INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 05 · n. 02 · maio/agosto 2024 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.5.n.2

05

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

International Journal of Digital Law – IJDL
ISSN 2675-7087
DOI: 10.47975/digital.law.vol.5.n.2.melo

A regulamentação da proteção de dados pessoais e seus desafios no contexto da tragédia dos (anti)comuns – Evitando a tragédia da desconfiança

Regulating personal data protection and its challenges in the context of the (anti)commons tragedy – Avoiding the tragedy of distrust

Lígia Maria Silva Melo*
I Universidade Federal do Ceará (Fortaleza, Ceará, Brasil)
meloligia@gmail.com
https://orcid.org/0000-0001-7987-4381

Nélida Astezia de Castro Cervantes**
I Universidade Federal do Ceará (Fortaleza, Ceará, Brasil)
nelidacervantes@hotmail.com
https://orcid.org/0000-0003-0614-9300

William Magalhães Lessa***
I Universidade Federal do Ceará (Fortaleza, Ceará, Brasil)
williamlessa_1@hotmail.com
https://orcid.org/0000-0002-9692-4536

Como citar esse artigo/*How to cite this article*: MELO, Lígia Maria Silva; CERVANTES, Nélida Astezia de Castro; LESSA, William Magalhães. A regulamentação da proteção de dados pessoais e seus desafios no contexto da tragédia dos (anti)comuns – Evitando a tragédia da desconfiança. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 11-29, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.melo.

* Docente da Faculdade de Direito da Universidade Federal do Ceará (Fortaleza, Ceará, Brasil). Doutora em Direito Econômico e Desenvolvimento pela PUCPR. Mestra em Direito do Estado pela PUC-SP. Presidente do Instituto Cearense de Direito Administrativo – ICDA. Diretora do Instituto Brasileiro de Direito Administrativo – IBDA. Coordenadora Regional do Instituto Brasileiro de Direito. *E-mail*: meloligia@gmail.com.

** Docente da Faculdade de Direito da Universidade Federal do Ceará (Fortaleza, Ceará, Brasil). Doutora em Ciências Políticas pela Universidade de Lisboa (ISCSP). Mestra em Direito Constitucional pela UFC-CE. Coordenadora do Núcleo de Prática Jurídica da Faculdade de Direito da UFC-CE. *E-mail*: nelidacervantes@hotmail.com.

*** Mestrando do Programa de Pós-Graduação em Direito da Universidade Federal do Ceará (Fortaleza, Ceará, Brasil). Especialista em Direito Processual Civil pelo Centro Universitário Damásio de Jesus. *E-mail*: williamlessa_1@hotmail.com.

Recebido/Received: 26.08.2024 / August 26th, 2024
Aprovado/Approved: 28.09.2024 / September 28th, 2024

Resumo: O presente estudo busca realizar uma análise econômica dos modelos regulatórios da privacidade e proteção de dados pessoais, tomando por referência o clássico texto *A tragédia dos comuns*, a metodologia adotada partiu da literatura de referência nacional e estrangeira. Inicialmente, apresentou-se breve exposição das características e etapas da regulação acerca do tema para daí iniciar uma análise econômica da privacidade – seja como bem econômico, seja como lastro da confiança na economia da informação. O objetivo deste trabalho é analisar como o modelo da tragédia dos comuns pode auxiliar na crítica da regulação do tema e identificar melhorias e forma de operacionalizá-las. A relevância da pesquisa insere-se no contexto da necessidade de uma mais eficiente regulamentação da proteção de dados pessoais no Brasil e das dificuldades de um consentimento informado pelos titulares de dados pessoais face a relações assimétricas com os controladores e processadores. Concluiu-se que a missão regulatória segue incompleta, mostrando-se necessária a responsabilização dos controladores, e assim como o fomento da confiança dos titulares de dados. A partir desta realidade, foram apresentadas algumas propostas de soluções tecnológicas para fomentar essa confiança, na figura das chamadas PETs, tecnologias de aprimoramento de privacidade, mesmo considerando que a difusão dessas tecnologias esbarra na ausência de adesão por ausência de uma regulação vinculante acerca do tema.

Palavras-chave: Proteção de dados pessoais; tragédia dos comuns; regulamentação; sociedade da informação; tecnologia.

Abstract: This study seeks to carry out an economic analysis of regulatory frameworks for privacy and personal data protection, taking the classic text "The Tragedy of the Commons" as a reference. The methodology adopted was based on national and foreign reference literature. Initially, a brief presentation was made of the characteristics and stages of regulation on the subject, in order to begin an economic analysis of privacy – both as an economic good and as a basis for trust in the information economy. The aim of this work is to study how the "Tragedy of the Commons" model can help to critically investigate the regulation of the subject and identify improvements and ways of making them operational. The research is relevant in the context of the need for more efficient regulation of personal data protection in Brazil and the difficulties of informed consent by personal data subjects in the face of asymmetrical relationships with controllers and processors. In conclusion, the regulatory mission is still incomplete and there is a need to hold controllers accountable, as well as to foster the trust of data subjects. Based on this reality, some proposals were put forward for technological solutions to foster such trust, in the form of the so-called PETs, privacy enhancing technologies, even considering that the diffusion of these technologies comes up against the lack of adherence due to the absence of binding regulation on the subject.

Keywords: Personal data protection; Tragedy of the commons; Regulation; Information society; Technology.

1 Introdução

As constantes transformações, em nível mundial, têm apresentado reflexos nos mais diversos setores, quer sejam econômicos ou políticos. A partir da metade do século XX e início do século XXI. É evidente que a tecnologia foi responsável

por grande parte dessas transformações, contudo, junto aos avanços tecnológicos, surge a insegurança na proteção do que é disponibilizado na internet, sobretudo de dados pessoais.

Transacionar com base em dados pessoais para se ter acesso a diferentes tipos de produtos e serviços não é uma opção na sociedade da informação,[1] mas uma necessidade. Todavia, a economia da informação não implica uma renúncia automática da privacidade – devendo-se fugir de simplificações nesse sentido.

De acordo com dados do Banco Interamericano de Desenvolvimento (BID), em 2021, danos decorrentes de delitos cibernéticos alcançaram incríveis seis bilhões de dólares. Ademais, de acordo com pesquisas realizadas, menos de 50% (cinquenta por cento) da população mundial com acesso à internet acredita que a tecnologia melhorará sua vida, o que representa uma crescente falta de confiança no que tange à privacidade e à proteção de dados.[2]

A regulação do tema se sofisticou substancialmente nas últimas décadas, desde o enfoque em gigantescos bancos de dados estatais, evoluindo para dar lugar a um protagonismo do consentimento qualificado dos cidadãos titulares de seus dados.

