

# Aplicabilidade dos princípios do direito ambiental ao meio ambiente digital: o princípio da prevenção e a proteção da saúde no Brasil

Applicability of environmental law principles to the digital environment: the prevention principle and the health protection in Brazil

Ricardo Libel Waldman<sup>1</sup>; Gabrielle Jacobi Kölling<sup>2</sup>

**DOI:** [https://doi.org/10.37767/2591-3476\(2025\)57](https://doi.org/10.37767/2591-3476(2025)57)

**Fecha de envío:** 30.10.2025

**Fecha de aceptación:** 05.12.2025

## RESUMO:

A sociedade contemporânea, marcada pela revolução tecnológica vivencia a consolidação do meio ambiente digital como espaço essencial de convivência humana. Esse ambiente, composto por pessoas, redes e dispositivos tecnológicos, configura uma nova dimensão do meio ambiente, tanto material quanto simbólica, na medida em que a vida social e biológica passa a depender do ambiente digital. A pesquisa propõe o reconhecimento jurídico do meio ambiente digital como parte integrante do conceito de meio ambiente, sujeito à tutela do direito e aos princípios da proteção ambiental no Direito Brasileiro. Busca-se, assim, analisar fundamentos teóricos e normativos que justifiquem tal reconhecimento, compreender a evolução conceitual do tema, examinar suas conexões éticas e sociais com o meio natural e avaliar a aplicação dos princípios, em especial o da prevenção por exemplo na área da saúde, por meio de abordagem bibliográfica e interdisciplinar.

1 Doutor em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS). Mestre em Direito do Estado pela UFRGS. Realizou estudos de Pós-Doutorado na Universidade de Salerno. Professor Doutor da Faculdade de Direito da UPM. O presente artigo é parte da pesquisa realizada no âmbito do Grupo de Pesquisa Meio Ambiente Digital e Direitos Humanos da UPM. Advogado; E-mail: ricardolibelwaldman@yahoo.com; <https://orcid.org/0000-0002-5437-648X>

2 Pós-Doutorado em Direito pelo Centro Universitário do Distrito Federal (UDF). Doutorado em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Mestre em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Graduado em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Professora de la UPM/SP; USCS/SP y UDF/DF E-mail: koll.gabrielle@gmail.com ORCID: <https://orcid.org/0000-0003-2225-555X>

**RESUMEN:**

La sociedad contemporánea, marcada por la revolución tecnológica, experimenta la consolidación del medio ambiente digital como un espacio esencial de convivencia humana. Este entorno, compuesto por personas, redes y dispositivos tecnológicos, configura una nueva dimensión del medio ambiente, tanto material como simbólica, en la medida en que la vida social y biológica depende cada vez más del ámbito digital en el Derecho Brasileño. La investigación propone el reconocimiento jurídico del medio ambiente digital como parte integrante del concepto de medio ambiente, sujeto a la tutela del derecho y a los principios de protección ambiental. Se busca analizar los fundamentos teóricos y normativos que justifican dicho reconocimiento, comprender la evolución conceptual del tema, examinar sus conexiones éticas y sociales con el medio natural y evaluar la aplicación de los principios ambientales, en especial el de la prevención, con énfasis en la área de la salud, mediante un enfoque bibliográfico y interdisciplinario.

**ABSTRACT**

Contemporary society, marked by the technological revolution, is experiencing the consolidation of the digital environment as an essential space for human coexistence. This environment, composed of people, networks, and technological devices, represents a new dimension of the environment—both material and symbolic—since social and biological life increasingly depends on the digital sphere. The research proposes the legal recognition of the digital environment as an integrated part of the concept of environment, subjected to the protection of law and environmental principles, in Brazilian Law. It aims to analyze the theoretical and normative foundations that justify such recognition, understand the conceptual evolution of the topic, examine its ethical and social connections with the natural environment, and assess the applicability of environmental principles, especially that of prevention, for example in the area of health, through a bibliographical analysis and an interdisciplinary approach.

**PALAVRAS-CHAVE:** meio ambiente digital; infosfera; licenciamento ambiental; prevenção; saúde; regulação.

**PALABRAS CLAVE:** medio ambiente digital; infosfera; licenciamiento ambiental; prevención; regulación.

**KEY WORDS:** digital environment; infosphere; environmental licensing; prevention; precaution; regulation.

**I. Introdução**

A sociedade contemporânea é marcada por inúmeras transformações, dentre as quais o ambiente tecnológico e digital. Nesse contexto, é disruptiva a discussão relacionada ao meio ambiente digital. Mas o que é o meio ambiente digital?

Trata-se de um conjunto de pessoas e equipamentos e redes de tecnologias da informação e da comunicação, facilitado por, mas não, resumido a, infraestruturas tecnológicas, redes de informação, dados e interações humanas mediadas por dispositivos digitais. Frequentemente ele é tratado pela doutrina e legislação com referência ao meio

ambiente natural: fala-se, assim, em ecossistema ou ambiente digital ou infosfera, ciberespaço e suas variações. Isso se explica pelo fato de que somos cercados e interagimos com essas tecnologias de maneira ubíqua.

Cada vez mais, as interações sociais são quase obrigatoriamente efetivadas ao menos de maneira parcialmente digital, ao ponto de se falar em direito a desconexão ao mesmo tempo em que é necessário um direito ao acesso.

Assim, de um ponto de vista fático se pode dizer que o meio ambiente ganhou mais uma dimensão em sua composição, tanto no sentido denotativo quanto conotativo. No denotativo, porque as informações circulam materialmente como impulsos elétricos no ar, retransmitidas por uma miríade de antenas e satélites posicionados dentro e fora da órbita da Terra. No sentido conotativo, o fluxo de informações circulando é comparável ao ar que respiramos por sua quantidade e qualidade.

Além disso, ambas os sentidos e fundem, quando a relação com o meio ambiente (natural) é cada vez mais mediada pelo meio ambiente (digital) criando uma situação na qual a vida do ser humano concreto enquanto ser biológico depende da qualidade de seu acesso ao meio ambiente (digital) (FLORIDI, 2004: 155-156, BOLLINI, 2020: 55). Observa-se, portanto, que a terminologia que Floridi utiliza, infosfera, não contempla pessoas e hardware em seu conceito.

A esse reconhecimento fático, deveria corresponder um reconhecimento jurídico, estendendo o regimento jurídico ambiental para o meio ambiente digital, tendo em vista os desafios que gera, os quais são externalidades do processo produtivo da economia da informação ou de plataforma.

Nesse contexto, o problema de pesquisa que orienta este estudo pode ser assim formulado: de que modo os princípios do direito ambiental podem ser utilizados para tutelar o meio ambiente digital no âmbito do Direito brasileiro?.

A hipótese que se busca examinar é a de que o meio ambiente digital, enquanto espaço de convivência e produção de vida social, deve ser juridicamente reconhecido como parte integrante do conceito de meio ambiente, exigindo a aplicação de princípios ambientais e de direitos fundamentais adaptados à realidade informacional e digital contemporânea. Como exemplo, se exploram as consequências da aplicação do princípio da prevenção ao meio ambiente digital.

