UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Eduarda Beutinger Paiva

ANONIMIZAÇÃO DE DADOS E RAZOABILIDADE DOS MEIOS DE REVERSÃO:

a concreção de um conceito jurídico indeterminado a partir de um diálogo interdisciplinar

Porto Alegre
2024

EDUARDA BEUTINGER PAIVA

ANONIMIZAÇÃO DE DADOS E RAZOABILIDADE DOS MEIOS DE REVERSÃO:

a concreção de um conceito jurídico indeterminado a partir de um diálogo interdisciplinar

Dissertação de Mestrado apresentada como requisito parcial para obtenção do título de Mestre em Direito junto ao Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Fabiano Menke

Porto Alegre

2024

FICHA CATALOGRÁFICA

A ficha catalográfica, gerada pelo Sistema para Geração Automática de Ficha Catalográfica para Teses, Dissertações e TCCs da UFRGS, deve ser copiada como imagem e colada aqui.

EDUARDA BEUTINGER PAIVA

ANONIMIZAÇÃO DE DADOS E RAZOABILIDADE DOS MEIOS DE REVERSÃO:

a concreção de um conceito jurídico indeterminado a partir de um diálogo interdisciplinar

Dissertação de Mestrado apresentada como requisito parcial para obtenção do título de Mestre em Direito junto ao Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Fabiano Menke

Porto Alegre, novembro de 2024.

BANCA EXAMINADORA:

Prof. Dr. Fabiano Menke
Universidade Federal do Rio Grande do Sul
Orientador

Prof. Dr. Jéferson Campos Nobre
Universidade Federal do Rio Grande do Sul

Prof. Dr. Leonardo Netto Parentoni
Universidade Federal de Minas Gerais

Profª. Drª. Maria Cláudia Cachapuz
Universidade Federal do Rio Grande do Sul

Ao resiliente povo gaúcho,
que com solidariedade e esperança enfrentou as enchentes de maio de 2024,
mostrando ao mundo que aqui, nesta terra, o que mais floresce é o amor.

AGRADECIMENTOS

Na banca de qualificação deste trabalho, comparou-se o percurso até a banca de defesa da dissertação a uma corrida de Fórmula 1. Interessante comparação. Na mesma hora pensei em trazer isso para o trabalho. Cá estou eu fazendo exatamente isso. De início, pergunto: qual é o papel do piloto? Muitos acham que o piloto é a essência do esporte; a peça principal. A condução do veículo é, sem dúvidas, um elemento fundamental. Ao conduzir o veículo na pista, o piloto deve contar com as suas habilidades pessoais. Mesmo conhecendo a pista de corrida, o percurso pode surpreender e adversidades podem acontecer. Chuvas repentinas, problemas mecânicos no veículo, incidentes na pista... É o piloto quem sente as dificuldades durante a condução. Contudo, sem uma equipe, o piloto sequer chega ao grid de largada.

Esta piloto teve e tem a sorte de ter uma equipe excepcional oferecendo todo o suporte necessário no box. Houve bandeiras amarelas durante o percurso que impuseram a redução da velocidade em determinados trechos da corrida. Mas nos pit stops, com as trocas de pneus e o reabastecimento do combustível promovidos pela equipe, conferiu-se ao veículo as melhores condições para que a piloto fosse resiliente frente às dificuldades encontradas na pista. Sem o papel da equipe, a performance na corrida não teria sido a mesma. É a esta equipe que passo a agradecer.

Aos meus dois pilares em qualquer corrida desta vida, pai e mãe. Pai, meu Professor com "P" maiúsculo, o meu "quando eu crescer, quero ser igual". Se eu nasci curiosa e com sede de "investigar", foi por conta do meu pai, que me abastecia com livros e documentários desde que me conheço por gente. Admiro o pesquisador e o professor que és. Estaremos juntos em cada corrida, seja qual for a cor da bandeira. Mãe, meu eterno porto seguro, a principal fonte do meu combustível (emocional). Obrigada por não medir esforços para me apoiar e me acolher. É graças ao incentivo de vocês que eu abro asas para ir atrás dos meus sonhos e voar pelos cantos do mundo em busca de conhecimento e crescimento.

Pedro, meu "engenheiro de performance". Obrigada por ser o melhor parceiro de vida que eu poderia pedir. Obrigada por abraçar meus sonhos como se teus fossem. Que sigamos assim. Dando apoio um ao outro para que, juntos, vençamos mais e mais corridas.

Ao meu "diretor técnico", meu orientador, Prof. Fabiano Menke, agradeço por abrir as portas da pesquisa acadêmica para a Eduarda de 18 anos, pelo incentivo para estudar a língua alemã, por acreditar no meu trabalho e me acompanhar em cada evolução. O trabalho de hoje não teria sido o mesmo sem o apoio concedido desde 2017. A pesquisadora que me tornei (ou melhor, que estou me tornando) deve muito à orientação recebida em cada projeto, tanto em

nível de iniciação científica, quanto de pós-graduação. Nesta dissertação, em especial, agradeço por confiar em mim e acolher o desafio que me propus a realizar em trazer um olhar técnico à abordagem feita neste trabalho. Foi uma grande felicidade ter o senhor como meu "Mastervater".

Ao Centro de Estudos Europeus e Alemães agradeço pelo incentivo fundamental que prestam aos estudantes. O nível de pesquisa chega a outro patamar graças ao apoio do CDEA. Obrigada pelos cursos de alemão, pelas palestras exclusivas, pelas estadias de pesquisa na Alemanha. Estes recursos fizeram toda a diferença para que este trabalho atingisse os objetivos colocados.

Aos queridos professores que me recepcionaram em minhas estadias na Alemanha, Prof. Dr. Indra Spiecker gen. Döhmann, que fez eu me sentir em casa, tanto na Goethe Universität quanto na Universität zu Köln, e me proporcionou as mais incríveis experiências acadêmicas, e Prof. Dr. Gerald Spindler (*in memoriam*), a quem devo meu profundo agradecimento por abrir as portas da Lehrstuhl e proporcionar minha primeira experiência acadêmica na Alemanha, na Georg-August-Universität Göttingen. Herzlichen Dank für alles!

Agradeço aos professores da banca de qualificação, Prof. Jéferson Nobre, que conferiu ajuda fundamental na parte técnica com a indicação de leituras basilares para a construção do trabalho, e Prof. Leonardo Parentoni, que com seus *insights* ímpares que entrelaçam Direito e técnica proporcionaram o abrir de horizontes a diversos capítulos desta dissertação.

Aos meus avós, minhas jóias raras, pelo apoio em minhas viagens e pela paciência com os dias em que ficava no quarto escrevendo. À minha tia, figura feminina da docência que me inspira e pela qual tenho tanta admiração. À minha irmã pelo apoio de sempre. À Cacau pelas horas e horas de companhia na elaboração deste trabalho. Muito obrigada.

Por fim, mas não menos importante, agradeço aos colegas que estiveram ao meu lado em diferentes etapas dessa corrida. Rafael, por desde o início me auxiliar em cada passo dado no Mestrado. Victória e Andressa, por serem minhas parceiras de eventos acadêmicos na Alemanha e cabeças pensantes que em muito me auxiliaram a clarear determinadas ideias colocadas nesta dissertação. Daniel e Lucas, pela companhia na nossa amada Goethe Universität e por cada momento de troca que tivemos. Linda e Julia, meus presentes da Alemanha; não mediram esforços para me incluir nos eventos acadêmicos e enviar artigos e livros que diziam respeito ao meu tema de pesquisa. Ihr zwei seid die Besten!

Obrigada.

"[...] a healthy public debate will depend on everyone being knowledgeable about the technology, its benefits, and its risks. The benefits will be massive, and the best reason to believe that we can manage the risks is that we have done it before."

Bill Gates

RESUMO

A presente pesquisa destina-se ao estudo do conceito jurídico indeterminado da razoabilidade, alicerce da noção relativa de anonimização adotada pelo legislador na Lei Geral de Proteção de Dados Pessoais (LGPD). O reconhecimento da robustez do processo de anonimização aplicado – e, portanto, a qualificação dos dados como anonimizados – depende de uma ponderação da razoabilidade dos meios de reversão. Em sendo esses irrazoáveis, a possibilidade de reversão é considerada deveras remota, de modo que a anonimização implementada reduz suficientemente o grau de identificabilidade dos dados. A consequência jurídica de tal constatação é o afastamento da incidência normativa da LGPD. A razoabilidade é, pois, um critério legal para determinar um risco tolerável de reversão do processo de anonimização. Ao passo que a adoção do referido conceito possibilita a adaptabilidade da norma à evolução tecnológica, a sua elevada abstração cria um cenário de insegurança jurídica. Com base no exposto, o trabalho tem como objetivo definir critérios mínimos que auxiliem na concreção da razoabilidade, com o fim último de auxiliar na redução de discricionariedades e inseguranças que permeiam a aplicabilidade prática da anonimização. Far-se-á o uso do método de abordagem dedutivo e, como método de procedimento, a pesquisa bibliográfica e documental de jurisprudência. O trabalho propõe a construção de um diálogo interdisciplinar entre Direito e Ciência da Computação. Entende-se que a compreensão da perspectiva técnica da anonimização é fundamental para a atividade jurídica de preenchimento do conceito legal da razoabilidade. Com base nessa premissa, o trabalho é dividido em três partes. O primeiro capítulo ocupa-se em apresentar o olhar técnico da anonimização de dados, desde o seu funcionamento e papel na Ciência de Dados até as fragilidades que podem levar à sua reversão. O segundo capítulo aborda os contornos jurídicos da anonimização no contexto da proteção de dados pessoais, e discute a sua abordagem na LGPD e as influências, sobretudo europeias, que culminaram na adoção da noção relativa de anonimização pelo legislador brasileiro. O terceiro capítulo é a ponte entre as duas áreas do conhecimento: utilizam-se conceitos e abordagens técnicos para a construção de critérios mínimos que, com base na ideia da anonimização como processo, visam orientar a concretização da ponderação da razoabilidade dos meios de reversão. Ao final, são apresentadas as conclusões construídas ao longo do estudo.

Palavras-chave: Anonimização de dados. Grau de identificabilidade. Abordagem baseada no risco. Critério da razoabilidade.