Há muito a literatura de referência debate entre modelos de intervenção estatal forte e de autorregulação do setor pelas corporações controladoras e processadoras de dados pessoais – havendo relativo consenso na relevância da participação do titular dos dados mediante seu consentimento. Normalmente, esse consentimento é expresso nos famosos "avisos de privacidade" que aparecem ao se acessar *sites* e aplicações eletrônicas, pressupondo que o usuário leu e revisou extensas políticas de privacidade.

Nas palavras de Stefano Rodotà,[3] a questão não é mais "regulação, sim ou não", pois isso há muito foi superado. Trata-se, na realidade, de como atribuir um valor orientador para essa regulação, para o futuro. Para formular categorias e conceitos envolvendo contratantes hipossuficientes e sua privacidade, cujo sistema de tutela em grande parte ainda remonta a uma época em que a informação não era um recurso central para a economia e para a sociedade.

---

1 Termo aqui adotado na acepção de Manuel de Castells: "O termo sociedade da informação enfatiza o papel da informação na sociedade [...] Ao contrário, o termo [sociedade] informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico". *Vide*: CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2005. p. 64-65.

2 BANCO INTERAMERICANO DE DESENVOLVIMENTO; ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Cibersegurança*: riscos, avanços e o caminho a seguir na América Latina e no Caribe. Relatório de Cibersegurança. 2020. Disponível em: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

3 RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução de Danilo Doneda e Lucial Cabral Doneada. Rio de Janeiro: Renovar, 2008. p. 57.

O presente estudo pretende fazer uma breve análise da evolução dos marcos e modelos regulatórios sobre privacidade e proteção de dados pessoais e correlacioná-la com um modelo clássico de análise econômica, chamado *tragédia dos comuns*, de Garrett Harding.

A literatura existente traz interessantes contributos correlacionando o modelo a análises da privacidade como um bem econômico e sua função na geração e manutenção de confiança na sociedade, servindo como premissa para criticar modelos regulatórios e pensar em contribuições.

Nesse contexto, o estudo tem como objetivo central analisar como o modelo da *tragédia dos comuns* pode auxiliar na crítica da regulação do tema e identificar melhorias e forma de operacionalizá-las.

Parte do desafio é vislumbrar os titulares de dados pessoais e da privacidade como *stakeholders* (interessados) fundamentais nas transações informacionais e cuja confiança é fundamental para o sustento e sucesso da economia da informação, pensando em maneiras de romper as assimetrias entre estes e os controladores e processadores de dados, representados pelo Estado e pelas grandes corporações – especialmente no caso brasileiro.

A metodologia proposta será qualitativa e aplicada, tendo por procedimento a pesquisa analítico-descritivo da literatura de referência (artigos científicos, livros, periódicos), com a técnica proposta sendo a pesquisa bibliográfica e documental.

2 A evolução dos marcos regulatórios de proteção de dados pessoais

O presente estudo organizará a regulamentação da privacidade e da proteção de dados pessoais, por meio da sua evolução histórica em *gerações*, seguindo o critério de Viktor Mayer-Schönberger –[4] que as divide em quatro gerações – com as contribuições de Bruno Bioni[5] e Danilo Doneda[6] acerca do tema.

Cumpre ressalvar que a análise de Mayer-Schönberger se limita ao universo norte-americano e europeu, pelo que não reflete a evolução da matéria em todo o mundo.

4 MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection. *In*: ROTENBERG, Marc; AGRE, Philip E. *Technology and privacy*: The new landscape. [s.l.]: [s.n.], 1998. p. 219.

5 BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 170-173.

6 DONEDA, Danilo César Maganhoto. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2020. p. 166-169.

Geração	1ª – Normas de proteção para dados	2ª – Proteção contra ofensores maiores e diferentes	3ª – O direito à autodeterminação informativa	4ª – Perspectivas holísticas e setoriais
Características	– Receio de uma realidade orwelliana de controle estatal por meio de dados. – Enfoque na função social do processamento de dados, não na proteção individual. – Necessidade de autorização governamental para criação de grandes bancos de dados.	– Proteção de direitos individuais (privacidade como um direito de ser "deixado só"). – Obrigação de o titular escolher entre exclusão social e transações informacionais.	– O direito do indivíduo de definir quais dados e em que medida serão processados. – Pressuposição do exercício de direitos. – Proteção de dados continua sendo um direito reservado a poucos. – Surgimento das autoridades nacionais de proteção de dados.	– Certos tratamentos de dados recebem maior regulação independentemente do consentimento (*e.g.*, dados sensíveis). – Preocupação com o equilíbrio entre titular e controlador de dados. – Setorização da matéria (proteção de dados para a saúde, para a administração pública etc.). – Permanece o protagonismo do consentimento.
Tecnologia	Bancos de dados centralizados estatais.	Corporações privadas adquirem os meios para criar e manter grandes bancos de dados. Início de trocas internacionais de dados baseadas em "reciprocidade".	Disseminação dos bancos de dados interligados e dificuldade em se localizar onde se realizava efetivamente o tratamento.	Disseminação de políticas de privacidade e avisos de consentimento.
Marco legal	Lei Estadual de Proteção de Dados de Hesse (1970).	Estatuto de proteção de dados francês (1978).	Decisão do Tribunal Constitucional alemão sobre o censo (1983). Convenção nº 108 do Conselho da Europa (1980).	*General Data Protection Act* (GDPR, 2016).
Outros exemplos	Estatuto de Proteção de Dados do Estado de Reno-Pfalz (1974). *Privacy Act* estadunidense (1974).	Estatutos de proteção de dados austríaco e dinamarquês.	Ato de Registro de Pessoas Naturais, Finlândia (1987).	LGPD brasileira (2018).

Pode-se perceber que o modelo adotado em *gerações* não é suficiente para esclarecer o processo evolutivo dos marcos regulatórios em todas as instâncias.

