FGV EBAPE

RAP
REVISTA DE ADMINISTRAÇÃO PÚBLICA

Artigo

A segurança como fator-chave para a cidade inteligente, a confiança dos cidadãos e o uso de tecnologias

Giulie Furtani Romani [1]
Luis Hernan Contreras Pinochet [1]
Vanessa Itacaramby Pardim [2]
Cesar Alexandre de Souza [2]

[1] Universidade Federal de São Paulo / Escola Paulista de Política, Economia e Negócios, Osasco / SP – Brasil
[2] Universidade de São Paulo / Faculdade de Economia, Administração, Contabilidade e Atuária, São Paulo / SP – Brasil

As cidades inteligentes vêm crescendo ao redor do mundo, impulsionadas por inovações tecnológicas. Com elas surgem diversas oportunidades, mas também novas ameaças à segurança e privacidade do usuário nessa realidade interconectada. Este estudo tem como objetivo investigar a percepção de segurança e confiança na tecnologia por parte dos cidadãos e como esta afeta a propensão ao seu uso e, consequentemente, à vida na cidade inteligente. Para tanto, conduziu-se um *survey* (n = 601), por meio do método PLS-SEM, para testar as hipóteses formuladas. Os resultados obtidos confirmam que o modelo proposto demonstra ser consistente. As relações "confiança e segurança subjetiva" e "segurança objetiva e privacidade de dados" obtiveram relações mais consistentes, assegurando a forte influência das barreiras "tangíveis" e "intangíveis" da percepção de segurança. Dessa forma, para obter e manter a confiança dos usuários, as instituições por trás da tecnologia precisam estar atentas à opinião deles e da sociedade, de forma a manter uma boa reputação para que possam, assim, perpetuar uma percepção positiva de segurança. Conclui-se, assim, que o conceito de segurança adquire uma nova dimensão no contexto da cidade inteligente por ser um componente crucial para toda a sua base e estar intimamente ligado à tecnologia, além de se apresentar como uma preocupação fundamental para os governos e as entidades que buscam implementar soluções e aplicações do conceito.
Palavras-chave: cidades inteligentes; segurança; confiança; propensão para o uso de tecnologia; PLS-SEM.

La seguridad como factor clave para la ciudad inteligente, la confianza de los ciudadanos y el uso de las tecnologías

Las ciudades inteligentes están creciendo en todo el mundo, impulsadas por las innovaciones tecnológicas. Con ellas surgen diversas oportunidades, pero también nuevas amenazas a nuestra seguridad y privacidad en esta realidad interconectada. Este estudio tiene como objetivo investigar la percepción de los ciudadanos sobre la seguridad y la confianza en las tecnologías y cómo afectan la propensión a usarlas y, en consecuencia, la vida en la ciudad inteligente. Para ello, se realizó una encuesta (n = 601) utilizando el método PLS-SEM para contrastar las hipótesis formuladas. Los resultados obtenidos confirman que el modelo propuesto resulta ser consistente. Las relaciones 'confianza y seguridad subjetiva' y 'seguridad objetiva y privacidad de datos' obtuvieron relaciones más consistentes, confirmando la fuerte influencia de las barreras 'tangibles' e 'intangibles' de la percepción de seguridad. De esta forma, para obtener y mantener la confianza de los usuarios, las instituciones que están detrás de las tecnologías deben estar atentas a su opinión y a la de la sociedad a los efectos de mantener una buena reputación, para que puedan, así, mantener una percepción positiva de la seguridad. Se concluye que el concepto de seguridad adquiere una nueva dimensión en el contexto de la ciudad inteligente, ya que es un componente crucial de toda su base, estrechamente vinculado a la tecnología además de presentarse como una preocupación fundamental para los gobiernos y entidades que buscan implementar soluciones conceptuales y aplicaciones.
Palabras clave: ciudades inteligentes; seguridad; confianza; propensión a usar tecnologías; PLS-SEM.

DOI: http://dx.doi.org/10.1590/0034-761220220145
ISSN: 1982-3134
Artigo recebido em 07 maio 2022 e aceito em 16 jan. 2023.
Editora-chefe:
Alketa Peci (Fundação Getulio Vargas, Rio de Janeiro / RJ – Brasil)
Editora adjunta:
Gabriela Spanghero Lotta (Fundação Getulio Vargas, São Paulo / SP – Brasil)
Pareceristas:
Adilson Giovanini (Universidade do Estado de Santa Catarina, Florianópolis / SC – Brasil)
Teresa Cristina Monteiro Martins (Universidade Federal de Lavras, Lavras / MG – Brasil)
Relatório de revisão por pares: o relatório de revisão por pares está disponível neste link.

Security as a key factor for the smart city, citizens' trust, and the use of technologies

Smart cities are growing around the world, driven by technological innovations. With them come several opportunities and new threats to our security and privacy in this interconnected reality. This study investigates citizens' perception of security and trust in technologies and how they affect the propensity to use them and, consequently, life in the smart city. Therefore, a survey was conducted (n = 601) using the PLS-SEM method to test the formulated hypotheses. The results obtained confirm that the proposed model proves to be consistent. The relationships between 'trust and subjective security' and 'objective security and data privacy' obtained stronger relationships, confirming the strong influence of the 'tangible' and 'intangible' barriers of the perception of security. Thus, to obtain and maintain users' trust, the institutions behind the technologies need to be attentive to the opinion of their users and society to keep a good reputation and a positive perception of security. The users' opinion is a crucial component of smart cities' entire base, closely linked to technology, and presents as a fundamental concern for governments and entities that seek to implement concept solutions and applications.

Keywords: smart cities; safety; trust; propensity to use technologies; PLS-SEM.

INTRODUÇÃO

A cidade inteligente surgiu como um novo paradigma para otimizar dinamicamente o ambiente, melhorar a qualidade de vida dos habitantes, o uso dos recursos da cidade (Sookhak, Tang, He, & F. R. Yu, 2019), a sustentabilidade e diminuir os danos ao meio ambiente (Rao & Deebak, 2022). Esses princípios dependem de uma receita de competência e otimização técnica, invenções tecnológicas e históricos de dados em tempo real (Bhushan et al., 2020).

Nesse contexto, os cidadãos terão acesso contínuo e onipresente a informações que lhes permitam controlar suas vidas, usando a inteligência tecnológica coletiva, por meio da qual a cidade fornece soluções inovadoras e sustentáveis baseadas em Tecnologia da Informação e Comunicação (TIC). Portanto, percebe-se que os objetivos de uma cidade inteligente são multifacetados (Elmaghraby & Losavio, 2014; Haque, Brushan, & Dhiman, 2022; Ismagilova, Hughes, Rana, & Dwivedi, 2020; Javed et al., 2022).

Dessa forma, a proposta de um olhar humanístico sobre os avanços técnicos levanta discussões mais profundas acerca dos aspectos éticos e humanos inerentes às iniciativas das cidades inteligentes. Isso ocorre, pois a evolução das cidades inteligentes emerge de inovações em tecnologias que, embora criem novas oportunidades econômicas e sociais, trazem ameaças às expectativas de segurança e privacidade (Kasar & Kshirsagar, 2021).

Nesse sentido, emergem dois novos desafios importantes e complexos: a segurança e a privacidade de dados (Adil & Khan, 2021). A segurança considera aspectos como o acesso ilegal às informações e ataques cibernéticos, que podem causar interrupção na disponibilidade dos serviços. Já a privacidade leva em consideração, por exemplo, o uso de dados de forma indiscriminada, sem consentimento ou conhecimento do usuário, visto que os cidadãos digitais são cada vez mais instrumentalizados com dados disponíveis sobre sua localização e atividades (Sookhak et al., 2019).

O estado da arte da literatura sobre privacidade e segurança em cidades inteligentes apresenta desafios que incluem a preservação da privacidade com dados, estabelecimento de práticas de compartilhamento de dados e utilização adequada de tecnologia para encorajar maior exploração dos desafios das cidades inteligentes antes de sua construção (Braun, Fung, Iqbal, & Shah, 2018; Sookhak et al., 2019). Além disso, a falta de privacidade pode resultar em discriminação social e possibilitar

uma sociedade fundamentalmente desigual (Eckhoff & Wagner, 2018), o que precisa que as cidades gerenciem as informações e a comunicação diante de avanços urbanos (Hasbini, Eldabi, & Aldallal, 2018; Javed et al., 2022). Assim, para que haja confiança e aceitação das cidades inteligentes, se fazem necessárias a integração de mecanismos de segurança e preservação da privacidade dos usuários, o que se constitui uma lacuna que esta pesquisa buscou explorar (L. S. Grandhi, S. Grandhi, & Wibowo, 2021; Habib, Alsmadi, & Prybutok, 2019).

Desse modo, o objetivo deste estudo é investigar a percepção de segurança e a confiança na tecnologia de cidades inteligentes por parte dos cidadãos e como ela afeta a propensão ao seu uso e, consequentemente, à vida na cidade.

