REVISTA CONVERSAS CIVILÍSTICAS

ISSN 2763-8448

# LEGALIDADE VIRTUAL *VERSUS* ILEGALIDADE REAL. O PORQUÊ O TRATAMENTO DE DADOS PESSOAIS PODE REPRESENTAR O AUMENTO DO PODER DE FOGO DO ESTADO PERANTE À CIDADANIA

**Gabriel Pereira Freitas Pinheiro** [1]

## RESUMO

O trabalho analisou os riscos para a privacidade dos cidadãos quanto ao exercício de sua liberdade a partir do conceito de legalidade discriminatória, a partir do qual se observou que a forma de construção das cidades inteligentes no momento mais atual leva a uma terceirização das atividades de instalação de equipamentos e desenvolvimento das conexões de rede a partir do uso de tecnologias da informação e da comunicação por empresas privadas. O risco incorrido reside para além do desvio de finalidade e do tratamento de dados pelas empresas para fins diversos daqueles originalmente declinados para realizar a recolha de dados, todavia, o potencial de perigo está não só na periferia do poder, isto é, nos parceiros privados contratados pelos entes públicos, como também no próprio desvio de finalidade pelo Estado no tratamento de dados. Os dados pessoais coletados pelos entes públicos através dos parceiros podem ser tratados à margem da legalidade de forma intencional a mando do poder público e suas conclusões utilizadas para, ao legislar em abstrato, trazer dados concretos a grupos particulares da população, ou se pode dar ares de legalidade a práticas discriminatórias através de legislação aparentemente abstrata para impedir a concretização de direitos legal ou judicialmente assegurados como aqueles referentes a aborto em casos legalmente excepcionados.

## ABSTRACT

The paper analyzed the risks to citizens' privacy regarding the exercise of their freedom based on the concept of discriminatory legality, from which it was observed that the way in which smart cities are built at the current time leads to outsourcing of installation activities of equipment and development of network connections based on the use of information and communication technologies by private companies. The risk incurred lies beyond the misuse of purpose and the processing of data by companies for purposes other than those originally intended to collect data. However, the potential for danger is not only on the periphery of power, that is, in *stakeholders* hired by public entities, but as well as in the misuse of purpose by the State in the processing of data. Hence,

[1] Bacharel em Direito pela Universidade Federal da Bahia. Mestrando em Direito na Universidade Federal da Bahia. Advogado com atuação em Direito Empresarial e Direito Digital & Proteção de Dados.

ISSN 2763-8448

personal data collected by public entities through partners may be intentionally treated outside of legality at the behest of public authorities and their conclusions used to, when legislating in the abstract, bring concrete data to particular groups of the population, or it may be given the appearance of legality to discriminatory practices through apparently abstract legislation to prevent the accomplishment of legal, moral or judicial rights, such as those relating to abortion in legally exceptional cases.

## 1. INTRODUÇÃO

Inteligência. Como subjetivo, se trata de característica cultuada e buscada pelas pessoas. Se há diversos caracteres que podem ser imputados a alguém, dificilmente inteligência poderia ser vista como irrelevante, certamente seria impossível reputá-la um atributo negativo, então não surpreende pensar que chamar de “inteligente” a uma cidade desperta a curiosidade de o que ela seria, como ela se tornou “inteligente” e, por fim, por que uma cidade seria caracterizada como “inteligente”.

Se a inteligência humana tem que ver com a capacidade de processar informações, conectá-las e delas produzir conhecimento e a intensidade, expressa na facilidade, com que tal processo é realizado por uma pessoa, então poderíamos supor que o processo de tornar uma cidade inteligente teria que ver com a capacidade dessa cidade de gerir informações, dados, seu intercruzamento, suas relações entre si e outros dados e, por fim, extrair um saber a partir desses dados. Não se trata de uma inferência injusta. Pode não ter sido o começo daquilo que hoje se conhece como cidade inteligente, porém, se pode ter em mente que essa é uma característica atual das cidades inteligentes: tratar e colher dados, colher e tratar dados.

Bem, o termo “cidades inteligentes”, hoje, configura um fenômeno daqueles que todos já ouviram falar, porém, é incerto para a maioria o que esse fenômeno significa conceitualmente.

Assim, precisa-se dizer que “cidades inteligentes” foi um termo cunhado com finalidade comercial, portanto não foi forjado com uma base conceitual para demarcar, na linguagem técnica, uma coisa. A origem do termo está associada por Lima (2024) à empresa IBM, a qual teria buscado vender, a partir

ISSN 2763-8448

de 2009, ideias sobre como tornar sustentável uma cidade. O surgimento do termo cidades inteligentes, então, está calcado, em seu surgimento, na ideia de sustentabilidade. Essa associação, por sua vez, remete à redução dos danos ambientais representados pelos ambientes urbanos, em que a vida envolve o consumo de recursos naturais para fabricação de itens de consumo não-duráveis e duráveis, além da alteração do espaço natural e da vegetação por arranha-céus e outros equipamentos de infraestrutura urbana. A tecnologia da informação e comunicação (TIC) somente entrou nesse processo a posteriori (LIMA, 2024).

A realidade atual é bastante diferente.

Não se abandonou a ideia de sustentabilidade, porém, se agregou a ela o uso intensivo de TICs, especialmente a Internet das Coisas e do Big Data (TORRES, 2022; LIMA, 2024). A primeira possui um aspecto elementar de que se a cidade precisa saber colher dados, então ela precisa de ferramentas que funcionem como coletoras de dados, portanto equipamentos eletrônicos capazes de registrar dados, informações e erros, processá-los e os enviar para uma rede, de onde tais informações são remetidas para um servidor num data center e lá são tratados para as finalidades de que se encarrega o controlador. Um bom exemplo é o trânsito como comandado pelo Centro de Operações Rio, do Município do Rio de Janeiro, no qual se monitoram o trânsito e se faz o controle das previsões do tempo para mapear riscos de desabamentos e inundações na Cidade Maravilhosa (BNDES, 2018).

Assim, dispositivos os mais diversos, desde celulares com aplicativos de tempo e de mobilidade urbana – como o Città Mobi – até sinaleiras podem ser transformados em objeto com sensores capazes de captar volumosas informações e as remeter a um centro para tratamento. Dentro de residências, geladeiras, televisores e até lâmpadas hoje podem estar interligados a serviços baseados em internet das coisas. O primeiro ponto então é que a cidade precisa ter sensores para ter dados, afinal de contas, para se ter sustentabilidade e inteligência se precisa colher dados, o que implica num ponto de contato com o ambiente para traduzir para a máquina o que se passa na realidade. Só que a realidade vem fragmentada.

ISSN 2763-8448

São muitos dados colhidos, pequenas informações aos milhões. Registros de segundo a segundo que conta uma história difícil de ser triada, afinal trata-se de um volume de informações sem fim. De fato, sem fim, pois os dados são colhidos a todo o tempo, sobre coisas as mais diversas e dão azo a conclusos variadas e com usos diferentes. Isto é o Big Data – volume, velocidade e variedade (LIMA, 2024). Essa montanha de dados geradas pelos pontos de coleta de dados forma uma massa de dados não-relacionais, cuja decodificação, significação e tratamento para os tornar manejáveis e cognoscíveis aos seres humanos com vistas à destinação em atividades tradicionais, como a prestação de serviços públicos demanda uma força computacional capaz de organizar os dados coletados.