No Brasil, por exemplo, o processo de regulação das leis de privacidade e proteção de dados seguiu um caminho distinto. A própria Constituição de 1988 trouxe dispositivos esparsos acerca do tema, como exemplo: o direito fundamental à privacidade (art. 5º, X, CF); mecanismos de acesso e retificação de dados, como *habeas data* (art. 5º, XXXIV, a); direito de petição (art. 5º, LXXII); acesso à informação na administração pública (art. 5º, XXXIII, 37, §2º, III).[7]

Quanto à legislação infraconstitucional, verifica-se que o Código de Defesa do Consumidor (Lei nº 8.072/1990) –[8] a exemplo da legislação estadunidense anterior – trouxe parâmetros para bancos de dados consumeristas (art. 43); a Lei de Acesso à Informação (Lei nº 12.257/2011)[9] foi importantíssima para a transparência de dados pessoais ou não tratados pela administração pública. O Marco Civil da Internet (Lei nº 12.965/2014),[10] por sua vez, regulamentou os provedores de internet e trouxe uma promessa de regulamentação acerca da proteção de dados pessoais (art. 10).

Esta regulação finalmente veio com a promulgação da LGPD –[11] já considerada uma lei da chamada quarta geração, vez que surgida e assemelhada ao *General Data Protection Regulation* (GDPR) europeu. Todavia, os últimos desdobramentos da regulação da proteção de dados no país vieram com o ingresso do Brasil no Comitê Observador da Convenção nº 108,[12] marco legal mundial de compromisso com a proteção de dados, que elevou a Autoridade Nacional de Proteção de Dados

---

7 BRASIL. *Constituição da República Federativa do Brasil de 5 de outubro de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 jun. 2022.

8 BRASIL. *Código de Defesa do Consumidor*. Lei nº 8.078 de 11 de setembro de 1990. Ementa: Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 1º jun. 2022.

9 BRASIL. *Lei de Acesso à Informação*. Lei nº 12.527 de 18 de novembro de 2011. Ementa: Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 1º jun. 2022.

10 BRASIL. *Marco Civil da Internet*. Lei nº 12.965 de 23 de abril de 2014. Ementa: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1º jun. 2022.

11 BRASIL. *Lei Geral de Proteção de Dados*. Lei nº 13.709 de 14 de agosto de 2018. Ementa: Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1º jun. 2022.

12 Importante ressalvar que o Brasil ainda não ratificou a Convenção, sendo membro de seu Comitê Observador que se reúne em Estrasburgo 2 vezes ao ano para debater questões mundiais acerca do tema. *Vide*: BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. ed. 1. fev. 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais#:~:text=0%20Brasil%20n%C3%A3o%20%C3%A9%20signat%C3%A1rio,de%20prote%C3%A7%C3%A3o%20de%20dados%20pessoais. Acesso em: 10 jun. 2022.

ao nível de autarquia autônoma[13] e incitando a promulgação da Emenda Constitucional nº 115/2022.

A constitucionalização da proteção de dados pessoais não é medida que todos os países tomam, porém, no caso brasileiro, a EC nº 115/2022[14] não procurou apenas acrescer nova garantia ao rol do art. 5º (novo inc. LXXIX), mas principalmente uniformizar a competência legislativa acerca da matéria, tornando-a competência exclusiva da União (novo art. 21, XXVI).

Na América Latina, verifica-se que Argentina e Uruguai lideraram na regulamentação matéria, já possuindo regramentos consolidados em seus ordenamentos acerca do tema há bastante tempo. No caso argentino, também se optou por constitucionalizar a proteção aos dados pessoais (art. 43, §3º, da Constituição Federal argentina) ainda em 1994, com a promulgação da Lei de Proteção de Dados Pessoais (Lei nº 25.326) em 2001, regulamentada pelo Decreto nº 1.558. Em 2019, houve a adesão da Argentina à Convenção nº 108.[15]

O Uruguai, a seu turno, não constitucionalizou esse direito, porém há muito mantém um regramento coerente sobre a proteção de dados pessoais. Promulgou sua Lei de Proteção de Dados Pessoais em 2018 (Lei nº 18.331), regulamentando-a no ano seguinte (via Decreto nº 414), aderindo à Convenção nº 108 ainda em 2012. Com o lançamento do GDPR europeu em 2018, o Uruguai tão somente realizou adaptações em seu ordenamento por via do Decreto nº 64/2020.

Malgrado os diferentes processos regulatórios, a literatura segue constatando o grande protagonismo do consentimento do titular como um dos pilares da regulamentação da privacidade e da proteção de dados pessoais. Isso traz grandes implicações para o sucesso das normas, uma vez que permanecem fortemente dependentes de decisões individuais para que a proteção seja efetiva.

Para os objetivos do presente estudo, será útil fazer uso de um modelo econômico de análise para estudar as repercussões de decisões de agentes individuais sobre direitos comuns a todos.

3 A tragédia dos (anti)comuns aplicada à privacidade e à proteção de dados pessoais

Em 1968, no artigo *A tragédia dos comuns*, Garrett Harding[16] propôs um modelo de análise acerca da maneira como indivíduos, agindo em interesse próprio,

[13] Isso ocorreu com a publicação da MP nº 1.124/2022, que torna a ANPD autarquia federal especial.

[14] SENADO FEDERAL DO BRASIL. *Proposta de Emenda à Constituição nº 17/2019*. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline. Acesso em: 13 jun. 2022.

[15] DATA PROTECTION LAW OF THE WORLD. *Legislação*. Disponível em: https://www.dlapiperdataprotection.com/index.html. Acesso em: 2 jun. 2022.

[16] HARDIN, Garrett. The tragedy of the commons: the population problem has no technical solution; it requires a fundamental extension in morality. *Science*, v. 162, n. 3859, p. 1243-1248, 1968.

podem esgotar um recurso natural comum e limitado, caso regras não sejam estabelecidas. O exemplo era de pecuaristas explorando um pasto coletivo – eventualmente todos o exploravam até nada restar. A criação do direito à propriedade seria uma forma de romper o impasse e assegurar um uso razoável dos bens coletivos.

