VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

D597

Direito, governança e novas tecnologias III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires José Rover; Edson Ricardo Saleme; Jéssica Amanda Fachin. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-157-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

TEXTO INICIAL

GT DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III.

Nos dias 24, 25, 26 e 27 de junho de 2025, realizou-se o VIII Encontro Virtual do CONPEDI com a temática “Direito Governança e Políticas de Inclusão”. O evento objetivou promover a socialização das pesquisas jurídicas, desenvolvidas nos programas de pós-graduação e na graduação no Brasil, com ênfase na governança e das diversas políticas tecnológicas adotadas no Brasil. Com aporte em debate qualificado, coordenado pelos professores doutores Edson Ricardo Saleme (Universidade Católica de Santos), Jéssica Fachin (Universidade de Brasilia e Universidade de Londrina e Aires José Rover (Universidade Federal de Santa Catarina) no âmbito do GT Direito, Governança e Novas Tecnologias III. Observou-se no debate a configuração de agenda que buscou investigar as novas formas de governança, bem como estudar as atuais demandas contemporâneas que emergem das novas tecnologias, impactando nos diversos campos do Direito Nessa agenda foram revisitados, sob diversas abordagens, como temas complexos relacionados aos desafios conectados à regulação de novas tecnologias, a participação democrática no âmbito das relações digitais e ainda outras de fundamental importância à temática.

Nesse diapasão, o primeiro trabalho tratou do tema “Desafios regulatórios das tecnologias disruptivas: inteligência artificial, biotecnologia e blockchain no contexto jurídico brasileiro”, abordando as inovações propostas relativas a normatização da temática, ressaltando as tensões em torno dos problemas mais frequentes relacionados ao tema. O próximo tema “A

no caso PIX DO BRASIL: entre a liberdade de expressão e a responsabilidade nas redes sociais", o qual ponderou que, apesar da proposta de modernização e inclusão financeira, o Pix pode ser alvo de desinformações que minam a confiança sobre essa ferramenta.

O próximo artigo "Exposição digital infanto-juvenil e os limites da personalidade como Direito fez análise teórico-jurídica das deepfakes; enfocou a perspectiva da Teoria do Direito e a construção conceitual dos direitos da personalidade, os riscos emergentes impostos pelas tecnologias de inteligência artificial de falsificação e, especialmente as deepfakes, à privacidade e intimidade de crianças e adolescentes em ambiente digital. A seguir passou-se a explanação do artigo intitulado "do entusiasmo à desilusão: uma reflexão sobre a participação democrática na vida virtual", com enfoque na evolução da participação democrática em tempos digitais, analisando tanto o entusiasmo inicial quanto o ceticismo subsequente que emergiram com o avanço da internet". A seguir expôs-se a temática "A vulnerabilidade digital na sociedade informacional: uma análise econômica da democracia e tecnologia no sistema jurídico brasileiro", que ressaltou a necessidade de reavaliar políticas públicas para alcançar justiça social e eficiência democrática.

Na sequência, o artigo "Inclusão social na era da Smart Cities: o papel do Direito e da governança de tecnologias urbanas", fez analise critica na relação entre Direito, governança tecnológica e inclusão social no contexto das cidades inteligentes. O tema a seguir: "Boas práticas de conformidade à LGPD no desenho de bancos de dados relacionais" teve como objetivo apresentar um conjunto de boas práticas para o design de bancos de dados que atendam aos princípios da LGPD, como finalidade, necessidade, segurança e responsabilização. O próximo artigo: "Os impactos das tecnologias de fronteira na proteção integral de crianças e adolescentes: analise sobre o relatório da UNICEF THE STATE OF THE WORD`S CHILDREN no contexto internacional" buscou identificar as principais tendências que moldam o mundo atual e como prever seus efeitos no futuro dos jovens até 2050.

apresentou-se o “Estudo de caso sobre o potencial de satélites refletores de luz solar da start up ‘‘Reflect Orbital’ para o setor agrícola brasileiro”, o qual observa as novas oportunidades para a geração de energia renovável a exemplo de sua aplicação para aumento da produção agrícola, quanto crescimento e produção de culturas, a evolução de tecnologias para este fim se mostra essencial para a humanidade como um todo.

Importante também o “Estudo de caso da Start Up Reflect Orbital como impulsionadora na produção de energia fotovoltaica e seus aspectos jurídicos à luz da Lei 14.200/2022, que busca determinar o potencial energético e sua conformidade com os aspectos legais e diretrizes da Lei 14.300/2022 que regulamenta a geração de energia por consumidores finais. Outra importante reflexão foi o artigo: “Influência das redes sociais na formação da opinião pública: o papel do Direito na regulação de plataformas digitais” que analisa o papel do Direito na regulação das plataformas digitais, buscando identificar mecanismos jurídicos que garantam a proteção dos direitos fundamentais sem comprometer a liberdade de expressão. O estudo denominado “Neurodireitos na sociedade da transparência: o alerta da série adolescência da Netflix”, que parte da ideia do autor Byung-Chul Han sobre a sociedade da transparência para apontar os riscos da hiperexposição nas redes sociais, diante do uso desses dados pelas neurotecnologias no intuito de controle e manipulação.

Outra discussão relacionada aos temas expostos foi realizada com o levantamento da opinião dos presentes, que registraram sua opinião acerca dos diversos temas enfocados. O Grupo de Trabalho foi para o ultimo bloco a partir do tema “Sistema de registro eletrônico de imóveis – SREI: avanços e desafios ante a sobreposição de terras – análise de Adrianópolis – PR, Vale do Ribeira” que estuda o Sistema de Registro Eletrônico de Imóveis – SREI e sua relevância no contexto jurídico moderno, envolto em significativos avanços tecnológicos. Sequencialmente expôs-se o trabalho “Lei 14.932/2024 – utilização do Cadastro Ambiental Rural – CAR para fins de apuração da área tributável a compatibilização dos dados eletrônicos disponibilizados à Administração Pública para uma gestão mais eficaz”, cujo argumento indica que a Administração Pública já está utilizando inovações tecnológicas em

fundamental foi uma reflexão acerca da complexa relação entre modernidade, tecnologia e direito, com foco nas peculiaridades da modernidade periférica. Na sequência o trabalho "Edição genética de plantas: benefícios, riscos e regulamentação" destacou técnicas como CRISPR/Cas9 como ferramenta promissora para enfrentar desafios globais, como segurança alimentar e mudanças climáticas. O último artigo "Big techs e plataformas digitais: o Direito à informação e à liberdade de expressão no ecossistema tecnológico e a reconfiguração do estado-nação" questiona se as Big Techs e players tecnológicos a partir do direito à informação e à liberdade de expressão podem exercer alguma interferência no ecossistema digital possibilitando a reconfiguração do Estado-Nação contemporâneo.