Coletar dados e tratar dados, como dito desde o princípio, são elementares a uma cidade inteligente. Se você colhe, precisa saber tratar, então o binômio Big Data-Internet das Coisas possui singelo papel em viabilizar esta cidade que se quer inteligente para ser sustentável. O que ainda se pode questionar é o porquê de se quererem tantos dados.

Pensemos num exemplo trivial. As soluções para problemas de sustentabilidade e economia de recursos não são novas, mas já foram mais rudimentares. Comumente se vê em corredores de edifícios residenciais ou de edifícios comerciais sensores para acender luzes de corredor apenas se houve alguém que as use. O seu acender deriva da detecção de calor ou de movimentos de uma pessoa, tais sistemas existem há mais de 20 (vinte) anos e possuem relevante função, mas o que foi agregado a eles foi uma capacidade de coleta de dados e compreensão da realidade do meio ambiente.

Essa pontuação aparentemente repetitiva reflete a silenciosa mudança que aconteceu e que provoca um processo de alienação do ser humano que lembra aquele descrito por Marx (2010) quando do cercamento dos campos: o ser humano passou a ser a fonte de trabalho do material eletrônico. O seu comportamento e conduta passaram a ser a base para o funcionamento dos equipamentos. Se no início dos anos 2000 um sensor era ativado e inativado quando houvesse uma pessoa na sala, hoje, com seu funcionamento durante 1 mês, já se pode ter noção se e quando, em determinado dia, em qual turno,

ISSN 2763-8448

período de tempo ou horário se poderia desligar um setor inteiro de um prédio. Se vale à pena, ou não, desligar um elevador, pois os dados colhidos pelos equipamentos eletrônicos dão precisão de informações cujo alcance não se possuía no início dos anos 2000.

Para trazer para o ambiente da cidade, não basta dizer que se controla melhor os dados, quer dizer até que se pode saber se há vazamentos de água, quando ocorrem e ter dados que apontem o que tem provocado tais vazamentos de água. É possível medir a incidência solar e perceber se as luzes podem ser ligadas minutos mais tarde num bairro em relação ao outro na mesma cidade. Esse avanço do estado da técnica permite o maior domínio humano sobre a natureza e permite o manejo da cidade para fins de sustentabilidade, todavia o manejo dos dados nas cidades inteligentes permite mais do que o aumento do domínio sobre a natureza para a proteção desta última.

Ela permite o domínio do ser humano sobre o ser humano para fins de controle e deturpação da privacidade.

É que os dados coletados nas cidades inteligentes, como descrito por Torres (2022), através da exposição do diagrama montado por Van Zooten, aponta que os dados podem ser pessoais ou impessoais, além poderem ser subdivididos em pessoais para fins de serviços e pessoais para fins de vigilância, além de impessoais para serviços e impessoais para vigilância. Os dados impessoais nada dizem sobre pessoas, então o risco para os humanos da recolha destes dados é, de fato, baixo. Já os dados pessoais demonstram um poder de fogo sobre as pessoas, especialmente aqueles usados para vigilância. A espécie do dado e a classificação do seu propósito podem revelar a capacidade de danos ao ser humano.

Pela definição do art. 2º do Estatuto das Cidades, a cidade deve focar no bem estar do cidadão, pois a construção das cidades de maneira sustentável, com a garantia do direito à cidade para realizar o pleno potencial humano, deve assegurar a função social e a participação popular com cooperação e planejamento urbano que centralizem em seu núcleo o bem estar do cidadão. As TIC deveriam cumprir um papel de potencializar a melhoria e o

ISSN 2763-8448

bem-estar dos cidadãos, todavia o panorama atual aponta para a existência de brechas para que os dados colhidos sejam monetizados à revelia do cidadão e que suas informações sejam apropriadas indevidamente para vigilância e controle.

Começaremos o capítulo segundo deste artigo com a conceituação do que seria uma cidade inteligente e se discutirá a estrutura de governança digital criada no Brasil, a se espraiar da administração pública federal para as administrações municipais. No terceiro capítulo falaremos do que seria o "direito informacional" criado pela estrutura de governança da informação estruturada legislativamente e, por derradeiro, discutir-se-á os riscos da forma como se dá a implementação das TICs no âmbito das cidades inteligentes para a privacidade no quarto capítulo. A conclusão nos levará a refletir sobre as perversões do direito e o exponencial aumento de risco que as TICs impõem aos cidadãos pela malversação de dados.

## 2. DEMOCRACIA DIGITAL E CIDADANIA DIGITAL

Para falar de governança digital, há que se definir o que seria a cidade inteligente. Do ponto de vista dos problemas, podemos nos servir da síntese trazida por Torres (2022) dos perigos das tecnologias usadas pelas cidades inteligentes, as quais "combinam as três tecnologias que mais ameaçam a privacidade no presente, quais sejam, a internet das coisas (IoT), o *big data* e a computação em nuvem". Além do quanto explanado sobre as duas primeiras, Torres (2022) aponta que a computação em nuvem permite a interconexão e o armazenamento, por prazos muito maiores, de quantidades massivas de dados. A capacidade de guardar os dados reflete um poder muito maior porque tem condão para apontar padrões com maior precisão. Quanto maior a amostra de uma tendência, maior a confiabilidade do padrão repetitivo.

Isso é válido para apontar tendências climáticas e igualmente verdadeiro para condutas humanas.

ISSN 2763-8448

## 2.1 O que são as cidades inteligentes: como orientar o debate em torno da cidadania

Ainda assim, isto não nos ajuda a conceituar o fenômeno das cidades inteligentes. O que nos põe na direção adequada é perceber o quanto trazido por Torres (2022) no que tange aos conceitos existentes, os da iniciativa privada

> trazem a empresa emissora do conceito como ponto de passagem obrigatório, fornecendo definições baseadas em tecnologias que estas são capazes de oferecer. Essas conceituações costumam ser oferecidas em panfletos acompanhados das diversas soluções vendidas pelas empresas, demonstrando como o modelo de cidade descrito pode ser atendido pelas tecnologias disponíveis.

As conceituações panfletárias do setor privado tendem a ser autorreferentes, o que é de se esperar já que há intento de utilizar do conceito para remeter à própria capacidade de atender à demanda identificada e prover a solução para o problema identificado, cujo escopo pode envolver produtos e serviços de maneira integrada. Já o poder público tende a enxergar a cidade por outra matiz, ainda que muito semelhante à iniciativa privada, os conceitos trazidos pelo Poder Público remetem o interesse dos cidadãos ao papel central nas definições e conceituações. Como exemplo disto, tem-se a Carta Brasileira para as Cidades Inteligentes (CBCI), feita pelo Governo Federal através do Ministério do Desenvolvimento Regional em parceria com a GIZ Brasil (2020) cujo intento era o de prover aos gestores públicos e privados e orientar a construção de cidades inteligentes com foco no cidadão. A definição trazida pela CBCI sobre cidade inteligente aponta que estas são

> cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação. (BRASIL, 2020).

ISSN 2763-8448

Essa conceituação agrega ao debate das cidades inteligentes a proteção de dados pessoais, o que não aparece nas definições do setor privado – até porque há interesse, mais ou menos escamoteado – no uso de dados de toda a espécie, especialmente os de natureza pessoal, como o caso do Wi-Fi "livre" de São Paulo, anterior à Lei Geral de Proteção de Dados, em que foi excluído do projeto de lei 01-00367/2017 sobre o Plano Municipal de Desestatização da Gestão João Dória dispositivo que visava a blindar o fornecimento de dados pessoais dos usuários às empresa privadas que fornecessem a infraestrutura de acesso à internet de maneira "gratuita". O projeto de lei original previa a desnecessidade de dados pessoais, porém, foi feita exclusão do dispositivo por se entender que a as informações de tráfego dos usuários, os cookies e as informações de acesso deles seria a "moeda" necessária para contraprestação dos serviços aos desenvolvedores (ANJOS E COELHO, 2017).