O objetivo geral consiste em analisar os fundamentos teóricos e normativos que justificam a tutela jurídica do meio ambiente digital. Como objetivos específicos, pretende-se: a) compreender a evolução conceitual do meio ambiente digital a partir da literatura filosófica e jurídica; b) identificar as conexões entre o meio ambiente natural e o digital, destacando suas implicações éticas e sociais; c) examinar a possibilidade de aplicação dos princípios da proteção ambiental “tradicional” ao ambiente digital no Direito brasileiro.

Metodologicamente, trata-se de uma pesquisa bibliográfica, desenvolvida por meio de análise de obras doutrinárias, artigos científicos e documentos normativos nacionais e internacionais, com enfoque interdisciplinar entre o Direito, a Filosofia e a Ética.

O artigo está estruturado em três seções principais: na primeira, apresenta-se o desenvolvimento histórico e conceitual do meio ambiente digital; na segunda, discute-se a interface entre o meio ambiente natural e o digital sob a ótica dos direitos fundamentais; e, na terceira, analisam-se os fundamentos jurídicos para o reconhecimento e a tutela do meio ambiente digital. Por fim, são expostas as considerações finais, com destaque para os desafios e perspectivas de consolidação desse novo campo de proteção jurídica.

## **II. Abrangência e escopo do meio ambiente digital**

O desenvolvimento do meio ambiente digital ocorreu de maneira rápida e abrangente, especialmente a partir da década de 1990, impulsionado por fatores econômicos que tornaram vantajosos os investimentos nesse campo. Após enfrentar crises nas décadas anteriores, o capitalismo vislumbrou nas novas tecnologias um meio de retomada da produção de riqueza. Além disso, o cenário pós-ataque de 11 de setembro de 2001 reforçou a necessidade de vigilância, promovendo uma aliança entre o Estado e a economia da informação, por meio da qual o governo passou a ter acesso indireto a dados fornecidos pelos consumidores às empresas privadas (MANTELERO, 2018, p. 651).

Nesse sentido, as chamadas big techs, atualmente, são as maiores empresas do mundo. Elas têm como matéria prima os dados pessoais e outros, (como anonimizados, sobre a economia e natureza) utilizados para a predição comportamento humano, da natureza e a criação de uma inteligência artificial. Nesse processo, muitos benefícios foram e são produzidos, como a facilidade de interação entre as pessoas, de compartilhamento de ideias e de conhecimento, do gerenciamento de negócios, de diagnósticos médicos, etc. Todas essas facilidades são precificadas pelas empresas, mesmo no caso em que os serviços são prestados aos usuários de maneira supostamente gratuita. Mas, ao lado desses benefícios, talvez sem precedentes, também tem surgido uma série de malefícios, tais como o rápido compartilhamento do discurso de ódio e de desinformação, cyberbullying, distúrbios na saúde mental causados pelo uso exagerado da tecnologia, além do uso indevido e do vazamento de dados (ZUBOFF, 2019).

Os referidos malefícios, em grande parte, não são precificados pelas empresas, porque elas não são responsabilizadas por tais danos, na medida em que se considera, de modo geral, que elas não são responsáveis pelo conteúdo de terceiros que veiculam, salvo se notificadas pelo interessado, por exemplo, no caso brasileiro, a nudez não autorizada (art. 21 da Lei nº 12.965/2014, cujo alcance foi ampliado pelo STF nos Recursos Extraordinários 1.037.396 e 1.057.258, para incluir crimes e atos ilícitos em geral). Assim, por exemplo, a sociedade absorve a redução da cobertura vacinal por campanhas de desinformação que as big techs ajudam a espalhar por milhares de pessoas desinformação que leva ao medo infundado na vacinação, ou ao suicídio de crianças e adolescentes em razão do cyberbullying, ou ao aumento da intolerância. Tais malefícios, para além do gasto de energia e do uso de matéria prima natural tanto para a produção quanto para utilização do hardware, são a “poluição” digital.

Isso é precisamente o que acontecia e ainda acontece em alguma medida, em matéria de meio ambiente natural: a sociedade produzia sem limites, gerando poluição da terra, da água e do ar e escassez sem ser responsabilizada por isso, o que acabou por gerar a chamada crise ambiental, ou seja, o risco de ficarmos sem recursos naturais para a manutenção da vida como conhecemos.

Essa realidade provocou o surgimento do direito ambiental, com princípios como a prevenção, precaução, poluidor pagador e desenvolvimento sustentável. O direito ambiental pressupõe que os danos ambientais são, com muita frequência, irreparáveis ou de difícil reparação, bem como imprevisíveis, podendo causar danos severos à vida e à saúde das pessoas, animais e vegetais, mas também ao meio ambiente artificial (a cidade), meio ambiente cultural e meio ambiente do trabalho (MILARÉ, 2011).

O direito ambiental pode ser explicado através da teoria do risco de Ulrich Beck (1998), que demonstra como as sociedades contemporâneas, caracterizam-se pela continua geração de riscos, possibilidades de danos decorrentes de decisões políticas, os quais são distribuídos por toda a sociedade (embora nem todos os sofram da mesma forma) e são, muitas vezes, imprevisíveis quanto a forma, local e momento de sua concretização. O meio ambiente, bem tutelado pelo direito ambiental, tem natureza jurídica distinta dos demais bens tutelados juridicamente, eis que é bem de uso comum do povo, assim qualificado constitucionalmente no Brasil. A ninguém é lícito apropriar-se dele, dispor dele, nem mesmo o Estado. Diferente, dos bens ou micro bens ambientais que o compõe (HERMANN-BENJAMIN, 1993, p. 69-72).

### **III. Tutela jurídica do meio ambiente digital: do direito individual ao interesse difuso na sociedade**

A questão, neste sentido, deve ser analisada do ponto de vista da função objetiva que o meio ambiente como um todo exerce na sociedade e não, apenas, dos direitos subjetivos dos envolvidos. Como toda função, a função do meio ambiente, utiliza-se de um bem – o meio ambiente – para atingir uma finalidade “a qualidade ambiental como valor importante da qualidade de vida”. Tal bem é um macro bem composto de uma infinidade de micro bens assim entendidos os elementos da hidrosfera, da litosfera, da atmosfera, da biosfera (HERMANN-BENJAMIN, 1993, p.59-60) e podemos incluir a infosfera.

Para a compreensão do interesse difuso da sociedade, é necessário que compreendamos o meio ambiente digital como um bem comum. A teoria do comum desenvolvida por Pierre Dardot e Christian Laval representa uma das mais relevantes tentativas contemporâneas de repensar os fundamentos do político e do jurídico diante da crise das formas tradicionais de propriedade e gestão coletiva. Em *Comum: ensaio sobre a revolução no século XXI*, os autores afirmam que o comum não se confunde com um bem natural ou econômico, mas consiste em uma prática social e política que se define pelo uso compartilhado e pela autogestão democrática dos recursos coletivos (DARDOT; LAVAL, 2017), tais como o meio ambiente digital, por exemplo. Ou seja, o bem de uso comum não é um dado pela natureza, mas sim algo construído, visto que ele se materializa pela ação coletiva, configurando-se como um princípio normativo e organizacional capaz de contrapor-se tanto à lógica privatista do mercado quanto à lógica centralizadora do Estado.