ABSTRACT

This study aims to analyze the legal concept of reasonableness, which is one of the bases of the relative approach to anonymization adopted in the Brazilian General Data Protection Law (LGPD). Robustness recognition of the applied anonymization process, and therefore data qualification as anonymized, depends on the reasonableness evaluation of the efforts for anonymization reversal. If the efforts are deemed unreasonable, reversing is considered remote. Therefore, the anonymization process implemented must have sufficiently reduced the degree of identifiability of the data. As a result, the LGPD will not apply. Reasonableness is a legal criterion for determining the tolerable risk of reversal of the anonymization process. The adoption of this concept enables the rule to be adapted to technological advancements. However, its high level of abstraction creates legal uncertainty. Based on the above, this work aims to establish minimum criteria to contribute concretizing reasonableness, with the ultimate goal of reducing discretion and uncertainties that permeate the practical applicability of anonymization. It uses the deductive method of approach and bibliographic research as the method of procedure. The study proposes the construction of an interdisciplinary dialogue between Law and Computer Science. It is understood that comprehending the technical perspective of anonymization is crucial for defining the legal concept of reasonableness. The work is divided into three parts. The first chapter presents the technical view of data anonymization, including its operation and role in Data Science, as well as the weaknesses that can lead to its reversal. The second chapter discusses the legal contours of anonymization in the context of personal data protection. This section examines the conception of anonymization taken by the LGPD as well as the European influences that led to the adoption of the relative approach of anonymization by the Brazilian legislator. The third chapter serves as a bridge between Law and Computer Science, utilizing technical concepts and approaches to establish minimum criteria to define what shall be considered reasonable efforts to reverse the anonymization process. The development of the criteria is based on the notion of anonymization as a process. Finally, the conclusions of the research are presented.

Keywords: Data anonymization. Degree of identifiability. Risk-based approach. Reasonableness criterion.

ZUSAMMENFASSUNG

Ziel dieser Studie ist es, den unbestimmten Rechtsbegriff der Wahrscheinlichkeit zu untersuchen, der die Grundlage für den relativen Begriffsverständnis der Anonymisierung im brasilianischen Datenschutzgesetz (LGPD) bildet. Um die Robustheit des verwendeten Anonymisierungsverfahrens zu erkennen - und damit die Daten als anonymisiert zu klassifizieren - muss die Wahrscheinlichkeit der Umkehrung berücksichtigt werden. Wenn die Umkehrung als unwahrscheinlich angesehen wird, bedeutet dies, dass der Anonymisierungsprozess den Grad der Identifizierbarkeit der Daten ausreichend reduziert hat. In Anbetracht dieser Feststellung sollte die LGPD in dieser Situation nicht angewendet werden. Die Angemessenheit ist daher ein rechtliches Kriterium für die Bestimmung eines hinnehmbaren Risikos der Umkehrung des Anonymisierungsprozesses. Die Übernahme des Wahrscheinlichkeitskonzepts ermöglicht zwar eine Anpassung der Bestimmung an die technologische Entwicklung, doch schafft der hohe Abstraktionsgrad ein Szenario der Rechtsunsicherheit. Basierend auf den obigen Ausführungen hat diese Studie das Ziel, Mindestkriterien zu definieren, um die Wahrscheinlichkeit zu verstehen und letztendlich den Ermessensspielraum und die Unsicherheit zu verringern, die die praktische Anwendbarkeit der Anonymisierung beeinträchtigen. Es wird ein deduktiver Ansatz verwendet und die bibliographische Recherche wird als Verfahrensmethode eingesetzt. Die Arbeit schlägt vor, einen interdisziplinären Dialog zwischen Recht und IT aufzubauen. Es wird angenommen, dass das Verständnis der technischen Perspektive der Anonymisierung für die Definition des Rechtsbegriffs der Wahrscheinlichkeit entscheidend ist. Ausgehend von dieser Prämisse ist die Studie in drei Teile gegliedert. Das erste Kapitel wirft einen technischen Blick auf die Datenanonymisierung, von ihrer Funktionsweise und Rolle in der Datenwissenschaft bis hin zu den Schwachstellen, die zu ihrer Umkehrung führen können. Das zweite Kapitel befasst sich mit den rechtlichen Konturen der Anonymisierung im Kontext des Schutzes personenbezogener Daten und erörtert ihren Ansatz in der LGPD sowie die Einflüsse, insbesondere europäischer Art, die zur Annahme des relativen Begriffs der Anonymisierung in der LGPD geführt haben. Das dritte Kapitel bildet die Brücke zwischen Recht und IT. Anhand von Konzepten und technischen Ansätzen werden Mindestkriterien aufgestellt, die, ausgehend von der Idee der Anonymisierung als Prozess, als Leitfaden für die Umsetzung des Nachweises der Wahrscheinlichkeit der Umkehrbarkeit dienen. Abschließend werden die Schlussfolgerungen der Forschung vorgestellt.

Schlüsselwörter: Anonymisierung von Daten. Grad der Identifizierbarkeit. Risikobasierter Ansatz. Wahrscheinlichkeitskriterium.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABREVIATURA	SIGNIFICADO
ADI	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
DDDM	Data-driven decision making
EUA	Estados Unidos da América
LGPD	Lei Geral de Proteção de Dados Pessoais
HIPAA	Health Insurance Portability and Accountability Act
IA	Inteligência Artificial
RDB	Relational Database
RGPD	Regulamento Geral de Proteção de Dados
MIT	Massachusetts Institute of Technology
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PII	Personal identifiable information
PPDP	Privacy Preserving Data Publishing
ROI	Retorno sobre o Investimento em Segurança
TI	Tecnologia da Informação
TJUE	Tribunal de Justiça da União Europeia

SUMÁRIO

1 INTRODUÇÃO

Em 1983, a Motorola introduzia no mercado o primeiro modelo de telefone celular portátil. O aparelho, que pesava 1,1 kg e se limitava à funcionalidade de realizar ligações, funcionava de 20 a 30 minutos até que a bateria se esgotasse e fosse necessária a recarga, que demorava cerca de 10 horas para que fosse concluída[1]. Em menos de 40 anos desde o comércio do primeiro telefone celular, chega-se aos tempos atuais: entre Android e iOS, os *smartphones* desempenham papel fundamental na rotina dos indivíduos, contando com câmeras profissionais, memórias que chegam a 1 TB, conexão em rede 5G e acesso a uma variada gama de serviços por meio de aplicativos monetizados. Este acelerado movimento evolutivo se deu em vários ramos da tecnologia – televisão e entretenimento, música, *games*, computador, etc. – e tem como tendência a continuidade em uma velocidade cada vez maior. O acompanhamento das complexidades oriundas da evolução tecnológica na esfera social se tornou um dos grandes desafios enfrentados pelo Direito. A elaboração de soluções jurídicas eficazes frente às constantes mudanças do estado da arte da tecnologia está entre o foco das discussões políticas e legislativas ao redor do mundo. A grande problemática que permeia os debates é, essencialmente, a mesma: encontrar o equilíbrio entre a garantia da inovação e a vedação de violações de direitos, valores e interesses tradicionalmente protegidos pelo Direito.

A busca por respostas a este cenário de constantes inovações tecnológicas afasta o Direito da ideia de estabilidade eterna dos institutos jurídicos. A pretensão de se conservar ao longo do tempo engessa os sistemas legais, que, ao contrário, devem estar aptos a se adaptar às condições de mudança[2]. Em vista disso, para evitar desatualizações e obsolescências, o Direito, ao lidar com questões atinentes ao advento de novas tecnologias, tem caminhado na direção da adoção de regimes e de categorias jurídicas mais flexíveis, que permitam um

[1] MURPHY, Tom. 40 Years After the First Cell Phone Call By Tom Murphy Who is inventing tomorrow's future? **IEEE Consumer Electronics Magazine**, Brno, v. 2, n. 4, p. 44-46, out. 2013. DOI: https://doi.org/10.1109/MCE.2013.2273653. p. 45.

[2] CENTRE FOR STUDIES IN ECONOMICS AND FINANCE. **Working Paper nº. 256**: Legal Institutions, Innovation, and Growth. Naples: CSEF, 2010. 37 p. Disponível em: https://www.csef.it/WP/wp256.pdf. Acesso em: 10 nov. 2023. p. 1.

[3] SHADIKHODJAEV, Sherzod. Technological Neutrality and Regulation of Digital Trade: How Far Can We Go? **European Journal of International Law**, [S.l.], v. 32, n. 4, p. 1221-1247, nov. 2021. DOI: https://doi.org/10.1093/ejil/chab054. p. 1222.

[4] DONEDA, Danilo; MACHADO, Diego. Proteção de dados pessoais e Criptografia: Tecnologias Criptográficas Entre A Informação Pessoal e A Informação Pública. In: DONEDA, Danilo; MACHADO, Diego (coord.). **A Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. E-book.

[2] CENTRE FOR STUDIES IN ECONOMICS AND FINANCE. **Working Paper nº. 256**: Legal Institutions, Innovation, and Growth. Naples: CSEF, 2010. 37 p. Disponível em: https://www.csef.it/WP/wp256.pdf. Acesso em: 10 nov. 2023. p. 1.

diálogo permanente com a realidade que se pretende regular[3]. A "neutralidade tecnológica" é uma estratégia regulatória compatível à inovação, tendo como objetivo a construção de mecanismos legais que permitem a aplicabilidade da regulação em qualquer contexto tecnológico. Para tanto, o legislador recorre à implementação de conceitos abertos, que devem ser interpretados conforme as circunstâncias fáticas que envolvem a aplicação da norma (o que inclui o estado da arte da tecnologia). Ainda que seja uma interessante ferramenta para evitar a defasagem regulatória face à evolução tecnológica, tal técnica legislativa abre espaço para discricionariedades e, consequentemente, para insegurança jurídica. Questiona-se se tal estratégia é efetiva para promover a tutela de direitos ou se regulações desta natureza apresentam tal nível de incerteza que acabam provocando resultados ilusórios, não havendo, pois, aplicabilidade prática da norma.

Uma clara expressão deste embate se dá com relação à abordagem instituída pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) no tocante aos dados anonimizados. Os dados submetidos a procedimentos (robustos) de anonimização perdem o elemento vinculante ao titular, razão pela qual não estão inseridos no escopo protetivo de incidência da Lei, que abrange apenas os dados categorizados como pessoais. Por influência da experiência europeia, forjada com base em estudos desenvolvidos na área da Ciência da Computação que demonstravam a possibilidade de reverter processos de anonimização, o legislador brasileiro adota uma noção relativa de dado anonimizado[4]. Em outras palavras, as técnicas de anonimização de dados não são tidas como procedimentos irreversíveis e absolutos, de modo que se reconhece o risco de reversão e de recuperação da identificabilidade dos dados. Este risco está ligado, justamente, aos avanços das (contra)tecnologias e à crescente disponibilização de dados impulsionada pelos processos de digitalização. Assim, o artifício utilizado pelo legislador para a categorização de um dado como anonimizado depende de uma ponderação de razoabilidade de meios de reversão. O chamado "critério da razoabilidade" tem como fim último a realização de uma estimativa de risco de reversão – se, diante dos recursos disponíveis para a reversão do processo de anonimização, o risco for considerado remoto, estar-se-á a lidar com dados anonimizados; se, por outro lado, o risco for razoável, os dados não serão considerados anonimizados e

[3] SHADIKHODJAEV, Sherzod. Technological Neutrality and Regulation of Digital Trade: How Far Can We Go? **European Journal of International Law**, [S.l.], v. 32, n. 4, p. 1221-1247, nov. 2021. DOI: https://doi.org/10.1093/ejil/chab054. p. 1222.