Em contraste, a literatura propôs também o cenário inverso, em que o excesso de regras cria uma tragédia dos "anticomuns", no qual poucos ou ninguém conseguem acessar bens pela existência de demasiadas limitações

A ideia da racionalidade do jogo busca explicar como os indivíduos, que compõem as organizações e instituições sociais, agem individualmente, por meio do cálculo consciente da sua racionalidade, para atingir seus objetivos pessoais. Costa, corroborando esse entendimento, explicita que "Indivíduos, políticos, burocratas, empresários, partidos e o próprio governo (ou quem o representa) agem em função de seus próprios interesses",[17] contudo, apenas os indivíduos decidem, já que a sociedade, o Estado e o governo não têm preferências, sendo a escolha pública a soma das preferências individuais. A ação racional é a que foi eleita, dentre as várias possíveis, como a melhor pelo ator, exprimindo suas preferências, desejos e crenças.[18]

A premissa da teoria da escolha racional é a de que o valor agregado[19] à sociedade se baseia na soma de todas as escolhas feitas pelos indivíduos, que se confrontam com várias alternativas possíveis de ação, os quais escolhem de acordo com os seus interesses e limitações.

Os seres humanos, na realidade, não se comportam, exatamente, como prescreve a teoria da escolha racional; contudo, os indivíduos tendem a reconhecer a força normativa da racionalidade, e isso influencia as suas ações — que se aproximam, ao menos um pouco, daquilo que criaturas de racionalidade ideal fariam nas mesmas circunstâncias. O comportamento é regido pela necessidade de sobrevivência e crescimento das instituições sociais nas quais as regras são seguidas e desempenhadas.[20]

Embora o indivíduo conheça o ambiente (mercado) e otimize suas ações para atingir os fins desejados, essa teoria considera, também, a falibilidade humana. Nesse sentido, a teoria da escolha racional considera que a racionalidade é limitada ao cognitivo (racionalidade limitada) fruto da coleta e processamento de informações

[17] COSTA, Frederico Lustosa da. Bases teóricas e conceituais da reforma dos anos 1990: crítica do paradigma gerencialista. *Revista Brasileira de Administração Política*, 2.2. p. 79.

[18] FEREJOHN, John; PASQUINO, Pasquale. The countermajoritarian opportunity. Universidade da Pensilvânia. *Pan Carey Law*, v. 13, p. 353, 2010.

[19] Valor agregado é o valor criado por um agente econômico a um bem, quando este é modificado durante o processo produtivo. É o valor que o processo produtivo adiciona a determinado bem.

[20] FEREJOHN, John; PASQUINO, Pasquale. A teoria da escolha racional na ciência política: conceitos de racionalidade em teoria política. *Revista Brasileira de Ciências Sociais*, v. 16, p. 5-24, 2001.

pelo homem.[21] A teoria também encontra interessante aplicação na análise de diferentes políticas públicas,[22] mostrando-se oportuna especialmente quando a política brasileira de proteção de dados pessoais está literalmente sendo formulada e consolidada pela ANPD, pelos titulares e pelos controladores e processadores de dados no país.

João Luís Nogueira Matias e Afonso de Paula Pinheiro Rocha aplicam o modelo de Garrett Harding à evolução do direito da propriedade, explicando que retrata um cenário em que os benefícios da atividade econômica são internalizados por apenas alguns pecuaristas e os custos externalizados para os demais produtores, que não poderão fazer uso do pasto. A criação de um regime de propriedade para parametrizar o uso racional do recurso comum é uma das maneiras para romper esse impasse:[23]

> Os direitos de exclusividade/propriedade são necessários e surgiram exatamente para delimitar o uso desses recursos. Retornando ao exemplo dos terrenos baldios, se os criadores de gado delimitarem as áreas, irão internalizar os benefícios referentes ao seu terreno sem onerar os terrenos designados para os outros.

Se o direito à propriedade é uma das maneiras de se romper o impasse gerado pelas disputas em torno de bens comuns e livremente acessíveis na sociedade, a absolutização da propriedade – típica dos momentos (neo)liberais – pode trazer um outro tipo de tragédia, a chamada tragédia dos anticomuns ou antibaldios.[24] Os autores oferecem um exemplo brasileiro bem peculiar: o de concentração fundiária em prejuízo da máxima eficiência na utilização da terra em favor de outras culturas.

Noutras palavras, a propriedade como ferramenta regulatória – como todo remédio – depende de sua *dosagem* para alcançar melhores efeitos ou mesmo para evitar a criação de outros entraves.

Fairfield e Engels, por sua vez, aplicaram o modelo da tragédia dos comuns para analisar a privacidade e a proteção de dados pessoais como bens comuns da sociedade. Nessa perspectiva:[25]

---

21 CYERT, R.; MARCH, J. *A behavioral theory of the firm*. Englewood Cliffs: Prentice Hall, 1963.

22 CERVANTES, Nélida Astezia Castro. *A influência do TRIPS no Programa da SIDA no Brasil*: uma investigação no âmbito da perspectiva neoinstitucional da teoria da escolha racional. Tese (Doutorado em Ciências Sociais) – Universidade de Lisboa, Lisboa, 2021. Disponível em: https://www.repository.utl.pt/handle/10400.5/21855. Acesso em: mar. 2023.

23 MATIAS, João Luis Nogueira; ROCHA, Rocha. *Repensando o direito de propriedade*. [s.l.]: [s.n.], 2006. p. 13-14.

24 HELLER, Michael. The tragedy of the anti-commons: property in the transition from Marx to Markets. *Harvard Law Review*, n. 111, jun. 1997.

25 FAIRFIELD, Joshua A. T.; ENGEL, Christoph. Privacy as a public good. *Duke LJ*, v. 65, 2015. p. 423. Tradução livre pelo autor. No original: "Translated to privacy, the public-goods model assumes that at least some individuals calculate the following way: If I disclose information, I will receive a private benefit— access to

> Em verdade, nós defendemos que a privacidade é um bem público no sentido literal da literatura econômica. A privacidade pode ser vítima de dilemas sociais. [...] E sem uma intervenção ponderada, as decisões informadas de indivíduos sobre a privacidade tendem a reduzir a privacidade de todos, mesmo se todos apreciarem-na igual e intensamente.

Para Fairfield e Engels, portanto, a privacidade e a consequente necessidade de proteção dos dados pessoais dos indivíduos seriam bens econômicos do tipo não exclusivos (*nonexcludable*, no sentido de disponíveis a todos) e não competitivos (*non-rivalrous*, no sentido de que seu consumo não limita o consumo de outros). E aqui os autores reconhecem o desafio da economia baseada em produtos e serviços informacionais como geradores da sensação nos indivíduos de que, malgrado seu desejo pessoal por privacidade, não a terão de toda forma, sendo os possíveis prejuízos futuros e difusos –[26] a exemplo de um futuro vazamento de dados.