Oportunizou-se mais uma sequência de discussões com contribuições benéficas para os assuntos discutidos e participação de grande parte dos presentes até o final dos trabalhos.

DESANONIMIZAÇÃO DE DADOS: CONCEITOS E DESAFIOS PARA A SOCIEDADE

DATA DE-ANONYMIZATION: CONCEPTS AND CHALLENGES FOR SOCIETY

Alvaro Ramos de Medeiros Raposo

Resumo

Este artigo visa explorar o tema da anonimização de dados, se debruçando sobre os riscos decorrentes que sua reversão, a desanonimização (também chamada de reidentificação), podem acarretar para os direitos fundamentais do cidadão. Para tal, além de um breve histórico sobre a evolução jurídica da temática da Proteção de Dados no ordenamento brasileiro, foram trazidos os principais conceitos desenvolvidos pela literatura específica e pela produção acadêmica da área. Por fim, foi realizado um levantamento a respeito das normas mais recentemente produzidas pela Autoridade Nacional de Proteção de Dados (ANPD), responsável pela fiscalização e aplicação de sanções nessa seara. Posto isso, ainda que seja perceptível a evolução do entendimento da problemática que envolve a anonimização de dados e os riscos envolvidos quanto a sua reidentificação, a prática dos órgãos brasileiros ainda se encontra em estágio bastante incipiente quanto a esforços que tenham o como alvo inibir práticas que comprometam direitos fundamentais e causem danos a seus titulares.

Palavras-chave: Anonimização, Direito ao esquecimento, Big data, Regulação, Proteção de dados

Abstract/Resumen/Résumé

This article aims to explore the topic of data anonymization, focusing on the risks that its reversal, de-anonymization (also called re-identification), can entail for the citizens' fundamental rights. To achieve this goal, in addition to a brief history of Data Protection in the Brazilian legal system, the main concepts developed by specific literature and academic production in the area were brought up. Finally, the most recent standards produced by the

1. INTRODUÇÃO

O reconhecimento ao direito à proteção de dados pessoais não é algo recente. A proteção à privacidade, consequência lógica do princípio da dignidade da pessoa humana e indissociável do direito do cidadão se autodeterminar, está previsto em diversas declarações e pactos internacionais, como a Declaração Universal de Direitos Humanos de 1948[1] e o Pacto de San Jose da Costa Rica de 1969[2].

O aumento do armazenamento e uso de dados pessoais por meio de ferramentas automatizadas vem atraindo a atenção internacional, que se mobilizou para reforçar o arcabouço normativo relativo ao tema. A primeira iniciativa de destaque foi a Convenção 108 do Conselho da Europa para a Proteção Pessoal em relação ao Tratamento Automatizado de Dados de Caráter Pessoal, datada de 28 de janeiro de 1981. Esse instrumento se propôs a "ampliar a proteção dos direitos e das liberdades fundamentais de todas as pessoas" e, ao mesmo tempo, "empenhar-se em favor da liberdade de informação sem limite de fronteiras". A ANPD representa o Brasil nas reuniões do Conselho Consultivo da referida convenção, posto que o país foi convidado a participar enquanto observador (BRASIL, 2024).

Posteriormente, a importância da Proteção de Dados Pessoais foi reforçada, no âmbito europeu com a Diretiva 95/46/CE de 1995, que destacou o papel dos sistemas de tratamento de dados que, segundo o documento, "estão a serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares", bem como "contribuir para o progresso econômico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos" (UNIÃO EUROPEIA, 1995).

Contudo, somente em 2009 a proteção de dados pessoais passou a ter efeito vinculante na União Europeia (PARLAMENTO EUROPEU, 2024), o que se deu na vigência do Tratado de Lisboa que, entre outros dispositivos, afirma que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" e ainda que "o cumprimento dessas regras fica sujeito a fiscalização por parte de uma autoridade independente"[3].

---

[1] Art. 12 da Declaração Universal de Direitos Humanos de 1948 ao afirmar que "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação."

[2] Art. 11 do Pacto de San Jose da Costa Rica de 1969: "Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação."

[3] Art. 16 do Tratado de Lisboa de 2007.

Seguindo a tendência europeia, a Constituição Brasileira de 1988 mostrou, ainda que tardiamente, que a preocupação com a Proteção de Dados Pessoais veio para ficar. O art. 5º, XII consagrou a inviolabilidade dos dados referentes a correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas. Até então, as cartas magnas do país fizeram somente referência a correspondências e comunicações telegráficas / telefônicas, ainda que já reconhecessem a proteção à intimidade, à vida privada e à imagem como direitos fundamentais (QUINTILIANO, 2021).

Contudo, somente no Projeto de Lei 4.060/2012 viu-se uma iniciativa parlamentar robusta o suficiente para pavimentar o início de um debate sobre a elaboração de um arcabouço normativo mais específico. Arcabouço esse que viria a ganhar forma com o Projeto de Lei 5.276/2016, de iniciativa da Presidência da República (LUCENA, 2021).

Como justificativa para a necessidade de uma Lei Geral sobre a temática, nossos parlamentares buscaram inspiração na própria Diretiva 95/46/CE da União Europeia. Assim foram trazidas reflexões fundamentais como a necessidade de criar parâmetros para a solução de controvérsias que envolvam a privacidade de dados, o desenvolvimento econômico e outros direitos fundamentais[4].