[4] DONEDA, Danilo; MACHADO, Diego. Proteção de dados pessoais e Criptografia: Tecnologias Criptográficas Entre Anonimização E Pseudonimização de Dados. *In*: DONEDA, Danilo; MACHADO, Diego (coord.). **A Criptografia no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. *E-book*.

continuarão submetidos ao regime legal de proteção de dados pessoais. A razoabilidade é, pois, um artifício do legislador para estabelecer um risco *tolerável*.

A ponderação da razoabilidade de meios é delegada aos agentes de tratamento, os quais deverão definir se a anonimização implementada aos dados que estão tratando é suficientemente robusta. O §1º do artigo 12 da LGPD dispõe que "A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios". Nota-se que o legislador opta por não indicar elementos que devem ser obrigatoriamente considerados pelos agentes quando da avaliação da robustez [5] da anonimização aplicada. O dispositivo se limita a trazer exemplificações de alguns fatores objetivos que podem ser avaliados quando da ponderação a ser realizada.

Identificam-se duas principais controvérsias envolvendo o regime adotado pelo legislador brasileiro em relação aos dados anonimizados: (i) "não existem dados anonimizados"[6] - em vista da crescente complexidade em produzir dados efetivamente anonimizados por conta da contínua e acelerada evolução tecnológica, o regime de exceção dos dados anonimizados à tutela legal, com previsão no artigo 12, *caput*, da LGPD, abriria margem para o aumento da vulnerabilidade do titular de dados, razão pela qual a diferenciação entre dados pessoais e dados anonimizados feita na Lei seria colocada em questão; (ii) ainda que conceda maior grau de adaptabilidade em relação aos avanços da técnica, a adoção do conceito jurídico indeterminado da razoabilidade traz insegurança jurídica aos agentes de tratamento, em razão, principalmente, da inexistência de indicação de requisitos mínimos que orientem a ponderação a ser por eles realizada, o que acaba (ii.i) desincentivando o uso de técnicas de anonimização de dados e/ou (ii.ii) abrindo espaço para discricionariedades de modo que níveis diferentes de robustez (e, consequentemente, de proteção aos titulares) acabam sendo implementados.

---

[5] O termo 'robustez' será utilizado neste trabalho com o sentido de "suficiente para afastar a reversibilidade razoável da anonimização". Utilizar-se-á, também, 'adequação'.

[6] "*There's no such thing as anonymous data*" (em tradução livre, "não existem dados anonimizados/anônimos") é a máxima do posicionamento cético relativo à anonimização de dados. A frase se popularizou depois da publicação de Scott Berinato, em 2015, na qual ele relata o estudo do cientista do Instituto de Tecnologia de Massachusetts (Massachusetts Institute of Technology – MIT), Yves-Alexandre de Montjoye, que demonstra a aplicação de engenharia reversa a processo de anonimização aplicado em dados de transações feitas com cartão de crédito. O caso será abordado no capítulo 2 do presente trabalho. BERINATO, Scott. There's No Such Thing as Anonymous Data. **Harvard Bussiness Review**, Boston, fev. 2015. Disponível em: https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data. Acesso em: 10 nov. 2023.

Perante os pontos expostos, o presente trabalho se destina a responder a seguinte pergunta: com o propósito de reduzir o cenário de insegurança jurídica envolvendo a definição da robustez da anonimização aplicada em um contexto específico de tratamento de dados, quais os vetores mínimos podem ser utilizados para orientar a concreção do conceito de razoabilidade, critério utilizado pelo legislador para determinar um risco tolerável de reversão?

A hipótese em teste é a seguinte: o regime de exceção aplicável aos dados anonimizados é justificável pois está em consonância com a abordagem baseada no risco adotada pelo legislador brasileiro na LGPD. A anonimização de dados diminui riscos, mas não os anula, de modo que, assim como ocorre com o tratamento de dados pessoais, o uso de dados anonimizados também impõe uma convivência com o risco. Partindo desta premissa, o regime aplicável aos dados anonimizados deve ter como enfoque o processo - a implementação de técnicas de anonimização e a manutenção do controle destas (e, consequentemente, do risco envolvido) - e não o resultado - produzir dados "verdadeiramente" anonimizados. A ponderação da razoabilidade permite estipular a existência de um risco de reversão que, mesmo que residual, deve ser permanentemente avaliado e controlado pelos agentes de tratamento. Para que se reduza a insegurança jurídica relativa à ponderação da razoabilidade no âmbito nacional, necessária a elaboração de critérios mínimos a serem observados, os quais devem estar alinhados à técnica e ao contexto que envolvem os dados a serem anonimizados.

A anonimização de dados pode ser uma grande aliada na garantia de maior segurança à atividade desempenhada pelos agentes de tratamento, tanto em perspectiva interna (ameaças provenientes de dentro da organização - *e.g,* compartilhamento indevido de dados por funcionários), quanto externa (ameaças provenientes de terceiros - *e.g.* ataques *hackers*). Outrossim, para fins de pesquisa, contexto em que há o compartilhamento de dados com inúmeros agentes ou, até mesmo, a disponibilização ao público, a anonimização se coloca quase como uma imposição. Ao reduzir a possibilidade de identificabilidade dos titulares, os riscos de danos a estes indivíduos são, da mesma forma, proporcionalmente reduzidos. Logo, pode-se dizer que, em última análise, a anonimização é uma forma de promover a proteção de dados.

A implementação de técnicas de anonimização ainda é uma questão incipiente no Brasil, sendo objeto de dúvidas de ordem legal e técnica. Entre erros comuns que podem ser constatados estão a criação de falsa expectativa, sobretudo aos titulares, de garantia de segurança absoluta se os dados estiverem anonimizados; a confusão entre conceitos legais que

acabam produzindo efeitos de caráter prático e jurídico (como, por exemplo, confundir anonimização e pseudonimização); a implementação de técnicas de anonimização como estratégia para "se livrar" da necessidade de observância das disposições da LGPD; a adoção da noção "aplicar e esquecer" após anonimizar os dados, sem gestão posterior da robustez das técnicas de anonimização empregadas; etc.

Com a finalidade de contribuir no debate para a redução desta conjuntura de dúvidas e consequente insegurança jurídica[7], o estudo tem como objetivo geral estabelecer diretrizes mínimas que auxiliem a compatibilizar as concepções jurídica e a técnica de dado anonimizado. Surgem, assim, objetivos secundários que nortearão a divisão dos capítulos: (i) esclarecer os contornos legais conferidos à anonimização na LGPD, bem como os motivos que justificam o regime de exceção aplicável aos dados anonimizados; (ii) indicar vetores mínimos a serem observados pelos agentes de tratamento quando da ponderação dos riscos que influem na robustez da anonimização aplicada, visando, desta forma, trazer maior concretude ao critério da razoabilidade de meios de reversão.

O trabalho tem como objeto de análise o tratamento legal conferido a uma aplicação tecnológica. Para regulamentar tecnologias, entende-se ser necessário conhecer o seu funcionamento técnico e as consequências de ordem prática advindas da sua implementação, para que, assim, se tenha maior propriedade para elaborar normas que sejam compatíveis com a realidade. Partindo de tal pressuposto, no que tange à metodologia adotada, o estudo se propõe a construir uma ponte entre Direito e Ciência da Computação por meio de uma abordagem interdisciplinar, a fim de que esta área se torne um apoio no desenvolvimento daquele. Os ataques e falhas técnicas demonstrados em estudos e relatórios da Ciência da Computação evidenciam quais os pontos aos quais os agentes de tratamento devem estar atentos quando da aplicação de processos de anonimização. Tal experiência prévia será utilizada para nortear a indicação de vetores mínimos que devem ser observados quando da ponderação da razoabilidade de meios de reversão. Os trabalhos técnicos serão, portanto, a base para preenchimento do conceito jurídico indeterminado da razoabilidade, já que o exame desses permitirá identificar quais os principais fatores que influenciam no aumento ou na diminuição do risco de reversão dos processos de anonimização.

Utilizar-se-á o método de abordagem dedutivo, por meio da análise do regime legal instituído aos dados anonimizados e da experiência prática com a implementação de técnicas

[7] Não é objetivo do trabalho esgotar a discussão e fornecer uma solução para colocar fim às dúvidas que permeiam a temática. Pretende-se auxiliar a trilhar caminhos que possam guiar a construção desta futura solução, edificando o diálogo com a realidade técnica e, consequentemente, trazendo maior grau de concretude aos institutos jurídicos já existentes na LGPD.

de anonimização, para, a partir das premissas constatadas, elaborar critérios mínimos que orientem a concretização da ponderação da razoabilidade de meios de reversão do processo de anonimização aplicado. Quanto ao método de procedimento, serão adotados: (i) pesquisa bibliográfica de estudos nacionais e estrangeiros (essencialmente, da União Europeia e dos Estados Unidos da América, locais em que a discussão da temática está com desenvolvimento mais avançado); (ii) pesquisa documental de jurisprudência, pareceres e guias orientativos do Brasil e da União Europeia, dada a influência desta na elaboração da Lei Geral de Proteção de Dados brasileira[8].

Para o fim de responder a questão colocada, o desenvolvimento do trabalho é dividido em três capítulos, sendo cada um deles composto por dois subcapítulos. O primeiro capítulo ocupa-se em apresentar o olhar técnico da anonimização de dados, proveniente da Ciência da Computação. O subcapítulo que inaugura essa parte faz uma introdução sobre a anonimização na Ciência de Dados, subárea da Ciência da Computação. Apresenta-se o ecossistema de dados em que se insere o processo de anonimização, as técnicas de anonimização e o seu funcionamento, e, por fim, a relação entre anonimização e utilidade dos dados e a influência deste fator em determinados cenários de aplicação. O segundo subcapítulo trata do aspecto patológico da anonimização. Aborda-se a reidentificação enquanto um sistema, os métodos utilizados para atingi-la (os chamados "ataques"), casos relevantes em que a reidentificação foi alcançada e como a Ciência da Computação busca contornar o problema por meio da adoção de métricas de mensuração de risco.

O segundo capítulo explora os contornos jurídicos da anonimização no contexto da proteção de dados pessoais. Primeiramente, apresenta-se o regime jurídico aplicável aos dados anonimizados, baseado na dualidade mutuamente excludente entre esta categoria e a dos dados pessoais. Os prós e os contras relativos à adoção do regime de exceção aos dados aonimizados são discutidos, dando ênfase à situação do titular dos dados em tal cenário. Passa-se, então, no segundo subcapítulo, à abordagem do Direito à reversibilidade da anonimização. São expostas as influências, sobretudo europeias, que culminaram na adoção da noção relativa de anonimização pelo legislador brasileiro e como esta impõe, por meio da adoção do conceito jurídico indeterminado da razoabilidade, uma convivência com o risco.