Isto é, sem a possibilidade de tratar os dados e os usar, além da remuneração do serviço contratado, o Município outorgaria licença aos parceiros privados para colher dados dos cidadãos. Naquele momento, isto foi entendido como um fator capaz de tirar o incentivo à iniciativa privada para o projeto. Como dito pelos Autores Anjos e Coelho (2017), era visto como possibilidade "que as empresas que assumem essas concessões vendam informações acerca dos usuários de suas redes de forma a viabilizar retornos econômicos aos investimentos de infraestrutura necessários para a instalação de wi-fi". A venda de informações pessoais fez parte do cenário das cidades inteligentes e a iniciativa privada possui interesse neste gênero de informações.

A definição da CBCI consegue fornecer ainda a dimensão de preocupação com a segurança cibernética e a transparência no uso dos dados, informações, algoritmos e dispositivos, ao passo que preocupado com o letramento digital e a consequente inclusão digital que deve derivar para ampliar a proteção de dados. Dados e códigos abertos, trazidos pela CBCI (2020), são ferramentas ao alcance da cidadania para controle do Poder Público.

A aparente contradição de falar em "proteção de dados" ao mesmo tempo

ISSN 2763-8448

em que se fala de operar com “dados abertos” não pode passar desapercebida. A apenas aparente contradição se soma à falsa dicotomia “privacidade vs acesso a serviços público” (ANJOS E COELHO, 2017). Quando se fala em dados abertos, não se fala em expor dados pessoais, pois estes devem ser tratados por ferramentas de proteção, ou seja, os dados abertos devem permitir acesso do cidadão às bases de dados usadas para prestação dos serviços públicos, sejam eles geridos diretamente pelo poder público ou por contratação de empresas privadas. Estes dados podem ser pseudonimizados, anonimizados, ou até criptografados, o que implica que estas bases de dados devem ser formatadas com a exigência da utilização do conceito do *privacy by design* (FABRÈGUE E BOGONI, 2023).

A exposição dos dados, dos algoritmos e dos códigos em plataformas abertas permite a auditabilidade das iniciativas e serviços digitais prestados pelo Poder Público. Através destas plataformas abertas, entidades sem fins lucrativos, indivíduos, grupos de estudos, grupos de pesquisa, universidade e outros atores poderão analisar o uso dos dados e a destinação das políticas públicas. Do mesmo jeito que pensar que a privacidade é diametralmente oposta ao acesso aos serviços públicos está equivocado, também se equivoca quem pensa serem opostos os interesses em plataformas abertas e a proteção de dados. Ao contrário, a proteção de dados pode ter um laboratório para testar a qualidade das ferramentas de privacidade implementadas pelo Poder Público para apagar a relação entre a pessoa e o dado colhido; caso o processo possa ser revertido até a pessoa, haverá um problema de privacidade na base de dados.

Fizemos estas considerações para passar ao conceito que parece mais adequado.

Gabriel Ribeiro de Lima (2024) define cidade inteligente como

> uma área *geográfica circunscrita*, preenchida por uma *infraestrutura urbana sustentável* e *habitada por uma aglomeração humana permanente*, que possui *atividades* de desenvolvimento urbano, tecnológico, cultural, econômico, social e ambiental, potencializadas tanto pela inserção eficiente de bens e serviços urbanos tecnológicos como pelo aprimoramento do indivíduo e das organizações públicas e privadas sobre a tecnologia, e *protegidas, planejadas e*

ISSN 2763-8448

> *organizadas* pela administração pública, em cooperação com os demais setores da sociedade, com os *objetivos principais* de garantir o bem estar do cidadão, das gerações futuras e a preservação do meio ambiente, observadas a proteção dos dados pessoais, a privacidade, a segurança da informação, a inclusão social e os demais valores juridicamente protegidos.

O conceito elaborado por Lima concede fazer o percurso de sair da cidade tradicional para a cidade inteligente ao integrar a cidade do ponto de vista do direito urbanístico ao direito digital ao lhe acoplar a eficiência e o aprimoramento das políticas públicas em conjunto com a proteção de dados, a segurança da informação e a privacidade. Acertadamente, Lima (2024) pontua que o direito digital e o direito urbanístico qualificam uma cidade e uma ideia de cidade já existente. A esta conceituação, pretendemos agregar a observação de que a cidadania precisa ter ferramentas de auditabilidade das políticas públicas, de modo que o poder de fiscalização não pode ser tolhido pela opacidade das ferramentas digitais.

## 2.2 Governança digital: estrutura legislativa e seus reflexos sobre a cidadania digital

À estruturação do conceito de cidade inteligente se somam os antecedentes e os consequentes legislativos das cidades inteligentes. Uma digressão se faz necessária: a construção da CBCI (2020) e das iniciativas públicas sobre Cidades Inteligentes buscam alinhamento com a Agenda ONU 2030, no bojo da qual se veiculam os Objetivos de Desenvolvimento Sustentável a serem atingidos pelas nações signatárias. O Objetivo 11 estabelece a meta de tornar as cidades e os assentamentos humanos inclusivos, seguros, resilientes e sustentáveis. Para atingir tais objetivos, no que tange à gestão das TICs implementadas no serviço público, a CBCI estabeleceu os atores envolvidos para concretizar o “Objetivo Estratégico 3: Estabelecer sistemas de governança de dados e de tecnologias, com transparência, segurança e privacidade” (BRASIL, 2020).

ISSN 2763-8448

Para tanto, deve-se estabelecer uma estrutura de tomada de decisões, comando e controle dos mecanismos de TICs implementados nas cidades. Isso é o que pode ser vislumbrado como “Governança Digital”, a partir do que nos traz Fonseca (2023). Segundo a Autora

> “A cidade digital tem a governança inteligente assente no modelo DIKW *(Data- Driven-Knowledge-Wisdom*): ou seja, na escolha de decisões a partir do modelo Pirâmide, tendo na base a informação ou os dados, seguindo-se a análise dos dados tendo em vista a produção de conhecimento, e por fim a decisão futura, com ponderação” (FONSECA, 2023).

Por meio dessa modelagem as cidades têm ao seu alcance o “e.governance”, ou seja, “quer dizer que a autarquia dispõe de back-end data base systems, a começar pela implementação do próprio Website, que recolhe informação, e pela e.procedimentalização, que se faz sobretudo através de plataformas digitais” (FONSECA, 2023). Estas plataformas devem estar dotadas de interoperabilidade com plataformas de outros entes federativos. Essa infraestrutura tem sido construída no Brasil pela plataforma “gov.br” e pelas políticas de integração de softwares municipais e estaduais entre si e com a plataforma do governo federal.