Além das considerações trazidas pela norma estrangeira, o Projeto de Lei 4060/2012 buscou contextualizar a importância de uma Lei de Proteção de Dados "em face do crescimento desse tipo de atividade e da comercialização ilegal desse tipo de informação" e ressaltou o poderio das chamadas Big Techs, em especial citando o enorme poder de influência de empresas como o Facebook e o Google por violarem "a privacidade de seus usuários, franqueando o acesso a esses dados à NSA, a agência de segurança americana" e presumirem que seus usuários estejam cientes de que o conteúdo confiado a essas empresas é tratado por ferramentas de processamento automático (CÂMARA DOS DEPUTADOS, 2012).

Assim nasceu a Lei 13.709/2018 destinada à uniformização da matéria e a colocar a dignidade da pessoa humana no centro das discussões. A Lei Geral de Proteção de Dados (LGPD), teve inspiração na General Data Protection Regulation (GDPR) (LORENZON, 2021, pg. 43), legislação que unificou a proteção de dados no continente europeu e, assim como a lei brasileira, dispõe sobre o tratamento de dados pessoais, inclusive nos meios

[4] Considerando nº 2 da Diretiva 95/46/CE ao afirmar que "os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos".

digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade dos cidadãos.

Entre as ações previstas na GDPR e que inspiraram a LGPD está a necessidade de anonimização de dados, que possibilita o seu armazenamento, uso e, ao mesmo tempo, a salvaguarda a privacidade de seus titulares (LORENZON, 2021, pg. 46). O procedimento está descrito no art. 5º, XI da lei geral brasileira como "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

Já a Agência Nacional de Proteção de Dados (ANPD) define a anonimização como "um processo pelo qual os dados com capacidade de identificar um titular são transformados de maneira que a probabilidade de associá-los, diretamente ou indiretamente, a um titular específico é reduzida." (BRASIL, 2023, pg. 4).

Há, portanto, algo em comum tanto o conceito legal quanto no oferecido pela agência: a impossibilidade de se garantir que a anonimização persistirá em face da constante evolução tecnológica. Como afirmam ambos os textos, 'meios técnicos razoáveis' são empregados visando reduzir uma 'probabilidade de associação' de dados presente no momento em que as técnicas são empregadas.

Assim, cabe à regulação buscar unir neutralidade, flexibilidade e efetividade para que possa enfrentar a tarefa árdua de tentar acompanhar a inovação tecnológica, no caso em análise, a evolução das técnicas de desanonimização. Constatando essa evolução é sempre mais veloz que o desenvolvimento regulatório Vermeulen et al. (2016, pg. 5) afirma que:

> Desenvolver uma estrutura regulatória que garanta a segurança de seus usuários e da população em geral, ao mesmo tempo em que facilita o uso comercial e a satisfação do consumidor com a inovação disruptiva não é nada fácil. Isso é ocorre particularmente em cenários contemporâneos, onde a inovação é mais rápida e a disseminação global da tecnologia é muito mais veloz.

Extremamente sensível à evolução tecnológica, o objetivo desse artigo é discorrer sobre a anonimização e a reidentificação de dados, elencando os principais conceitos adotados pela literatura e pela academia, além de trazer uma breve análise da produção documental recente desenvolvida pela ANPD, órgão que detém a competência legal de fiscalizar e aplicar sobre esse assunto.

2. ANONIMIZAÇÃO E REIDENTIFICAÇÃO: CONCEITOS E DESAFIOS

A coleção de dados, pessoais ou não, em escala cada vez maior é parte integrante do que passou a ser chamado de Economia Digital (FERNANDES; GAMA, 2007, pg. 1). Dados sobre o uso de sites de busca, histórico de navegação, redes sociais, históricos médicos, entre outros, são coletados e compartilhados com órgãos do governo, pesquisadores, plataformas de comunicação (digitais ou não) e anunciantes. Muitos destes entes afirmam, por ignorância ou não, compartilhar essas informações somente de modo não pessoalmente identificável, ou seja, utilizando-se de técnicas de anonimização.

Contudo, conforme Narayanan e Shmatikov (2010, pg. 25), muitas vezes esses entes partem da premissa que os dados capazes de identificar seu titular consistem em um conjunto fixo de atributos e que, uma vez anonimizados, garantam a privacidade do indivíduo.

Concordando com a afirmação acima, outros autores, dentre os quais Bioni (2020, pg. 193), são categóricos ao afirmar a falibilidade do processo de anonimização. Ao discorrer sobre a razoabilidade exigida pela LGPD (em seu art. 5º, III) para a escolha de meios técnicos para realização da anonimização, o autor a divide em dois eixos. O eixo objetivo diz respeito ao estado da arte da tecnologia, que envolve uma análise do custo e do tempo que se levaria para reverter o processo de anonimização quando esta é empregada. Já o eixo subjetivo considera a capacidade do próprio agente de tratamento de dados em reverter esse processo. Por exemplo, o acesso a uma segunda base de dados que permita a identificação das pessoas constantes na primeira, o que convencionou-se chamar de pseudoanonimização.

Além dos meios tecnológicos para reidentificação dos dados ainda é possível a reunião de informações constantes em várias fontes de forma que se consiga identificar. Essa prática é chamada de ‘Efeito Mosaico’ e é uma preocupação relevante especialmente quando grandes conjuntos de dados são processados (BIONI, 2020, pg. 1).

Esse cenário tende a ser cada vez mais comum conforme o poder de processamento dos dispositivos eletrônicos aumenta. De acordo com Kitchin (2014, pg. 99), até então a tecnologia era limitada pelo que ficou conhecido como “Os Três V’s” (Volume, Velocidade e Variedade). Contudo, hoje se fala em de petabytes de dados processados em tempo real de forma estruturada ou não. A junção dessas três características é chamada pelo autor de Big Data e é a mola propulsora de inovações disruptivas em conjunto com outras tecnologias como Machine Learning, Inteligência Artificial e a Internet das Coisas.

Em conjunto ou não, o processamento de dados em larga escala realizado utilizando-se dessas tecnologias ficou comumente conhecido como Mineração de Dados (Data Mining), conceito que Oliveira Filho (2020, pg. 43) divide em duas etapas. A primeira consiste na análise realizada por softwares no sentido de encontrar padrões, referências ou conexões nos dados coletados. A segunda etapa consiste na análise preditiva, ou seja, em suposições sobre ocorrências futuras.