O terceiro e último capítulo do desenvolvimento é o momento em que o diálogo entre as duas áreas do conhecimento – Direito e Ciência da Computação – se perfectibiliza. Após

[8] Salienta-se que não se trata de um trabalho de Direito Comparado, porém, tanto a pesquisa bibliográfica quanto a documental englobarão materiais estrangeiros. O propósito é analisar como diferentes jurisdições têm enfrentado a problemática colocada, para construir uma resposta mais adequada às particularidades do cenário brasileiro.

tratar, nos capítulos anteriores, sobre as respectivas abordagens conferidas à anonimização em cada uma das áreas e como a questão da possibilidade de reversão e reidentificação dos titulares (ou seja, o risco) é por elas enfrentada, busca-se, neste capítulo, construir uma ponte entre ambas as perspectivas para responder a questão que o trabalho se propõe a investigar. A partir da experiência técnica e com a importação de conceitos deste meio, indicam-se vetores mínimos que, com base na ideia da anonimização como processo, visam a orientar a concretização da ponderação da razoabilidade dos meios de reversão.

Ao final, são apresentadas as conclusões edificadas ao longo do estudo.

REFERÊNCIAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Orientaciones y garantías en los procedimientos de anonimización de datos personales**. Madrid: AEPD, 2016. 24 p. Disponível em: https://www.aepd.es/guias/guia-orientaciones-procedimientos-anonimizacion.pdf. Acesso em: 28 ago. 2024.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **10 Misunderstandings Related To Anonymisation**. Madrid: AEPD, 2021. 7 p. Disponível em: https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf. Acesso em: 21 jun. 2024.

AGGARWAL, Charu C.; YU, Philip S. A General Survey of Privacy-Preserving Data Mining Models and Algorithms. *In*: AGGARWAL, Charu C.; YU, Philip S. (ed.). **Privacy-Preserving Data Mining**: Models and Algorithms. New York: Springer, 2008. p. 11-52.

ALBUQUERQUE, Aline. Pesquisa com prontuário: análise ético-jurídica à luz dos Direitos Humanos dos Pacientes. **Cadernos de Ética em Pesquisa**, Brasília, v.1, n. 1, p. 41-52, ago. 2019.

CENTRE FOR STUDIES IN ECONOMICS AND FINANCE. **Working Paper nº. 256:** Legal Institutions, Innovation, and Growth. Naples: CSEF, 2010. 37 p. Disponível em: https://www.csef.it/WP/wp256.pdf. Acesso em: 10 nov. 2023.

ANONYMITY. *In*: CAMBRIDGE Dictionary. Disponível em: https://dictionary.cambridge.org/dictionary/english/anonymity. Acesso em: 20 set. 2024.

AOL apologises for revealing users' search data. **New Scientist**, [S.l.], ago. 2006. Disponível em: https://www.newscientist.com/article/dn9700-aol-apologises-for-revealing-users-search-data/. Acesso em: 20 set. 2024.

ARANHA, Diego F. O que é criptografia fim a fim e o que devemos fazer a respeito? *In*: DONEDA, Danilo; MACHADO, Diego (coord.). **A Criptografia no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. *E- book.*

ARBUCKLE, Luk; RITCHIE, Felix. The Five Safes of Risk-Based Anonymization. **IEEE Security & Privacy**, [S.l.], v. 17, n. 5, p. 84-89, set./out. 2019. DOI: https://doi.org/10.1109/MSEC.2019.2929282.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 25237**: Informática em saúde - Pseudonimização. Rio de Janeiro: ABNT, 2020. 72 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005**: Segurança da informação, segurança cibernética e proteção à privacidade – Orientações para gestão de riscos de segurança da informação. 4. ed. Rio de Janeiro: ABNT, 2023. 75 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Sobre a normalização. **ABNT**, [S.l.]. Disponível em: https://abnt.org.br/normalizacao/sobre-a-normalizacao/. Acesso em: 29 fev. 2024.

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA. **O que está em jogo no debate sobre dados pessoais no Brasil?** Relatório final sobre o debate público promovido pelo ministério da justiça sobre o anteprojeto de lei de proteção de dados pessoais. São Paulo: Internetlab, 2015. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 24 set. 2024.

AUGUSTO, Cristian *et al*. Test-driven Anonymization for Artificial Intelligence. *In*: IEEE International Conference on Artificial Intelligence Testing, 1., 2019, Newark. **Proceedings** [...]. [S.l.]: IEEE Computer Society, 2019. p. 103-110. DOI: https://doi.org/10.1109/AITest.2019.00011.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Estudo preliminar**: Anonimização e Pseudonimização para a proteção de dados pessoais. Brasília: ANPD, 2023. 48 p. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/37060. Acesso em: 03 mar. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Estudo técnico sobre a anonimização de dados na LGPD**: análise jurídica. Brasília: ANPD, 2023. 27 p. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd___analise_juridica.pdf. Acesso em: 03 mar. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Estudo técnico sobre a anonimização de dados na LGPD:** uma visão de processo baseado em risco e técnicas computacionais. Brasília: ANPD, 2023. 28 p. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_uma_visao_de_processo_baseado_em_risco_e_tecnicas_computacionais.pdf. Acesso em: 03 mar. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo**: tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Brasília: ANPD, 2023. 57 p. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 12 out. 2024.

ÁVILA, Humberto. **Teoria dos princípios**: da definição à aplicação dos princípios jurídicos. 18. ed. São Paulo: Malheiros, 2018.

ÁVILA, Humberto. Conteúdo, limites e intensidade dos controles de razoabilidade, de proporcionalidade e de excessividade das leis. **Revista de Direito Administrativo**, Rio de Janeiro, v. 236, p. 369-384, abr./jun. 2004.

BAMBAUER, Derek E. The myth of perfection. **Wake Forest Law Review Online**, [S.l.], v. 2, p. 9-15, 2012.

BARBARO, Michael; ZELLER JR., Tom. A Face Is Exposed for AOL Searcher No. 4417749. **New York Times**, New York, ago. 2006. Disponível em: https://www.nytimes.com/2006/08/09/technology/09aol.html. Acesso em: 27 abr. 2024.

BARROSO, Luís Roberto. Os princípios da razoabilidade e da proporcionalidade no Direito Constitucional. **Revista de Direito do Ministério Público**, Rio de Janeiro, v. 4, p. 160-175, 1996.

BARTH-JONES, Daniel. The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now. **SSRN Electronic Journal**, [S.l.], p. 1-19, jul. 2012. DOI: http://dx.doi.org/10.2139/ssrn.2076397.

BENNET, Colin J.; MULLIGAN, Deirdre K. The governance of privacy through codes of conduct: international lessons for U.S. Privacy Policy. *In*: PRIVACY LAW SCHOLARS CONFERENCE, 2012, Washington D.C. Washington D.C.: George Washington University, 2012. DOI: http://dx.doi.org/10.2139/ssrn.2230369.

BENNETT, Colin J.; RAAB, Charles D. **The Governance of Privacy:** policy instruments in global perspective. 2. ed. Cambridge: MIT Press, 2006.

BENNETT, Colin J.; RAAB, Charles D. Revisiting the governance of privacy: Contemporary policy instruments in global perspective. **Regulation & Governance**, [S.l.], v. 14, n. 3, p. 447-464, jul. 2020. DOI: https://doi.org/0.1111/rego.12222.

BERINATO, Scott. There's No Such Thing as Anonymous Data. **Harvard Bussiness Review**, Boston, fev. 2015. Disponível em: https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data. Acesso em: 10 nov. 2023.

BERNSTEIN, Peter L. **Against the Gods**: The Remarkable Story of Risk. New York: John Wiley & Sons, 1996.

BERTINO, Elisa; FERRARI, Elena. Big Data Security and Privacy. *In*: FLESCA, Sergio *et al*. (org.). **A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years**. Cham: Springer, 2018, p. 425-439.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei no 13.709/2018) - A caminho da efetividade:** contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020. p. 39-54.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. *E-book*.

BIONI, Bruno Ricardo. **Regulação e proteção de dados pessoais**: o princípio da *accountability*. Rio de Janeiro: Forense, 2022.

BIONI, Bruno Ricardo. **Xeque-mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI-USP, 2015.

BISCHOFF, Claudia; DRECHSLER, Julian. Pseudonymisierung und Anonymisierung im Rahmen klinischer Prüfungen von Arzneimitteln (Teil II). **Pharma Recht**, [S.l.], v. 7, p. 389-396, jul. 2020.

BOEHME-NEßLER, Volker. Das Ende der Anonymität - Wie Big Data das Datenschutzrecht verändert. **Datenschutz und Datensicherheit**, [S.l], v. 7, p. 419-423, jul. 2016.

BORGESIUS, Frederik Zuiderveen. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition. **European Data Protection Law Review**, Berlin, v. 3, n. 1, p. 130-137, jan. 2017. DOI: https://doi.org/10.21552/edpl/2017/1/21.

BORGESIUS, Frederik J. Zuiderveen. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. **Computer Law & Security Review**, [S.l.], v. 32, n. 2, p. 256-271, abr. 2016. DOI: https://doi.org/10.1016/j.clsr.2015.12.013.

BREKNE, Tønnes; ÅRNES, André. Circumventing IP-address pseudonymization. *In*: INTERNATIONAL CONFERENCE ON COMMUNICATIONS AND COMPUTER NETWORKS, 3., 2005, Marina del Rey. **Proceedings** [...]. Calgary: IASTED, 2005. p. 43-48.

BREYER, Patrick. Personenbezug von IP-Adressen. **Zeitschrift für Datenschutz - ZD**, [S.l.], v. 8, p. 400-405, ago. 2014.

BUNDESVERBAND DER DEUTSCHEN INDUSTRIE E.V. **Anonymisierung personenbezogener Daten:** Ein branchenübergreifender Praxisleitfaden für Industrieunternehmen. Berlin: BDI, 2020. 40 p. Disponível em: https://bdi.eu/publikation/news/anonymisierung-personenbezogener-daten. Acesso em: 27 jul. 2024.

BUCCI, Maria Paula Dallari. O princípio da razoabilidade em apoio à legalidade. **Revista de Direito Constitucional e Internacional**, São Paulo, v. 16, p. 173-177, jul./set. 1996.

BURKHARDT, Marcus. **Digitale Datenbanken**: Eine Medientheorie im Zeitalter von Big Data. Bielefeld: Transcript Verlag, 2015. Disponível em: https://www.transcript-verlag.de/978-3-8376-3028-2/digitale-datenbanken/?number=978-3-8394-3028-6. Acesso em: 27 jan. 2024. *E-book*.

BURT, Andrew; STALLA-BOURDILLON, Sophie. The definition of ‘anonymization’ is changing in the EU: Here’s what that means. **IAPP**. Portsmouth, jun. 2023. Disponível em: https://iapp.org/news/a/the-definition-of-anonymization-is-changing-in-the-eu-heres-what-that-means/. Acesso em: 17 set. 2024.

CACHAPUZ, Maria Cláudia. **Intimidade e vida privada no novo Código Civil brasileiro**: uma leitura orientada no Discurso Jurídico. Porto Alegre: Sergio Antionio Fabris Editor, 2006.