O estudo se justifica porque o conceito "cidades inteligentes" está ganhando importância em função do crescimento exponencial das populações urbanas e da necessidade de expandir a capacidade da cidade, melhor administrar seus recursos, aumentar a qualidade de vida dos cidadãos e otimizar a eficiência e a qualidade dos serviços prestados (Habib et al., 2019), principalmente por entidades e empresas governamentais (Kasar & Kshirsagar, 2021). Além disso, a construção de uma cidade inteligente depende da coleta intensiva de dados que podem ser utilizados, de forma inovadora e criativa, para a criação de aplicações integradas que melhorem os serviços da cidade e o uso de seus recursos. A cultura de *data-driven* se mostra cada vez mais vital à medida que dados e informações são utilizados com maior intensidade (Bibri, 2021).

Por fim, esta pesquisa busca contribuir para o aprofundamento do tema da segurança e privacidade, de forma a compreender os conceitos e as premissas envolvidos, propondo a elaboração de um novo modelo teórico, adaptado da literatura correlata ao tema (Abu-Shanab, 2017; Al-Sharafi, Arshah, Abo-Shanab, & Elayah, 2016; F. Cui, Lin, & Qu, 2018a; Hansen, Saridakis, & Benson, 2018; Mittenford, 2016; Sepasgozar, Hawken, Sargolzaei, & Foroozanfa, 2019; Urmetzer & Walinski, 2014), com componentes associados à confiança e segurança (objetiva e subjetiva) que afetam a propensão ao uso de tecnologias em cidade inteligente, focando no comportamento do cidadão. Para este propósito, conduziu-se um *survey* (n = 601) na cidade de São Paulo e o PLS-SEM foi utilizado para testar as hipóteses formuladas.

FUNDAMENTAÇÃO TEÓRICA

2.1. Cidades inteligentes, componentes e suas características

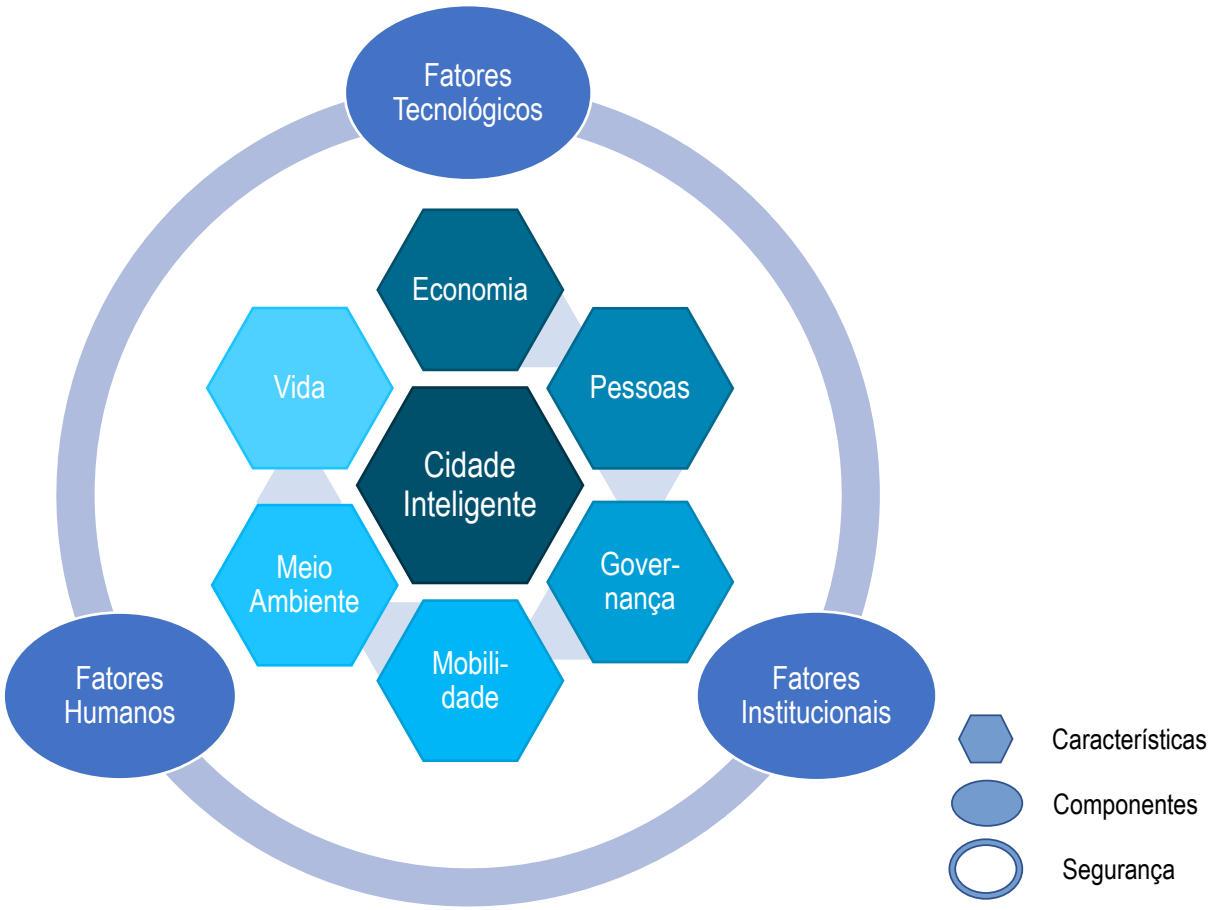
Uma das definições sobre cidade inteligente é a que corresponde ao lugar em que a Tecnologia da Informação e Comunicação (TIC) é combinada com infraestrutura, arquitetura, objetos e pessoas para melhorar processos e lidar com problemas sociais, econômicos e ambientais, possibilitando que dispositivos inteligentes se conectem à infraestrutura existente para otimizar a qualidade de vida e a produtividade nas cidades, assim como resolver problemas por meio de soluções baseadas nessas tecnologias e em parcerias governamentais com diversos *stakeholders* (Bhushan et al., 2020; Habib et al., 2019; Rao & Deebak, 2022).

A revisão da literatura indica que o principal foco da cidade inteligente é o avanço das TICs. Contudo, diferentes disciplinas estão propondo definições que transcendem a ideia do mecânico e englobem mais do que apenas esse fator, levando em consideração um aspecto primordial: os cidadãos (Hasbini et al., 2018; Javed et al., 2022). Eles são um ingrediente-chave no desenvolvimento da cidade

inteligente, pois são os criadores e usuários dos serviços e da tecnologia, sendo a maior fonte de ideias e *feedback* sobre a cidade (Elmaghraby & Losavio, 2014; Ismagilova et al., 2020).

Em suma, uma cidade inteligente é aquela "que possua inteligência coletiva, que tenha responsabilidade ambiental, que promova o desenvolvimento social e que estimule o crescimento econômico equilibrado por todo o território da cidade" (Projeto de Lei 01-00830/2017), de forma a minimizar os custos econômicos e sociais (Câmara Municipal de São Paulo, 2019). Desse modo, procura-se utilizar as TICs conjuntamente com o capital humano para solucionar problemas urbanos e aprimorar os processos dentro da cidade, buscando promover uma melhora na qualidade de vida dos cidadãos.

FIGURA 1 COMPONENTES E CARACTERÍSTICAS DA CIDADE INTELIGENTE



Fonte: Adaptada de Ristvej, Lacinák, e Ondrejka (2020).

Várias são as TICs encontradas nas cidades inteligentes, entre elas Big Data, Cloud and Edge Computing, Artificial Intelligence (AI), Internet of Things (IoT), Blockchain, Geospatial Technology. Contudo, não são apenas essas tecnologias emergentes que podem ser citadas quando se trata de

aplicações nas cidades inteligentes, pois surgem muitas possibilidades com a inovação (Z. Yu, Song, Jiang, & Sharafi, 2021). Diante disso, é importante salientar que não há cidade inteligente sem tecnologia e inovação, pois são justamente esses fatores que diferenciam-na de uma cidade comum (Eckhoff & Wagner, 2018).

Assim, estudar o arquétipo formulado e adaptado de Ristvej et al. (2020) possibilita entender a cidade inteligente (Figura 1) e percebe-se que existem três componentes-base que caracterizam o conceito: Fatores Tecnológicos (TICs), Fatores Humanos (*input* dos cidadãos) e Fatores Institucionais (elementos que viabilizam a coletividade, como políticas e regulamentações). Esses componentes são facilitadores e recursos que possibilitam e impulsionam as seis características (Economia, Mobilidade, Ambiente, Pessoas, Vida e Governança). Alguns elementos dos componentes pertencem a uma característica específica (como sistemas de reciclagem), outros podem ser considerados horizontais ou habilitadores (como Big Data e IoT), abrangendo várias características, como as formuladas por Giffinger et al. (2007) e apresentados no Quadro 1.