Os autores verificam que a política de proteção de dados pessoais tem se posicionado no sentido de empoderar os indivíduos – tomando-os como principais interessados (*stakeholders*) na tutela de sua privacidade e dados – a despeito de certo niilismo em relação à viabilidade de uma efetiva proteção. Essa proteção tem se manifestado em uma abordagem individualista, ou seja, voltada à revisão de políticas de privacidade extensas, manifestação do consentimento e, eventualmente, o manejo do direito de acesso ou à deleção dos dados tratados.

Todavia, tal abordagem individualista está sujeita às heurísticas e vieses clássicos[27] que atingem o indivíduo, alcançando efeitos cada vez menores, pelo que Farfield e Engels propõem uma abordagem mais voltada à interação de grupos de indivíduos:[28]

---

an online site or service, for example. This imposes a cost on me, based on the personal information I have given up, and it imposes a cost on everyone because I have contributed to the overall lack of privacy in the culture. Yet as long as the sum of my direct costs and my share of the social costs (resulting from my own release of private information) is less than the private benefit I gain, I will choose to give up information to access the site or service. Thus, it makes sense to examine privacy as a social construct, subject to the problems of social production.185 Indeed, we contend that privacy is a public good as that term is strictly defined in the economics literature. Privacy will fall prey to social dilemmas. In weighing important decisions about privacy, individual and group incentives diverge. And without measured intervention, individuals' fully informed privacy decisions tend to reduce overall privacy, even if everyone cherishes privacy equally and intensely".

[26] FAIRFIELD, Joshua A. T.; ENGEL, Christoph. Privacy as a public good. *Duke LJ*, v. 65, 2015. p. 425.

[27] Fala-se no "paradoxo da privacidade", os indivíduos declaram se preocupar com sua privacidade quando questionados, mas falham em agir quando necessário. Para maiores informações, *vide*: GERBER, Nina; GERBER, Paul; VOLKAMER, Melanie. Explaining the privacy paradox: A GERBER, Nina; GERBER, Paul; VOLKAMER, Melanie. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, v. 77, p. 226-261, 2018.

[28] FAIRFIELD, Joshua A. T.; ENGEL, Christoph. Privacy as a public good. *Duke LJ*, v. 65, 2015. p. 457. Tradução livre pelo autor. No original: "This Article proposes giving groups tools for this struggle. Policymakers should consider the size, composition, and cohesion of online groups when they attempt to create an environment conducive to privacy protection. Tools should not be centered on individual rights of review and deletion,

> Os responsáveis pelas políticas de proteção de dados – públicos e particulares – deveriam enfocar no tamanho, composição e coesão de grupos online ao tentar criar um ambiente condutor para a proteção da privacidade. Tais ferramentas não devem enfocar em simples revisão e deleção, que já se mostraram pouco efetivas. Em verdade, deveriam enfocar na comunicação de grupos, sanções e no fomento de gamificação[29] e no senso de comunidade.

Portanto, assim como a propriedade individual, extremada ou livre de parâmetros como a função social, falha em tutelar bens comuns e caros à sociedade – a proteção de dados pessoais e da privacidade também depende de mecanismos sociais e jurídicos mais sofisticados que o empoderamento dos indivíduos para consentirem ou não no tratamento de seus dados. A proposta dos autores supramencionados enfoca em estratégias de grupo para evitar maior intervenção regulatória estatal ou mantê-la em um mínimo possível.

Dennis Hircht, a seu turno, critica a abordagem anterior, apontando uma omissão importante na análise: a ausência das grandes corporações na análise do problema da privacidade e do consentimento emanado por indivíduos e/ou grupos de indivíduos. Segundo este autor, o centro do problema estaria nos principais interessados em explorar a privacidade e a proteção de dados como bens comuns, interiorizando os benefícios e externalizando os custos. As corporações cumpririam esse papel na economia da informação.

Embora reconheça a contribuição de Fairfield e Engels na superação de um marco regulatório excessivamente focado no indivíduo (mediante avisos e políticas de privacidade), em favor de modelos que favoreçam a ação coletiva (reitere-se, focados, na sanção, comunicação de grupos e gamificação), Hircht entende que tais medidas não seriam suficientes:[30]

---

which have proven largely ineffective. Rather, tools should focus on group communication, sanction, and fostering a sense of repeat play and community. Even the way that we speak about the nature of the problem can have an impact on whether people cooperate to produce the public good of privacy".

29 Nota de tradução: o original tratava de *repeat play*, como interações sucessivas entre os titulares de dados pessoais e seus direitos, com finais indeterminados, de maneira a criar uma experiência no titular acerca da defesa de seus interesses relacionados à privacidade e proteção de dados.

30 HIRSCH, Dennis D. Privacy, public goods, and the tragedy of the trust commons: a response to professors Fairfield and Engel. *Duke LJ Online*, v. 65, 2015. p. 67. Tradução livre pelo autor. No original: "The overuse of personal information is leading to a tragedy of the commons but it is not the one that Fairfield and Engel identify. Instead, it is a tragedy of the trust commons. All economies depend on trust. 'We trust that merchants will accept the small, green pieces of paper that we've earned in exchange for goods and services. We trust that airplanes will arrive safely and to the correct airport. We trust that professionals in our service will act in our best interest…' The information economy is no different. When we engage in a digital transaction, visit a Web site, enter a search query, or make a purchase from an online store, we trust the provider to supply us with goods and services that will not hurt us, just as we do in the brick-and-mortar economy".

> A exploração excessiva de dados pessoais está levando a uma tragédia dos comuns, mas não uma do tipo que Fairfield e Engel identificam. Na verdade, é uma tragédia da confiança comum. Todas as economias dependem de confiança. Confiamos que comerciante aceitarão pequenos pedaços de papel verde que recebemos em troca de bens e serviços. Confiamos que aviões chegarão segura e pontualmente. Confiamos que profissionais a nosso serviço atuarão em nosso melhor interesse... A economia da informação não é diferente. Quando nos engajamos numa transação digital, visitamos um site na *Web*, fazemos uma busca, ou procuramos um produto virtualmente, confiamos que o controlador de dados nos oferecerá produtos e serviços que não nos prejudicarão, assim como na economia tradicional.

Em um cenário hipotético, caso a confiança em torno das transações baseadas em privacidade e proteção de dados seja perdida, as pessoas podem começar a reter tais dados pessoais ou mesmo passar a oferecer dados falsos ou incompletos, gerando uma crise de confiança semelhante à crise de 2008 nos mercados financeiros. No cenário atual, porém, uma tragédia de anticomuns nesse contexto parece improvável, mas certamente não se apresenta impossível.

