente às evoluções tecnológicas e o poder da inferência dos algoritmos atuais. A partir de dados não sensíveis, como os hábitos alimentares, é possível chegar-se a dados sensíveis, então não se está verdadeiramente protegendo os dados com o sistema atual.

Ademais, tal tipo de proteção desconsidera que há tanto dano ao titular em situações envolvendo dados pessoais não sensíveis quanto em situações envolvendo dados sensíveis. Sabe-se que estes são justificados perante a lei porque se trata de um conteúdo que, caso conhecido e processado, trariam vulnerabilidade ao titular. Entretanto, outras informações também abrem espaço para a discriminação e violação de liberdades fundamentais, mas não estão inclusas no artigo 5º, inciso II, como o gênero, a idade, as informações sobre a situação financeira.

Portanto, faz-se necessário pensar em uma modificação na Lei de Proteção de Dados brasileira a fim de que esta se adeque à realidade de maneira mais eficaz, sem que a solução seja apenas modificar seu texto adicionando novas previsões de tipos de dados sensíveis. Assim, traz-se como sugestão que as situações envolvendo o tratamento de dados e as violações de privacidade sejam analisadas a partir do viés do risco e do dano.

Sabe-se que o tratamento de dados é uma atividade que possui um risco eminente. Portanto, uma proteção baseada em danos e riscos pode ser mais adequada, pois analisará cada situação concreta e aplicará proporcionalmente a melhor solução independentemente do tipo de dado pessoal em questão.

REFERÊNCIAS

ADAM, Hammad; YANG, Ming Ying; CATO, Kenrick; BALDINI, Ioana; SENTEIO, Charles; CELI, Leo Anthony; ZENG, Jiaming; SINGH, Moninder; GHASSEMI, Marzyeh. Write It Like You See It: Detectable Differences in Clinical Notes By Race Lead To Differential Model Recommendations. **5th AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society, AIES**, p.7-21, 2022. Disponível em: https://arxiv.org/abs/2205.03931 . Acesso em: 13 dez. 2023.

BERETTA, Pedro. Sem meios eficazes, Lei Carolina Dieckmann até atrapalha. **Consultor Jurídico**, São Paulo, 10 maio 2014. Disponível em: www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha. Acesso em: 1 dez. 2023.

BERNARDES, Jade. **Regulação de risco na Lei Geral de Proteção de Dados**: análise de variáveis jurídicas relacionadas ao modelo teórico da regulação do risco sob o enfoque comparado do modelo TLICS. 88 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) — Universidade de Brasília, Brasília, 2022.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020

BIONI, Bruno Ricardo. **Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. GPoPAI/USP, 2015. Disponível em: https://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em: 4 dez. 2023.

BLACK, Julia; BALDWIN, Robert. Really responsive risk-based regulation. **Law and Policy**, v. 32, p. 181-213, 2010. Disponível em: https://eprints.lse.ac.uk/27632/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Black,%20J_Really%20responsive%20risk-based%20regulation_Black_Really%20responsive%20risk-based%20regulation_2014.pdf. Acesso em: 8 jan. 2024.

BRASIL. **Código de Defesa do Consumidor**. Lei n. 8.078, de 11 de setembro de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 1 dez. 2023.

BRASIL. **Constituição da República Federativa do Brasil**. Promulgada em 05 de outubro de 1988. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 1 dez. 2023.

BRASIL. **Lei do Cadastro Positivo**. Lei n. 12.414, de 9 de junho de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 1 dez. 2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 nov. 2023.

BRASIL. **Marco Civil da Internet**. Lei n. 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1 dez. 2023.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2130619**, do Tribunal de Justiça do Estado de São Paulo, DF, 23 de maio de 2022. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=AREsp%202130619. Acesso em: 8 dez. 2023.

BRIDGES, Khiara. **The Poverty of Privacy Rights**. Stanford, California: Stanford Law Books, 1ª edição, 2017.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura,** v. 1. São Paulo: Paz e Terra, 1999.

CITRON, Danielle; SOLOVE, Daniel. Privacy Harms. **GWU Legal Studies Research Paper,** v. 102, n. 2021-11, p. 793-863, 2021. Disponível em: https://ssrn.com/abstract=3782222or http://dx.doi.org/10.2139/ssrn.3782222. Acesso em: 10 jan. 2024.

CONSELHO DA EUROPA. **Explanatory Report on No. 108 of the Council of Europe Treaty Series —** Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 1981. Disponível em: https://rm.coe.int/16800ca434. Acesso em: 6 dez. 2023.

DONEDA, Danilo**.** A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL],** *[S. l.]*, v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 28 nov. 2023.

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

DONEDA, Danilo. Iguais mas Separados: O Habeas Data no Ordenamento Brasileiro e a Proteção de Dados Pessoais. **Cadernos da Escola de Direito**, v. 2, n. 9, 4 abr. 2017. Disponível em: https://portaldeperiodicos.unibrasil.com.br/index.php/cadernosdireito/article/view/2607/2180. Acesso em: 28 nov.2023.

EUROPA. **General Data Protection Regulation (GDPR).** Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 4 dez. 2023.

GREENLEAF, Graham. California's CPPA 2.0: Does de US Finally Have a Data Privacy Act?. **Privacy Laws & Business International Report**. v. 168, p 13-17, 2020. Disponível em: https://ssrn.com/abstract=3793435. Acesso em: 6 dez. 2023.