A estrutura normativa que embasa tal política pública é elementar para entender o atual estado do que se chama “cidadania digital”. A estrutura normativa cuja ponta-de-lança vem a ser o gov.br se inicia com o art. 12 da Declaração Universal dos Direitos Humanos para se referir ao direito à privacidade como direito ínsito ao ser humano e proteção legal contra qualquer intervenção indevida em sua vida privada e, no Brasil, ganha relevo com o disposto no art. 5º, incisos X, XI e XII da Constituição da República Federativa do Brasil. Interessante denotar que a construção dos nuances, limites e da abrangência do direito à privacidade no âmbito constitucional pode servir a embasar a lógica usada para se falar em dados abertos, afinal a privacidade comporta violação e acesso aos dados se houver justificativa razoável para tanto. Pode-se dizer, inclusive, que o direito constitucional falava, a partir do princípio da concordância prática (MENDES E BRANCO, 2010) entre direitos

ISSN 2763-8448

fundamentais e obrigações do Estado, quanto à necessidade de delimitar a privacidade ou discutir aquilo que hoje a LGPD denomina “base legal” para tratamento de dados.

O STF entendia que as comunicações e os dados obtidos pelas comunicações, ainda que pessoais – antigamente referidas como comunicações privadas – poderiam ser acessadas quando em curso investigação criminal, desde que feito conforme procedimento estabelecido para quebra de sigilo de telecomunicações. O acesso a dados pessoais pelo Estado, nestes casos, equivaleria ao que hoje poderíamos enquadrar como cumprimento de obrigação legal, afinal a segurança pública é dever do Estado, aliás, é um dos mais antigos deveres do Estado. Se o acesso pelo Estado possui margem constitucional, o elemento infraconstitucional adveio do Código de Defesa do Consumidor, nos arts. 43 e 44, os quais estipulam o caráter público das bases de dados pessoais criadas por fornecedores para entender o funcionamento de sua clientela e asseguram o direito de acesso, retificação e apagamento das informações constantes destas bases de dados.

Esse elemento de controle da privacidade de autodeterminação informacional obteve no *Habeas Data* e sua regulamentação pela Lei 9.507/97 força expressiva para se impor, afinal, o *Habeas Data* poderia ser usado contra agente públicos, mas o caráter público das bases de dados, ainda que feita por privados, poderia ensejar *Habeas Data*. Ainda assim, a privacidade e a proteção de dados não tiveram um maior apelo.

A estrutura normativa de que se fala foi complementada apenas a partir de 2012 pela Lei de Acesso à Informação, a qual criou o regime jurídico de guarda, tratamento e manejo dos dados gerados e das informações produzidas e documentadas pelo Poder Público. O art. 40 da LAI teve o cuidado de tratar do sigilo das informações pessoais colhidas e as hipóteses de acesso a tais informações. Esse cuidado revela a preocupação em proteger a privacidade das pessoas envolvidas contingencialmente nos procedimentos e atos da Administração Pública, pois a revelação de documentos e informações poderia expor e afetar indevida e/ou desnecessariamente pessoas que tenham atuado nos processos administrativos.

ISSN 2763-8448

O Marco Civil da Internet tem papel crucial em transplantar as garantias de proteção à privacidade já consagradas em sua modelagem legislativa mais principiológica para a regulação da internet. A preocupação em determinar que o acesso aos dados de conexão para identificação e responsabilização por atos ilícitos na internet se desenvolvesse por ordem judicial se revelou uma forma – talvez excessiva – de proteger a privacidade de quem atuava na internet e, principalmente, nas redes sociais. Por fim, essa estrutura protetiva é fechada pela LGPD, especialmente pelos arts. 7º, 11 e 26, §1º, pois delimitam a obrigação de fidelidade do executor privado de serviços públicos, isto é, o compartilhamento dos dados pessoais por ente público se restringe à finalidade de execução do serviço delegado, sem possibilidade de extensão para outras atividades (TASSO, 2019).

Por derradeiro, temos a Lei do Governo Digital, Lei 14.129/2021, cujo objetivo foi o de lançar as bases para que a digitalização dos serviços públicos se desse para aumento de eficiência da Administração, cuja abrangência extrapola os órgãos federais e demanda atuação no mesmo sentido dos entes parciais. A legislação erige a transparência, a proteção de dados e a interoperabilidade de sistemas como forma de simplificar a burocracia e facilitar o acesso do cidadão aos serviços públicos e a utilização de dados abertos conjugada à anonimização de dados pessoais para elaboração de pesquisas científicas e políticas públicas. Estas legislações lançam a estruturação daquilo que importa para a cidadania digital: a possibilidade de acessar serviços públicos com a manutenção da privacidade.

Para tanto, o Plano Nacional de Internet das Coisas (decreto 9.854/2019) estipulou que as cidades estariam entre as prioridades mínimas para implementação da Internet das Coisas. Isso sinaliza o direcionamento para oferta de melhores serviços públicos nas cidades através dos dados gerados como trabalhado anteriormente, pois o Decreto 9.854/2019 aponta a indexação dele próprio ao Decreto 9.319/2018, qual seja o Plano Nacional de Transformação Digital, cujo eixo 2 se volta para a transformação digital e seus reflexos na cidadania. Do quanto disposto no Decreto 9.319/2018, vê-se que o eixo 2 entende a cidadania digital como a cidadania tradicional, mas agora

ISSN 2763-8448

subsidiada pelas novas tecnologias.

Estas TICs possuiriam como vantagens a potencialização da cidadania tradicional para fiscalizar o exercício do Poder Público, afinal os dados abertos e o reforço da transparência permitiriam aumento da possibilidade de o indivíduo analisar as informações geradas pelo Poder Público. Neste ponto, os fragmentos de sentido das disposições legais sobre a cidadania digital se irmanam com o conceito de D'Almonte e Franco (2023), para quem a cidadania digital seria um desdobramento do conceito tradicional, no qual estão embutidos "uma relação com o Estado, o acesso a uma herança cultural e a um status socialmente compartilhado, agora mediada pelas tecnologias da informação e comunicação" (D'ALMONTE E FRANCO, 2023) e estes elementos implicam "universalização da participação individual e coletiva na sociedade, por meio do acesso aos recursos tecnológicos, incluindo a capacidade individual para utilizá-los e para participar dos processos decisórios sobre o próprio ambiente".

Essas conceituações remetem ancilarmente à premissa trazida pelos referidos autores de que essas ferramentas seriam mecanismos de integração da sociedade. Integração essa que, ao nosso ver, tende a acontecer mediada nas cidades inteligentes naquilo que o Decreto 9.319/2018 chamou de "Um Mundo de Dispositivos Conectados" (vide Eixo de Transformação Digital I, "(b)" do referido decreto). Neste subeixo de transformação digital se objetiva o desenvolvimento de soluções tecnológicas para construção de cidades inteligentes, as quais estão enquadradas na estrutura normativa trazida.

Essa estrutura possui problemas, também no plano internacional, quanto à sua generalização. A transposição dessas diretrizes de boa governança encontra assimetrias em sua implementação nas cidades, a depender da preocupação dos gestores municipais com a gestão da informação e daquilo que podemos chamar de direito informacional, o que comprova que cidades com ampla utilização de TIC podem ser "inteligentes" quanto a se municiarem de ferramentas tecnológicas, porém demonstrarem pouco interesse em proteção de dados e segurança da informação. Isso representa um risco para a cidadania digital.

ISSN 2763-8448

As assimetrias na assimilação de ferramentas de proteção de dados pessoais nas cidades inteligentes podem ser observadas nos exemplos trazidos por Fabrègue e Bogoni (2023), o que vai ao encontro das pesquisas empreendidas por Fonseca (2023). As pesquisas, conduzidas na Europa, em diferentes países e comparando cidades dentro do mesmo país, mostram que o rigor da regulação europeia atinge de forma distinta as localidades analisadas, ou seja, a preocupação com a implementação de técnicas de segurança da informação e de proteção de dados demanda esforço local. Enquanto perduram as assimetrias, observa-se que há possibilidades de perversão do direito a partir delas.