A título de exemplo, diferentes pessoas utilizaram a proteção de dados pessoais conferida pela legislação para dados médicos, considerados sensíveis, como uma maneira de recusar informações sobre a participação ou não em campanhas de vacinação durante a pandemia de Covid-19.[31]

A economia da informação, portanto, baseia-se em confiança digital, que dá ensejo a transações baseadas nos dados pessoais dos cidadãos – essa confiança sim seria um bem de livre acesso e parcialmente competitivo (no sentido de que, em havendo sucessivas violações e vazamentos, os titulares de tais dados podem começar a retê-los ou não os compartilhar adequadamente).

Embora não opte por um modelo particular, Hircht relaciona modelos regulatórios que contemplam as corporações, baseados na autorregulação das empresas, regulamentação estatal ou modelos mistos combinando ambos.

Outra forma de classificar tais modelos seria baseada no *design* do tratamento de dados, exigindo tipos específicos de aviso de privacidade para determinados tipos de tratamento de dados; ou na *performance* de segurança do tratamento, que determinam que as empresas evitem certos tipos ou níveis de risco, mas deixam-nas livres para escolher como atingir tais níveis de segurança.[32]

---

[31] HALDER, Steve. Is it a HIPAA Violation to Ask for Proof of Vaccine Status? *HIPAA Journal*, Dec. 25, 2021. Disponível em: https://www.hipaajournal.com/is-it-a-hipaa-violation-to-ask-for-proof-of-vaccine-status/. Acesso em: 28 jun. 2022.

[32] HIRSCH, Dennis D. Privacy, public goods, and the tragedy of the trust commons: a response to professors Fairfield and Engel. *Duke LJ Online*, v. 65, 2015. p. 12-13.

Em 2021, nos 40 anos da Convenção nº 108, contemplando os avanços europeus na regulação da privacidade e proteção de dados pessoais, Mayer-Schönberger[33] propôs que o próximo marco regulatório para fomentar a confiança na economia da informação seria a garantia de *accountability*, ou seja, da responsabilidade de todos os envolvidos nesse complexo normativo que vem sendo instalado no mundo há décadas:

> Há uma última razão para mudar nossa atenção para enfocar em responsabilidade, e isso se relaciona a todos nós. Se dizemos a pessoas que elas têm poder em teoria, mas na prática percebem que são frequentemente vítimas de abusos, não agentes de mudança, elas normalmente se afastam e desconfiam do uso de dados pessoais.

O autor ainda ressalva que, sem confiança nas instituições e na capacidade coletiva de criar mecanismos de tutela eficaz para a proteção dos dados pessoais, às vésperas do aniversário da Convenção nº 108, haveria o risco de se estar inaugurando uma nova era da ignorância.

Partindo destas premissas, vê-se que, malgrado acentuados avanços na regulação de privacidade e proteção de dados, ainda não se pode dar por acabada a missão regulatória, nem mesmo nos sistemas mais antigos, como o europeu.

Surge o questionamento de como países cuja preocupação com a proteção de dados foi mais tardia podem operacionalizar a tutela deste direito, constitucionalizado no caso brasileiro, gerando a confiança e a responsabilidade de que trata Mayer-Schönberger. A literatura apresenta algumas ideias nesse sentido.

4 Operacionalizando a privacidade e a proteção de dados pessoais

Na evolução dos marcos regulatórios, ficou bastante evidente a correlação entre a evolução das tecnologias e das normas correspondentes. Os telefones e computadores portáteis distribuíram os riscos e os benefícios da economia da informação em escala global e têm sido acompanhados por políticas de privacidade e técnicas de segurança cada vez mais sofisticadas.

Bruno Bioni, embora reconheça os esforços dos reguladores e da própria indústria em tornar o consentimento do titular de dados pessoais menos automático e mais consciente, critica fortemente a viabilidade de um modelo regulatório baseado em repetidas decisões do indivíduo acerca do tratamento de dados em cada *site*

[33] MAYER-SCHÖNBERGER, Viktor. Paradigm shift. *Computer Law and Security Review*, v. 40, 2020. p. 3.

ou aplicação que utiliza. Identifica permanecer na prática uma forte assimetria em controlador e titular de dados, havendo uma hipervulnerabilidade do segundo.[34]

O modelo regulatório de proteção de dados pessoais no país, para ser humanista e realizar os objetivos da Constituição Federal, precisa estar centrado na figura do titular dos dados pessoais. Logo, cabe à Administração Pública se pautar em dispositivos legais voltados ao desenvolvendo humano e numa "atuação planejada e, também, regulatória, firme na condução de comportamentos que possam se reverter em ganhos coletivos",[35] noutras palavras, no empoderamento do grupo de titulares na condição de cidadãos em rede, que estão no exercício de seu direito fundamental de ver protegidas suas projeções pessoais (como nome, endereço, dados sensíveis e diversos outros) no uso constante e inevitável das TICs.

Uma interessante proposta nesse sentido é mediante a utilização das chamadas *Privacy Enhancing Tecnologies* (PETs), tecnologias de aprimoramento da privacidade para facilitar a árvore de decisões do titular de dados como usuário dessas tecnologias.

O *World Wide Web Consortium* (W3C) é uma entidade privada que advoga a defesa de tecnologias de privacidade para preservação da autonomia e liberdade do usuário da internet. Nesse sentido, o órgão já propôs diferentes técnicas para facilitar a manifestação do consentimento pelo usuário:

a) Tecnologias *Do Not Track* (DNT) – o "não rastreio": partindo da ideia de *opt-in* e *opt-out*, tratar-se-ia de uma tecnologia vinculada aos navegadores de internet (Google Chrome, Firefox, Windows Edge e outros) para permitir ao usuário "aceitar" ou "recusar" os infinitos *cookies* e outros rastreadores virtuais de suas atividades antes ou durante a navegação *no próprio navegador* e em caráter geral, não mais precisando reiterar essa decisão a cada acesso,[36] o próprio navegador comunicaria essa decisão a cada acesso, reduzindo a carga decisória do usuário.
b) A *Platform for Privacy Preferences* (P3P) ou Plataforma para Preferências de Privacidade – mais sofisticada que a primeira tecnologia proposta, mas também vinculada ao navegador utilizado para se acessar a internet, a P3P funciona como uma análise automatizada de políticas de privacidade. O usuário preencheria um breve questionário de suas preferências de privacidade e proteção de dados pessoais e a plataforma tomaria as decisões adequadas de acordo com a política de privacidade de cada *site* ou aplicação visitada.