QUADRO 1 CARACTERÍSTICAS DE UMA CIDADE INTELIGENTE

Característica	Definição	Autor
Economia Inteligente	[…] economia baseada em conhecimento, promovendo criatividade […] parcerias público-privadas e conexões internacionais (intercâmbio de pesquisas). Capacidade de inovação.	Cunha, Przeybilovicz, Macaya, e Burgos (2016)
Pessoas Inteligentes	[…] cidadãos são a maior fonte de desenvolvimento urbano e força motriz para a criação de conhecimento, melhor educação, infraestrutura social e promoção da criatividade com inteligência coletiva.	Gil-Garcia, Pardo, e Nam (2015)
Governança Inteligente	[…] baseada na transparência, participação pública, interação com os agentes públicos e privados, cooperação e livre acesso aos dados de informação por meio das TICs. Estrutura que permite que haja colaboração, troca de dados, integração entre os serviços e comunicação na administração da cidade.	Giffinger et al. (2007)
Mobilidade Inteligente	[…] recursos de transporte e infraestrutura tecnológica da cidade para a gestão do fluxo de demanda e locomoção da população. Acessibilidade é essencial para promover maior inclusão social e evitar isolamentos dos guetos urbanos modernos.	Benevolo, Dameri, e D'Auria (2016)
Meio Ambiente Inteligente	[…] condições naturais atraentes, gestão de recursos e esforços de proteção ambiental (sustentabilidade). Busca-se diminuir os impactos causados pela urbanização com o auxílio da tecnologia, propondo alternativas otimizadas para os problemas da gestão ambiental. Ademais, é fundamental ter projetos de conscientização.	Braun et al. (2018); Giffinger et al. (2007)
Vida Inteligente	[…] aumento na qualidade de vida, acessibilidade, praticidade e eficiência na relação com a cidade. Desde a percepção da segurança e condições de moradia até acesso a recursos de saúde e educação, entre outros. Maior foco é a integração com a cidade, buscando maior coesão social e senso de pertencimento da população.	Cunha et al. (2016); Giffinger et al. (2007)

Fonte: Elaborado pelos autores.

Entende-se que o conceito de segurança permeia todas as características propostas por Giffinger et al. (2007) no contexto da cidade inteligente e é um componente crucial para toda a sua estrutura intimamente ligado à tecnologia. Essas características são utilizadas em vários estudos que organizam as cidades inteligentes em categorias analíticas (Elmaghraby & Losavio, 2014; Ismagilova et al., 2020).

2.2. Segurança e privacidade na cidade inteligente

Ao analisar os desafios de segurança e privacidade das cidades inteligentes, é importante perceber que muitos deles já existem na realidade cotidiana, embora não ofereçam tanto impacto no presente quanto ocorreria no contexto totalmente interconectado da cidade inteligente (Adil & Khan, 2021; Braun et al., 2018; Javed et al., 2022).

Entende-se que a cidade inteligente requer os mais altos níveis de segurança, por ser composta, principalmente, por tecnologia digital intensiva em coleta e análise de dados, um elemento crítico na infraestrutura dessa sociedade futura. Muitas das inovações relacionadas com o conceito buscam uma forma de aprimorar e disponibilizar mais serviços por meio de tecnologia e aplicativos para os *stakeholders* que fazem parte do sistema da cidade (Habib et al., 2019). Assim, se faz necessário que haja uma arquitetura abrangente, com segurança incorporada desde o início, para que se obtenham confiança e aceitação da cidade inteligente por parte dos cidadãos (Kasar & Kshirsagar, 2021).

L. Cui et al. (2018) afirmam que a infraestrutura de uma cidade inteligente é composta por milhares de dispositivos e aplicações que visam aperfeiçoar processos e proporcionar benefícios para os cidadãos, como *smart healthcare* e *smart home*, entre outros. Contudo, a utilização dessas aplicações e sistemas pode trazer diversos problemas relacionados com a segurança e a privacidade (Adil & Khan, 2021), por causa de vulnerabilidades existentes nesse sistema inteligente, já que eles não apenas coletam uma grande variedade de informações sensíveis de pessoas e seus círculos sociais, mas também controlam as instalações da cidade e influenciam a vida dos cidadãos (Zhang et al., 2017).

Braun et al. (2018) afirmam que a segurança é um conceito dinâmico e não estagnado. Pode ser definido como um esforço para prevenir danos por meios digitais e físicos, tanto diretos como indiretos. Numa cidade inteligente, a segurança pode ser considerada um componente geral, pois abrange todas as características da cidade, ao passo que também está inclusa em todos os aspectos que a compõem (Ristvej et al., 2020).

Assim, a segurança é uma condição essencial que pode ser vista como fator de higiene (que leva à insatisfação se não contemplada), sendo considerada um dos itens mais importantes em pesquisas de aceitação de tecnologia (AlHogail, 2018; L. S. Grandhi et al., 2021; Sepasgozar et al., 2019; Urmetzer & Walinski, 2014). Ademais, seu entendimento engloba muito mais do que apenas fatores técnicos, possuindo um forte aspecto dependente do fator humano, em toda a sua funcionalidade (Braun et al., 2018), incluindo também facetas subjetivas relacionadas com a percepção dos indivíduos. Dessa forma, o conceito pode ser dividido em duas dimensões de segurança, a objetiva e a subjetiva (Ceccato, 2013; Meskaran, Ismail, & Shanmugam, 2013).

A segurança objetiva é o aspecto "tangível" da proteção técnica, baseada na criptografia, na declaração de políticas de segurança, no conhecimento dos riscos "estatísticos" (Ceccato, 2013). Em outras palavras, é ter sua proteção assegurada por uma solução tecnológica e ter consciência, racionalmente, do que realmente constitui uma ameaça e dos mecanismos que garantem sua segurança. Já a segurança subjetiva é bastante "intangível" e pode ser definida como a sensação ou percepção que

o usuário tem sobre sua segurança em determinado ambiente ou situação. Ela pode ser facilmente influenciada por fatores externos, como confiança e opinião de amigos, familiares e até terceiros. No contexto da tecnologia da cidade inteligente, se esse sentimento diz ao indivíduo que pode haver um problema na segurança, esse potencial usuário não se tornará um usuário real, mesmo estando garantido, do ponto de vista tecnológico (Urmetzer & Walinski, 2014). Isso significa que, mesmo com as melhores abordagens e soluções técnicas, ao desconsiderar a percepção dos cidadãos sobre a segurança, estas podem se tornar irrelevantes.

É importante destacar que as duas dimensões – segurança objetiva e subjetiva – não são disjuntas nem independentes (Ceccato, 2013; F. Cui et al., 2018). Contudo, a percepção subjetiva de segurança dos indivíduos não afeta as medidas objetivas de segurança enquanto o contrário ocorre.

Desse modo, a privacidade é um conceito complexo, inicialmente considerado um direito básico pela Convenção Europeia de Direitos Humanos (1950) e estabelecido como "respeito à vida privada" (Council of Europe, 2020). Desde então, houve diversas tentativas de definir o melhor o conceito de privacidade que se adapte a cada nova mudança na realidade. Mais recentemente, ele foi descrito como integridade contextual (Eckhoff & Wagner, 2018), ou seja, existe a necessidade de entender o contexto no qual o conceito se insere para que seja possível estabelecer os limites da integridade individual.

No contexto tecnológico, a privacidade de dados é relacionada com a forma como essa informação é coletada, compartilhada e utilizada, sendo uma garantia de que não ocorrerá a manipulação dos dados sem a autorização do usuário (S. E. Chang, Liu, & Shen, 2017), e apresenta-se, então, como um grande desafio no contexto atual em razão do crescente fluxo de informações e da expansão do uso de tecnologia de monitoramento, entre outros (Adil & Khan, 2021)the global research communities are working relentlessly by harnessing the emerging technologies to develop the safest diagnosis, evaluation, and treatment procedures, and Internet of Things (IoT).

Nota-se que muitos cidadãos não percebem – ou não sabem – os riscos que correm ao fornecer suas informações on-line, em aplicativos ou sites, e a possibilidade de terem seus dados vendidos a terceiros. Com ferramentas como Big Data e People Analytics em voga, ter acesso às informações dos consumidores é uma grande fonte de vantagem competitiva para empresas e instituições (Y. Chang, Wong, Libaque-Saenz, & Lee, 2018), mas é necessário que haja um limite a essa liberdade para preservar a integridade individual.

É relevante salientar que apenas recentemente o Brasil elaborou uma legislação capaz de delimitar e regulamentar o uso de dados sensíveis por terceiros. Assim, em agosto de 2020, entrou em vigor a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), que estabelece regras e proteção especial sobre o processamento de "dados pessoais sensíveis".

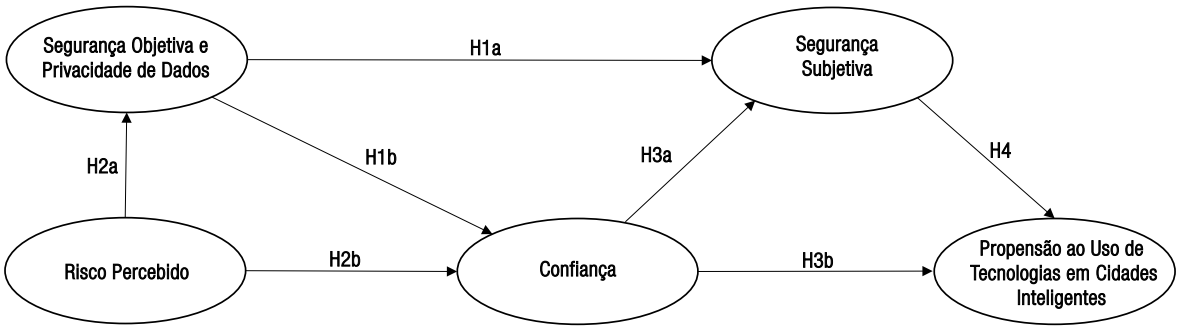
Por fim, ainda há ameaças comuns como vírus e interceptação de comunicação, invasão de servidores e vazamento de informações sensíveis, sendo estas algumas das principais causas de violações de privacidade (L. Cui et al., 2018). Assim, faz-se necessário entender os perigos e criar barreiras para manter os usuários seguros (Alraja, Farooque, & Khashab, 2019; L. Cui et al., 2018; Eckhoff & Wagner, 2018).