No próximo capítulo, estes riscos serão expostos a partir da realidade da massificação da implantação de TICs nas cidades inteligentes

## 3. DIREITO INFORMACIONAL E A PERVERSÃO DO DIREITO: O MANEJO DOS DADOS E A INFORMAÇÃO COMO OBJETO JURÍDICO

Apesar de não ser o objetivo do trabalho, uma conclusão eventual pode ser observada na análise dos corpos legislativos esparsos reunidos anteriormente: há uma área jurídica com o que se desenha como dogmática própria exsurgida da revolução das tecnologias da informação e comunicação. Esse direito é o direito informacional, um ramo dogmático que possui a informação como centro nevrálgico de sua preocupação, isto é, a informação como fenômeno jurídico principal. Em certos pontos, ela se relaciona à pessoa humana, noutros tem que ver com os afazeres do Estado, em certas situações se refere à segurança nacional se houver informações que ponham em risco o Estado brasileiro e há a procedimentalização do tratamento da informação. Se há o ponto da autonomia, há também a transversalidade.

A gestão da informação também abrange recortes de outras áreas jurídicas, como o direito ambiental e, no caso das cidades inteligentes, o direito urbanístico. Pela sua particularidade, o direito informacional parece merecer

ISSN 2763-8448

tratamento similar ao dispensado ao direito ambiental, por exemplo. Tratamento que perpassa a regulamentação por normas gerais de direito federal, normatização complementar pelos Estados ou Municípios e, eventualmente, normas suplementares municipais.

Essa forma particular de gerir as municipalidades, inovação da Constituição de 1988, demonstra a força do municipalismo no Brasil, além de ser uma possibilidade oriunda da luta pela democracia. A forma de proteção à privacidade e à informação sobre as pessoas presente no ordenamento jurídico brasileiro, com limitações à invasão de privacidade, adveio do enfrentamento aos vícios da ditadura militar. A informação é gerida de maneira distintas por governos democráticos do que seria por governos autoritários.

Neste ponto, a teoria do direito de José Rodrigo Rodriguez pode nos auxiliar a perceber como os dados pessoais coletados podem servir à perversão da forma democrática do Estado Brasileiro através da perversão do Direito.

Segundo José Rodrigo Rodriguez (2013), a democracia é um elemento central da análise da qualidade jurídica das decisões tomadas no Direito Brasileiro. Segundo o autor, o papel da Teoria do Direito é revelar o que de fato são os conceitos dogmáticos analisados sob a ótica da evidência. Seria, então, papel da Teoria do Direito compreender e explicar como funciona a disputa de sentido das cláusulas gerais e conceitos abertos, discutir os caminhos para se chegar a melhores decisões e como estruturar um sistema que tenha mecanismos de controle das decisões. A disputa pelos sentidos, pelas cláusulas abertas, para fazer evoluir o significado das postulações da dogmática, está no escopo da Teoria do Direito (RODRIGUEZ, 2012).

No âmbito do Estado de Direito, a dogmática se presta ao papel de controle do Poder e de reflete a estabilização de expectativas politicamente construídas, ao passo que a evolução da dogmática ocorre em simultâneo à apropriação da gramática normativa por grupos sociais novos, novas “minorias” e grupos de pressão que adquirem força no seio de uma sociedade (RODRIGUEZ, 2016). O Estado de Direito, por si, é um conceito que está em disputa. O mesmo pode ser dito dos rumos das políticas públicas e da forma

ISSN 2763-8448

como se veem os dados pessoais: se estes serão vistos como moeda, tal qual o caso do Wi-Fi público de São Paulo, ainda que de forma disfarçada em face da existência da LGPD no cenário atual, ou se serão vistos como direitos da personalidade.

Numa democracia, o Estado de Direito demanda que as decisões do Poder sejam justificadas adequadamente, ou seja, de maneira racional. A racionalidade, porém, sequer pode ser reputada aparente em determinados momentos, noutros a racionalidade existe, porém ela se equipara ao fenômeno da simulação presente como conceito no Direito das Obrigações. A simulação se encontra nas intenções de efeitos a serem produzidos na prática, apesar da estética de texto neutro, amplo e abstrato típico das formulações legislativas. Aí reside o que Rodriguez (2017) denominou de “falsa legalidade” e se estende para abranger o fenômeno da legalidade discriminatória.

O Brasil pode ser considerado exemplar em construir experimentos de falsa legalidade, a começar por uma legalidade outorgada pela força e espúria, pois embasada na ruptura institucional. Sem sequer mencionar a outorga de uma, ou duas, constituições no período de governo militar, a Ditadura mostrou a sua capacidade de criar uma legalidade autoritária ao corromper o ordenamento jurídico brasileiro e exarar seus atos institucionais, todavia os expedientes de falseamento da legalidade não cessam neste particular. Para Rodriguez (2016), os poderosos tentam perverter o direito, pois a eles interessa “utilizar o direito para conferir aparência jurídica a espaços de puro arbítrio nos quais seria possível agir sem o controle da sociedade civil, em função apenas dos interesses dos poderosos” (RODRIGUEZ, 2016).

Assim, as assimetrias quanto à governança de dados e da segurança da informação nas cidades inteligentes pode dar enseja à perversão do Direito, cujo conceito pode ser traduzido como a “manipulação das normas com o intuito de dar forma jurídica a atos arbitrários que não seriam tolerados caso as instituições estivessem funcionando normalmente; atos que destoam da literalidade das leis ou que violam práticas evidentemente legais”. Na realidade, o fenômeno já ocorre, mas o poder de fogo do autoritarismo se amplia pela coleta massiva de dados dos cidadãos.

ISSN 2763-8448

As cidades inteligentes, como se viu anteriormente, se ancoram na utilização dos dados, das informações precisas, das evidências, para prover melhores serviços públicos e serem mais eficientes, portanto fazerem mais com menos uso de recursos. A precisão depende do conhecimento, do saber mais apurado, daí a importância da computação em nuvem, do big data e da internet das coisas para as cidades inteligentes, contudo, a perversão do direito pelos detratores da democracia acha um campo para vicejar neste ponto.

Antes de chegarmos ao ponto definitivo dos riscos observados, deve-se definir a "falsa legalidade". Segundo Rodriguez (2016), chama-se falsa legalidade

> produção de normas aparentemente universais, mas que são efetivamente postas a serviço de interesses parciais, por exemplo, atingir apenas a determinados grupos sociais e não outros. Neumann discute a questão da falsa legalidade de maneira muito sugestiva em seu texto sobre "o conceito da liberdade política" (Neumann, 2013b: 146-148) ao analisar episódios do maccartismo norte-americano, em especial a perseguição a funcionários públicos por meio de inquéritos administrativos.

A conceituação da falsa legalidade permite identificar espaços em que normas e procedimentos aparentemente neutros, padronizados e comuns têm finalidade discriminatória. Essa finalidade pode ser desejada. Essa categoria teórica tem serventia para "evidenciar espaços de arbítrio no interior do estado de direito, espaços que passariam despercebidos se nos ativéssemos apenas ao texto das leis sem prestar atenção em sua aplicação e em seus efeitos sobre a sociedade" (RODRIGUEZ, 2017), como também serve para demonstrar que desvio aos ditames da LGPD podem se dar pela contratação dos parceiros privados da Administração Pública.