CAMINITI, Susan. Why UnitedHealth, Change Healthcare were targeted by ransomware hackers, and more cybercrime will hit patients, doctors. **CNBC**, [S.l.], mar. 2024. Disponível em: https://www.cnbc.com/2024/03/15/why-unitedhealth-change-healthcare-were-targets-of-ransomware-hackers.html. Acesso em: 28 ago 2024.

CARVALHO, Artur Potiguara *et al*. Big Data, Anonymisation and Governance to Personal Data Protection. *In*: ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 21., 2020, Seoul. **Proceedings of the 21st** [...]. New York: ACM, 2020. p. 185-195. DOI: https://doi.org/10.1145/3396956.3398253.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: DONEDA, Danilo et al. (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 361-374.

CAVOUKIAN, Ann. **Privacy by Design**: The 7 Foundational Principles. Ontario: IPC, 2011. 5 p. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Acesso em: 10 out. 2024.

COHEN, Aloni; NISSIM, Kobbi. Towards Formalizing the GDPR's Notion of Singling Out. **Proceedings of the National Academy of Sciences**, Washington, DC, v. 117, n. 15, p. 8344-8352*,* abr. 2020. DOI: https://doi.org/10.1073/pnas.1914598117.

CORDEIRO, A. Barreto Menezes. **Direito da Proteção de dados**: à luz da RGPD e da Lei n.º 58/2019. Coimbra: Al Medina, 2020.

COUTO E SILVA, Clóvis V. do. **A obrigação como processo**. Rio de Janeiro: Editora FGV, 2006.

CURADO, Lúcio Mauro C. F. Dados abertos governamentais e a proteção de dados pessoais. *In*: BRASIL. Ministério Público Federal, 3ª Câmara de Coordenação e Revisão. **Sistema brasileiro de proteção e acesso a dados pessoais**: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados. Brasília: MPF, 2019. Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3. Acesso em 20 nov. 2023.

DALENIUS, Tore. Finding a needle in a haystack or identifying anonymous census record. **Journal of Official Statistics**, Sweden, v. 2, n. 3, p. 329-336, 1986. Disponível em: https://www.scb.se/contentassets/ca21efb41fee47d293bbee5bf7be7fb3/finding-a-needle-in-a-haystack-or-identifying-anonymous-census-records.pdf. Acesso em: 13 nov. 2023.

DATA Governance Act explained. **European Commission**, Brussels, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained. Acesso em: 12 ou. 2024.

DATA PROTECTION COMMISSION. **Guidance on Anonymisation and Pseudonymisation**. Dublin: DPC, 2019. 16 p. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. Acesso em: 21 jun. 2024.

DEMO, Pedro. **Conhecimento moderno**: sobre ética e intervenção do conhecimento. Petrópolis: Vozes, 1998.

DEWES, Andreas. Verfahren zur Anonymisierung und Pseudonymisierung von Daten. *In*: ROHDE, Marieke; BÜRGER, Matthias; PENEVA, Kristina; MOCK, Johannes (ed.). **Datenwirtschaft und Datentechnologie**: Wie aus Daten Wert entsteht. Berlin: Springer Vieweg, 2022. p. 183-201. *E-book*. DOI: https://doi.org/10.1007/978-3-662-65232-9_14.

DIAS, Tatiana. Vigiar e lucrar - Nós identificamos dois clientes dos dados de localização "anônimos" vendidos pela Vivo. **Intercept Brasil**, Rio de Janeiro, abr. 2020. Disponível em: https://www.intercept.com.br/2020/04/13/vivo-venda-localizacao-anonima/. Acesso em: 20 abr. 2024.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo; MACHADO, Diego. Proteção de dados pessoais e Criptografia: Tecnologias Criptográficas Entre Anonimização E Pseudonimização de Dados. *In*: DONEDA, Danilo; MACHADO, Diego (coord.). **A Criptografia no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. *E- book*.

DWORK, Cynthia. Differential Privacy. *In*: INTERNATIONAL COLLOQUIUM ON AUTOMATA, LANGUAGES, AND PROGRAMMING, 33., 2006, Venice. **Proceedings** [...]. Heidelberg: Springer, 2006. p. 1-12. DOI: https://doi.org/10.1007/11787006_1.

ELLIOT, Mark *et al*. Functional anonymisation: Personal data and the data environment. **Computer Law & Security Review**, Southampton, v. 34, n. 2, p. 204-221, abr. 2018. DOI: https://doi.org/10.1016/j.clsr.2018.02.001.

ELLIOT, Mark; MACKEY, Elaine; O'HARA, Kieron. **The Anonymisation Decision-Making Framework**: European Practitioners' Guide. 2. ed. Manchester: UKAN Publications, 2020. 118 p. Disponível em: https://msrbcel.files.wordpress.com/2020/11/adf-2nd-edition-1.pdf. Acesso em: 27 fev. 2024.

EL EMAM, Khaled; ARBUCKLE, Luk. **Anonymizing Health Data**: Case Studies and Methods to Get You Started. Sebastopol: O'Reilly Media, 2013.

EL EMAM, Khaled; ARBUCKLE, Luk. **Building an Anonymization Pipeline** - creating safe data. Sebastopol: O'Reilly, 2020.

EL EMAM, Khaled *et al*. Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records. **The Canadian Journal of Hospital Pharmacy**, Ottawa, v. 62, n. 4, p. 307-319, jul./ago. 2009. DOI: https://doi.org/10.4212/cjhp.v62i4.812.

EL EMAM, Khaled. **Principles of De-identification**. 2018. Disponível em: https://training.cochrane.org/sites/training.cochrane.org/files/public/uploads/resources/downloadable_resources/Part%202%20Principles%20of%20De-identification%20slides.pdf. Acesso em: 10 out. 2024.

EUROPEAN COMMISSION. **Data governance and data policies at the European Commission**. Brussels: EC, 2020. 20 p.
Disponível em: https://commission.europa.eu/system/files/2020-07/summary-data-governance-data-policies_en.pdf. Acesso em: 10 out. 2024.

EUROPEAN MEDICINES AGENCY**. External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use**. London: EMA, 2016. 91 p. Disponível em: https://www.ema.europa.eu/en/clinical-data-publication/support-industry-clinical-data-publication/external-guidance-implementation-european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use. Acesso em: 31 ago. 2024.

EUROPEAN UNION AGENCY FOR CYBERSECURITY - ENISA. **Privacy by design in big data** - An overview of privacy enhancing technologies in the era of big data analytics. Heraklion: ENISA, 2015. 79 p. Disponível em: https://www.enisa.europa.eu/publications/big-data-protection. Acesso em: 27 ago. 2024.

FALEIROS JÚNIOR, José Luiz de Moura; MARTINS, Guilherme Magalhães. Proteção de dados e anonimização: perspectivas à luz da Lei nº 13.709/2018. **Revista Estudos Institucionais**, Rio de Janeiro, v. 7, n.1, p. 376-397, jan./abr. 2021. DOI: https://doi.org/10.21783/rei.v7i1.476.

FEDERAL PRIVACY COUNCIL. Fair Information Practice Principles (FIPPs). **FPC**, 2022. Disponível em: https://www.fpc.gov/resources/fipps/. Acesso em 03 mai. 2024.

FINCK, Michèle; PALLAS, Frank. They who must not be identified - distinguishing personal from non-personal data under the GDPR. **International Data Privacy Law**, Oxford, v. 10, n. 1, p. 11- 36, 2020.

FLORIDI, Luciano. **Information**: A Very Short Introduction. New York: Oxford University Press, 2010.

FOLZ, Jakob; WAHL, Florian; WILHELM, Sebastian. Open Personal Data: Anonymisierung im Spannungsfeld zwischen Informationsgehalt und Robustheit. *In*: DATA SHARING: DATENKAPITALISMUS BY DEFAULT? - FORUM PRIVATHEIT, 2023, Berlin. **Posterproceedings [...]**. Karlsruhe: Fraunhofer ISI, 2023. p. 36-39. Disponível em: https://publica-rest.fraunhofer.de/server/api/core/bitstreams/fe2f9d4d-8610-4c9c-8178-ae1e81284933/content. Acesso em: 20 nov. 2023.

FRANCO, Muriel Figueredo. **CyberTEA**: a Technical and Economic Approach for Cybersecurity Planning and Investment. 2023. 276 f. Dissertation (Doctor of Science - PhD) – Faculty of Business, Economics and Informatics, University of Zurich, Zurich, 2023.

FUTURE PRIVACY FORUM; LGBT TECH. **The Role of Data Protection in Safeguarding Sexual Orientation and Gender Identity Information**. [S.l.]: FPF, 2022. 26 p. Disponível em: https://fpf.org/wp-content/uploads/2022/06/FPF-SOGI-Report-R2-singles-1.pdf. Acesso em: 27 ago. 2024.

GELLERT, Raphaël. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. **International Data Privacy Law**, [S.l.], v. 5, n. 1, p. 3-19, fev. 2015. DOI: https://doi.org/10.1093/idpl/ipu035.

GELLERT, Raphäel. **The Risk-Based Approach to Data Protection**. New York: Oxford University Press, 2020.

GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. **Computer Law & Security Review**, [S.l.], v. 34, n. 2, p. 279-288, abr. 2018. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364917302698. Acesso em: 15 abr. 2024.

GELLERT, Raphäel. We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection. **European Data Protection Law Review**, Berlin, v. 2, n. 4, p. 481-492, 2016. DOI: https://doi.org/10.21552/EDPL/2016/4/7.

GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In*: PALHARES, Felipe (coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020. p 245-271.

GOVERNMENT STATISTICAL SERVICE. **The future of statistical disclosure control**. London: The National Statistician's Quality Review, 2018. 38 p. Disponível em: https://arxiv.org/pdf/1812.09204. Acesso em: 30 ago. 2024.

GRATTON, Éloïse. If personal information is privacy's gatekeeper, then risk of harm is the key: a proposed method for determining what counts as personal information. **Albany Law Journal of Science and Technology**, Albany, v. 24, n. 1, p. 105-209, jul. 2013. DOI: http://dx.doi.org/10.2139/ssrn.2334938.

GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 4/2007 sobre o conceito de dados pessoais**. Bruxelas: GT29, 2007. 28 p. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf. Acesso em: 15 nov. 2023.

GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 5/2014 sobre técnicas de anonimização**. Bruxelas: GT29, 2014. 37 p. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf. Acesso em: 15 nov. 2023.

HARFF, Graziela; DUQUE, Marcelo Schenk. A proteção dos dados sensíveis no ordenamento jurídico brasileiro. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 29, n. 8, p. 57-88, out./dez. 2021.

HERBST, Tobias. Was sind personenbezogene Daten? **Neue Zeitschrift für Verwaltungsrecht**, Frankfurt a. M., v. 13, p. 902-906, jul. 2016.

HEURIX, Johannes *et al*. A taxonomy for privacy enhancing technologies. **Computers & Security**, [S.l.], v. 53, p. 1-17, set. 2015.