Parte inerente a essas duas etapas e ao objetivo central da mineração de dados está a busca pela utilidade dessas informações por áreas diversas como medicina, educação, segurança pública etc. Assim, as soluções que proponham garantir a privacidade dos indivíduos por meio da anonimização costumam considerar o quanto dessa utilidade pode se perder na aplicação dessas técnicas (GROSSMAN et al, 1999, pg. 1).

2.1. O PROCESSO DE ANONIMIZAÇÃO DE DADOS

Assim como a tecnologia para cruzamento de informações passou por grandes mudanças, a ciência que fundamenta a anonimização dos dados também precisou evoluir. Nessa perspectiva, autores buscaram formas de sistematizar o processo de anonimização de dados, de forma que se possa encontrar etapas bem definidas que garantam a privacidade dos dados da melhor maneira possível.

Primeiramente, a ciência buscou categorizar unidades dados de acordo com a possibilidade de identificação pessoal que cada uma possui. Quanto a isso, Lubarsky (2017, 203) definiu que dados podem ser classificados como Identificadores Diretos, Identificadores Indiretos, Dados Relativos a Múltiplos Indivíduos e Dados Não Relacionados a Indivíduos.

Assim, identificadores diretos são dados como nome, número de documentos (CPF, título de eleitor, CNH etc), número de telefone, entre outros. Já os identificadores indiretos são dados identificáveis a partir da combinação de poucos elementos como gênero, data de nascimento e CEP (LUBARSKY, 2017, 203).

Os dados relativos a múltiplos indivíduos ou, segundo Oliveira Filho (2020, pg. 7) os Dados Coligados, são os que se conectam com preferências ou características comuns de vários indivíduos como restaurantes frequentados ou medidas físicas.

Há também os dados que não dizem respeito a nenhuma pessoa específica, como dados agregados de censo e resultados gerais de pesquisas. Por último, há os dados

impessoais, que não dizem respeito a pessoas, como dados sobre clima e sobre a geografia de um local (LUBARSKY, 2017, 203).

Após classificar os dados quanto ao nível de identificação pessoal, Lubarsky (2017, 205) definiu as formas de anonimização de dados em si. Para o autor existem quatro formas de anonimização de dados pessoais: Remoção de dados (Remove / Redact), substituição por pseudônimos (Pseudonyms), inclusão de ruídos estatísticos (Statistical Noise) e agregação.

O primeiro método, a Remoção de Dados é quase autoexplicativa. Consiste na exclusão de informações que possam diretamente identificar uma pessoa, por exemplo: o nome ou o número de documentos como RG e CPF (LUBARSKY, 2017, 205).

A pseudonimização consiste na substituição de dados por outros gerados aleatoriamente ou por meio de um algoritmo. A abordagem visa manter a utilidade da informação para fins de cruzamento, porém sem identificar seu titular. Ela é menos prática, já que nem sempre a substituição de identificadores é possível ou mantém a utilidade dos dados. É aberta, também, a possibilidade de identificação por engenharia reversa, caso a pseudonimização não tenha sido realizada aleatoriamente (LUBARSKY, 2017, 206).

Já a introdução de ruído estatístico, consiste no acréscimo de informações que tornem o dado menos preciso, mas sem substituí-lo. O que, na prática, torna apenas tornando a identificação mais difícil. Dentre várias formas de inclusão de ruído, o autor cita a generalização, a perturbação e o intercâmbio, que podem ser descritas como:

> Generalização: Valores específicos podem ser informados em intervalos. Por exemplo, a idade de um paciente pode ser informada como 70-80 ao invés da divulgação da data de nascimento completa.
>
> Perturbação: Valores específicos podem ser ajustados de forma aleatória em um conjunto de dados. Por exemplo, a adição ou subtração do mesmo número de dias de quando um paciente deu entrada em um hospital.
>
> Intercâmbio: Dados podem ser trocados entre registros de um conjunto de dados (LUBARSKY, 2017, 207) (tradução nossa).

A agregação possui similaridades com o ruído estatístico no sentido de tornar o dado menos preciso, porém ao invés de serem exibidos os dados propriamente ditos (após generalização, perturbação ou intercâmbio), somente um resumo dessas informações é publicizado. Por exemplo, ao invés de mostrar dados sobre pacientes de um hospital, mostra-se somente sua quantidade dividida em subgrupos como masculino/feminino, crianças/adultos, etc. Dessa forma, tanto os identificadores diretos como indiretos são removidos da publicação (LUBARSKY, 2017, 208).

Como toda técnica de anonimização, quanto mais identificadores diretos ou indiretos forem alterados ou removidos, menos útil podem se tornar os dados para análises. Considerando que esses dados são capturados, armazenados e processados para um determinado fim, a ponderação entre utilidade e finalidade deve ser considerada.

2.1. O PROCESSO DE REIDENFIFICAÇÃO DE DADOS

Após trabalharmos os pontos importantes quanto a anonimização (também chamada de desidentificação), chega o momento de traçar o caminho inverso. Conforme Santanna (2023, pg. 85) a desanonimização ou reidentificação ocorre quanto dados aparentemente não identificáveis, ao serem confrontados por informações de outras fontes, podem ser vinculados a uma identidade pessoal por meio da descoberta de identificadores diretos ou indiretos. Conforme já dito, esse processo sofre grande influência do desenvolvimento tecnológico, nos últimos anos especialmente a evolução de tecnologias como Big Data e Machine Learning.

Logo, ainda que seja adotado um processo rigoroso de anonimização e que se siga leis e regulamentos, não há garantias que o procedimento será bem-sucedido de maneira perene.

Segundo Lubarsky (2017, pg. 209) existem três métodos para a reidentificação de dados: desidentificação insuficiente, reversão de pseudônimos e combinação de conjuntos de dados.

A desidentificação insuficiente ocorre quando o processo de eliminação de identificadores direito e indiretos é incompleto. Assim, é possível desanonimizar os dados a partir do aproveitamento de identificadores remanescentes tanto em informações estruturadas quanto desestruturadas (LUBARSKY, 2017, pg. 209).