Se a cidade inteligente, na atualidade, tem sido construída por atores privadas, de modo que o Estado fragmenta suas tarefas e delega seus interesses a pessoas jurídicas de direito privado, cujo interesse nos dados perpassa sua serventia, a contratação por uma gestão descompromissada com a proteção aos dados pessoais pode virar um risco à democracia. Além do risco para as pessoas, os dados sobre elas podem ser usados por grupos políticos e

ISSN 2763-8448

milicianos.

### 3.1 E se O Conto da Aia se tornasse realidade? A perversão do Direito pela "falsa legalidade"

Se a distopia parecia distante, as ferramentas de TIC podem aproximá-las da realidade.

Em continuação ao quanto dito no capítulo anterior, há permanentemente o risco do desvio de finalidade pelos parceiros privados da Administração Pública no processo de criação da "cidade inteligente". Do mesmo modo que uma empresa privada como a *Standard Innovation* teve interesse em omitir a coleta de dados pessoais sensíveis em seu aparelho *We-Vibe 4* (MULHOLLAND, 2018), os dados pessoais sensíveis referentes a temperatura corporal e ritmo de uso de vibradores, então não seria de imaginar que, no contexto de acirramento político brasileiro houvesse interesse por dados pessoais outros dos cidadãos. Dados sensíveis como referentes a procedimentos de saúde podem servir para perseguições políticas, assim como dados sobre preferências políticas.

Do mesmo modo que em *O Conto da Aia*, a tomada do Congresso com a matança generalizada dos congressistas e sua substituição por um governo de inspiração religiosa e autoritário conseguiu se fazer crer inofensivo para perverter o direito e solapar as liberdades gozadas pela população, as ferramentas de TIC podem ser convertidas em armas contra a cidadania. Se na ficção as mulheres foram privadas de seus direitos pouco a pouco, a começar pelo cartão de crédito, a realidade pode se tornar nebulosa a partir do cerceamento das miudezas cotidianas.

Aqui, neste ponto é que a falsa legalidade pode ser útil aos interesses dos perversos em guerra com no Direito na sua forma democrática: o somatório da coleta de dados e o descompromisso com a proteção dos dados pessoais deixa o cidadão exposto perante o Poder Público; melhor do que nunca o Estado saberá quem é o cidadão. Em tempos de investigação sobre tentativas

ISSN 2763-8448

de golpe de estado no Brasil, a proliferação de grupos milicianos, o fortalecimento do crime organizado e de partidos de extrema-direita expõe o interesse de grupos marginais em afrontar o Estado democrático de Direito. A serviço destes, estão os dados.

Se há a possibilidade de que certo grupo criminoso organizado tenha se apossado de uma concessão de transporte público no município de São Paulo, então o que impediria o Poder Público de ter, com ou sem consciência de quem estaria por detrás da empresa concessionária, de compartilhar dados pessoais de passageiros, se houvesse uma base legal que o justificasse? O uso de técnicas de anonimização e *privacy by design* poderiam impedir maiores danos aos cidadãos, todavia, diante das assimetrias na implementação de governança de dados, é provável que os grupos marginais tenham facilidade de obter informações sobre os munícipes.

Saber se um inimigo se locomove de ônibus, para qual destino e com qual origem dentro da cidade, e em qual horário pode ser uma arma nas mãos de grupos extremistas.

A situação piora se um dos grupos mencionados, ou outro, conseguir ascender politicamente ao Poder Executivo e trabalhar em conjunto com outros prefeitos para fragilizar as bases da democracia. Os dados colhidos pelas cidades inteligentes podem virar uma arma contra os opositores dos que se opõem à democracia. O começo da fragilização pode ser bastante sutil, como a atuação do Conselho Federal de Medicina ao adotar a Resolução 2.378/2024, suspensa por Medida Cautelar deferida na ADPF nº 1.141 sob relatoria do Min. Alexandre de Morais, o CFM se utilizou de um expediente de legalidade discriminatória.

A falsa legalidade começa a partir dos considerandos, os quais invocam diplomas internacionais, direitos fundamentais e o combate ao relativismo moral, perpassando a invocação da valorização da vida e se encerra pela proibição da realização da assistolia fetal. Essa medida serve de lastro para outros membros da cruzada conservadora antiaborto. Conquanto o CFM não tenha poderes para se sobrepor ao legislativo, ele tenta mitigar os poderes dos profissionais de medicina ao restringir os procedimentos técnicos sob alcance

ISSN 2763-8448

dos médicos para realizar o aborto em casos autorizados pela lei.

O *podcast* O Foro de Teresina, no episódio “A Economia, as eleições e a estupidez”, em 21 de julho de 2024, relatou que a Prefeitura de São Paulo se acoplou ao expediente de disputa dos sentidos iniciado pelo CFM. O número de procedimentos de assistolia fetal tem diminuído na cidade de São Paulo tanto pela criação de óbices fáticos: aumento do tempo de espera, imposição de entrega de um volume de documentos descomunal e outras dificuldades para acessar o direito. Por fim, o *podcast* traz a informação de fontes ouvidas de que a ordem seria “não documentar”, mas “cumprir a Resolução do CFM”, ou seja, utilizar de um diploma infralegal e que se resume a uma categoria em detrimento da legislação.

Isso releva o poderia ideológico a se opor, por convicções morais e políticas, aos direitos assegurados pelo processo político alvo de pretensões reacionárias. A falsa legalidade, neste caso, assumiu uma faceta diversa daquela da ditadura militar, em que se documentavam as práticas de perseguição e de tortura, ela busca não deixar rastros. Enquanto busca não deixar rastros, pode seguir os rastros dos cidadãos.

Os dados são recursos compartilhados nas cidades inteligentes (D’ALMONTE E FRANCO, 2023) e podem ser acessados também por um Estado que vise a ameaçar, por dentro, a democracia. Esses recursos, uma vez tratados, podem ser armazenados. No aplicativo Ouvindo Nosso Bairro (D’ALMONTE E FRANCO, 2023), promovido pela Prefeitura de Salvador, se pode observar que a Prefeitura de Salvador fez a recolha de dados pessoais sensíveis dos cidadãos, mas não ficou claro, nas políticas de privacidade, qual seria a finalidade concreta, tampouco espaço para manifestação dos cidadãos sobre o que de fato queriam. Apenas a imposição de escolha entre opções pré-definidas.

Não ficou claro o que foi feito dos dados pela COGEL, nem se esses dados foram mantidos, com qual finalidade, até quando e se seriam deletados. Vê-se mais um exemplo de recolha de dados sem preocupação com a sua adequada governança por parte do Município de Salvador. Esses dados possuem valor ínsito, pois permitem aos gestores a atuar com precisão, porém

ISSN 2763-8448

esta precisão pode ser para elaborar políticas antidemocráticas e expedientes de falsa legalidade.

Políticas de legalidade discriminatória, como a arquitetura hostil, cujo objetivo é afastar os moradores de ruas de determinados locais podem ser disfarçadas de paisagismo: basta colocar plantas espinhosas debaixo de viadutos aonde essas populações se alocam. Na prática, isso já existe há muito, porém, os dados pessoais coletados via TIC, quando tratados permitem ver hábitos de que comungam, dentro de uma mesma cidade, pessoas LGBT, mulheres, pessoas *trans*, entre outros grupos alvo da sanha conservadora, sem prejuízo das forças de segurança se dados pessoais caírem na mão do crime organizado.