HINTZ, Jan; SINHA, Yamini; SIEGERT, Ingo. **Anonymisierung - Der Heilige Gral?**. 2023. Forum Privatheit: Data Sharing – Datenkapitalismus by Default? em 5 dez. 2023. Disponível em: https://plattform-privatheit.de/p-prv/jahreskonferenzen/jahreskonferenz-2023.php. Acesso em: 31 set. 2024.

HOFFMAN-RIEM, Wolfgang. **Teoria geral do direito digital**: desafios para o direito. FUHRMANN, Italo (trad.). 2 ed. Rio de Janeiro: Forense, 2022.

HOOD, Christopher; ROTHSTEIN, Henry; BALDWIN, Robert. **The government of risk**: understanding risk regulation regimes. New York: Oxford University Press Inc., 2001.

HORNUNG, Gerrit; WAGNER, Bernd. Anonymisierung als datenschutz-relevante Verarbeitung? Rechtliche Anforderungen und Grenzen für die Anonymisierung personenbezogener Daten. **Zeitschrift für Datenschutz**, [S.l.], v. 5, p. 223-228, mai. 2020.

IHE IT INFRASTRUCTURE TECHNICAL COMMITTEE. **Handbook – De-identification**. Madison: IHE, 2013. Disponível em: https://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification_Rev1.0_2014-03-14.pdf. Acesso em: 27 fev. 2024.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO; INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION. **Big Data and Innovation, Setting the Record Straight**: De-identification *Does* Work. Toronto: IPC Ontario, 2014. 13 p. Disponível em: https://www2.itif.org/2014-big-data-deidentification.pdf. Acesso em: 12 out. 2024.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO. **De-identification Guidelines for Structured Data**. Toronto: IPC Ontario, 2016. Disponível em: https://www.ipc.on.ca/en/resources-and-decisions/de-identification-guidelines-structured-data. Acesso em: 15 abr. 2024.

INSTITUTE OF MEDICINE OF THE NATIONAL ACADEMIES. **Sharing clinical trial data**: maximizig benefits, minimizing risks. Washington D.C.: The National Academies Press, 2015. DOI: https://doi.org/10.17226/18998.

IP ADDRESS. *In*: A DICTIONARY of Marketing. 3. ed. New York: Oxford University Press, 2011. Disponível em: https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100010535. Acesso em: 29 jun. 2024.

JAIN, Priyank; GYANCHANDANI, Manasi; KHARE, Nilay. Big data privacy: a technological perspective and review. **Journal of Big Data**, [S.l.], v. 3, n. 25, p. 1-25, nov. 2016. DOI: https://doi.org/10.1186/s40537-016-0059-y.

JANMEY, Victor; ELKIN, Peter L. Re-Identification Risk in HIPAA De-Identified Datasets: The MVA Attack. *In*: AMERICAN MEDICAL INFORMATICS ASSOCIATION ANNUAL SYMPOSIUM, 2018, San Francisco. **Proceedings** [...]. San Francisco: AMIA, 2018. p. 1329-1337.

JONES, David J. K.; HOOD, Christopher. Introduction. *In*: JONES, David J. K.; HOOD, Christopher (ed.). **Accident and Design**: contemporary debates in risk management. London: UCL Press, 1996. p. 1-9.

KANWAL, Neel; JANSSEN, Emiel A.M.; ENGAN, Kjersti. Balancing Privacy and Progress in Artificial Intelligence: Anonymization in Histopathology for Biomedical Research and

Education. *In*: INTERNATIONAL CONFERENCE ON FRONTIERS OF ARTIFICIAL INTELLIGENCE, ETHICS, AND MULTIDISCIPLINARY APPLICATIONS, 1., 2023, Athens. **Proceedings** [...]. Singapore: Springer, 2024. p. 417-429. DOI: https://doi.org/10.1007/978-981-99-9836-4_31.

KARG, Moritz. DSGVO Art. 4 Nr. 1 Begriffsbestimmung „Personenbezogenes Datum“. *In*: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER GEN. DÖHMANN, Indra (ed.). **Datenschutzrecht – DSGVO mit BDSG**. 1. ed. Baden-Baden: Nomos, 2019. *E-book*.

KELLEHER, John D.; TIERNEY, Brendan. **Data Science**. Cambridge: The MIT Press, 2018.

KITCHIN, Rob. **The Data Revolution**: A Critical Analysis of Big Data, Open Data & Data Infrastructures. 2. ed. London: SAGE Publications Inc., 2022.

KITCHIN, Rob; MCARDLE, Gavin. What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets. **Big Data & Society**, [S.l.], v. 3, n. 1, p. 1-10, jan./jun. 2016. DOI: https://doi.org/10.1177/2053951716631130.

KLABUNDE, Achim; Horváth, Anna Zsófia. DS-GVO Art. 4 Begriffsbestimmungen. *In*: EHMANN, Eugen; SELMAYR, Martin (ed.). **DSGVO - Kommentar**. 3. ed. München: Beck, 2024. *E-book*.

KÜHLING, Jürgen; KLAR, Manuel. DS-GVO Art. 4 Nr. 1 personenbezogene Daten (inkl. betroffene Person). *In*: KÜHLING, Jürgen; BUCHNER, Benedikt (ed). **DS-GVO/BDSG**: Kommentar. 4. ed. München: Beck, 2024. *E-book.*

LANEY, Doug. **3D Data Management: Controlling Data Volume, Velocity, and Variety**. Meta group, 6 fev. 2001. Disponível em: https://studylib.net/doc/8647594/3d-data-management--controlling-data-volume--velocity--an.... Acesso em: 12 nov. 2023.

LEENES, Ronald. Do They Know Me? Deconstructing Identifiability. **University of Ottawa Law and Technology Journal**, Ottawa, v. 4, n. 1-2, p. 135-161, 2007.

LI, Ninghui; LI, Tiancheng; VENKATASUBRAMANIAN, Suresh. *t*-Closeness: Privacy Beyond *k*-anonymity and *l*-Diversity. *In*: INTERNATIONAL CONFERENCE ON DATA ENGINEERING, 23., 2007, Istanbul. **Proceedings** [...]. Istanbul: IEEE, 2007. p. 106-115. DOI: https://doi.org/10.1109/ICDE.2007.367856.

LISBOA, Roberto Senise. Boa-fé e confiança na Lei Geral de Proteção de Dados brasileira. **Revista do Advogado**, São Paulo, ano 39, n. 144, p. 6-11, nov. 2019.

LUBARSKY, Boris. Re-identification of “Anonymized” Data. **Georgetown Law Technology Review**, [S.l.], v. 1, n. 1, p. 202-213, abr. 2017. Disponível em: https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/. Acesso em: 24 abr. 2024.

LYNSKEY, Orla. **The Foundations od EU Data Protection Law**. Oxford: Oxford University Press, 2015

MACENAITE, Milda. The “Riskification” of European Data Protection Law through a two-fold Shift. **European Journal of Risk Regulation**, Cambridge, v. 8, n. 3, p. 506-540, set. 2017. DOI: https://doi.org/10.1017/err.2017.40.
MAJEED, Abdul; LEE, Sungchang. Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. **IEEE Access**, [S.l.], v. 9, p. 8512-8545, jan. 2021. DOI: https://doi.org/10.1109/ACCESS.2020.3045700.

MALIN, Bradley *et al*. Identifiability in biobanks: models, measures, and mitigation strategies. **Human Genetics**, [S.l.], v. 130, n. 3, p. 383-392, jul. 2011. DOI: https://doi.org/10.1007/s00439-011-1042-5.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 3. ed. São Paulo: Saraiva Educação, 2024. *E-book*.

MARTINS-COSTA, Judith. O Direito Privado como um “Sistema em construção” - As Cláusulas Gerais no Projeto de Código Civil Brasileiro. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, v. 15, n. 4, p. 129-154, jul./set. 1998. DOI: https://doi.org/10.22456/0104-6594.70391.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469-483, nov./dez. 2018.

MENKE, Fabiano. A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). *In*: DONEDA, Danilo; MACHADO, Diego (coord.). **A Criptografia no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. *E- book.*

MENKE, Fabiano; GOULART, Guilherme Damásio. Segurança da informação e vazamento de dados. *In*: DONEDA, Danilo *et al.* (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 339-359.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Guia sobre privacidade desde a concepção e por padrão**. Brasília: PPSI, 2024. 50 p. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_privacidade_concepcao.pdf. Acesso em: 10 out. 2024.

MIVULE, Kato. Utilizing Noise Addition for Data Privacy, and Overview. *In*: INTERNATIONAL CONFERENCE ON INFORMATION AND KNOWLEDGE ENGINEERING, 2012, Las Vegas. **Proceedings […]**. [S.l.]: arXiv, 2013. p. 65-71. DOI: https://doi.org/10.48550/arXiv.1309.3958.

MOREIRA, João Mendes; DE CARVALHO, André Carlos Ponce de Leon Ferreira; HORVÁTH, Tomáš. **A general introduction to data analytics**. Hoboken: John Wiley & Sons, 2019. *E-book*.

MULHOLLAND, Caitlin 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**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. DOI: http://dx.doi.org/10.18759/rdgf.v19i3.1603.

MURPHY, Tom. 40 Years After the First Cell Phone Call By Tom Murphy Who is inventing tomorrow's future? **IEEE Consumer Electronics Magazine**, Brno, v. 2, n. 4, p. 44-46, out. 2013. DOI: https://doi.org/10.1109/MCE.2013.2273653.

MÜHLENBECK, Robin L. **Anonyme und pseudonyme Daten**. Baden-Baden: Nomos, 2023.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-Anonymization of Large Sparse Datasets. *In*: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 28., 2008, Oakland. **Proceedings** [...]. Los Alamitos: IEEE Computer Society, 2008. p. 111-125. DOI: https://doi.org/10.1109/SP.2008.33.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and fallacies of "Personally Identifiable Information". **Communications of the ACM**, Austin, v. 53, n. 6, p. 24-26, jun. 2010.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NISTIR 8053**: De-identification of Personal Information. Gaithersburg: NIST, 2015. DOI: http://dx.doi.org/10.6028/NIST.IR.8053.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST SP 800-188**: De-identifying Government Datasets: Techniques and Governance. Gaithersburg: NIST, 2023. DOI: http://dx.doi.org/10.6028/NIST.SP.800-188.

NEITZEL, Frank *et al*. Vibration monitoring of bridges. **Reports on Geodesy and Geoinformatics**, Warsaw, v. 90, n. 3, p. 331-340, mar. 2011.

NEUBAUER, Thomas; HEURIX, Johannes. A methodology for the pseudonymization of medical data. **International Journal of Medical Informatics**, [S.l.], v. 80, n. 3, p. 190-204, mar. 2011. DOI: http://dx.doi.org/10.1016/j.ijmedinf.2010.10.016.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

NISSENBAUM, Helen. The Meaning of Anonymity in an Information Age. **The Information Society**, Philadelphia, v. 15, n. 2, p. 141-144, 1999. DOI: https://doi.org/10.1080/019722499128592.