2.3. Construção do modelo e hipóteses de pesquisa

A fim de identificar os aspectos-chave que influenciam a intenção comportamental dos usuários, de usar e continuar usando a tecnologia das cidades inteligentes, foram formados constructos e hipóteses com base em uma ampla revisão da literatura.

Na Figura 2, é representado o modelo de pesquisa proposto com os constructos e as hipóteses formuladas. As próximas subseções contemplam as respectivas definições.

FIGURA 2 MODELO DE PESQUISA



Fonte: Elaborada pelos autores.

2.3.1. Segurança Objetiva e Privacidade de Dados (SOPD)

Sabe-se que a segurança objetiva é a característica técnica tangível, ou seja, no contexto da cidade inteligente, é a solução tecnológica de fato, como o antivírus e a criptografia, entre outros (Urmetzer & Walinski, 2014). Já em relação à privacidade de dados, tem-se que as garantias estruturais são os principais fatores que influenciam a confiança. Por ser fortemente relacionada com questões técnicas de tecnologia, **é** conveniente a junção entre os conceitos de segurança objetiva e privacidade de dados.

No contexto da cidade inteligente, a existência de segurança objetiva e privacidade de dados é um fator crítico para o desenvolvimento da segurança subjetiva e da confiança dos cidadãos (Ortega & Román, 2011), pois é uma garantia de que estes possuem salvaguardas, tanto em relação à prestação de serviço ou ao produto adquirido quanto ao vazamento ou ao uso inadequado de informações pessoais (S. E. Chang et al., 2017).

Ademais, o nível de proteção técnica influencia a percepção de segurança do indivíduo ou, como já foi tratado na literatura, a segurança subjetiva. Nesse contexto, se faz necessário um nível de segurança objetiva considerável, capaz de influenciar o indivíduo em sua percepção de segurança e confiança na tecnologia para que ele possa, em consequência, adotá-la. Assim sendo, foram estabelecidas as seguintes hipóteses:

H1a: SOPD tem uma influência positiva na SS.
H1b: SOPD tem uma influência positiva na CO.

2.3.2. Risco Percebido (RP)

Segundo Alraja et al. (2019), o risco percebido é o julgamento subjetivo do que as pessoas fazem sobre as características e a gravidade de um risco, sendo eles geralmente associados a um produto ou serviço. No contexto das cidades inteligentes, os riscos percebidos estão majoritariamente relacionados com tecnologia, por causa da sua forte presença em produtos e serviços, como é o caso da IoT, que compõe a base da vida na cidade (AlHogail, 2018; Ismagilova et al., 2020; Z. Yu et al., 2021)

A sensação de falta de controle, seja sobre os dados, seja sobre a tecnologia, é um dos fatores agravantes da maior percepção de risco, fazendo com que haja incompatibilidade entre o nível de risco real, a segurança objetiva e a privacidade dos dados, bem como a confiança individual na tecnologia observada no constructo "segurança objetiva e privacidade de dados" (AlHogail, 2018). Ademais, vários estudos mencionam o risco percebido como um preditor de alta influência negativa sobre a confiança (Meskaran et al., 2013). Dessa forma, foram estabelecidas as seguintes hipóteses:

H2a: O RP tem uma influência negativa na SOPD.
H2b: O RP tem uma influência negativa na CO.

2.3.3. Confiança (CO)

A confiança corresponde às expectativas do que outras pessoas farão no futuro com base em experiências anteriores, sendo um fator importante para se estabelecerem relações, especialmente em ambientes em que há incerteza e risco, como nas transações on-line, por exemplo (Mittendorf, 2016). Dessa forma, ela é aplicada particularmente no contexto das relações entre usuário e tecnologia, uma vez que nem sempre há regras e regulamentos claros, pois a confiança é decisiva para que esse vínculo seja estabelecido. No contexto da tecnologia, a confiança se consolida na garantia pessoal de que a instituição por trás do serviço (ou produto) cumprirá suas obrigações, se comportará como esperado (não vai tirar vantagem das vulnerabilidades) e prezará pela satisfação e o bem-estar do usuário, ou seja, na crença do atendimento das expectativas de que o que se espera será entregue (Mushtaq, Jingdong, Ahmed, & Ali, 2019). Dessa forma, considera-se que a confiança desempenha um papel importante na segurança subjetiva e na adoção da tecnologia em cidades inteligentes, de modo que são formuladas as seguintes hipóteses:

H3a: A CO tem uma influência positiva na SS.
H3b: A CO tem uma influência positiva na PUTCI.

2.3.4. Segurança Subjetiva (SS)

A segurança subjetiva é o aspecto intangível da segurança, sendo a sensação percebida do usuário sobre a segurança de modo geral, que é influenciada pela opinião social e crenças já estabelecidas, além do fator de segurança objetiva e privacidade de dados (Urmetzer & Walinski, 2014). Pesquisas apontam que a segurança não é apenas uma questão técnica, mas humana e organizacional (Meskaran et al., 2013), e, ao reconhecer o impacto da segurança subjetiva na propensão do indivíduo, muitos estudos passaram a investigar a influência da segurança percebida (subjetiva) em vez de da segurança objetiva (F. Cui et al., 2018).

No contexto da cidade inteligente, ela é a sensação percebida que o usuário (em potencial ou não) tem sobre o quão segura é a tecnologia, independentemente das salvaguardas técnicas (criptografia, entre outros) que ela possua (Urmetzer & Walinski, 2014). Ademais, principalmente no caso de países em desenvolvimento, se nota uma necessidade mais forte da percepção de segurança para que haja a aceitação e o uso de novas tecnologias (AlHogail, 2018; Sepasgozar et al., 2019). Assim sendo, foi formulada a seguinte hipótese:

H4: A SS tem uma influência positiva na PUTCI.

2.3.5. Propensão para o Uso de Tecnologia em Cidades Inteligentes (PUTCI)

A intenção comportamental é um dos constructos-chave de modelos de aceitação de tecnologia, sendo derivado da teoria da Ação Racional (L. S. Grandhi et al., 2021; Sepasgozar et al., 2019; Verma & Sinha, 2018). Tais modelos buscam explicar e antecipar a disposição dos indivíduos em relação à aceitação de tecnologia da informação. Assim, esse constructo representa a intenção de ação do usuário sobre o objeto de estudo afetado por um conjunto de variáveis propostas.

No contexto desta pesquisa, esse constructo foi definido como a "propensão para o uso da tecnologia em cidades inteligentes" (Al-Sharafi et al., 2016; Sepasgozar et al., 2019), sendo a variável dependente do estudo, que é influenciada pelas variáveis: confiança (Abu-Shanab, 2017; Mittendorf, 2016), segurança subjetiva (F. Cui et al., 2018; Urmetzer & Walinski, 2014), segurança objetiva e privacidade de dados (Abu-Shanab, 2017; Sepasgozar et al., 2019) e risco percebido (Hansen et al., 2018).

3. MÉTODO

3.1 Escolha e caracterização da amostra

Este estudo é classificado como empírico exploratório-descritivo e a abordagem da pesquisa adotada foi a quantitativa com um corte transversal. A amostra é não probabilística e foi constituída por conveniência (Duhamel, Langerak, & Schillewaert, 1998).

Em estudos empíricos exploratório-descritivos, como neste caso, a representatividade da amostra passa a ser preocupação secundária, já que o principal objetivo é analisar o fenômeno e não extrapolar os resultados para a população (Churchill, 1999). Além disso, a heterogeneidade se faz importante para que a pesquisa não fique restrita a um grupo específico de usuários de tecnologia, ou seja, abranja maior diversidade dentro da caracterização da amostra.

Assim, como critério, foram selecionados apenas indivíduos que teriam condições de realizar uma avaliação mais precisa sobre o consumo de tecnologia oferecido pela cidade de São Paulo em virtude de seu nível de literacia digital e de acesso à tecnologia. Portanto, os respondentes precisariam ser usuários de *smartphone* e aplicativos, o que os tornariam potenciais usuários na busca de informações sobre serviços disponibilizados pela cidade para atender aos cidadãos (Oyewo, Vo, & Akinsanmi, 2020).

São Paulo foi escolhida por figurar como a cidade mais inteligente do Brasil pelo *ranking* Connected Smart Cities da Urban Systems (Urban Systems, 2021) e ocupar a 42ª posição no mundo, de acordo com o Global Power City Index 2021 (Yamato et al., 2021).

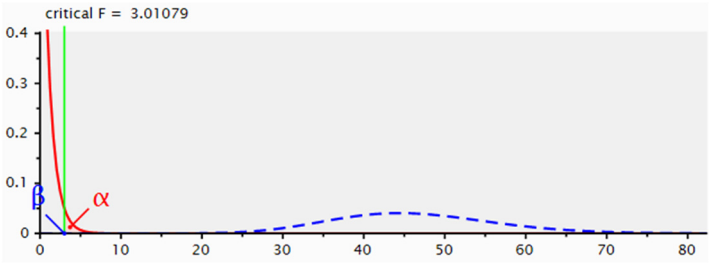
A condução do *survey* ocorreu entre dezembro de 2022 e janeiro de 2023, por meio de um questionário on-line distribuído pelo serviço QuestionPro. Antes disso, o instrumento de pesquisa passou por uma tradução reversa, sendo analisado por especialistas. Na sequência, foi realizado um pré-teste com 40 respondentes para realizar a validação do instrumento.