Assim, o meio ambiente digital pode ser compreendido como uma expressão contemporânea do comum, o qual é forjado por infraestruturas tecnológicas, redes de informação, dados e interações humanas mediadas por dispositivos digitais. O meio ambiente digital tornou-se então um espaço essencial de convivência, produção simbólica e exercício da cidadania. Sua natureza híbrida — ao mesmo tempo material e imaterial — revela que a vida social, econômica e até biológica depende, em larga medida, da qualidade e do acesso a esse ambiente informacional. Isso acontece porque o acesso

ao trabalho, por exemplo, com frequência implica a interação com esse ambiente para a busca de oportunidades, para participar de processos seletivos e das próprias atividades profissionais, afetando suas condições de sobrevivência. Assim como o meio ambiente natural, o meio ambiente digital constitui uma condição de possibilidade para a vida humana, justificando sua proteção jurídica enquanto bem de uso coletivo (FLORIDI, 2013; BOLLINI, 2020).

A perspectiva do bem de uso comum está em risco em função da atuação das plataformas, ou seja, as grandes corporações tecnológicas, ao capturarem e monetizarem os fluxos de informação e as interações dos usuários, transformam o produto da cooperação social em recurso privado, apropriando-se de bens informacionais de natureza coletiva. Essa lógica de expropriação do comum — expressão utilizada por Dardot e Laval (2017) — reflete-se na concentração de poder econômico e informacional nas mãos de poucos agentes, com impactos diretos sobre a autonomia individual, a democracia e a sustentabilidade do ecossistema digital.

Dardot e Laval fornecem base teórica para que a teoria do comum forneça fundamento jurídico e político para a regulação do meio ambiente digital. Abre-se a possibilidade de compreender o meio ambiente digital não mais como um espaço de exploração econômica ou como domínio estatal, mas sim reconhecê-lo como patrimônio coletivo, sujeito a princípios de governança democrática, transparência e corresponsabilidade. Temos, assim, um elemento de conexão com as proposições teóricas de Floridi no tocante à “infosfera” como ecossistema informacional que deve ser preservado por razões éticas e existenciais. A aplicação de princípios ambientais clássicos — como precaução, prevenção e sustentabilidade — ao campo digital pode, assim, orientar um direito do comum digital, capaz de proteger a integridade do ambiente informacional e de garantir o acesso equitativo e seguro aos seus recursos.

Quando a sociedade e o Estado reconhecem o meio ambiente digital como bem comum, estamos diante da possibilidade de expandir o alcance da tutela ambiental para a esfera informacional, articulando os valores da solidariedade e da cooperação à proteção dos novos espaços de vida coletiva. Isso demanda repensar o papel do Estado, das corporações e dos próprios usuários na cogestão democrática desse ambiente, promovendo o que Dardot e Laval chamam de “instituição do comum”. O desafio moderno é a democratização do ciberespaço, garantindo que o meio ambiente digital seja efetivamente um bem de todos, gerido por todos e em benefício de todos.

Podemos identificar, nos termos da teoria econômica, o meio ambiente, como macrobem, como um bem comunal, é utilizável por todos, não podendo ninguém ser excluído juridicamente de seu uso, mas o uso por alguns pode levar à exclusão dos demais. Por exemplo, se uma indústria polui um rio, pode estar impedindo sua fruição como água potável pelos demais (Hermann-Benjamin, 1993, p. 59-60). O mesmo se pode dizer da rede mundial de computadores, todos devem ter acesso, mas o uso por uns, por exemplo, as redes sociais funcionando de maneira opaca, na forma como se utilizam dos dados de seus usuários, pode inviabilizar o uso seguro pelos próprios usuários e pelo restante da sociedade. Veja-se que os malefícios em ambos os casos são coletivos e, por vezes, indivisíveis. Assim, torna-se necessário atribuir a titularidade desse bem a alguém que se encarregará de protegê-lo (HERMANN-BENJAMIN, 1993, p. 61).

Dada a complexidade desse bem, não convém atribuir esta responsabilidade a apenas um órgão. Assim, o meio ambiente, enquanto macrobem, em nossa Constituição brasileira tem titularidade difusa. Entretanto, seus recursos individuais, podem ser objeto de propriedade do Estado, ou de particulares, sendo sempre funcionalizados à proteção ambiental. Então, a propriedade de um imóvel urbano, por exemplo, é um dever de exercício solidário, delimitado, ou melhor, funcionalizado, pela Constituição, pelo Código Civil, pelo Estatuto da Cidade e pelo Plano Diretor, dentre outras normas. A proteção do bem não é feita apenas por seu titular, mas pelo Estado e pela sociedade, na medida em que fiscalizam e exigem o cumprimento dessa obrigação. (HERMANN-BENJAMIN, 1993, p.62).

Pois bem, tudo isso se aplica com muita clareza ao meio ambiente digital. Aliás, essa abordagem baseada no risco, foi adotado na Europa no Regulamento Geral sobre Proteção de Dados e no Regulamento sobre Inteligência Artificial, ambos com influência no Direito Brasileiro, respectivamente, em nossa Lei Geral de Proteção de Dados e no Projeto de Lei nº 2338/2023.

Muito importante é referir, como já desenvolvido em outro trabalho (VIGLIAR, WALDMAN & LIMA, 2023), que nesse contexto o direito à proteção de dados pessoais tem uma dimensão individual e uma dimensão difusa. Nesse sentido, ao lado do direito do titular dos dados pessoais à chamada autonomia informativa, a decidir se e como seus dados serão tratados pelo controlador, existe um direito difuso em toda a sociedade, ou seja, que o meio ambiente digital seja um local seguro para o tratamento dos dados pessoais de todos. Isso porque os dados possuem uma variedade de usos na sociedade que podem causar prejuízo para os direitos fundamentais de todos, por exemplo, e em especial a democracia.

É importante entender que o meio ambiente digital e as tecnologias a ele inerentes funcionam a partir do tratamento de dados. Isso inclui a big data analytics que se refere ao processamento de dados com quantidades, fontes, velocidades e ou fatores, impossíveis para a analítica tradicional (INFORMATION COMMISSIONER'S OFFICE, 2017). As novas TIC existem justamente porque captam e tratam dados, ou seja, a vigilância é da estrutura desse meio ambiente. (RODOTÀ, 2004, p. 135).

Uma forma de proteger os indivíduos nesse contexto é a anonimização dos dados. Entretanto, eles são utilizados para a criação de perfis de grupos, com base, por exemplo, no Código Postal, os quais, por sua vez, são utilizados para atribuir ou retirar direitos ou benefícios. Estes perfis são sempre parciais e incompletos, além se sua validade científica ainda for discutível (RODOTÀ, 2004, p. 136-138).