NOGUEIRA, Rodrigo Borges; PUTTINI, Ricardo Staciarini. On Unique Personal Identifiers. **Journal of Internet Technology and Secured Transactions (JITST)**, London, v. 4, n. 1, p. 366-372, mar. 2015. DOI: https://doi.org/10.20533/jitst.2046.3723.2015.0046.

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **The De-Identification Decision-Making Framework**. [S.l.]: CSIRO Reports, 2017. Disponível em: https://www.csiro.au/en/research/technology-space/cyber/A-framework-for-data-de-identification. Acesso em: 28 ago. 2024.

OLEJNIK, Lukasz; RIEMANN, Robert. Quantum Computing and Cryptography. **EDPS TechDispatch publications**, v. 2, p. 1-3, ago. 2020. Disponível em:

https://www.edps.europa.eu/sites/default/files/publication/07-08-2020_techdispatch_quantum_computing_en_0.pdf. Acesso em: 27 set. 2024.

OLIVEIRA, José Roberto Pimenta. Discricionariedade e razoabilidade. **Revista eletrônica da Faculdade de Direito da PUC-SP**, São Paulo, v. 1, p. 1-54, 2008.

OH, Junhyoung; LEE, Kyungho. Data De-identification Framework. **Computers, Materials & Continua**, [S.l.], v. 74, n. 2, p. 3579-3606, 2023. DOI: https://doi.org/10.32604/cmc.2023.031491.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. **UCLA Law Review**, Los Angeles v. 57, n. 6, p. 1701-1778, ago. 2010. Disponível em: https://www.uclalawreview.org/broken-promises-of-privacy-responding-to-the-surprising-failure-of-anonymization-2/. Acesso em: 15 abr. 2024.

O'NEILL, Liam; DEXTER, Franklin MD; ZHANG, Nan. The Risks to Patient Privacy from Publishing Data from Clinical Anesthesia Studies. **Anesthesia & Analgesia**, [S.l.], v. 122, n. 6, p. 2017-2027, jun. 2016. DOI: https://doi.org/10.1213/ANE.0000000000001331.

ONLINE PRIVACY ENFORCEMENT, RIGHTS ASSURANCE & OPTIMIZATION. **D4.3 – Guidelines for data anonymization report**. [S.l.]: OPERANDO, 2016. 33 p. Disponível em: http://www.operando.eu/servizi/moduli/moduli_fase01.aspx?Campo_126=68. Acesso em: 15 nov. 2023.

OOSTVEEN, Manon. Identifiability and the applicability of data protection to big data. **International Data Privacy Law**, [S.l.], v. 6, n. 4, p. 299-309, nov. 2016. DOI: https://doi.org/10.1093/idpl/ipw012.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Paris: OECD, 2002. 62 p. DOI: https://doi.org/10.1787/9789264196391-en.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. Initial policy considerations for generative artificial intelligence. **OECD Artificial Intelligence Papers**, Paris, n. 1, p. 1-40, set. 2023. Disponível em: https://www.oecd-ilibrary.org/docserver/fae2d1e6-en.pdf?expires=1720379926&id=id&accname=guest&checksum=9E44F7C00137994353A9788BF6977E04. Acesso em: 15 jun. 2024.

ORTEGA-FERNANDEZ, Ines; MARTINEZ, Sara El Kortbi; ORELLANA, Lilian Adkinson. Large Scale Data Anonymisation for GDPR Compliance. *In*: SOLDATOS, John; KYRIAZIS, Dimosthenis (ed.). **Big Data and Artificial Intelligence in Digital Finance**: Increasing Personalization and Trust in Digital Finance using Big Data and AI. Cham: Springer, 2022. p. 325-335.

PAAR, Christof; PELZL, Jan. **Understanding cryptography:** a textbook for students and practitioners. London: Springer, 2010.

PAREDAENS, Jan *et al.* **The structure of the relational database model**. Heidelberg: Springer Science & Business Media, 2012. *E-book*.

PARENTONI, Leonardo. Compartilhamento de dados pessoais e a figura do controlador. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Editora Revista dos Tribunais, 2021. p. 699-740.

PEREIRA, Mariana Viale; CACHAPUZ, Maria Cláudia. Big data, cruzamento de dados e proteção à privacidade. **Revista eletrônica [do] Tribunal Regional do Trabalho da 9ª Região**, Curitiba, v. 10, n. 96, p. 95-106, fev. 2021. Disponível em: https://hdl.handle.net/20.500.12178/184392. Acesso em: 20 jul. 2024.

PERSONAL DATA PROTECTION COMMISSION. **Guide to basic anonymisation**. Singapore: PDPC, 2022. 58 p. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf. Acesso em: 03 mar. 2024.

POLONETSKY, Jules; TENE, Omer; FINCH, Kelsey. Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification. **Santa Clara Law Review**, Santa Clara, v. 56, n. 3, p. 593-629, jun. 2016. Disponível em: https://digitalcommons.law.scu.edu/lawreview/vol56/iss3/3. Acesso em: 12 dez. 2023.

PROVOST, Foster; FAWCETT, Tom. Data Science and its Relationship to Big Data and Data-Driven Decision Making. **Big Data**, [S.l.], v. 1, n. 1, p. 51-59, fev./mar. 2013. DOI: https://doi.org/10.1089/big.2013.1508.

PROVOST, Foster; FAWCETT, Tom. **Data Science for Business**: What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly Media, 2013.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology**, London, v. 10, n. 1, p. 41-81, 2018. DOI: http://dx.doi.org/10.2139/ssrn.3036355.

QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. **European Journal of Risk Regulation**, Cambridge, v. 9, n. 3, p. 502-526, set. 2018. DOI: https://doi.org/10.1017/err.2018.47.

RAGHUNATHAN, Balaji. **The Complete Book of Data Anonymization**: from planning to implementation. Boca Raton: CRC Press, 2013.

RAJENDRAN, Keerthana; JAYABALAN, Manoj; EHSAN RANA, Muhammad. A Study on *k*-anonymity, *l*-diversity, and *t*-closeness Techniques focusing Medical Data. **International Journal of Computer Science and Network Security**, Seoul, v. 17, n. 12, p. 172-177, dez. 2017.

RITCHIE, Felix. The 'Five Safes': a framework for planning, designing and evaluating data access solutions. *In*: Data for Policy: Government by Algorithm?, 2017, London. **Proceedings** [...]. [S.l.]: Zenodo, 2017. DOI: http://dx.doi.org/10.5281/zenodo.897821.

ROSAS, Luiza Barros. Conceitos jurídicos indeterminados e discricionariedade administrativa. **Cadernos Jurídicos**, São Paulo, v. 20, n. 47, p. 191-201, jan./fev. 2019.

ROßNAGEL, Alexander. Anonymisierung personenbezogener Daten und Nutzung anonymer Daten - Eine Schlüsselfrage der künftigen Digitalisierung. **Datenschutz und Datensicherheit**, [S.l], v. 8, p. 513-520, ago. 2024.

ROßNAGEL, Alexander; GEMINN, Christian L. Vertrauen in Anonymisierung - Regulierung der Anonymisierung zur Förderung Künstlicher Intelligenz. **Zeitschrift für Datenschutz**, [S.l.], v. 9, p. 487-490, set. 2021.

ROßNAGEL, Alexander; SCHOLZ, Philip. Datenschutz durch Anonymität und Pseudonymität Rechtsfolgen der Verwendung anonymer und pseudonymer Daten. **Multimedia und Recht**, [S.l.], v. 12, p. 721-731, dez. 2000.

RUBINSTEIN, Ira S.; HARTZOG, Woodrow. Anonymization and Risk. **Washington Law Review**, Seattle, v. 91, n. 2, p. 703-760, jun. 2016. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol91/iss2/18/. Acesso em: 15 abr. 2024.

SALTZ, Jeffrey S.; STANTON, Jeffrey M. **An introduction to data science**. 1. ed. Los Angeles: SAGE, 2018. *E-book*.

SAMARATI, Pierangela; SWEENEY, Latanya. Achieving k-anonymity privacy protection using generalization and suppression. **International Journal of Uncertainty, Puzziness and Knowledge-Based System**s, [S.l.], v. 10, n. 5, p. 571-588, 2002. Disponível em: https://ics.uci.edu/~projects/295d/papers/achieving-k-anonymity-privacy-protection-using-generalization-and-suppression.pdf. Acesso em: 11 mar. 2024.

SÁNCHEZ-BORDONA, Manuel Campos. **Processo C-582/14**. Conclusões do Advogado-Geral. [S.l.], 12 mai. 2016. 19 p. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=178241&doclang=PT. Acesso em: 24 mai. 2024.

SANTOS, Douglas; NOBRE, Jéferson Campos. Identificação de vulnerabilidades em sistemas operacionais GNU/Linux através de raciocínio baseado em casos. **Revista de informática teórica e aplicada**. Porto Alegre, v. 26, n. 3, p. 13-25, set. 2019. DOI: https://doi.org/10.22456/2175-2745.82079.

SATELL, Greg. Yes, Big Data Can Solve Real World Problems. **Forbes**. Jersey City, dez. 2013. Disponível em: https://www.forbes.com/sites/gregsatell/2013/12/03/yes-big-data-can-solve-real-world-problems/. Acesso em: 31 ago. 2024.

SCHIMIDT, Eric. **Closing Keynote Presentation & Interview**. The Guardian, jul. 2010. Disponível em: https://www.theguardian.com/media/video/2010/jul/02/google-eric-schmidt-activate. Acesso em: 12 nov. 2023.

SCHÜTZE, Bernd. Nutzung medizinischer Routinedaten außerhalb der Patientenversorgung–Königsweg Pseudonymisierung. **Deutsche Medizinische Wochenschrift - DMW**, Stuttgart, v. 137, n. 16, p. 844-850, jan. 2012. DOI: http://dx.doi.org/10.1055/s-0031-1299040.

SCHWARTMANN, Rolf *et al*. **Anonymisierung und Pseudonymisierung von Daten** - Gesetzestexte, Leitfaden und Grundregeln für die Praxis. Heidelberg: C.F. Müller GmbH, 2023.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. **New York University Law Review**, New York, v. 86, n. 6, p. 1814- 1894, dez. 2011.

SHADIKHODJAEV, Sherzod. Technological Neutrality and Regulation of Digital Trade: How Far Can We Go? **European Journal of International Law**, [S.l.], v. 32, n. 4, p. 1221-1247, nov. 2021. DOI: https://doi.org/10.1093/ejil/chab054.

SIEGEL, Bob. **What is the difference between privacy and security?** Privacy REF, mai. 2016. Disponível em: https://privacyref.com/blog/difference-privacy-security/. Acesso em: 17 mai. 2024.