HINDS, J; JOINSON AN. What demographic attributes do our digital footprints reveal? A systematic review. **PLoS ONE,** v. 13, 2018. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0207112 . Acesso em: 9 dez. 2023.

KITCHENER, Michael ; ANANTHARAMA, Nandini ; ANGUS, Simon D. ; RASCHKY, Paul A. Predicting political ideology from digital footprints. **ArXiv**. Disponível em: https://arxiv.org/abs/2206.00397v1. Acesso em: 17 nov. 2023.

KOSINSKI, Michal. Private traits and attributes are predictable from digital records of human behavior. **PNAS,** v. 110, 2013. Disponível em: https://www.pnas.org/doi/epdf/10.1073/pnas.1218772110. Acesso em: 19 dez 2023.

MALDONADO, Viviane; BLUM, Renato. **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Thomson Reuters Brasil, 2022.

MASSO, Fabiano; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio. **Marco Civil da Internet**: Lei 12.965/2014. São Paulo: Editora Revista dos Tribunais, 2014.

MATSUMI, Hideyuki, Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?. **Cumberland Law Review**, v. 48, p. 149-210, 2018. Disponível em: https://ssrn.com/abstract=3222217. Acesso em: 9 dez. 2023.

MCCULLAGH, Karen. Data Sensitivity: Proposals for Resolving the Conundrum. **Journal of International Commercial Law and Technology**, V. 2, p. 190-201, Disponível em: https://ssrn.com/abstract=1378121. Acesso em: 6 dez. 2023

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

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v. 120, p.469-483, 2018. Disponível em: https://www.academia.edu/42741127/Reflex%C3%B5es_iniciais_sobre_a_nova_lei_geral_de_prote%C3%A7%C3%A3o_de_dados. Acesso em: 16 dez. 2023.

MORAES, Maria Cecília Bodin de. **Na medida da pessoa humana**: estudo de direito civil-constitucional. Rio de Janeiro: Renovar, 2010.

MULHOLLAND, C. S. 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, p. 159–180, 2018. DOI: 10.18759/rdgf.v19i3.1603. Disponível em:

https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 4 nov. 2023.

OHM, Paul. Sensitive Information. **Southern California Law Review**, Vol. 88, 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2501002. Acesso em: 8 jan. 2024.

PESSÔA, Camila. O que são cookies na internet e como funcionam. **Alura**. 2023. Disponível em: https://www.alura.com.br/artigos/o-que-sao-cookies-como-funcionam. Acesso em: 19 dez. 2023.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2020.

SCAICO, Pasqueline Dantas; DE QUEIROZ, Ruy José G. B.; SCAICO, Alexandre. O conceito big data na educação. *In*: WORKSHOP DE INFORMÁTICA NA ESCOLA (WIE), 20. , 2014, Dourados. **Anais**. Porto Alegre: Sociedade Brasileira de Computação, 2014 . p. 328-336. Disponível em: https://doi.org/10.5753/cbie.wie.2014.328. Acesso em: 19 dez. 2023.

SOLOW-NIEDERMAN, Alicia. Information Privacy and the Inference Economy, **Northwestern University Law Review**, V. 117, n. 2, p. 357-424, 2022. Acesso em: https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1. Acesso em: 9 dez. 2023.

RODOTÁ, Stefano. **A vida na sociedade de vigilância** - a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SCHWARTZ, Paul; SOLOVE, Daniel. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. **New York University Law Review**, Vol. 86, p. 1814-1894, 2011.

SERPRO. **Seu consentimento é lei!**. Disponível em: https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei . Acesso em: 4 dez. 2023.

SETZER, Valdemar. Dado, Informação, Conhecimento e Competência. **Revista de Ciência da Informação,** v.1, n.0, dez. 1999. Disponível em: https://www.ime.usp.br/~vwsetzer/datagrama.html. Acesso em: 6 dez. 2023.

SOLOVE, Daniel J. Data is What Data Does: Regulation Based on Harm and Risk Instead of Sensitive Data. **GWU Law School Public Law Research Paper**, No. 2023-22, 11 jan. 2023. Disponível em: https://ssrn.com/abstract=4322198. Acesso em: 4 out. 2023.

SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely. carnegie Mellon Univ., School of Computer Science , Data Privacy Lab., Working Paper No. 3, 2000.

UNIÃO EUROPEIA. Parlamento Europeu. Conselho Europeu. **Diretiva n. 95/46/CE**, 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. Bruxelas, 24 out. 1995. Disponível em: https:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5. Acesso em: 6 dez. 2023.

UNIÃO EUROPEIA. Comitê Europeu para Proteção de Dados (EDPB). **Guidelines on Automated Individual Decision Making and Profiling for the Purposes of Regulation 2016/679.** Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 9 dez. 2023.

WARREN S. D; BRANDEIS, L. D. **The right to privacy**. Harvard Law Review, Boston, V. 4, n. 5, dec, 1890. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 4 set. 2023.

ZANATTA, Rafael. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? **ANAIS Rede**, s.n, p. 147-193, 2017. Disponível em: http://www.redegovernanca.net.br/public/conferences/1/anais/Anais_REDE_2017-1.pdf#page=179. Acesso em: 8 jan. 2024.