As pessoas, nesse processo, têm seu desenvolvimento pessoal afetado negativamente por um processo mediante o qual o indivíduo cede o controle de seus dados pessoais em troca do acesso a determinados bens ou facilidades (RODOTÀ, 2004, p. 136) “As tics parecem ter uma ‘natural’ tendência de entrar em conflito com o direito de construir livremente a própria esfera privada, entendida como autodeterminação informativa, como poder de controlar a circulação das próprias informações.” (RODOTÀ, 2004, p. 136 – tradução nossa).

Essa autodeterminação informativa se consolidou em diversos sistemas jurídicos, inclu-



sive o brasileiro, como direito à proteção de dados pessoais. Esse direito, como aponta Rodotà, é de dimensão pública, tanto que sua proteção é atribuída a uma autoridade independente (RODOTÀ, 2004, p. 169-170).

O capitalismo de vigilância está no cerne deste contexto. Segundo Shoshana Zuboff ele é uma forma sem precedentes do capitalismo em que a matéria prima é o exercício da nossa liberdade, nossas escolhas, naquilo que ela chamou de superávit comportamental. Nesse contexto, por diversas razões, as pessoas são levadas a fornecer seus dados sob a justificativa de melhoria de serviços e produtos fornecidos, o que acontece, mas em medida muito menor que o proveito extraído pelas big techs. Essas empresas vendem a predição de comportamento de consumidores e mesmo a sua capacidade de influenciar o comportamento deles com base nos sofisticados algoritmos. Esse poder aumenta conforme as pessoas cedem mais dados. Trata-se do que a autora chama de mercado de mecanismos futuros (ZUBOFF, 2019, p. 21-22).

Nesse contexto, o que aconteceu foi que surgiu um modelo econômico que oferece aos indivíduos e empresas serviços que os tornam real ou supostamente mais eficientes ou mais vendáveis. Chegar ao sucesso e se manter lá exige que o próprio indivíduo se torne um bem de consumo, uma mercadoria (BAUMAN, 2012, p. 9-11). E aí que entram as empresas de tecnologia que possibilitam aos indivíduos obterem informações e contatos necessários para tornarem-se vendáveis, especialmente em um momento de crise do capitalismo, pós 2008 em que os limites do sistema estavam ficando evidentes e a desigualdade social crescia cada vez mais. Assim, foi permitida a aquisição de uma quantidade tal de dados, a qual passou a permitir o referido superávit comportamental.

Entretanto, esse tratamento, cada vez mais, é feito não no interesse do titular do dado e sim no interesse daquele que vai pagar para ter acesso às informações geradas por aquele tratamento. Isso começou no final dos anos 1990, início dos anos 2000, quando o Google, que havia acumulado uma grande quantidade de usuários os ajudando em suas buscas, percebeu que poderia lucrar muito mais com as apostas alheias no comportamento deles do que atendendo a suas necessidades (ZUBOFF, 2019: 141).

A esse argumento, acresce-se que, por diversos motivos, os indivíduos não têm condições de entender as consequências da cessão dos seus dados. Isso inclui questões como falta de tempo e conhecimento para entender os termos de uso dos dados (WALDMAN, ZAMBRANO E RONHA, 2023: 16-17) e a sua utilização anonimizada para a composição de perfis de grupo de dentre outros problemas, os quais se aprofundam com o uso do big data (MANTELARO, 2018: 654) e da inteligência artificial.

A Organização Mundial da Saúde (OMS) lançou a "Chamada para Soluções de Tecnologias Inovadoras em Saúde para Situações de Recursos Limitados", destacando as tecnologias selecionadas no "Compêndio de Tecnologias Inovadoras em Saúde: Dispositivos Médicos, Soluções e-Health". Outro passo importante desse Organismo Internacional foi a promulgação da Resolução WHA60.29, que tem como escopo garantir a melhoria no acesso, qualidade e uso seguro dos dispositivos médicos (DA SILVA; VITA, 2022). Nesse sentido, novas tecnologias podem ser utilizadas pelos profissionais e pelos sistemas de saúde.

É inegável o grande potencial do tema no tocante aos seus aspectos práticos, sua eficácia



depende de vários fatores, como a precisão e a confiabilidade dos dados coletados. Existem preocupações relacionadas à exatidão dos sensores e à correta interpretação das informações por pacientes e profissionais de saúde. Além disso, o grande volume de dados gerados exige sistemas robustos para armazenamento e processamento, bem como métodos eficazes para filtrar as informações mais relevantes (MOREIRA et al., 2024).

Por tudo isso, a proteção de dados pessoais e anonimizados não é apenas um interesse dos seus titulares, mas de toda a sociedade. A regulamentação é necessária e precisa ser feita de um ponto de vista coletivo, porque os dados podem ser utilizados de formas muito danosas para todos e, do ponto de vista individual, os incentivos são para a concessão de dados quase como estratégia de sobrevivência. Nesse sentido, vale destacar a decisão do Supremo Tribunal Federal no Recursos Extraordinários 1.037.396 e 1.057.258 (julgados pelo Pleno em 26/05/2025) os quais tratam da (in)constitucionalidade do art. 19 do Marco Civil da Internet (Lei nº 12.965/14). Nesse caso, os Ministros, para além de declarar, por maioria de votos, a inconstitucionalidade do referido dispositivo, estabeleceram hipóteses em que as plataformas são responsáveis pelo conteúdo de terceiros, mesmo sem ordem judicial. Entretanto, embora, os votos ainda não tenham sido publicados, percebe-se que não ficou delineada uma principiologia para tema, mas sim uma tentativa de mapear temas que exigem maior proteção como o Estado Democrático de Direito e criança e adolescente etc. O tema da saúde, por exemplo, não foi mencionado na decisão.

Entretanto, a Constituição já tem um modelo de regulação delineado que não está sendo reconhecido pelo STF nesse caso, ao menos não de forma direta, de modo que é preciso apresentar uma visão crítica sobre seus fundamentos e uma proposta sobre como devem ser aplicados.

Então, esse trabalho procura oferecer justamente um direcionamento com base na Constituição Federal para essa normatização e pretende dialogar com a referida decisão, e com a doutrina e jurisprudência sobre o tema, de forma crítica, com base no seguinte paradigma: o direito brasileiro que, por meio de dois elementos, estabeleceu de lege lata, a inclusão do meio ambiente digital na proteção ambiental em sentido amplo.

#### **IV. A proteção do meio ambiente digital na Constituição Brasileira e o princípio da prevenção**

O primeiro elemento que a Constituição Brasileira oferece à nossa análise é a previsão do art. 216, II da Constituição Federal. Essa previsão inclui o meio ambiente digital no âmbito do patrimônio cultural, eis que “os modos de criar, fazer e viver” hoje são em importante parte, digitais, ou seja, hoje nos relacionamos, trabalhamos, pagamos contas, gerenciamos negócios, tramitamos processos judiciais, assistimos filmes, nos informamos e ouvimos música, dentre outras atividades, online. O patrimônio cultural é chamado de meio ambiente, portanto, o meio ambiente digital é parte do meio ambiente cultural (FIORILLO, 2015: loc. 2054-2080). O STF já reconheceu essa aplicação na ADPF 743, Rel. para o Acórdão Min. Flávio Dino, julgado pelo Pleno em 20/03/2024.