A reversão de pseudônimos pode acontecer pelo fato de, muitas vezes, a aplicação desse processo de anonimização ter sido escolhida com a intenção de que uma possibilidade de reversão exista. Tal qual uma forma de criptografia, é criada uma chave que, se não for mantida de forma segura, pode ocasionar vazamento de dados. Além disso, quando o pseudônimo é utilizado por diversas vezes, ele se pode se tornar um padrão que deixa pistas quanto a seu significado real (LUBARSKY, 2017, pg. 210).

Já a combinação de conjuntos de dados (datasets) é bastante intuitiva. Quanto mais dados e mais diversas suas fontes, melhor ocorrerá o processo de reidentificação. Essa se dá

a partir da junção de informações de um mesmo indivíduo em conjuntos diferentes. Mesmo informações aparentemente desimportantes podem ser potenciais causas de vazamento de dados pessoais se processadas por tecnologias e profissionais especializados (LUBARSKY, 2017, pg. 211).

2.2. A ANONIMIZAÇÃO E O DIREITO AO ESQUECIMENTO

Diante do exposto até então, resta evidente que a chance de reidentificação reside não somente na 'má anonimização', mas, conforme já dito, na evolução da tecnologia utilizada para processamento, cruzamento e análise de dados aplicada com esse objetivo. Assim, não é exagero afirmar que há um risco inerente de vazamento de dados pessoais em todo e qualquer compartilhamento. Por conta disso, uma questão poderia parecer sanada e invariavelmente continuará em pauta é a do Direito ao Esquecimento.

Segundo Fujita e Barreto Junior (2020, pg. 15), o Direito ao Esquecimento significa:

> É o direito de ser deixado em paz, de ficar no anonimato, que se encontra inserido no conceito de vida privada, da qual é parte. É o direito de eliminar, ocultar e cancelar aquelas informações ou feitos pretéritos relativos à vida das pessoas físicas e que podem condicionar o seu futuro".

A problemática que contrapõe o Direito ao Esquecimento à Anonimização nasce na consideração de "Dados Pessoais" como oposto a "Dados Anonimizados". Como vimos, a própria LGPD entende, em seu art. 5º, III, que o emprego de meios técnicos na remoção de identificadores deve ser considerado com razoabilidade, na medida em que não há como garantir que essa operação seja irreversível.

Por isso, ao discorrer sobre a problemática de dados presentes em prescrições médicas, Oliveira Filho (2020, pg. 83) afirma:

> No momento que informações prescricionais são captadas pelas farmácias, pacientes deveriam ser informados que informações anonimizadas seriam compartilhadas com terceiros, mesmo diante dos riscos de re-identificação. Caso não aceitem, as informações deveriam ser excluídas dos bancos de dados através de solicitação expressa. Essa forma garantiria ao paciente o direito ao esquecimento.

Contudo, o próprio autor reconhece a inviabilidade técnica da exclusão desses dados. Isso ocorre pois, na prática, as próprias empresas ou órgãos deveriam ter capacidade para a reidentificá-los previamente antes de apagá-los (OLIVEIRA FILHO, 2020, pg. 83). Em outras palavras, essa exigência consistiria em impor o ônus a empresas de sempre estarem

buscando o ‘estado da arte’ em matéria de tecnologia voltada a anonimização/desanonimização, indo além dos ‘meios técnicos razoáveis’ exigidos pela lei.

Com isso, considerando que não há mais vínculo pessoal com os dados após o processo de anonimização e estes estando, portanto, livres para serem compartilhados, a LGPD remove a responsabilidade dos agentes de tratamento em caso de uma futura reidentificação.

Logo, é possível afirmar que não há uma proteção contra a reidentificação de forma abstrata, ou seja, que permita ação preventiva por parte do direito, restando à regulação a responsabilização de quem, agindo com culpa ou dolo, causar dano ao titular dos dados após a sua reidentificação. Sobre a responsabilização Oliveira Filho (2020, pg. 86) afirma:

> A LGPD trata de duas espécies de responsabilidade: civil e administrativa. A responsabilidade administrativa prevê sanções dispostas pelo artigo 52, através da Autoridade Nacional de Proteção de Dados. Já a responsabilidade civil possui fundamento no artigo 42 da LGPD, atribuindo dever de reparação por danos causados pelo uso de dados pessoais, sendo a teoria da responsabilidade do Código Civil um importante complemento.

Com isso, fica claro que a mineração de dados em si, por parte de empresas especializadas não é uma ação passível de punições enquanto não for caracterizado o prejuízo gerado ao titular de seus dados, claramente limitando direitos fundamentais como o da privacidade e igualdade.

Na medida em que a ausência de proteção em abstrato contra a reidentificação de dados incentiva a contínua mineração de dados, na prática, os titulares dessas informações são vigiados e catalogados constantemente em espécies de perfis sociais que podem se tornar, em último caso, fontes de discriminação e permitir a elaboração de legislações segregatórias, entre outras práticas, a depender de quem tiver posse dessas informações (LESSIG, 2006, pg. 235).

Portanto, essa problemática ainda precisará de um debate maior e mudanças legislativas serão ser necessárias para uma maior proteção à sociedade em face à mineração de dados.

3. A ANONIMIZAÇÃO, A DESANONIMIZAÇÃO E O BRASIL

Os frutos do desenvolvimento tecnológico nascem e são assimilados pela sociedade de forma mais célere do que as mudanças legais necessárias para regulá-los. Trazendo o exemplo de Vermeulen et al. (2016, pg. 6) sobre carros autônomos, a regulação dessa seara

não ocorre somente no sentido de que a circulação destes veículos seja permitida pela legislação de trânsito, mas também por questões de segurança, comunicação e, principalmente, quanto a proteção da enorme quantidade de dados gerados. Visto isso, fica claro que a complexidade e a indeterminação envolvidas na tentativa de regulação de novas tecnológicas ocorre em um grau maior do que outrora.

Isso acontece porque a base de toda e qualquer regulação, segundo o mesmo autor, se dá na avaliação de fatos que ocorrem na sociedade e a partir dessa análise obter a resposta para três perguntas: “O que regular?”, “Quando regular?” e “Como regular?” (VERMEULEN et al., 2016, pg. 7).