De posse dos dados pessoais coletados pela cidade inteligente, a legalidade autoritária pode se escamotear com mais facilidade. Pode regular o transporte público de modo a piorar a vida de certa população numa região em que a votação do gestor público foi pior na última eleição, como também pode servir para mudar os horários dos serviços públicos para dificultar o acesso de mães solteiras como forma de desincentivar – ou só de punir moralmente – mulheres que se divorciem.

As cidades inteligentes demandam adequada governança digital para que os dados colhidos pelas cidades não se tornem armas para corrosão da própria sociedade e para que se faça a implosão dos direitos e da própria democracia através de atos com aspecto de legalidade e forma jurídica aparentemente regular, mas cuja juridicidade, no âmago, inexiste. Inexistência essa afeita ao conteúdo concreto dos efeitos produzidos pelo ato normativo. A prevenção pela governança digital adequada se revela a melhor forma de coibir os avanços da falsa legalidade, pois uma vez que essa se instala a insidiosidade, a variedade e o caráter pseudojurídico destas artimanhas podem levar ou a grandes controvérsias sobre sua ilegalidade – o tempo pode custar caro na preservação da democracia, vide o episódio de 08 de janeiro de 2023 – ou os efeitos da falsa legalidade já se podem ter concretizado na prática.

ISSN 2763-8448

## 4. CONCLUSÃO

As possibilidades da cidade inteligente trazem consigo a preocupação do poder de fogo que os dados pessoais trazem aos gestores públicos. Preocupação ou empoderamento, a depender da ótica com que se meça a situação. Vimos que a estrutura normativa que protege o direito informacional pode ser erodida por expedientes de falsa legalidade, o que poderíamos olhar como o equivalente de uma “neoplasia jurídica”.

Essa tentativa de criar formas discriminatórias para realização de expedientes ideológicos, preservação do poder político ou de realização de pretensões criminosas já acontece na atualidade. Os dados, a evidência, pelo seu volume e pelas conclusões que dele podem se extrair aumentam a precisam do ataque a ser perpetrado pela falsa legalidade. Basta operar, nas sombras, conselhos de classe, entidades financiadoras internacionais e outras formas de guerra híbrida para instruir governantes a permitirem um compartilhamento irregular de dados, com base na suposta legalidade de um contrato e apostar na demora dos órgãos fiscalizadores, inclusive da ANPD, para fazer cessar a violação, todavia, poderá ser tarde demais.

O risco, para além das intenções obscuras dos parceiros privados que operam o processo de digitalização das cidades inteligentes, pode residir no uso desses parceiros como fachadas para que os próprios governantes operem forças de desestabilização da democracia. A desestabilização, pela falsa legalidade, pode não só se tornar mais precisa, mas como operar de dentro pra fora, em simultâneo, a ressonar, a operação de fora para dentro.

Uma saída poderia ser ampliar o sistema em que opera a ANPD com a delegação de competências e estruturação de órgãos estaduais, tal qual fez o Inmetro e o sistema de metrologia nacional. Poderia ser uma forma de coibir as assimetrias entre municípios e fiscalizar a implementação das “cidades inteligentes”, seria uma forma de dividir os custos sobre a máquina federal, além de aumentar o contingente a postos para analisar e coibir ilicitudes ou acompanhar a implementação da governança de dados.

No mundo digital das cidades inteligentes, a legalidade virtual, seja ela

ISSN 2763-8448

por residir no ambiente digital, ou por ser mera projeção e embuste, pode se transformar numa ilegalidade de facetas reais e efeitos concretos.

## REFERÊNCIAS

ANJOS, Lucas da Costa; COELHO, Helena Carvalho. **Privacidade e Proteção de Dados no Modelo de Cidades Inteligentes Brasileiras**: um estudo de caso sobre o wi-fi "livre" de são paulo. Santiago: Anais do 5º Simposio Internacional Lavits | Vigilancia, Democracia y Privacidad En América Latina: Vulnerabilidades y Resistencias, 2017.

ANTONIALLI, Dennys; KIRA, Beatriz. Planejamento urbano do futuro, dados do presente: a proteçao da privacidade no contexto das cidades inteligentes. **Revista Brasileira de Estudos Urbanos e Regionais**, [S.L.], v. 22, n. 1, p. 1-25, 12 fev. 2020. Revista Brasileira de Estudos Urbanos e Regionais (RBEUR). http://dx.doi.org/10.22296/2317-1529.rbeur.202003.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Radar Tecnológico:** Cidades Inteligentes. Brasília: Autoridade Nacional de Proteção de Dados. 2024.. Disponível em**:** https://www.gov.br/anpd/ptbr/assuntos/noticias/anpd-inicia-serie-de-publicacoes-tecnicas-com-o-tema-cidades- inteligentes

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Tratamento de dados pessoais pelo Poder Público**: guia orientativo. 2. ed. Brasília: Autoridade Nacional de Proteção de Dados, 2023. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e- publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 23 jul. 2024.

BNDES – BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL. **Cartilha de Cidades**.

BOURGUY, Fernando; ALMEIDA, Gilberto Martins. Terapias e *terabytes:* saúde, dados pessoais e inteligência artificial. In: BECKER; Daniel; FERRARI, Isabela (coord.). **Regulação 4.0: novas tecnologia soba a perspectiva regualtória**. São Paulo: Thomson Reuter do Brasil. 2019. p. 191-210.

BRASIL; GIZ BRASIL. **Carta Brasileira para Cidades Inteligentes**. Brasília: Ministério do Desenvolvimento Regional, 2020. 101 p. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/209. Acesso em: 23 jul. 2024 Brasília/DF: BNDES, 2018. 64 p. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.bndes.gov.br/wps/wcm/connect/site/db27849e- dd37-4fbd-9046-6fda14b53ad0/produto-13-cartilha-das-cidades- publicada.pdf?MOD=AJPERES&CVID=m7tz8bf. Acesso em: 23 jul. 2024.

ISSN 2763-8448

CRUZ, Letícia Feliciana dos Santos; MELO, Stephanny Resende de; BARRETO, Victor Ribeiro. “O DILEMA DAS REDES” E AS TECNOLOGIAS DE VIGILÂNCIA NAS CIDADES GLOBALIZADAS: como se proteger? Revista de Direito, Governança e Novas Tecnologias, Florianópolis, v. 2, n. 8, p. 80-97, dez. 2022. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/issue/view/745. Acesso em: 23 jul. 2024.

D'ALMONTE, Edson; FRANCO, Fernando Novaes. Smart cities e cidadania: o programa ouvindo nosso bairro da prefeitura de salvador sob a ótica da governança de dados compartilhados. **Comunicação Mídia e Consumo**, São Paulo, v. 20, n. 59, p. 481-502, 29 dez. 2023. Escola Superior de Propaganda e Marketing (ESPM). http://dx.doi.org/10.18568/cmc.v20i59.2868.

FABRÈGUE, Brian. Franco G.; BOGONI, Andrea. Privacy and Security Concerns in the Smart City. **Smart Cities**,
FEDERAL. **Administração de Empresas em Revista**, Curitiba, v. 32, n. 2, p. 506-543, jun. 2023. Disponível em: https://revista.unicuritiba.edu.br/index.php/admrevista/issue/view/258. Acesso em: 23 jul. 2024.