A consequência jurídica desse reconhecimento é fundada no segundo elemento: é a concepção do meio ambiente em sentido amplo, segundo a qual a distinção entre meio ambiente natural, artificial, cultural e do trabalho é meramente didática (TRENNEPOHL, 2024: 16-19 e 21), eis que o meio ambiente é uno. Trata-se de um conceito amplo de

meio ambiente, adotado pela doutrina e jurisprudência brasileiras (SARLET; FENSTERSEIFER, 2023, p. 167). Nesse sentido, o meio ambiente digital é um aspecto do meio ambiente enquanto bem de uso comum no povo, no contexto do art. 225 da CF (FIORILLO, 2015, loc. 2763): “Art. 225. Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações.”

Decorrência lógica do desenvolvido até o momento é que os princípios de direito ambiental se aplicam ao meio ambiente cultural e, portanto, ao meio ambiente digital; isso implica que os princípios e regras de direito ambiental se aplicam *mutatis mutandis* a todos os aspectos do meio ambiente. A título de exemplo, podemos analisar o princípio da prevenção. Tal princípio estabelece que onde se sabe que um dano ambiental pode ocorrer se determinadas medidas não forem tomadas, as mesmas devem ser exigidas daqueles que atuam sobre o meio ambiente.

Esse princípio, reconhecido no caput do art. 225 da Constituição Federal e § 3º, também consta da Declaração do Rio de Janeiro sobre Meio Ambiente e Desenvolvimento de 1992 da Lei Política Nacional do Meio Ambiente (Lei nº 6938/1981), da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e do PL 2338/2023. A Lei nº 6938/1981 é, importante destacar, prevê em seu art. 9, IV: “o licenciamento e a revisão de atividades efetivas ou potencialmente poluidoras”. Ou seja, a necessidade de que aquele que realize tal atividade solicite e obtenha uma autorização do poder público para que possa exercê-la. Essa autorização é passível de revisão: ela não significa um direito adquirido a poluir, conforme posicionamento adotado pelo Superior Tribunal de Justiça no AgInt no REsp n. 1.676.609/SP, relatora Ministra Regina Helena Costa, Primeira Turma, julgado em 8/6/2020.

Vamos destacar alguns aspectos da implementação deste princípio no direito ambiental e como eles podem, e devem, por mandamento constitucional, ser implementados para o meio ambiente digital. O tema do licenciamento é um bom exemplo sobre como se poderia utilizar as regras de direito ambiental como modelo para o meio ambiente digital. Senão vejamos: conforme a Lei 15190/2025, licenciamento ambiental é o “processo administrativo destinado a licenciar atividade ou empreendimento utilizador de recursos ambientais, efetiva ou potencialmente poluidor ou capaz, sob qualquer forma, de causar degradação do meio ambiente.”

Entende-se a prestação de serviços ou venda de produtos do ambiente digital de ter prevista em Lei a realização de um processo de licenciamento conforme o tipo de impacto que pode ter no meio ambiente digital e outros direitos fundamentais envolvidos na realização daquele serviço.

Assim, por exemplo, redes sociais, mecanismos de busca, mecanismos de recomendação, devem ser objeto de licenciamento. Esse procedimento precisaria envolver uma discussão entre o órgão regulador e os requisitos necessários para o licenciamento. Isso é muito importante porque com o desenvolvimento cada vez mais veloz da tecnologia, cada serviço desses requer uma análise customizada sobre como melhor proteger o meio ambiente e os demais direitos fundamentais no ambiente digital, tendo em vista as características de cada serviço.

Para Mantelaro (2018), o fato de que o big data é tão centralizado em poucas companhias e pervasivo no tratamento de dados na sociedade, somado às limitações já mencionadas ao consentimento a tal tratamento pelos indivíduos (como se pode falar hoje sobre a inteligência artificial), faz com que seja necessário um sistema muito semelhante ao nosso licenciamento ambiental.

Vale lembrar que Rodotà já percebia as limitações do consenso individual em obra publicada ainda na década de 1970, afirmando que o consenso é, em grande parte, um mito da medida em que o indivíduo com frequência está em condições nas quais ele não vai tomar os devidos cuidados ao conceder acesso a seus dados pessoais, como no caso em que pede um empréstimo ou procura um emprego. Ele compara esta situação a outras, por exemplo, o transplante de órgãos, o qual é altamente regulado de modo a que pacientes não sejam levados, por medo da morte, a se sujeitarem a procedimentos arriscados e antiéticos. Os experimentos e as atividades de transplantes devem adotar procedimentos previstos em lei, para garantir que os direitos dos interessados sejam respeitados. Por exemplo, a equipe a realizar o transplante não pode ser a mesma que atesta a morte do doador (2018: 44-48). Ele, inclusive, trata o uso dos computadores para tratamento de dados como uma forma de poluição (2018: 73).

MANTELARO (2018, p. 647-648) faz uma analogia do atual momento da proteção de dados com o que acontecia no período da primeira geração da proteção de dados. Nesse período, a partir da década de 1960, os “mainframes”, grandes computadores que podiam ocupar prédios inteiros, permitiram que governos e grandes companhias pudessem obter e acumular grandes quantidades de dados sobre os indivíduos. A preocupação do legislador nesse momento não foi com a autonomia dos titulares dos dados, mas com a transparência no modo como esses dados eram tratados. Naquela época, as informações eram obtidas pelo governo por razões de interesse público, com a prestação de serviços pelo Estado, então, não havia a opção de não ceder os dados. As empresas, por seu lado, não usavam os dados com fins econômicos, mas apenas para a organização de suas atividades internas. Entretanto, havia o risco de uso para fins de controle e perseguição política e social, além da utilização para fins fiscais (RODOTÀ, 2018: 30).

Aduz ainda a problemática da dificuldade dos indivíduos, a época, de compreender o funcionamento daqueles computadores gigantes e compara com o atual desconhecimento sobre o big data (MANTELARO, 2018: 648), o que, se ressalta novamente, pode ser aplicado também para a inteligência artificial.

Assim, a questão, naquele momento, não era garantir o livre consentimento do titular, pois a coleta e tratamento de dados eram centralizados e inevitáveis, mas era controlar os bancos de dados existentes e o modo como o tratamento era feito. O direito do titular ao acesso aos dados que os controladores possuíam sobre ele também era garantido. Por fim, foram criadas autoridades independentes para fiscalizar os bancos de dados (MANTELARO, 2018: 648).

Pois bem, o autor entende, no mesmo sentido de outros autores já citados, que o tratamento de dados, em especial com o big data, é realizado por poucas companhias muito poderosas e que o consentimento dos titulares de dados é por demais frágil em nosso contexto social e tecnológico. Deste modo, considera que a situação atual é muito semelhante a da década de 1960 e 1970, e propõe uma legislação mais focada em um sistema

de proteção do interesse público e menos baseada no consenso (MANTELARO, 2018: 651-652).