[34] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 219-220.
[35] CASIMIRO, Lígia Maria Silva Melo de; CARVALHO, Harley. Para cidades justas, em rede e inteligentes: uma agenda pública pelo direito à cidade sustentável. *International Journal of Digital Law*, Belo Horizonte, ano 2, n. 1, p. 199-215, jan./abr. 2021. p. 201. DOI: 10.47975/IJDL/1casimiro.
[36] SINGER, David. Everything you need to know about "Do not track". *W3C Blog*, 26 ago. 2013. Disponível em: https://www.w3.org/2011/tracking-protection/drafts/dnt-for-users.html. Acesso em: 30 jun. 2022.

> Trata-se de um mecanismo mais sofisticado por não ser um simples *opt in* ou *opt out*, ou seja, o usuário ainda poderia ter a personalização de certas aplicações baseadas em seus dados pessoais, mas delimitar mais facilmente o escopo em que a captação deles ocorreria.[37]

Veja-se que as tecnologias acima propostas não são pretenciosas ou irrazoáveis e atuam com enfoque na facilitação do processo decisório pelo titular de dados pessoais, ou seja, reduzindo o esforço e aprimorando a árvore de decisões do titular do consentimento. Lamentavelmente, conforme Bruno Bioni esclarece, uma vez que não existe uma regulamentação que torne tais tecnologias compulsórias pelos navegadores de internet, sua adoção prática ou generalizada não tem ocorrido:[38]

> Tal como na experiência do DNT, a P3P esbarrou no mesmo problema de não ser executável. A ausência de uma ação regulatória que a tornasse cogente para os navegadores e as aplicações de Internet foi determinante para o seu insucesso. Assim, mais uma vez, o consumidor restou vulnerado nesse impasse regulatório, relegando-se uma promissora ferramenta que poderia executar eficientemente a sua autodeterminação informacional.

Dessa maneira, verifica-se que o próximo passo para gerar a confiança e a responsabilidade tratadas anteriormente no sentido de aprimorar a regulação da privacidade e proteção de dados, necessariamente, envolve não apenas a efetiva aplicação do quadro normativo instalado, mas empoderar os titulares de dados inclusive mediante aplicações de tecnologias como as PETs sugeridas acima.

Noutras palavras, não se mostra necessário afastar ou vulnerar o consentimento do tratamento de dados pelo titular, mas de facilitá-lo para que não se torne uma letra morta nas normas acerca do tema, mas um efetivo mecanismo de controle da economia da informação.

Outra interessante ideia para operacionalizar o direito fundamental à proteção de dados pessoais é fornecer para os controladores de dados uma forma clara e exata de conhecer seus deveres regulatórios, especialmente em casos complexos, bem como fornecer aos titulares de dados mecanismos claros para exercer seus direitos. O GDPR europeu estabeleceu essa técnica como uma *one-stop-shop* (OSS) ou "balcão único" regulatório.

O objetivo[39] é uniformizar como diferentes autoridades nacionais de proteção de dados de cada país-membro da União Europeia regulam as matérias, bem como

---

[37] W3C. *Plataform for Privacy Preferences (P3P) Project*. Disponível em: https://www.w3.org/P3P/. Acesso em: 30 jun. 2022.

[38] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 237.

[39] UNIÃO EUROPEIA. GDPR. *Considerando nº 127*. Disponível em: https://gdpr-text.com/pt/read/recital-127/. Acesso em: 30 jun. 2022.

apontar uma autoridade única para a qual o titular de dados poderá direcionar sua reclamação, a exemplo de uma situação em que um titular tem seu dado coletado na Itália, porém a sede do controlador fica na Suécia (no OSS europeu, a reclamação poderia ser aberta na Itália e haveria cooperação entre as autoridades de proteção dos dois países para processar e responder a uma reclamação de um titular).[40] O modelo poderia ser adaptado ao caso brasileiro.

Portanto, consistência por intermédio de padronização e uniformização é fundamental para operacionalizar a tutela do direito fundamental à proteção de dados pessoais.

5 Conclusões

O presente estudo teve como objetivo central analisar como o modelo da *tragédia dos comuns* pode auxiliar na crítica da regulação do tema e identificar melhorias e forma de operacionalizá-las.

Constatou-se que há farta e interessante literatura acerca dos aspectos econômicos da privacidade e proteção de dados pessoais, inicialmente como "bens econômicos" clássicos como elemento fundamental da confiança que movimenta a economia da informação.

A literatura aparenta ser unânime em criticar a concentração de responsabilidade depositada sobre os titulares de dados e a centralidade do consentimento para os diferentes modelos regulatórios. A crítica se justifica no sentido de que os indivíduos são sujeitos a vieses e heurísticas diversas que favorecem que a decisão tomada seja sempre pelo consentimento no tratamento de dados, em prejuízo de uma postura de autonomia ante o tratamento de dados pessoais.

Por outro lado, a depender da premissa econômica que se aceite, diferentes propostas de melhoria regulatórias são possíveis, desde medidas enfocadas em grupos de indivíduos de maneira a evitar mais regulamentação estatal, até medidas enfocadas em incluir as corporações no processo regulatório, seja mediante autorregulação, intervenção estatal ou combinações de ambas.

O fato é que a missão regulatória, a despeito dos avanços de décadas, segue incompleta – especialmente considerando os contínuos avanços tecnológicos e o processamento cada vez mais sofisticado de dados pessoais. Mostra-se necessária a responsabilização dos controladores de acordo com os normativos vigentes e o fomento da confiança dos titulares de dados.

[40] UNIÃO EUROPEIA. Comissão Europeia de Proteção de Dados Pessoais. *One-Stop-Shop Leaflet*. 2020. Disponível em: https://edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf. Acesso em: 29 jun. 2022.

Pôde-se constatar que existem propostas de soluções tecnológicas e institucionais para fomentar essa confiança, na figura das chamadas PETs, tecnologias de aprimoramento de privacidade – que se concentram em simplificar o processo decisório na manifestação do consentimento, automatizando-o, porém a difusão dessas tecnologias esbarra na ausência de adesão, por exemplo, dos navegadores de internet, por ausência de uma regulação vinculante acerca do tema. Da mesma maneira, a técnica do OSS adotada pela União Europeia mostrou um esforço de consistência para orientar controladores de dados pessoais e facilitar o exercício de direitos por titulares de dados.