Contudo, vimos que o rápido desenvolvimento tecnológico torna análise desses questionamentos mais complexa na medida em que nem sempre é simples avaliar o escopo da inovação trazida (O que), nem o momento ideal para adotar uma regulação que não desincentive a inovação (Quando), tampouco as formas e os limites que essa regulação deve possuir (Como).

Em se tratando de anonimização/desanonimização de dados esse quadro não se difere, posto que esses procedimentos envolvem inovações trazidas por meio de tecnologias como Machine Learning, Big Data e Inteligência Artificial, que trouxeram ganhos irreversíveis para a sociedade em todas as áreas do conhecimento humano.

Em janeiro de 2024 a ANPD abriu consulta pública sobre a minuta de um Guia de Anonimização e Pseudonimização para a Proteção de Dados Pessoais com o objetivo de ouvir opiniões sobre esse documento, então ainda fase de elaboração (BRASIL, 2024).

Para subsidiar as sugestões a agência elaborou três estudos técnicos sobre Anonimização de Dados. O primeiro aborda um processo baseado em risco e técnicas computacionais, o segundo aborda a perspectiva da análise jurídica e o terceiro reúne estudos de casos sobre anonimização de dados de acordo com a LGPD. O órgão também afirma que esses documentos:

> Juntos, sugerem que a anonimização de dados deve ser baseada em riscos, uma vez que não é totalmente confiável.
>
> Segundo os documentos, a rápida evolução da tecnologia afeta diretamente o processo. É possível, por exemplo, que um recurso superveniente identifique um dado até então anonimizado.
>
> Os estudos destacam, também, que todas as técnicas de anonimização têm vantagens e desvantagens. Os agentes de tratamento devem, portanto, tratar o assunto como um processo, administrando os riscos de cada técnica (BRASIL, 2024).

A seguir serão expostas considerações sucintas sobre os documentos de Análise Jurídica e de Visão de Processo Baseada em Riscos.

3.1. ANÁLISE JURÍDICA DA ANPD

A análise jurídica realizada pela ANPD traz conceitos que visam a formação de uma base teórica que possa fundamentar futuras diretrizes do órgão, especialmente quanto à problemática da anonimização.

Conceitos como anonimização e dado anonimização, presentes na Lei Geral, já foram abordados ao longo deste trabalho, mas são de fundamental importância na formação de um 'vocabulário comum' entre a Agência e seus jurisdicionados. Dentre esses conceitos podemos destacar o entendimento sobre identificadores diretos, indiretos, pseudonimização e desidentificação (BRASIL, 2023a, pg. 7).

Do caput do art. 12 da LGPD deve-se ter em mente que a anonimização de dados não é uma atividade estanque, mas sim um conjunto de ações que fazem parte de um processo composto pela aplicação de várias técnicas que visam ocultar identificadores presentes em um conjunto de dados. Quanto a isso, o órgão considera que o ato inicial de anonimização se trata de operação de tratamento de dados pessoais, portanto, deve obediência à LGPD até sua conclusão e, ainda, não tem o condão de tornar legais atos que previamente tenham sido tomados em desacordo com a norma jurídica, o que inclui princípios como o da finalidade, adequação e necessidade (BRASIL, 2023a, pg. 9).

Em relação ao conceito de Dados Pessoais a ANPD faz questão de salientar que a LGPD adotou o que chama de Perspectiva Expansionista. Essa perspectiva é concretizada no art. 5º, I, da Lei, e considera 'dado pessoal' a informação referente à Pessoa Natural Identificável, ou seja, aquela que pode ser identificada pela adoção de meios técnicos e esforços razoáveis seja por parte do agente de tratamento quanto por parte de terceiros (o que chama de abordagem absoluta ou objetiva). Assim, os chamados meios técnicos e razoáveis funcionam, na prática, como um limite para o que pode ser considerado um dado pessoal (BRASIL, 2023a, pg. 12).

De inspiração europeia, essa espécie de 'responsabilidade compartilhada' por dados passíveis de identificar seus titulares é, conforme a ANPD salienta, compatível com a Lei n. 12.695/2014 (Marco Civil da Internet) na medida em que o diploma legal exige a guarda de logs de conexão e de acesso tanto a provedores de conexão quanto provedores de aplicação, de forma a não concentrar os dados de navegação em um só serviço, promovendo uma

complexidade sistêmica no processo de reidentificação que garante uma maior proteção ao usuário (BRASIL, 2023a, pg. 15).

Embora expresso anteriormente, a Agência salienta que, ainda que existam critérios exemplificativos do que consistiria essa razoabilidade quanto aos meios utilizados na anonimização de dados, previstos em documentos como a Diretiva n. 95 /46/CE (Comissão Europeia), os casos concretos devem ser analisados considerando o momento e as circunstâncias em que estes ocorreram (BRASIL, 2023a, pg. 15).

Logo, é sugerido um emprego de recursos em técnicas de anonimização que considere uma Análise de Riscos. Assim, é recomendada a avaliação de 'possíveis ataques de reidentificação' e a probabilidade de eles serem bem-sucedidos.

3.2. VISÃO DE PROCESSO BASEADO EM RISCO E TÉCNICAS COMPUTACIONAIS

A ANPD realizou, em novembro de 2023, um Estudo Técnico sobre a aplicação de um modelo baseado em Análise de Riscos voltado para a Anonimização de Dados, com vistas a atender da melhor forma as exigências previstas na LGPD.

O documento gerado a partir deste estudo visa subsidiar a agência para que esta disponha sobre padrões e técnicas utilizadas em processos de anonimização, em atenção ao previsto no art. 12, §3º da LGPD. Além disso, o trabalho orienta agentes de tratamento a adotarem um padrão de anonimização de forma contínua e baseada em riscos, servindo como um guia de boas práticas (BRASIL, 2023b, pg. 4).

A ANPD salienta que é de fundamental importância que quem exerça o tratamento dos dados esteja ciente dos riscos envolvidos na sua atividade para assim atuar na mitigação de forma proporcional (BRASIL, 2023b, pg. 5).