SMITH, Mick; AGRAWAL, Rajeev. Anonymization Techniques. *In*: SCHINTLER, Laurie A.; MCNEELY, Connie I. (ed.), **Encyclopedia of Big Data**. Cham: Springer, 2022. p. 30-33. DOI: https://doi.org/10.1007/978-3-319-32010-6_9.

SOLOVE, Daniel J; HARTZOG, Woodrow. **Breached!** Why data security fails and how to improve it. New York: Oxford University Press, 2022.

SORIA-COMAS, Jordi; DOMINGO-FERRER, Josep. Big Data Privacy: Challenges to Privacy Principles and Models. **Data Science and Engineering**, [S.l.], v. 1, n. 1, p. 21-28, mar. 2016. DOI: https://doi.org/10.1007/s41019-015-0001-x.

SPIECKER GEN. DÖHMANN, Indra. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *In*: DONEDA, Danilo *et al.* (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 97-113.

SPINDLER, Gerald; SCHMECHEL, Philipp. Personal Data and Encryption in the European General Data Protection Regulation. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S.l.], v. 7, n. 2, p. 163-177, set. 2016.

STALLA-BOURDILLON, Sophie; KNIGHT, Alison. Anonymous Data v. Personal Data — A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. **Wisconsin International Law Journal**, Madison, v. 34, n. 2, p. 284-322, mar. 2017.

STUMMER, Sarah. Issues of Verifying Anonymity: An Overview. *In*: INFORMATIK, 52., 2022, Hamburg. **Proceedings** [...]. Bonn: Gesellschaft für Informatik, 2022. p. 179-194. DOI: https://doi.org/10.18420/inf2022_17.

SWEENEY, Latanya. Foundations of Privacy Protection from a Computer Science Perspective. *In*: STATISTICAL MEETING, 2000, Indianapolis. **Proceedings** [...]. Indianapolis: JSM, 2000. p. 1-65. DOI: https://doi.org/10.1184/R1/6622313.v1.

SWEENEY, Latanya. *k*-Anonymity: a model for protecting privacy. **International Journal on Uncertainty, Fuzziness and Knowledge-based Systems**, [S.l.], v. 10, n. 5, p. 557-570, 2002.

SWEENEY, Latanya. Only You, Your Doctor, and Many Others May Know. **Technology Science**, [S.l.], set. 2015. Disponível em: https://techscience.org/a/2015092903/. Acesso em 15 abr. 2024.

THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; THE INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27000**: Information technology - Security techniques - Information security management systems - Overview and vocabulary. 5. ed. [S.l.]: ISO/IEC, 2018. 27 p.

THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; THE INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 20889**: Privacy enhancing data de-identification terminology and classification of techniques. [S.l.]: ISO/IEC, 2018. 46 p.

THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; THE INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27559**: Information security, cybersecurity and privacy protection - Privacy enhancing data de-identification framework. [S.l.]: ISO/IEC, 2022. 22 p.

THE UK GDPR. Disponível em: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/. Acesso em: 27 ago. 2024.

THOMPSON, Stuart A.; WARZEL, Charlie. The Privacy Project – Twelve Million Phones, One Dataset, Zero Privacy. **The New York Times**. New York, dez. 2019. Disponível em: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. Acesso em: 16 ago. 2024.

TORBAY, Augusto Cesar. A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia. *In*: COUTINHO, Francisco Pereira; MONIZ, Graça Couto (coord.). **Anuário de Proteção de Dados - 2020**. Lisboa: CEDIS, 2020. p. 49-78. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/edicao-2020/. Acesso em: 10 nov. 2023.

TRANSPARÊNCIA Ativa. **Gov.br**. Disponível em: https://www.gov.br/acessoainformacao/pt-br/assuntos/transparencia-ativa. Acesso em: 19 jun. 2024.

UK INFORMATION COMMISSIONER'S OFFICE. **Anonymisation**: managing data protection risk code of practice. Wilmslow: ICO, 2012. Disponível em: https://ico.org.uk/media/1061/anonymisation-code.pdf. Acesso em: 16 nov. 2023.

UK INFORMATION COMMISSIONER'S OFFICE. **Draft – anonymisation, pseudonymisation and privacy enhancing technologies guidance – Chapter 2:** How do we ensure anonymisation is effective?. Wilmslow: ICO, 2021. 27 p. Disponível em: https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf. Acesso em: 22 jun. 2024.

UK INFORMATION COMMISSIONER'S OFFICE - ICO. **Draft – anonymisation, pseudonymisation and privacy enhancing technologies guidance – Chapter 4**:

Accountability and governance. Wilmslow: ICO, 2022. 18 p. Disponível em: https://ico.org.uk/media/about-the-ico/consultations/4019713/chapter-4-anonymisation-guidance-accountability-and-governance.pdf. Acesso em: 12 out. 2024.

UK INFORMATION COMMISSIONER'S OFFICE. **Introduction to anonymisation**: draft anonymisation, pseudonimisation and privacy enhancing technologies guidance. Wilmslow: ICO, 2021. Disponível em: https://ico.org.uk/media/1061/anonymisation-code.pdf. Acesso em: 16 nov. 2023.

UK INFORMATION COMMISSIONER'S OFFICE - ICO. **Privacy-enhancing technologies (PETs)**. Wilmslow: ICO, 2023. 66 p. Disponível em: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf. Acesso em: 20 fev. 2024.

VOKINGER, Kerstin N.; STEKHOVEN, Daniel J.; KRAUTHAMMER, Michael. Lost in Anonymization - A Data Anonymization Reference Classification Merging Legal and Technical Considerations. **The Journal of Law, Medicine & Ethics**, Boston, v. 48, n. 1, p. 228-231, mar. 2020. DOI: https://doi.org/10.1177/1073110520917025.

VOLUME of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. **Statista**, jun. 2021. Disponível em: https://www.statista.com/statistics/871513/worldwide-data-created/. Acesso em: 12 nov. 2023.

WAGNER, Isabel; ECKHOFF, David. Technical Privacy Metrics: a Systematic Survey. **ACM Computing Surveys**, [S.l.], v. 51, n. 3, p. 1-45, jun. 2018. DOI: https://doi.org/10.1145/3168389.

WANG, Rong *et al*. Privacy-Preserving Algorithms for Multiple Sensitive Attributes Satisfying *t*-Closeness. **Journal of Computer Science and Technology**, [S.l.], v. 33, n. 6, p. 1231-1242, nov. 2018. DOI: https://doi.org/10.1007/s11390-018-1884-6.

WIMMER, Miriam. Interfaces entre Proteção de Dados Pessoais e Segurança da Informação: um debate sobre a relação entre Direito e Tecnologia. *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei no 13.709/2018) - A caminho da efetividade:** contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020. p. 127-144.

YAKOWITZ, Jane. Tragedy of the Data Commons. **Harvard Journal of Law & Technology**, Cambridge, v. 25, n. 1, p. 1-68, mar. 2011.

YOUM, Heung Youl. An Overview of De-Identification Techniques and Their Standardization Directions. **IEICE Transactions on Information and Systems**, Tokyo, v. 103, n. 7, p. 1448-1461, jul. 2020. DOI: https://doi.org/10.1587/transinf.2019ICI0002.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? *In*: I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro. **Anais** [...]. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2017. p. 176-193. DOI: https://doi.org/10.13140/RG.2.2.16815.43684.

ZANATTA, Rafael A. F. **A proteção coletiva dos dados pessoais no Brasil**: vetores de interpretação. Belo Horizonte: Letramento, 2023.

Legislação, Jurisprudência e Atos Administrativos Normativos Consultados

BRASIL. Autoridade Nacional de Proteção de Dados. Conselho Diretor. **Resolução nº 11, de 27 de dezembro de 2023**. Altera a Agenda Regulatória para o biênio 2023-2024. Brasília: Autoridade Nacional de Proteção de Dados, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/resolucao_cd_anpd_11_2023-27122023.pdf. Acesso em: 11 nov. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Conselho Diretor. **Resolução nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília: Autoridade Nacional de Proteção de Dados, 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 22 mai. 2024.

BRASIL. Conselho Nacional de Saúde. **Resolução nº 466, de 12 de dezembro 2012**. Aprova as diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos e revoga as Resoluções CNS nº 196/96, 303/2000 e 404/2008. Brasília: Conselho Nacional de Saúde, 2012. Disponível em: https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf. Acesso em: 13 mai. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 05 abr. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 nov. 2023.

BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 19 jun. 2024.

BRASIL. **Lei nº 14.534, de 11 de janeiro de 2023**. Altera as Leis nº 7.116, de 29 de agosto de 1983, 9.454, de 7 de abril de 1997, 13.444, de 11 de maio de 2017, e 13.460, de 26 de junho de 2017, para adotar número único para os documentos que especifica e para estabelecer o Cadastro de Pessoas Físicas (CPF) como número suficiente para identificação do cidadão nos bancos de dados de serviços públicos. Brasília,

DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14534.htm. Acesso em: 27 fev. 2024.

BRASIL. Supremo Tribunal Federal. ADIs no 6.387, 6.388, 6.389, 6.390 e 6.393. Relatora: Ministra Rosa Weber. Brasília, 7 mai. 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 15 jun. 2024.

DEUTSCHLAND, **E-Government-Gesetz (EGovG), de 25 de julho de 2013**. Disponível em: https://www.gesetze-im-internet.de/egovg/. Acesso em: 20 nov. 2023.

DEUTSCHLAND. Bundesverfassungsgericht (BVerfGE) - Zweiten Senats. BVerfGE 49, 89 - Kalkar I. 08 ago. 1978. Disponível em: https://www.servat.unibe.ch/dfr/bv049089.html. Acesso em: 15 abr. 2024.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679, de 27 de abril de 2016**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679. Acesso em: 15 abr. 2024.

UNIÃO EUROPEIA. **Diretiva 95/46/CE, de 24 de outubro de 1995**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 15 abr. 2024.

UNIÃO EUROPEIA. Tribunal de Justiça – Terceira Secção. Processo C-70/10. Autor: Scarlet Extended SA. Réu: Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Relator: J. Malenovský. Luxemburgo, 24 nov. 2011. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070. Acesso em 27 abr. 2024.

UNIÃO EUROPEIA. Tribunal de Justiça – Segunda Secção. Processo C-582/14. Autor: Patrick Breyer. Réu: Bundesrepublik Deutschland. Relator: A. Rosas. Luxemburgo, 19 out. 2016. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-582/14. Acesso em 15 abr. 2024.

UNITED KINGDOM. **Regulation (UE) 2016/679 (with amendments), de 27 de abril de 2016**. Disponível em: https://www.legislation.gov.uk/eur/2016/679/introduction. Acesso em: 15 abr. 2024.

UNITED STATES OF AMERICA. **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule**. Address the use and disclosure of individuals' health information. Washington, D.C.: U.S. Department of Health and Human Services, 2000. Disponível em: https://www.hhs.gov/sites/default/files/privacysummary.pdf. Acesso em: 27 jun. 2024.