A análise econômica da privacidade e da proteção de dados pessoais revelou-se na pesquisa como uma perspectiva valiosa para se identificar as lacunas e fraquezas do sistema regulatório, bem como um ponto de partida para contribuições. No caso brasileiro em particular, as PETs facilitariam o exercício do consentimento informado pelos titulares pessoais em um país que ainda está conhecendo a proteção à privacidade de dados como um novo direito fundamental.

A finalidade do modelo regulatório, entre outras, é evitar uma tragédia dos (anti)comuns em relação à privacidade, ou seja, o esvaziamento da confiança das pessoas na economia da informação, seja em decorrência de vazamentos de dados, seja pela percepção de que o consentimento exigido pela legislação não se reverte em um efetivo empoderamento dos indivíduos. Ao contrário do apontado por parte da literatura, a pesquisa constatou que uma crise de desconfiança envolvendo a privacidade não é um cenário tão improvável assim.

Referências

BANCO INTERAMERICANO DE DESENVOLVIMENTO; ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Cibersegurança*: riscos, avanços e o caminho a seguir na América Latina e no Caribe. Relatório de Cibersegurança. 2020. Disponível em: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. ed. 1. fev. 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais#:~:text=0%20Brasil%20n%C3%A3o%20%C3%A9%20signat%C3%A1rio,de%20prote%C3%A7%C3%A3o%20de%20dados%20pessoais. Acesso em: 10 jun. 2022.

BRASIL. *Código de Defesa do Consumidor*. Lei nº 8.078 de 11 de setembro de 1990. Ementa: Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 1º jun. 2022.

BRASIL. *Constituição da República Federativa do Brasil de 5 de outubro de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 jun. 2022.

BRASIL. *Lei de Acesso à Informação*. Lei nº 12.527 de 18 de novembro de 2011. Ementa: Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 1º jun. 2022.

BRASIL. *Lei Geral de Proteção de Dados*. Lei nº 13.709 de 14 de agosto de 2018. Ementa: Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1º jun. 2022.

BRASIL. *Marco Civil da Internet*. Lei nº 12.965 de 23 de abril de 2014. Ementa: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1º jun. 2022.

CASIMIRO, Lígia Maria Silva Melo de; CARVALHO, Harley. Para cidades justas, em rede e inteligentes: uma agenda pública pelo direito à cidade sustentável. *International Journal of Digital Law*, Belo Horizonte, ano 2, n. 1, p. 199-215, jan./abr. 2021. DOI: 10.47975/IJDL/1casimiro.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2005.

CERVANTES, Nélida Astezia Castro. *A influência do TRIPS no Programa da SIDA no Brasil*: uma investigação no âmbito da perspectiva neoinstitucional da teoria da escolha racional. Tese (Doutorado em Ciências Sociais) – Universidade de Lisboa, Lisboa, 2021. Disponível em: https://www.repository.utl.pt/handle/10400.5/21855. Acesso em: mar. 2023.

COSTA, Frederico Lustosa da. Bases teóricas e conceituais da reforma dos anos 1990: crítica do paradigma gerencialista. *Revista Brasileira de Administração Política*, 2.2.

DATA PROTECTION LAW OF THE WORLD. *Legislação*. Disponível em: https://www.dlapiperdataprotection.com/index.html. Acesso em: 2 jun. 2022.

DONEDA, Danilo César Maganhoto. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2020.

FAIRFIELD, Joshua A. T.; ENGEL, Christoph. Privacy as a public good. *Duke LJ*, v. 65, p. 385, 2015.

FEREJOHN, John; PASQUINO, Pasquale. The countermajoritarian opportunity. Universidade da Pensilvânia. *Pan Carey Law*, v. 13, p. 353, 2010.

GERBER, Nina; GERBER, Paul; VOLKAMER, Melanie. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, v. 77, p. 226-261, 2018.

HALDER, Steve. Is it a HIPAA Violation to Ask for Proof of Vaccine Status? *HIPAA Journal*, Dec. 25, 2021. Disponível em: https://www.hipaajournal.com/is-it-a-hipaa-violation-to-ask-for-proof-of-vaccine-status/. Acesso em: 28 jun. 2022.

HARDIN, Garrett. The tragedy of the commons: the population problem has no technical solution; it requires a fundamental extension in morality. *Science*, v. 162, n. 3859, p. 1243-1248, 1968.

HELLER, Michael. The tragedy of the anti-commons: property in the transition from Marx to Markets. *Harvard Law Review*, n. 111, jun. 1997.

HIRSCH, Dennis D. Privacy, public goods, and the tragedy of the trust commons: a response to professors Fairfield and Engel. *Duke LJ Online*, v. 65, 2015.

MATIAS, João Luis Nogueira; ROCHA, Rocha. *Repensando o direito de propriedade*. [s.l.]: [s.n.], 2006.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection. *In*: ROTENBERG, Marc; AGRE, Philip E. *Technology and privacy*: The new landscape. [s.l.]: [s.n.], 1998.

MAYER-SCHÖNBERGER, Viktor. Paradigm shift. *Computer Law and Security Review*, v. 40, 2020.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução de Danilo Doneda e Lucial Cabral Doneada. Rio de Janeiro: Renovar, 2008.

SENADO FEDERAL DO BRASIL. *Proposta de Emenda à Constituição nº 17/2019*. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline. Acesso em: 13 jun. 2022.

SINGER, David. Everything you need to know about "Do not track". *W3C Blog*, 26 ago. 2013. Disponível em: https://www.w3.org/2011/tracking-protection/drafts/dnt-for-users.html. Acesso em: 30 jun. 2022.

W3C. *Plataform for Privacy Preferences (P3P) Project*. Disponível em: https://www.w3.org/P3P/. Acesso em: 30 jun. 2022.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

MELO, Lígia Maria Silva; CERVANTES, Nélida Astezia de Castro; LESSA, William Magalhães. A regulamentação da proteção de dados pessoais e seus desafios no contexto da tragédia dos (anti)comuns – Evitando a tragédia da desconfiança. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 11-29, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.melo.

Informações adicionais

Additional information

Editores responsáveis	
Editor-Chefe	Emerson Gabardo
Editor-Adjunto	Lucas Bossoni Saikali