Mantelaro, então, dada a semelhança da situação atual, defende um modelo que procura ser mais completo e envolve uma análise prévia de impacto do tratamento de dados com big data, incluindo questões como proteção de dados, vigilância social e discriminação, bem como questões éticas. Essa análise deve ser feita por uma entidade terceira e aprovada pela autoridade de proteção de dados, antes do tratamento de dados ser utilizado (2018, p. 656-657). Essa análise, diz Mantelaro, deve ser contínua, considerando todo ciclo de vida do serviço de tratamento (2018: 658).

A implementação desse modelo depende de muitas variáveis e vai além do objeto desse trabalho de descrevê-las, mas é possível indicar algumas possibilidades, em especial a partir do exemplo do Regulamento Europeu de Inteligência Artificial (Regulamento (UE) 2024/1689). Mantelaro (2024:16) analisa a Avaliação de impacto dos sistemas de IA de risco elevado sobre os direitos fundamentais, previsto no art. 27º do mencionado Regulamento, na qual, antes da entrada no mercado de um sistema de IA de risco elevado, são identificados os direitos e as pessoas que podem ser negativamente afetadas e se prevê medidas para atender os efetivamente prejudicados. O autor (Mantelaro, 2024:10-17) ainda propõe que essa avaliação deveria envolver a identificação de riscos para direitos fundamentais e a previsão de medidas para evitá-los ou mitigá-los. Trata-se de relevantes diretrizes para o caso brasileiro.

A regulamentação do meio ambiente digital no Brasil, então, deveria adotar esse modelo, com necessidade de licença do Estado para a atuação no mesmo, conforme o tipo de impacto que causa ou pode causar. O tema do direito à saúde no meio ambiente digital também exige uma abordagem preventiva.

Incorporar a lógica do licenciamento ambiental é oportuno, especialmente por meio da definição de critérios de impacto capazes de identificar atividades “potencialmente poluentes”. Esses critérios podem incluir a escala de usuários expostos, o tipo de algoritmo de recomendação empregado, o grau de opacidade e auditabilidade dos modelos, a velocidade de propagação de conteúdo, a existência de coordenação artificial (bots) e, especialmente, a evidência de danos à saúde pública associados à disseminação de desinformação. Organizações como a WHO (2024) e estudos mais contemporâneos (Hosseini, 2024; Feng, 2025) apontam que a detecção de desinformação em saúde demonstra que algoritmos otimizados por engajamento amplificam conteúdos nocivos, contribuindo para hesitação vacinal, adoção de práticas inseguras e aumento de riscos sanitários. De outro lado, a partir da perspectiva ambiental, relatórios da OECD (2024) indicam ainda que operações digitais intensivas — como grandes modelos de IA — produzem externalidades físicas relevantes, sobretudo consumo energético e impacto de data centers.

Assim, umas das possibilidades de indicador ou critério é o Índice de Risco Digital, que permita classificar plataformas e serviços segundo seu potencial de dano socioambiental e à saúde pública. É imperioso que haja um canal de comunicação e troca de dados entre as autoridades reguladoras ANPD, ANATEL, órgãos ambientais e autoridades de saúde, para que haja compartilhamento de informações, na análise de riscos e na imposição de medidas mitigatórias, permitindo, assim, a instauração de um processo de licenciamento ambiental-digital, especialmente quando houver risco significativo decorrente de

opacidade algorítmica, amplificação de desinformação ou impacto físico associado à infraestrutura digital.

Trata-se, em última análise, do uso do Princípio da Prevenção, que autoriza a atuação regulatória mesmo diante de incerteza científica quando há suspeita razoável de dano coletivo relevante. A cadeia causal que liga a degradação do ambiente digital a efeitos mensuráveis na saúde — amplamente documentada por estudos da OMS e por pesquisas sobre infodemia — demonstra que ambientes informacionais contaminados elevam riscos epidemiológicos e prejudicam políticas de saúde pública. Assim, um sistema integrado de classificação, auditoria, transparência e licenciamento torna-se instrumento fundamental para proteger tanto o ambiente digital quanto a saúde coletiva, alinhando o Brasil a padrões internacionais de governança responsável de tecnologias.

## **V. O princípio da prevenção na proteção da saúde**

Para maximizar o impacto das novas tecnologias, é fundamental que sejam estabelecidos padrões regulatórios claros para garantir a qualidade e a segurança dos dados coletados, prevenindo danos. Também são importantes as questões éticas e de proteção de dados associadas ao uso de “wearables” no monitoramento da saúde. A coleta contínua de dados pessoais e de saúde levanta preocupações significativas sobre a proteção da privacidade dos pacientes. Embora haja avanços na criptografia e no armazenamento seguro de dados, os riscos ainda persistem de vazamento de informações sensíveis (MOREIRA et al., 2024). Além disso, a precisão das medições fornecidas por esses dispositivos é outro ponto crítico e bastante discutido. Discrepâncias nos dados podem levar a diagnósticos errôneos ou a falhas no monitoramento de condições de saúde críticas (SANTOS et al., 2024).

Além disso, a comercialização dos dados de saúde, sem o consentimento explícito dos pacientes, pode resultar em implicações éticas profundas, como discriminação em seguros ou no mercado de trabalho (CHIRUVELLA, 2021). Portanto, a adoção de tecnologias inovadoras em saúde deve ser acompanhada de políticas rigorosas de proteção de dados, além de uma discussão contínua sobre os direitos dos pacientes em relação ao uso de suas informações de saúde.

Além dos desafios técnicos e éticos, há barreiras relacionadas à acessibilidade e à adesão dos pacientes. Embora essas tecnologias estejam cada vez mais acessíveis, ainda existem questões relacionadas ao custo, especialmente em populações de baixa renda. A distribuição desigual de dispositivos tecnológicos pode exacerbar as disparidades de saúde entre diferentes grupos socioeconômicos.

No cenário regulatório, uma das possibilidades de resposta possível para a identificação e desenvolvimento de soluções aos desafios ora trazidos, seria a adoção do sandbox regulatório (ambiente controlado e flexível criado por órgãos reguladores para que empresas possam testar produtos, serviços e modelos de negócio inovadores por um tempo determinado), que pode propiciar respostas mais rápidas e efetivas à evolução tecnológica dos dispositivos vestíveis. A terminologia sandbox tem sua origem na Tecnologia da Informação (TI), onde designa um ambiente isolado e seguro usado para testar softwares, códigos ou sistemas, sem comprometer a integridade dos sistemas principais ou expor dados sensíveis. Essa perspectiva foi adaptada para o contexto regulatório, mantendo a metáfora da chamada “caixa de areia” dos parques infantis, que permite

experimentação e flexibilidade para moldar novas estruturas (Rivelli, 2024).

O referido modelo regulatório é uma ferramenta relativamente recente. O Financial Conduct Authority (FCA) do Reino Unido foi pioneiro ao fazer uso de sandboxes regulatórios como ambiente isolado de experimentação voltados ao mercado financeiro, em 2015. A própria União Europeia, por meio da lei que regulamenta o uso e exploração da Inteligência Artificial (conhecida como “AI Act”), traz regras gerais para que o modelo funcione propriamente.