O estudo traz outros pontos já abordados como o conflito entre a utilidade do dado anonimizado versus o nível de anonimização adotado. Como dito anteriormente, o processo de anonimização é executado visando atender uma finalidade, o que é determinante para o estabelecimento do nível máximo de anonimização possível. Assim, o trabalho afirma haver um ponto ótimo em que a proteção aos dados pessoais é alcançada ao máximo sem comprometer a finalidade que se deseja atingir (BRASIL, 2023b, pg. 6).

Portanto, o entendimento da anonimização como um processo contínuo baseado em risco implica a existência de um contexto que deve ser entendido pelo agente de tratamento

para que assim haja a definição das técnicas utilizadas e do grau de utilidade necessário para o alcance da finalidade do órgão.

Para esse mapeamento contextual, o estudo sugere que seja documentado o processo de anonimização realizado e um controle dos estados que o conjunto de dados passou a apresentar ao longo do processo. Além disso a análise afirma:

> Em especial atenção, observa-se que o conjunto de dados resultante deve manter as propriedades estatísticas da base em sua forma original. Caso contrário a qualidade dos dados poderá ser degradada, diminuindo ou até mesmo impossibilitando alcançar a finalidade pretendida.
>
> Considerando que, majoritariamente, as técnicas de anonimização adicionam ruído aos dados, essa adição pode acarretar mudanças nas propriedades estatísticas do conjunto de dados (BRASIL, 2023b, pg. 7).

Logo, os registros tanto das mudanças de estado dos dados quanto das propriedades estatísticas são fundamentais para a ponderação entre utilidade e anonimização citada.

Outra questão importante para a gestão de riscos ocorre quanto ao nível de conhecimento que uma parte interessada possa ter sobre os dados que deseja reidentificar. Sobre o tema, o estudo realizado pela ANPD se apoia em pesquisa realizada pelo National Institute of Standards and Technology (NISTIR) que identificou dois cenários em que costuma ocorrer a reidentificação de dados: O primeiro foi chamado de Reidentificação do Promotor e o segundo de Reidentificação do Jornalista (NISTIR, 2015, 11).

> O primeiro é conhecido como reidentificação do promotor, que parte da hipótese de que o atacante conhece um indivíduo em particular do conjunto de dados e deseja encontrar o registro relacionado a ele. O segundo é conhecido por reidentificação do jornalista, que parte da hipótese de que o atacante não conhece um indivíduo em particular do conjunto de dados e deseja somente conseguir reidentificar qualquer indivíduo (Tradução nossa).

De posse dessas informações, ainda que cada processo de anonimização possua características únicas, a ANPD considerou que existam em comum algumas fases importantes.

Visando identificar um limite máximo de risco sobre um conjunto de dados, a agência chamou a primeira etapa de Determinação do Risco de Reidentificação Aceitável (RRA) e cita como exemplo de variáveis que devem ser observadas dentro de um contexto, como a presença de dados sensíveis ou financeiros como razão para diminuição da tolerância a risco (BRASIL, 2023b, pg. 8).

A segunda etapa se trata da aplicação dos procedimentos de anonimização em si e deve ser executada de forma que não seja ultrapassado o limite de risco acordado na fase antecedente (BRASIL, 2023b, pg. 9).

A fase seguinte é chamada de Determinação do Risco de Reidentificação Mensurado (RRM) e consiste na análise da probabilidade de um ataque de reidentificação ser bem-sucedido sobre um determinado conjunto de dados. A agência traz como exemplo o nível de publicização do conjunto de dados (se público, privado ou compartilhado).

O esgotamento das questões relacionadas a quantificação do risco de reidentificação de dados foge ao escopo deste trabalho, de forma que a leitura do estudo realizado pela ANPD é recomendada em sua integralidade, na medida em que o estabelecimento de métricas contextuais é desenvolvido a partir de conceitos de teoria dos conjuntos, como equivalência de classe, grau de unicidade etc. de forma a se calcular um nível probabilidade de reidentificação, ou seja, um valor de risco (BRASIL, 2023b, pg. 10).

Vale frisar que as formas de anonimização expostas anteriormente (como remoção de dados, generalização, perturbação e intercâmbio) tratam essencialmente de conjuntos de dados estruturados e estáticos. O estudo da ANPD é oportuno em lembrar que o desenvolvimento tecnológico vem tornando frequente o cenário em que fluxos de dados podem gerar riscos à privacidade de seus titulares e tornam a aplicação de técnicas de anonimização inviáveis em termos de quantidade de processamento (BRASIL, 2023b, pg. 12).

Essas formas de anonimização também se limitam a anonimização de textos, para anonimização de imagens há técnicas específicas (como pixelação, Fawkes, ruído gaussiano, entre outras), assim como existem técnicas de reidentificação voltadas para esse fim especialmente ligadas ao Machine Learning (BRASIL, 2023b, pg. 15).

Para profissionais e curiosos da área de tecnologia que visem buscar o aprofundamento quanto a técnicas de anonimização recomenda-se a leitura dos apêndices do trabalho realizado pela ANPD (Estudo técnico sobre anonimização de dados: Uma Visão de Processo Baseado em Risco e Técnicas Computacionais).

CONSIDERAÇÕES FINAIS

A anonimização de dados, embora uma prática importante para a preservação da privacidade dos cidadãos, enfrenta grandes desafios devido ao avanço contínuo das tecnologias de reidentificação. Em um mundo onde o Big Data e a Inteligência Artificial facilitam cada vez mais a análise e o cruzamento de grandes volumes de dados, o potencial de desanonimização aumenta de forma proporcional, revelando uma dicotomia entre o uso

dos dados para desenvolvimento econômico, progresso científico e inovação tecnológica, e o direito fundamental à privacidade.

A LGPD, inspirada pela regulamentação europeia (GDPR), foi um avanço significativo para fortalecer e modernizar a legislação brasileira nessa seara. Contudo, o tema e as práticas adotadas pelas empresas, em especial as Big Techs, ainda seguem em modificando a realidade social e econômica, de forma que os benefícios e prejuízos causados ainda estão sendo contabilizados.

Apesar das barreiras legais e técnicas, não existe uma solução que ofereça proteção absoluta contra a desanonimização. Logo, uma questão a ser discutida é a possibilidade jurídica de proteção abstrata dos cidadãos em face ao risco de desidentificação, principalmente considerando que as empresas especializadas em Data Mining estarão sempre à frente do desenvolvimento da tecnologia, aplicando técnicas avançadas e capazes cruzar dados anonimizados com outros que possam trazer à tona a identidade de seus titulares.