Das 631 respostas completas, foi feita a etapa da purificação de dados, por meio do critério da distância de Mahalanobis (D^2), para identificar *outliers*. Foram eliminados 30 registros, então, sobraram 601 questionários válidos, que foram tabulados em planilha e, posteriormente, analisados por meio dos softwares SPSS 25 e R Studio Build 353 (ver Apêndice 2).

3.2. Cálculo da amostra

Para estimar o tamanho da amostra mínima para esta pesquisa, foi utilizado o software G*Power 3.1.9 (Faul, Erdfelder, Buchner, & Lang, 2009). No modelo proposto, avalia-se o constructo que recebe o maior número de relações (setas) ou tem o maior número de preditores. Para o cálculo *a priori,* antes da coleta de dados, deve-se observar que há dois parâmetros: o poder do teste (*Power* = 1– $\beta_{erro\ prob\ II}$) e o tamanho do efeito (f^2). Cohen (1998) e Hair, Hult, Ringle, e Sarstedt (2014) recomendam o uso do poder como 0,80 e o f^2 mediano = 0,15. Diante disso, é sugerida uma amostra mínima a ser utilizada. A Figura 3 apresenta o resultado do software, contudo, em um teste *post hoc,* é possível observar qual seria a amostra ideal com o poder amostral em 100%. O modelo proposto traz o número de preditores = 2, o que possibilita realizar a pesquisa com apenas 68 respondentes, porém, em uma análise *post hoc,* observou-se que, com 601 respondentes, os parâmetros obtidos foram $F_{crítico}$ = 3.010 e poder amostral 100% (Figura 3).

FIGURA 3 TESTE *POST HOC* DO TAMANHO DO EFEITO DA AMOSTRA



Fonte: Software G*Power.

3.3. Instrumento de pesquisa

O instrumento de pesquisa era composto por escalas psicométricas adaptadas (ver Apêndice 1) possuía também questões introdutórias e uma parte sociodemográfica para a identificação do perfil do respondente. O modelo foi construído com 18 questões ancoradas em uma escala classificada como Likert com cinco pontos (1 - "discordo totalmente" até 5 - "concordo totalmente"). Na análise, foi empregada a técnica multivariada de dados, por meio da modelagem de equações estruturais, com estimação por mínimos quadrados parciais (PLS-SEM) para testar as hipóteses.

3.4. A escolha do método

O PLS-SEM foi identificado como o método de análise mais adequado por quatro razões principais: primeiro, para maximizar a variância de variáveis endógenas explicadas por variáveis exógenas. Segundo, por não exigir que a normalidade para a distribuição dos dados seja atendida, ideal nas ciências sociais aplicadas que tendem a ter distorções por assimetria e/ou curtose. Terceiro, é ideal para a estimativa de modelos novos e complexos. Finalmente, é preferido para os testes de interação porque não infla o erro de medição (Hair, Risher, Sarstedt, & Ringle, 2019). Na operacionalização do método, foi empregado o software R (SEMinR).

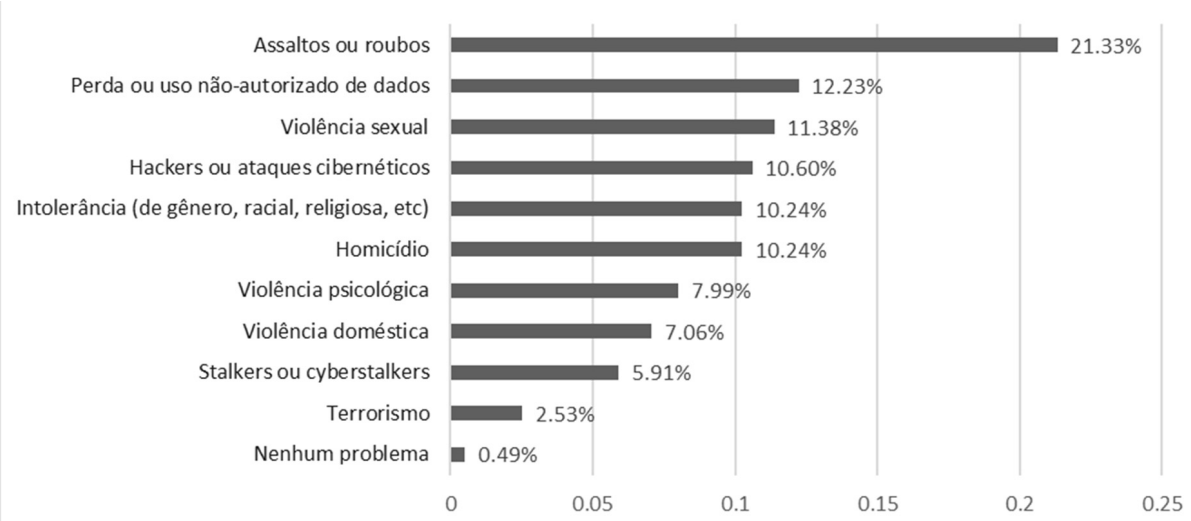
4. APRESENTAÇÃO E ANÁLISE DOS DADOS

4.1. Caracterização dos respondentes

Ao analisar os dados sociodemográficos da amostra, observou-se uma leve predominância do sexo feminino (57,9%/n = 348) em comparação com os respondentes masculinos (42,1%/n = 253). Ademais, em relação à faixa etária, grande parte da amostra encontra-se na faixa dos 18 aos 27 anos (61,04% /n = 367).

Nota-se, neste estudo, que a preocupação em relação à segurança é moldada pela realidade dos cidadãos. Na cidade de São Paulo, percebe-se a preocupação com os altos índices de violência primária, ou seja, as pessoas, em sua maioria, ainda possuem a necessidade básica de proteção à integridade física, sendo uma característica, advinda do cenário sociocultural do país, que o conceito de cidade inteligente busca amenizar e, idealmente, mitigar.

GRÁFICO 1 PROBLEMAS DE SEGURANÇA NA CIDADE



Fonte: Elaborado pelos autores.

Contudo, é interessante notar que, entre os cinco principais problemas na segurança da cidade (Gráfico 1) está a "perda ou o uso não autorizado de dados", que é uma questão mais relacionada com o cenário da cidade inteligente, que ficou em segundo lugar quando comparada com questões de segurança pública. Assim, esta é uma preocupação que vem crescendo e é relevante por causa do cenário de evolução tecnológica, sendo uma questão que não apenas pode causar dano por si só, mas que pode facilitar e contribuir para outros crimes. Além disso, os quatro principais itens apontados também podem estar vinculados a dados e informações de cidadãos em dispositivos móveis.

4.2. Normalidade, viés do método comum, viés de não respostas e colinearidade

A normalidade dos dados foi verificada pelo teste multivariado de Mardia. Os resultados obtidos para os indicadores foram altamente significativos, com $p < 0{,}001$, indicando não a normalidade, o que era esperado e necessário para o uso do PLS-SEM.

Uma vez que os dados são primários, foi necessário garantir que nenhum viés sistemático influenciasse as informações coletadas. Assim, verificou-se a variância do método comum, por meio da aplicação do teste de um fator de Harman (Podsakoff & Organ, 1986) nos 15 itens. A variância extraída do primeiro componente foi de 39,75%, inferior ao mínimo de 50%, o que valida o teste. Além disso, também foi realizada a análise do viés de não respostas, que buscou comparar duas subamostras em um teste T para verificar se existiria diferença entre as médias, o que não foi constatado, logo, foi possível executar a pesquisa com a amostra total.

No que concerne às variáveis preditoras relacionadas com a variável dependente "propensão ao uso da tecnologia em cidade inteligente", foi possível verificar que não ocorreu multicolinearidade no modelo, pois todos os valores dos Fatores de Inflação da Variância (VIFs) dos constructos ficaram abaixo de 3,3, sendo os respectivos valores: SOPD = 1,820; RP = 1,950; PUTCI = 1,993; SS = 2,276; e CO = 1,690.

4.3. Modelagem de equações estruturais

Depois do ajustamento do modelo na primeira iteração, foram apresentados os resultados das cargas fatoriais e a análise do modelo de mensuração para ajustar a validade discriminante. As variáveis com cargas fatoriais < 0,7 (SS1, CO4 e PUTCI4) foram excluídas para a obtenção de resultados mais adequados (Malhotra, 2012). A análise do modelo de mensuração deve preceder a análise das relações entre os constructos ou variáveis latentes. O próximo passo foi examinar o modelo de mensuração (Tabela 1): alfa de Cronbach (AC), confiabilidade composta (CC), variância média extraída (VME) e coeficientes de determinação (R^2) (Hair, Hult, Ringle, & Sarstedt, 2017).