Em seu capítulo 57, especificamente, ela define que cada um de seus Estados-Membros criem ao menos um sandbox regulatório para Inteligência Artificial, o que demonstra a relevância com que o tema é enxergado na região. E não é só. Referida exigência possui, ainda, a definição de um prazo mínimo (agosto de 2026) dentro do qual referidos sandboxes devem estar devidamente implementados e operacionais.

Vê-se, assim, a clara preocupação do legislador europeu em definir que o modelo de sandbox regulatório tenha natureza perene, definitiva, com o intuito de assegurar que iniciativas tecnológicas e inovadoras tenham espaço para a devida experimentação e prova de conceitos. Referida medida busca incentivar novas tecnologias e projetos de inovação que, de outra forma, poderiam não ter condições mínimas necessárias para se tornar realidade, especialmente em se tratando de projetos disruptivos que possam colidir com normas pré-existentes (e, em muitos casos, desatualizadas, não acompanhando a realidade atual).

No Brasil, essa modalidade regulatória tem sido discutida. Ela foi, inclusive, abordada no texto original do PL 2.338/2023, conhecido como “PL da Inteligência Artificial”, e permanece prevista na versão atual do texto, que fora recentemente aprovado pelo Senado Federal e remetido para a Câmara dos Deputados para a devida revisão. Nessa perspectiva regulatória, toca às autoridades competentes autorizar o funcionamento dos sandboxes regulatórios, podendo interromper a testagem ou emitir recomendações no intuito de preservar direitos fundamentais, segurança e proteção de dados pessoais.

Não obstante, é importante mencionar que a implementação da modalidade não é novidade no Brasil. Em 2021, por exemplo, foi autorizada pelo Banco Central do Brasil (BACEN) a sua implementação voltada para experimentações diversas relacionadas a blockchains e meios de pagamentos, possibilitando a validação de conceitos e a consequente prova de suas viabilidades (ou não) por parte de instituições financeiras pré-definidas.

Neste sentido, reforça-se, o estabelecimento de sandboxes regulatórios se apresenta como alternativa apta a atender os diferentes interesses existentes nesse cenário. Por um lado, há os interesses da sociedade civil, que estariam salvaguardados na medida em que o estabelecimento deste modelo envolve a definição dos requisitos mínimos a eles aplicáveis. Tópicos como a sua duração, abrangência e os próprios limites da experimentação almejada seriam pré-definidos, assim como os limites das responsabilidades legais aplicáveis aos seus participantes. Por outro lado, há os interesses de empresas e organizações diversas envolvidas em atividades de inovação, que acabariam atraídas pela existência de regras claras, ajustadas à realidade atual e previamente definidas para o desenvolvimento e teste de seus conceitos.

Mostra-se necessário, todavia, cuidar para que a implementação de regulamentações que viabilizem a modalidade traga consigo, também, as regras para que ela seja implementada de modo responsável. Nesse sentido, importante definir não apenas tópicos gerais e centrais (como os já mencionados: duração, abrangência, limites da experimentação e responsabilidades legais dos partícipes), mas também questões adicionais indispensáveis para o seu pleno funcionamento.

Um bom exemplo é a regra da transparência, que tem por objetivo assegurar o acesso aos detalhes do funcionamento de cada tecnologia, de modo a evitar a chamada “opacidade tecnológica” ou “opacidade algorítmica”, assim entendida como a não-clareza sobre o funcionamento da tecnologia e os critérios por ela considerados para as suas decisões. Apesar de controvertido, tendo em vista a dificuldade de estabelecimento do alcance dessa transparência quando confrontada com limitações técnicas e interesses comerciais.

É importante também referir a necessidade da constante avaliação dos produtos e serviços que caracteriza o sistema de licenciamento mencionado acima. Uma vez verificado que os produtos e serviços podem ser expandido para sociedade em geral, isso não significa que novos riscos para a proteção de dados e saúde das pessoas não aparecerão. Por isso as licenças precisam ser temporárias e revogáveis quando se verificar que os sistemas não seguros.

## **VI. Considerações finais**

O meio ambiente digital emerge como uma nova dimensão do ambiente tutelado pelo direito, na medida em que a vida humana contemporânea está profundamente interligada às infraestruturas tecnológicas e informacionais que estruturam o ciberespaço. A consolidação de uma sociedade hiperconectada, e mediada por dados, exige uma reinterpretação dos conceitos clássicos de meio ambiente, função social e bem comum, de modo a abarcar os desafios éticos, políticos e jurídicos decorrentes da transformação digital.

A sociedade em rede, como observa Floridi, desloca o eixo da experiência humana para a infosfera, isto é, o espaço imaterial em que circulam dados, informações e interações sociais mediadas por algoritmos e dispositivos digitais. Nesse contexto, o meio ambiente digital deve ser reconhecido como ecossistema informacional, cuja integridade é indispensável para a manutenção da vida democrática, da liberdade de expressão, da proteção de dados, da saúde e da própria dignidade da pessoa humana. Assim, trata-se de um ambiente existencial, que condiciona as formas de convivência, de produção e de exercício da cidadania, com garantias básicas para os indivíduos com o direito à saúde.

Sob essa perspectiva, e considerando a dicção do art. 216, II da Constituição Federal, no caso do Brasil, a aplicação dos princípios do Direito Ambiental para o domínio digital mostra-se um caminho teórico e normativo legítimo e necessário. A aplicação do princípio prevenção permite antecipar e mitigar danos coletivos decorrentes de práticas tecnológicas descontroladas — como a desinformação sistemática, o uso predatório de dados pessoais e a manipulação algorítmica de comportamentos sociais.

A regulação jurídica, portanto, deve transcender a lógica exclusivamente mercadológica e adotar uma visão ecossistêmica, que considere a interdependência entre tecnologia,



sociedade e ambiente. Isso é especialmente importante quando se fala no direito à saúde, o qual pode se beneficiar muito de novas tecnologias, mas precisa ser protegido de formas irresponsáveis que colocam em risco tal direito, além da proteção de dados, do direito a não discriminação, dentre outros direitos fundamentais. A estratégia do sandbox regulatório é uma forma de atentar para tais aspectos, mas pode garantir uma situação jurídica que não possa mais ser revista.

A incorporação da teoria do comum, proposta por Dardot e Laval, reforça a necessidade de conceber o meio ambiente digital como bem de uso coletivo, cuja gestão democrática é imprescindível à proteção dos direitos fundamentais e à preservação das condições de liberdade. Tal perspectiva encontra eco nas críticas de Zuboff ao capitalismo de vigilância, que transforma dados humanos em mercadoria e converte a experiência cotidiana em fonte de extração de valor econômico.