FERRARI, Isabela. Nova Governança: *insights* para o aprimoramento da regulação estatal. In: BECKER; Daniel; FERRARI, Isabela (coord.). **Regulação 4.0: novas tecnologia soba a perspectiva regualtória**. São Paulo: Thomson Reuter do Brasil. 2019. p. 35-54.

FONSECA, Isabel Celeste (org.). **Smart Cities And Law, E-Governance And Rights**. San Giuliano Mlianese: Geca S.R.L., 2023. 286 p. (Public AdministrAtion At the boundAries Studies and Perspectives on an Evolving Public Law). Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://smartcitiesandlaw.pt/wp-content/uploads/2023/10/pdf- FONSECA-9788813387761.pdf. Acesso em: 23 jul. 2024.

FONSECA, Isabel Celeste M. Cidades Inteligentes e Proteção de Dados Pessoais: algumas reflexões a propósito dos indicadores aplicados no projeto smart cities and law. **Boletim de Ciências Económicas**: homenagem ao prof. doutor Manuel Carlos Lopes Porto, Coimbra, p. 1345-1381, dez. 2024.

FONSECA, Isabel Celeste. As cidades inteligentes (em Portugal): (cada vez mais) entre a cidade de Deus e a dos homens. FONSECA, Isabel Celeste (org.). **Cidades inteligentes e direito, governação digital e direitos**: estudos. Coimbra: Almedina, 2023. 272 p.

HAN, Byung-Chul. **No enxame**: perspectivas do digital. Petrópolis: Vozes, 2018.
INTELIGENTES. **Revista da Faculdade de Direito da FMP**, Porto Alegre, v. 16, n. 2, p. 159-178, 16 dez. 2021. Fundacao Escola Superior do Ministerio Publico. http://dx.doi.org/10.53929/rfdf.v16i2. Disponível em: https://revistas.fmp.edu.br/index.php/FMP-Revista/issue/view/18. Acesso em: 23 jul. 2024.

ISSN 2763-8448

JUPIARA, Aloy; OTAVIO, Chico. **Os porões da contravenção**: jogo do bicho e ditadura militar: a história da aliança que profissionalizou o crime organizado. 8. ed. Rio de Janeiro: Record. 2024. P. 193.

LEGAL GROUNDS INSTITUTE. **Direito Civil e Novas Tecnologias:** contribuições à Comissão de Juristas responsável pela atualização do Código Civil. São Paulo: Legal Grounds Institute, 2024. Disponível em: https://bit.ly/45Ux436. Acesso: em 23/07/2024.

LEMOS, A. Privacidade e infopoder. In Santaella, L. (org). Simbioses do humano e tecnologias: Impasses, dilemas e desafios. São Paulo, Edusp/IEA-USP, 2022, p.33-50.

MAGALHÃES, Sara Rebelo. O programa do procedimento dos orçamentos participativos municipais: uma análise jurídica às regras do jogo. FONSECA, Isabel Celeste (org.). **Cidades inteligentes e direito, governação digital e direitos**: estudos. Coimbra: Almedina, 2023. 272 p.

MANSO, Bruno Paes. A República das Milícias: dos esquadrões da morte à era Bolsonaro. 1. Ed. São Paulo: Todavia. 2020. p. 302.

MENDES, Cássia Isabel Costa; BERTIN, Patrícia Rocha Bello. PROGRAMA DE GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 6. Ed, rev. e atual. São Paulo: Saraiva. 2011. P. 1544.

OLIVEIRA, Fernanda Paula. Cidades inteligentes, transição digital e gestão democrática das cidades. FONSECA, Isabel Celeste (org.). **Cidades inteligentes e direito, governação digital e direitos**: estudos. Coimbra: Almedina, 2023. 272 p.

OLIVEIRA, Thainara de Jesus. **COMUNICAÇÃO PÚBLICA, CIDADES E DADOS**: um olhar sobre comunicação e inovação na prefeitura de salvador (2020-2022). 2022. 83 f. Tese (Doutorado) - Curso de Jornalismo, Faculdade de Comunicação, Universidade Federal da Bahia, Salvador, 2022.

PARINI, Francyelli; PEGORARO, Luiz Nunes. O DIREITO À PRIVACIDADE E À IMAGEM NAS CIDADES

REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. **Revista Civilistica.com**. Rio de Janeiro: PUC-Rio. Vol. 11, N. 3. 2022, set-dez. Disponível em https://civilistica.emnuvens.com.br/redc/article/view/804/650. Acesso em 30 jul 2024.
**Revista Prolegómenos - Derechos y Valores**. Bogotá, Vol. XIX, n. 37, II, jan-jun, 2015, 99-108.

RODRIGUEZ, José Rodrigo. As figuras da perversão do direito: para um modelo crítico de pesquisa jurídica empírica.

RODRIGUEZ, José Rodrigo. **Como decidem as cortes:** Para uma crítica do Direito (Brasileiro). São Paulo: Editora FGV. 3ª Reimpressão: 2013.

ISSN 2763-8448

RODRIGUEZ, José Rodrigo. Dogmática é conflito: a racionalidade jurídica entre sistema e problema. In: MACHADO, Marta Rodriguez de Assis; PÜSCHEL, Flávia Portella; RODRIGUEZ, José Rodrigo (org.). **Dogmática é Conflito**: uma visão crítica da racionalidade jurídica, 2012, p. 21-32.

RODRIGUEZ, José Rodrigo. Perversão do direito (e da democracia): seis casos. **Revista Direito & Práxis**. Rio de Janeiro, Vol. 07, n. 4, 2016, p. 261-294.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 3. ed., rev., atual e ampl. São Paulo: Editora Revista dos Tribunais. 2014. P. 1407.

TASSO, Fernando Antonio. NOBREGA, Viviane; BLUM, Renato Ópice (coords.). **LGPD:** Lei Geral de Proteção de Dados Comentada. 2 ed. São Paulo: Thomson Reuters Brasil. 2019. E-book.

TEFFÉ, Chiara Spadaccini de. Marco Civil da Internet: considerações sobre a proteção da liberdade de expressão, neutralidade da rede e privacidade. In: BECKER; Daniel; FERRARI, Isabela (coord.). **Regulação 4.0: novas tecnologias sob a a perspectiva regualtória**. São Paulo: Thomson Reuter do Brasil. 2019. 279p.

TIMM, Luciano; DUFLOTH, Rodrigo. O futuro á tecnologia pertence. IN: SANTOS, M. J. P. dos; SCHAAL, Flavia Mansur Murad; GOULART, Rubeny (Coord). **Propriedade Intelectual e inteligência artificial.** São Paulo: Almedina, 2024. P. 364-380.

TORRES, Frederico Boghossian. **Proteção de Dados nas Cidades Inteligentes**. 2022. 146 f. Dissertação (Mestrado) - Curso de Direito, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2022. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.maxwell.vrac.puc-rio.br/64075/64075.PDF. Acesso em: 23 jul. 2024.
v. 6, p. 586–613, 2023. Disponível em: https://doi.org/10.3390/smartcities6010027.

XAVIER JUNIOR, Sara Filipa. Breves notas sobre o Orçamento Participativo. FONSECA, Isabel Celeste (org.). **Cidades inteligentes e direito, governação digital e direitos**: estudos. Coimbra: Almedina, 2023. 272 p.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (orgs). **Tecnopolíticas da Vigilância**: perspectivas da margem. São Paulo: Boitempo. 2018. P. 433.