TABELA 1 VALIDADE CONVERGENTE E DISCRIMINANTE

Constructos					Discriminantes				
	AC	CC	VME	R^2	(1)	(2)	(3)	(4)	(5)
(1) Segurança objetiva e privacidade dos dados	0,837	0,902	0,754	0,032	0,868				
(2) Risco percebido	0,782	0,873	0,696		-0,178	0,834			
(3) Propensão ao uso de tecnologia em cidades inteligentes	0,820	0,893	0,736	0,232	0,322	-0,190	0,858		
(4) Segurança subjetiva	0,812	0,889	0,727	0,576	0,618	-0,262	0,474	0,853	
(5) Confiança	0,856	0,912	0,777	0,314	0,540	-0,242	0,53	0,705	0,881

*AC: alfa de Cronbach (> 0,6); CC: confiabilidade composta (> 0,7); VME: variância média extraída (> 0,5).
Nota: a diagonal em destaque apresenta as raízes quadradas da VME pelo Critério de Fornell-Larcker.
Fonte: Software R (SEMinR).

Dado que todas as variáveis de um questionário utilizam a mesma escala de medição, o coeficiente é calculado com base na variância dos itens individuais. Os ACs foram considerados moderados; as CCs e as VMEs foram tidas muito boas e aceitáveis. Dessa forma, os coeficientes de AC indicaram alta consistência interna das escalas utilizadas, assim como as CCs (Hair et al., 2017) e as VMEs (Chin, 1998) para a indicação da existência de validade convergente. Além disso, acrescentou-se o critério heterotrait-monotrait ratio (HTMT). De acordo com Henseler, Ringle, e Sarstedt (2015), o valor HTMT deve estar abaixo de 0,90, o que significa que a validade discriminante foi estabelecida entre dois constructos reflexivos. Na Tabela 2, observa-se que esse critério também foi atingido.

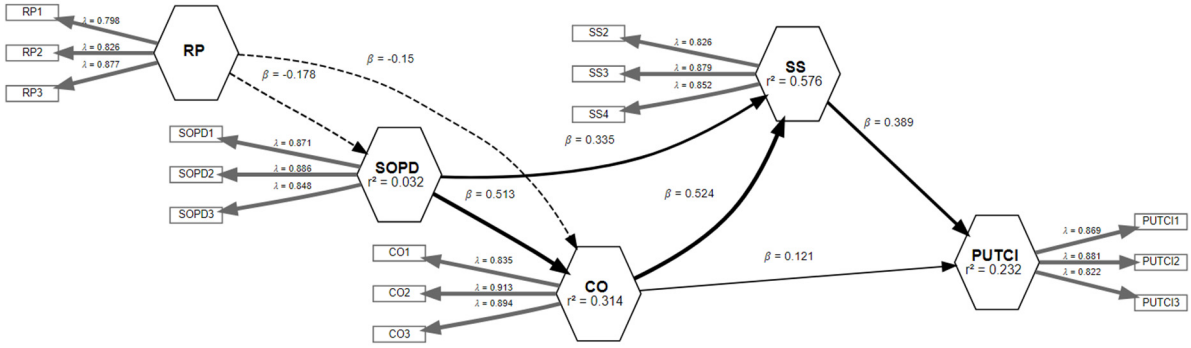
TABELA 2 APRESENTAÇÃO DO CRITÉRIO HTMT

	SOPD	RP	PUTCI	SS	CO
SOPD	.	.	.	.	.
RP	0,218	.	.	.	.
PUTCI	0,387	0,235	.	.	.
SS	0,748	0,325	0,583	.	.
CO	0,639	0,290	0,468	0,841	.

Fonte: Software R (SEMinR).

Na aplicação prática da modelagem de equações estruturais para o modelo de pesquisa proposto (Figura 4), observam-se as mensurações realizadas individualmente para cada constructo, para verificar sua validade e consistência interna e externa, bem como os resultados obtidos em seus caminhos e hipóteses.

FIGURA 4 RESULTADOS DO MODELO DE PESQUISA PROPOSTO



Nota: linhas contínuas, relação positiva; linhas tracejadas, relação negativa.
Fonte: Software R (SEMinR).

O modelo foi estimado utilizando-se a técnica *bootstrapping* (Tabela 3), em que se comparou a amostra original com as amostras geradas (Chin, 1998). Os resultados da análise de significância dos caminhos indicaram que todas as hipóteses foram suportadas. Além disso, verificou-se que todas as três mediações propostas no modelo foram parciais, ou seja, tanto a relação direta quanto a indireta tiveram resultados significativos semelhantes.

TABELA 3 CAMINHOS E HIPÓTESES

Hipóteses	*β*	*Bootstrapping (n = 5000)*	Desvio padrão	Teste T	Valor P	IC 2,5% 97,5%
Relações diretas						
H1a: SOPD SS	0,335	0,335	0,038	8,887	0,000	0,262 0,409
H1b: SOPD CO	0,513	0,513	0,037	13,906	0,000	0,437 0,582
H2a: RP SOPD	-0,178	-0,181	0,044	-4,097	0,000	-0,266 -0,096
H2b: RP CO	-0,150	-0,152	0,035	-4,337	0,000	-0,219 -0,085
H3a: CO SS	0,524	0,524	0,036	14,540	0,000	0,452 0,591

Continua

Hipóteses	β	*Bootstrapping (n = 5000)*	Desvio padrão	Teste T	Valor P	IC 2,5% 97,5%
H3b: CO → PUTCI	0,121	0,121	0,053	2,277	0.023	0,014 0,224
H4: SS → PUTCI	0,389	0,389	0,059	6,629	0,000	0,275 0,504
Relações indiretas (mediadoras)						
M1: RP → SOPD → CO	-0,091	-0,092	0,022	-4,080	0,000	-0,136 -0,049
M2: SOPD → CO → SS	0,268	0,268	0,026	10,265	0,000	-0,218 0,320
M3: CO → SS → PUTCI	0,204	0,203	0,035	5,802	0,000	0,137 0,276

Fonte: Elaborada pelos autores.

5. DISCUSSÃO DOS RESULTADOS

Ao analisar as hipóteses formuladas (Tabela 3), observou-se, de forma geral, que o modelo proposto conseguiu identificar, com base na literatura, um padrão robusto para o tema da propensão ao uso (Boon-itt, 2019) amplamente empregado em pesquisas de aceitação de tecnologia (L. S. Grandhi et al., 2021). Ademais, esta pesquisa traz como contribuição a percepção dos cidadãos de que, ao utilizar a tecnologia da cidade inteligente, obterão vantagem em relação aos sistemas tradicionais, mostrando um entendimento de que a tecnologia possui potencial para facilitar a vida no ambiente urbano.

Assim, para maior aderência ao conceito de cidade inteligente, visto que a tecnologia **é,** basicamente, o que move a cidade, é necessário promover essa percepção de valor. Ao observar a amostra coletada, é possível notar que a facilidade de acesso e a frequência de uso reforçam uma forte percepção de utilidade da tecnologia.

A hipótese H1a com o caminho 'SOPD → SS' foi suportada ($\beta = 0{,}335$; $p < 0{,}001$), corroborando o conceito de Linck (2006), de que a proteção técnica de um sistema possui forte influência sobre a percepção de segurança do usuário. Isso se deve ao fato de que grande parte da formação da concepção de segurança dos indivíduos, no geral, baseia-se em quesitos físicos e tangíveis, que, no contexto tecnológico, são traduzidos como criptografia, antivírus e autenticação, entre outros.

De modo semelhante, ao analisar as características da amostra, identificou-se uma forte percepção de valor sobre as informações pessoais, assim como uma grande preocupação com a perda e o uso indevido de dados. Da mesma forma ocorreu com a hipótese H1b com o caminho 'SOPD → CO' ($\beta = 0{,}513$; $p < 0{,}001$), que apresentou o segundo maior efeito de todas as hipóteses. Nesse caso, percebe-se a importância de que as salvaguardas estejam evidentes para que o usuário em potencial possa se sentir mais confiante e, consequentemente, propenso a expor suas vulnerabilidades e dar uma chance à tecnologia.

Já a relação negativa da hipótese H2a com o caminho 'RP→SOPD' ($\beta = -0{,}178$; $p < 0{,}001$) também foi suportada. Isso ocorreu porque ela compõe duas ideias opostas, ou seja, ao se constatar alta segurança técnica contra possíveis ameaças e uso inadequado de informações, a tendência é que a percepção da existência de riscos seja minimizada. Dessa forma, ao se precaverem contra-ataques e estabelecerem regras para o uso das informações obtidas, as instituições têm mais chances de aumentar a aderência a seus produtos e serviços (Habib et al., 2019).

Da mesma forma, a relação negativa da hipótese H2b com o caminho 'RP→CO' (β = -0,150; p < 0,001) foi suportada, conforme esperado, corroborando a ideia de que é um preditor de significante influência sobre a variável confiança que possui uma relação negativa e inversa (Meskaran et al., 2013). Trata-se, no contexto das cidades inteligentes, de preocupação majoritariamente relacionada com a disponibilização de informações na rede, mesmo em sites ou aplicativos conhecidos. Tal apreensão se dá pela incerteza quanto à utilização dos dados pessoais pela instituição, assim como por terceiros, em caso de eventual vazamento, tendo em vista que isso pode ocasionar diversos danos ao indivíduo.