Como vimos, a reflexão sobre a anonimização e a desanonimização de dados ultrapassa a esfera da privacidade, implicando também em questões de igualdade e justiça social. A utilização indevida de dados pessoais reidentificados pode levar medidas discriminatórias a partir da criação de perfis comportamentais (ou os tão falados Scores Sociais).

Quanto ao tema, além dos conceitos e técnicas de anonimização apresentados, foi citada a importante contribuição documental da ANPD. Contudo, deve ser ressaltado que ela ainda representa um pequeno e tardio avanço em relação ao tema. O nível atual de estruturação da Agência e a seriedade da problemática necessitam de passos e debates mais céleres, especialmente quanto a aspectos fiscalizatórios e sancionatórios.

Portanto, a proteção contra a desanonimização deve ser reavaliada de forma constante, buscando acompanhar o desenvolvimento tecnológico e analisando os prejuízos causados à sociedade. Para isso, o tema ser encarado como uma prioridade legislativa, acadêmica e ética, de modo que a tecnologia seja um instrumento para o bem coletivo e não uma ameaça à dignidade e a autonomia das pessoas.

REFERÊNCIAS

CÂMARA DOS DEPUTADOS. Projeto de Lei 4060/2012. Dispõe sobre o tratamento de dados pessoais. Disponível em

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2083188>. Acesso em 24 de janeiro de 2024.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos. São Paulo. nº. 53. Disponível em: https://is.gd/bb48ei. Acesso em 01/09/2024.

BRASIL. Agência Nacional de Proteção de Dados. ANPD abre consulta à sociedade sobre o Guia de Anonimização e Pseudonimização. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-a-sociedade-sobre-o-guia-de-anonimizacao-e-pseudonimizacao. Acesso em 10 set. 2024.

BRASIL. Agência Nacional de Proteção de Dados. ANPD participa da 41ª Reunião Plenária da Convenção 108 <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-representa-o-brasil-na-44a-reuniao-plenaria-do-comite-consultivo-da-convencao-108>. Acesso em 22 de janeiro de 2024.

BRASIL. Agência Nacional de Proteção de Dados. Estudo técnico sobre anonimização de dados: Análise Jurídica. Brasília. 2023a. Brasília. Disponível em https://shorturl.at/ujvpq. Acesso em 10 set. 2024.

BRASIL. Agência Nacional de Proteção de Dados. Estudo técnico sobre anonimização de dados: Uma Visão de Processo Baseado em Risco e Técnicas Computacionais. Brasília. 2023b. Disponível em https://shorturl.at/ujvpq. Acesso em 10 set. 2024.

FERNANDES, Ricardo; GAMA, Rui. Economia digital e políticas de desenvolvimento: uma abordagem territorial. Coimbra, Portugal. Disponível em: https://estudogeral.uc.pt/bitstream/10316/12406/1/Fernandes%26Gama_APDR_2007.pdf. Acesso em 20/09/2024

FUJITA, Jorge; BARRETO JUNIOR, Irineu. O Direito ao Esquecimento e a Liberdade de Informar na Sociedade da Informação. Revista Direitos Fundamentais e Democracia. V. 25. N. 2. 2020. Disponível em: https://doi.org/10.25192/issn.1982-0496.rdfd.v25i21392. Acesso em: 20/08/2024.

GROSSMAN, R et al. The Management and Mining of Multiple Predictive Models Using Predictive Modeling Markup Language (PMML). Information & Software Technology. V. 41. Elsevier. 1999.

KITCHIN, R. Big Data, Open Data, Data Infrastrutctures & their consequences. Los Angeles. SAGE Publications ltd. 2014.

LESSIG, Lawrence. Code Version 2.0. Nova Iorque. Basic Book. Ano 2006.

LORENZON, Laila Neves. Análise Comparada entre Regulamentações de Dados Pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus Respectivos Instrumentos de Enforcement. Revista do Centro de Excelência Jean Monet da FGV Direito Rio, v. 1, p. 47. Disponível em: https://periodicos.fgv.br/rpdue/article/view/83423/79192. Acesso em: 11 set. 2024.

LUBARSKY, B. Re-identification of “Anonymized Data”. Georgetown Law. 2017. Disponível em: https://perma.cc/86RR-JUFT. Acesso em 01/10/2024.

LUCENA, Andre. Breve introdução sobre o contexto histórico da LGPD. Disponível em <https://www.jusbrasil.com.br/artigos/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/1203647706>. Acesso em 23 de janeiro de 2024.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of “Personally Identifiable Information”. Communications of the ACM. v. 53, 6ª Edição. Disponível em: https://dl.acm.org/doi/10.1145/1743546.1743558. Acesso em 20/09/2024.

PARLAMENTO EUROPEU. EUROPARL. Fichas temáticas sobre a União Europeia - Tratado de Lisboa, 2024. Disponível em <https://www.europarl.europa.eu/factsheets/pt/sheet/5/it-trattat-ta-lizbona>. Acesso em 22 de janeiro de 2024.

SANTANNA, Mayara. O Impacto da Inteligência Artificial na Aplicabilidade da Transparência e Anonimização na Proteção de Dados. São Paulo. 2023. Disponível em: https://dspace.mackenzie.br/handle/10899/38252. Acesso em: 05/10/2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NISTIR 8053: De-Identification of Personal Information. 2015. Disponível em: https://shorturl.at/yvIuH. Acesso em: 10/09/2024.

OLIVEIRA FILHO, Eduardo Luiz. Re-indentificação de dados anonimizados: Considerações de privacidade e responsabilidade na mineração de prescrições médicas. FGV Direito SP. 2020. Disponível em: https://hdl.handle.net/10438/29504. Acesso em 01 set. 2024.

QUINTILIANO, Leonardo. Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD). Disponível em <https://www.jusbrasil.com.br/artigos/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/1203647706>. Acesso em 23 de janeiro de 2024.

VERMEULEN, Adrien et al. Regulation Tomorrow: What happens when technology is faster than the law. 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3204119. Acesso em 08 set. 2024.