Dessa forma, a pesquisa conduzida permite concluir que o reconhecimento jurídico do meio ambiente digital é uma necessidade estrutural para o século XXI. Assim como o Direito Ambiental surgiu em resposta às crises ecológicas da modernidade industrial, o Direito do Meio Ambiente Digital surge como resposta à crise ética e informacional da era tecnológica. O futuro da regulação digital depende da capacidade do Direito de integrar valores como transparência, solidariedade, equidade e sustentabilidade à dinâmica das inovações tecnológicas. Isso significa um modelo aberto à inovação para a melhoria da qualidade de vida, mas sempre atento aos riscos gerados pela própria inovação

---

## Referências

- Banco Central (2021). *Sandbox BC divulga projetos selecionados*. Disponível em: <https://www.bcb.gov.br/detalhenoticia/592/noticia>. Acesso em 27 mar. 2025.
- Bauman, Z. (2012). *Vida para consumo* [Edição digital]. Rio de Janeiro: Jorge Zahar.
- Beck, U. (1998). *Políticas ecológicas en la edad del riesgo: Antídotos a la irresponsabilidad organizada*. Barcelona: El Roure Editorial.
- Benjamin, A. H. V. (1993). *Função ambiental: Dano ambiental*. Disponível em: <https://core.ac.uk/download/pdf/79061973.pdf>. Acesso em 27 mar. 2025.
- Bollini, A. (2020). *Ambiente digital e direito*. Roma: Aracne.
- Chiruvella, V. et al. (2021). Ethical issues in patient data ownership. *Interactive journal of medical research*, 10, (2): e22269. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/34018968/>. Acesso em 27 mar. 2025.
- Da Silva, F. F.; Vita, Jonathan Barros. (2017) Wearables, telemedicina e o futuro da Saúde no Brasil: novas tendências em tecnologias em saúde para enfrentamento de pandemias, *Revista Hamanidades e Inovação*, 9(19): 195-211.
- Dardot, P., & Laval, C. (2017). *Comum: Ensaio sobre a revolução no século XXI*. São Paulo: Boitempo.
- Feng, X., et al. (2025). Health misinformation detection: Approaches, challenges and future directions. *JMIR*. Retrieved from <https://pmc.ncbi.nlm.nih.gov/articles/PMC12589804/>
- Fiorillo, C. A. P. (2015). *Princípios constitucionais do direito da sociedade da informação: A tutela do meio ambiente digital*. São Paulo: Saraiva.
- Floridi, L. (2004). The ontological interpretation of informational privacy. *Ethics and In-*

*formation Technology*, 7(4), 185–200. Disponível em: <https://doi.org/10.1007/s10676-004-6495-8> Acesso em 27 mar. 2025.

- Floridi, L. (2013). *The ethics of information*. Oxford: Oxford University Press.
- Hosseini, M., et al. (2024). A social-environmental impact perspective of generative AI. *Journal/Proceedings*. Elsevier. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2666498424001340>
- Information Commissioner's Office. (2017). Big data, artificial intelligence, machine learning and data protection. *Data Protection Act and General Data Protection Regulation*.
- Mantelaro, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review: The International Journal of Technology Law and Practice* 54, 106020. Disponível em: <https://doi.org/10.1016/j.clsr.2024.106020> Acesso em 27 mar. 2025.
- Mantelaro, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, 34(4). Disponível em: <https://doi.org/10.1016/j.clsr.2018.05.017> Acesso em 27 mar. 2025.
- Milaré, E. (2011). *Direito do ambiente: A gestão ambiental em foco* (7ª ed. rev., atual. e reformulada). São Paulo: Editora Revista dos Tribunais.
- Moreira, F. E. et al. (2024). O futuro da saúde digital: integração de wearables e monitoramento remoto de pacientes. *Contribuciones a las Ciencias Sociales*, [S. l.], 17(12): e12361. Disponível em: <https://doi.org/10.55905/revconv.17n.12-024>. Acesso em 27 mar. 2025.
- O'Neil, C. (2020). *Algoritmos de destruição em massa: Como o big data aumenta a desigualdade e ameaça a democracia* (1 ed.). Santo André, SP: Editora Rua do Sabão.
- OECD. (2024). *Measuring the environmental impacts of artificial intelligence: Compute and applications*. OECD Publishing. Retrieved from [https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/measuring-the-environmental-impacts-of-artificial-intelligence-compute-and-applications\\_3ddddd5/7babf571-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/measuring-the-environmental-impacts-of-artificial-intelligence-compute-and-applications_3ddddd5/7babf571-en.pdf)
- Pietro, M. S. Z. D. (2025). *Direito administrativo*. (38 ed.). São Paulo: Grupo GEN. Disponível em: <https://app.minhabiblioteca.com.br/books/9788530995935> Acesso em 27 mar. 2025.
- RIVELLI, Fábio. Papel do sandbox regulatório na regulação dos sistemas de IA, *Conjur*, publicado em 7 de dezembro de 2024. Disponível em: <https://www.migalhas.com.br/coluna/ia-em-movimento/421706/papel-do-sandbox-regulatorio-na-regulacao-dos-sistemas-de-ia>. Acesso em 27 mar. 2025.
- Rodotà, S. (2004). *Tecnopolitica: La democrazia e le nuove tecnologie della comunicazione* (2ª ed.). Roma-Bari: Laterza.
- Rodotà, S. (2018). *Elaboratori elettronici e controllo sociale* (Ristampa anastatica a cura di Guido Alpa). Nápoles: Jovene Editore.
- Rodrigues Mazzei, M., Silveira, S. da, & Oliveira Faria, L. (2024). O protetor-recebedor e o poluidor-pagador: A mudança de paradigma através da Lei nº 14.119/2021 e a importância do fomento de serviços ambientais e instrumentos de *soft law*. *JURIS - Revista da Faculdade de Direito*, 34(2), 171–185. Disponível em: <https://doi.org/10.14295/juris.v34i2.17565> Acesso em 27 mar. 2025.
- Santos, L. M. dos et al. (2024). O papel dos dispositivos vestíveis e aplicativos de saúde digital na monitorização e promoção da saúde: uma revisão da literatura. *Contribuciones a las ciencias sociales*, [S. l.], 17, (7): e8955. DOI: 10.55905/revconv.17n.7-455. Disponível em: <https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/8955>. Acesso em 27 mar. 2025.
- Sarlet, I. W., & Fensterseifer, T. (2023). *Curso de direito ambiental* [E-book]. São Paulo: Grupo GEN. Disponível em: <https://app.minhabiblioteca.com.br/books/9786559648603>

Acesso em 27 mar. 2025.

- Trennepohl, T. (2024). *Manual de direito ambiental* [E-book]. São Paulo: SRV Editora LTDA. <https://app.minhabiblioteca.com.br/books/9788553620265>
- Vigliar, J. M. M., Waldman, R. L., & Lima, F. R. S. (2023). A proteção de dados como direito difuso no direito brasileiro. *Revista Justiça do Direito*, 37, 135–170.
- World Health Organization. (2024). *Infodemic*. WHO Health Topics. Retrieved from <https://www.who.int/health-topics/infodemic>
- Zuboff, S. (2019). *The age of surveillance capitalism*. Nova Iorque: Public Affairs.