A hipótese H3a com o caminho 'CO→SS' (β = 0,524; p < 0,001) foi suportada com o maior efeito entre todas as hipóteses. Isso mostra que a percepção de segurança é um elemento importante para que haja confiança, em especial por causa do contexto tecnológico da cidade inteligente, que traz riscos e insegurança. Como é o caso de perda ou uso não autorizado de dados, como destacado pelos respondentes (Gráfico 1). Descuidos nesse quesito podem levar à perda de confiança nas instituições que realizam esse tipo de serviço, em função da exposição de dados cadastrais de pessoa física e jurídica (Adil & Khan, 2021; Kasar & Kshirsagar, 2021; Meskaran et al., 2013). Dessa forma, para obter e manter a confiança dos usuários, as instituições por trás dos serviços de tecnologia precisam estar atentas à opinião de seus usuários e da sociedade sobre ela, de forma a manter uma boa reputação, para que possam, assim, conquistar uma percepção positiva de segurança.

Na sequência, tem-se a hipótese H3b com o caminho 'CO→PUTCI' (β = 0,121; p = 0,023), que foi suportada. Isso mostra que a percepção dos cidadãos é que a tecnologia deve trazer a confiança esperada e que isso não ocorre apenas pela presença dela. O efeito da tecnologia nas cidades inteligentes pode impulsionar o valor e as vantagens desta, assim como faz com que sua intenção de uso seja mais forte, porém, como observado pela mediação (M3; β = 0,204; p < 0,001), a percepção da segurança subjetiva dos indivíduos é a que possibilita maior confiança na propensão ao uso da tecnologia nas cidades inteligentes (Mushtaq et al., 2019).

Dessa forma, a segurança subjetiva se provou um constructo de fundamental importância neste estudo, para estabelecer relações no contexto da cidade inteligente, que ainda é um ambiente com certo grau de incerteza e risco. Isso indica que a percepção que um indivíduo possui da segurança da tecnologia na cidade inteligente varia de acordo com a visão que a sociedade tem sobre ela (Kaushik, Agrawal, & Rahman, 2015; Meskaran et al., 2013), especialmente o que pensam as pessoas consideradas importantes para o indivíduo. Igualmente, confirma que a confiança na tecnologia pode ser construída com base em *feedbacks* positivos de outros usuários.

A hipótese H4 suportou a relação 'SS→PUTCI' (β = 0,389; p < 0,001), indicando que a segurança subjetiva é um preditor que explica a propensão ao uso da tecnologia nas cidades inteligentes, por exemplo, para realizar transações, utilizar serviços de mobilidade urbana e acreditar na segurança das plataformas, entre outros.

Por fim, as relações que envolveram o constructo "segurança objetiva e privacidade de dados" confirmaram a forte influência das barreiras "tangíveis" no reforço da percepção "intangível" da "segurança subjetiva".

Primordialmente, os resultados obtidos confirmaram que o modelo proposto demonstrou consistência, com ajustamentos adequados, de forma que está apto para ser replicado em pesquisas futuras. O artigo traz como contribuição uma discussão importante sobre a necessidade de que os padrões de privacidade inseridos no constructo "segurança subjetiva" sejam incorporados aos aspectos da "confiança", pois são cruciais para a gestão das cidades inteligentes (Braun et al., 2018). Além disso, fornece uma discussão sobre os benefícios de os cidadãos participarem, de forma mais ampla, do uso

de sistemas digitais para desenvolver a "confiança" na "propensão de uso".

De modo geral, este estudo trouxe resultados que podem servir para direcionar ações em políticas públicas para a sociedade, para conscientizar os cidadãos sobre como os seus dados e informações estão sendo utilizados por governos e empresas parceiras para oferecer serviços públicos (Habib et al., 2019). Diante disso, surge uma preocupação com o controle e a gestão dos diferentes níveis e recursos dos sistemas nas cidades inteligentes que, normalmente, são distribuídos entre diversas entidades. Isso pode trazer uma camada de preocupação e limitação de segurança por meio de redes (públicas e/ou privadas) (Rao & Deebak, 2022).

Ademais, percebe-se que a relação com a privacidade de dados também se altera, ao ser mais fácil perder o controle sobre esta, que fica mais vulnerável por causa de diversos fatores, como falta de cuidado por parte dos indivíduos (ao não lerem termos de consentimento), falta de barreiras (que permitem fácil acesso por terceiros mal-intencionados) e falta de opção (ao ser requisito básico para uso de certos serviços ou aplicativos), entre outros.

Em relação à questão da falta de limitações, foram observados alguns avanços por parte de instituições governamentais ao longo dos anos e, no Brasil, quando entrou em vigor a nova Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), que almeja sanar algumas questões relacionadas, como o poder dos agentes de tratamento (controladores e operadores da informação) sobre os dados do indivíduo.

É esperado que ocorram mudanças nas relações digitais desse momento em diante e, dessa forma, é interessante que sejam realizados estudos futuros que analisem mais a fundo esse tópico e seu impacto sobre a cidade inteligente.

6. CONCLUSÕES E IMPLICAÇÕES

O objetivo principal deste estudo foi investigar a percepção de segurança e confiança na tecnologia das cidades inteligentes por parte dos cidadãos, de forma a entender sua relação com a propensão ao uso e, consequentemente, com a vida na cidade. Pode-se dizer que esse objetivo foi alcançado com êxito, ao analisar o modelo proposto e validar as hipóteses formuladas.

Ademais, os resultados da pesquisa indicaram, sobretudo, a necessidade de que seja realizado um trabalho coletivo na cidade de São Paulo com maior divulgação de informações a respeito de questões referentes à segurança da informação, para que os cidadãos possam demonstrar, de forma individual, maior confiança na aceitação e propensão ao uso da tecnologia em cidades inteligentes e, consequentemente, vivenciá-las. Da mesma forma, confirma-se que a segurança da informação é uma temática que possui alta influência na utilização da tecnologia nas cidades inteligentes, e é necessário entender também, de forma mais ampla, os aspectos subjetivos e objetivos observados neste estudo e que demonstraram forte impacto.

A urbanização moderna é dependente de diferentes dispositivos que são analisados para uma melhor gestão estratégica da cidade. Nesse contexto, as pessoas das cidades inteligentes são monitoradas, por exemplo, para fins de segurança social. Assim, à medida que as cidades inteligentes prosperam, coletando e processando locais, informações pessoais e confidenciais dos cidadãos, qualquer violação de privacidade ameaça os indivíduos e a sociedade.

Nesse sentido, o estudo defende que a "confiança" no sistema de tecnologia de São Paulo ainda é um fator preocupante, sob o ponto de vista da segurança, e que poderá ser conquistada com a ampliação da educação digital para os cidadãos, fundamentada em medidas de segurança que sejam

orientadas por dados. Infelizmente, muitos riscos de segurança surgem, em qualquer tipo de sistema, fruto de erros humanos. Esse efeito é amplificado pelo grande número de usuários, assim como a discrepância que há em suas habilidades e níveis de consciência sobre segurança.

Contudo, pode-se dizer, ainda, que, no Brasil, "cidade inteligente" ainda é um conceito desconhecido para a maior parte da população, pois, apesar de o termo ganhar mais visibilidade com o passar do tempo, aparecendo em jornais e revistas, falta entendimento do assunto. Além disso, é um termo que ainda parece muito confuso e distante, principalmente para cidadãos que têm pouco conhecimento de tecnologia básica. Contudo, como apresentado por Bibri (2021), a cultura de *data-driven* pode ser uma solução promissora, à medida que dados e informações são utilizados em maior intensidade.

Os gestores públicos da cidade de São Paulo, no contexto de uma cidade inteligente, poderão ser beneficiados com uma política de segurança baseada em dados que poderá mensurar fatos, padrões de comportamento, correlações, *insights* e conhecimento de sua população. Esse conhecimento poderá ser usado para desenvolver ou revisar processos, atividades, sistemas, políticas e estratégias.

Iniciativas de cidades inteligentes têm caminhado de forma lenta, mas gradual, em muitas regiões brasileiras. Um exemplo muito proeminente é a cidade de São Paulo, que, por ser um dos principais polos de avanço tecnológico, é receptora de grande parte de projetos nesse sentido, sendo considerada a cidade mais inteligente do país pelo IESE Cities in Motion Index 2020 e 2021 (Berrone & Ricart, 2020).

Portanto, apesar de a capital paulista se destacar em mobilidade e acessibilidade, por conta das várias possibilidades de locomoção, ainda preocupa com relação a problemas mais comuns associados à privacidade, como acesso ou uso de dados para fins não autorizados, falhas e/ou instabilidade em sistemas/aplicativos e uso mal-intencionado de informações privadas, entre outros presentes na literatura (Bélanger & Crossler, 2011; S. E. Chang et al., 2017).

Dessa forma, é importante que os líderes de iniciativas de cidades inteligentes sejam capazes de promover essa percepção de valor, estejam atentos às tendências das massas e cultivem uma forte cultura de *feedback* e suporte ao usuário, cliente ou cidadão para que sejam feitas melhorias contínuas.

Por fim, para o governo e para os líderes de iniciativas de cidades inteligentes, é fundamental atentar para a questão da segurança não apenas tecnológica, mas em todos os aspectos no contexto da cidade, levando em consideração como a tecnologia pode ajudar na resolução desses problemas. No caso específico do Brasil, observando-se a questão da intolerância, que foi a segunda maior preocupação da amostra da pesquisa, pode-se considerar que uma parte desse problema se dê pela falta de informação e falta de questionamento e que ela pode ser abordada utilizando-se a tecnologia não só para monitorar os transgressores, mas para promover debates, divulgar conteúdos e informações para a população.

Diante das considerações anteriores, percebe-se a importância da realização de estudos que avaliem a aceitação, pelos cidadãos, e os potenciais problemas e barreiras para a efetiva implementação de soluções de cidade inteligente e para o avanço das melhorias. Ademais, entende-se que as questões subjetivas da percepção e o contexto ambiental possuem forte influência sobre a opinião coletiva ou individual, e é relevante explorá-los em estudos futuros.

REFERÊNCIAS

Abu-Shanab, E. A. (2017). E-government familiarity influence on Jordanians' perceptions. *Telematics and Informatics*, *34*(1), 103-113. Recuperado de https://doi.org/10.1016/j.tele.2016.05.001

Adil, M., & Khan, M. K. (2021). Emerging IoT applications in sustainable smart cities for Covid-19: network security and data preservation challenges with future directions. *Sustainable Cities and Society*, *75*, 103311. Recuperado de https://doi.org/10.1016/j.scs.2021.103311

Al-Sharafi, M. A., Arshah, R. A., Abo-Shanab, E. A., & Elayah, N. (2016). The effect of security and privacy perceptions on customers' trust to accept internet banking services: An extension of TAM. *Journal of Engineering and Applied sciences*, *11*(3), 545-552. Recuperado de https://doi.org/10.36478/jeasci.2016.545.552

AlHogail, A. (2018). Improving IoT technology adoption through improving consumer trust. *Technologies*, *6*(3), 64. Recuperado de https://doi.org/10.3390/technologies6030064

Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: the mediation role of risk perception. *IEEE Access*, *7*, 111341-111354. Recuperado de https://doi.org/10.1109/ACCESS.2019.2904006

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041. Recuperado de https://doi.org/10.2307/41409971

Benevolo, C., Dameri, R. P., & D'Auria, B. (2016). Smart mobility in smart city. In T. Torre, A. M. Braccini, & R. Spinelli (Eds.), *Empowering organizations* (Vol. 11, pp. 13-28). New York, NY: Springer Publishing.

Berrone, P., & Ricart, J. E. (2020). *IESE Cities in Motion Index 2020*. Pamplona, España: IESE Business School University of Navarra. Recuperado de https://media.iese.edu/research/pdfs/ST-0542-E.pdf

Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., & Debnath, N. C. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*, *61*, 102360. Recuperado de https://doi.org/10.1016/j.scs.2020.102360

Bibri, S. E. (2021). Data-driven smart sustainable cities of the future: an evidence synthesis approach to a comprehensive state-of the-art literature review. *Sustainable Futures*, *3*, 1000047. Recuperado de https://doi.org/10.1016/j.sftr.2021.100047

Boon-itt, S. (2019). Quality of health websites and their influence on perceived usefulness, trust and intention to use: an analysis from Thailand. *Journal of Innovation and Entrepreneurship*, *8*(1), 4. Recuperado de https://doi.org/10.1186/s13731-018-0100-9

Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society*, *39*, 499-507. Recuperado de https://doi.org/10.1016/j.scs.2018.02.039

Câmara Municipal de São Paulo. (2019, julho 16). *Regras para adequar São Paulo ao conceito de cidade inteligente são tema de projeto*. Recuperado de https://www.saopaulo.sp.leg.br/blog/regras-para-adequar-sao-paulo-ao-conceito-de-cidade-inteligente-sao-tema-de-projeto/

Ceccato, V. (2013). *Moving safely: crime and perceived safety in Stockholm's subway stations*. Lanham, MD: Lexington Books.

Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: a comparison of Facebook and LinkedIn. *Computers in Human Behavior*, *69*, 207-217. Recuperado de https://doi.org/10.1016/j.chb.2016.12.013

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, *35*(3), 445-459. Recuperado de https://doi.org/10.1016/j.giq.2018.04.002

Chin, W. W. (1998). The partial least squares approach for structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (2a ed., pp. 295-336). London, UK: Psychology Press.

Churchill, G. A., Jr. (1999). *Marketing research: methodological foundations* (8a ed.). Orlando, FL: Dryden Press.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2a ed.). New York, NY: Psychology Press.

Council of Europe. (2020). *Right to privacy*. Recuperado de https://www.coe.int/en/web/impact-convention-human-rights/right-to-privacy

Cui, F., Lin, D., & Qu, H. (2018). The impact of perceived security and consumer innovativeness on e-loyalty in online travel shopping. *Journal of Travel & Tourism Marketing*, *35*(6), 819-834. Recuperado de https://doi.org/10.1080/10548408.2017.1422452

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: challenges and opportunities. *IEEE Access*, *6*, 46134-46145. Recuperado de https://doi.org/10.1109/ACCESS.2018.2853985

Cunha, M. A., Przeybilovicz, E., Macaya, J. F. M., & Burgos, F. (2016). *Smart cities: transformação digital de cidades*. São Paulo, SP: Fundação Getulio Vargas. Recuperado de http://hdl.handle.net/10438/18386

Duhamel, T, Langerak, F., & Schillewaert, N. (1998). Non-probability sampling for WWW surveys: a comparison of methods. *International Journal of Market Research*, *40*(4), 1-13. Recuperado de https://doi.org/10.1177/147078539804000403

Eckhoff, D., & Wagner, I. (2018). Privacy in the smart city – applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, *20*(1), 489-516. Recuperado de https://doi.org/10.1109/COMST.2017.2748998

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491-497. Recuperado de https://doi.org/10.1016/j.jare.2014.02.006

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: tests for correlation and regression analyses. *Behavior Research Methods*, *41*, 1149-1160. Recuperado de https://doi.org/10.3758/BRM.41.4.1149

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N., & Meijers, E. (2007). *Smart cities – ranking of European medium-sized cities*. Vienna, Austria: Vienna University of Technology.

Gil-Garcia, J. R., Pardo, T. A., & Nam, T. (2015). What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization. *Information Polity*, *20*(1), 61-87. Recuperado de https://doi.org/10.3233/IP-150354

Grandhi, L. S., Grandhi, S., & Wibowo, S. (2021). A security – UTAUT framework for evaluating key security determinants in smart city adoption by the Australian city councils. In *Proceedings of the 21º ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, Ho Chi Minh City, Vietnam.

Habib, A., Alsmadi, D., & Prybutok, V. R. (2019). Factors that determine residents' acceptance of smart city technologies. *Behaviour & Information Technology*, *39*(6), 610-623. Recuperado de https://doi.org/10.1080/0144929X.2019.1693629

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: SAGE.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: SAGE.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. Recuperado de https://doi.org/10.1108/EBR-11-2018-0203

Haque, A. K. M., Brushan, B., & Dhiman, G. (2022). Conceptualizing smart city applications: requirements, architecture, security issues, and emerging trends. *Expert Systems*, *39*(5), e12753. Recuperado de https://doi.org/10.1111/exsy.12753

Hansen, J. M., Saridakis, G., & Benson, V. (2018) Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior*, *80*,197-206. Recuperado de https://doi.org/10.1016/j.chb.2017.11.010

Hasbini, M. A., Eldabi, T., & Aldallal, A. (2018). Investigating the information security management role in smart city organisations. *World Journal of Entrepreneurship, Management and Sustainable Development*, *14*(1), 86-98. Recuperado de https://doi.org/10.1108/WJEMSD-07-2017-0042

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135 Recuperado de https://doi.org/10.1007/s11747-014-0403-8

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: literature review and development of a smart city interaction framework. *Information Systems Frontiers*, *24*, 393-414. Recuperado de https://doi.org/10.1007/s10796-020-10044-1

Javed, A. R., Shahzad, F., Rehman, S. U., Zikria, Y. B., Razzak, I., Jalil, Z., … Xu, G. (2022). Future smart cities: requirements, emerging technologies, applications, challenges, and future aspects. *Cities*, *129*, 103794. Recuperado de https://doi.org/10.1016/j.cities.2022.103794

Kasar, S., & Kshirsagar, M. (2021). Open challenges in smart cities: privacy and security. In S. C. Tamane, N. Dey, & A. E. Hassanien (Eds.), *Security and privacy applications for smart city development* (pp. 25-36). New York, NY: Springer Publishing.

Kaushik, A. K., Agrawal, A. K., & Rahman, Z. (2015). Tourist behaviour towards self-service hotel technology adoption: trust and subjective norm as key antecedents. *Tourism Management Perspectives*, *16*, 278-289. Recuperado de https://doi.org/10.1016/j.tmp.2015.09.002

Lei nº 13.709, de 14 de agosto de 2018. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Recuperado de https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Malhotra, N. K. (2012). *Pesquisa de marketing: uma orientação aplicada*. Porto Alegre, RS: Bookman.

Meskaran, F., Ismail, Z., & Shanmugam, B. (2013). Online purchase intention: effects of trust and security perception. *Australian Journal of Basic and Applied Sciences*, *7*(6), 307-315. Recuperado de http://www.ajbasweb.com/old/ajbas/2013/April/307-315.pdf

Mittendorf, C. (2016). What Trust means in the Sharing Economy: A provider perspective on Airbnb.com. In *Proceedings of the 22º Americas Conference on Information Systems: Implications of Trust in Sharing Economy*, San Diego, CA.

Mushtaq, H., Jingdong, Y., Ahmed, M., & Ali, M. (2019). Building usage attitude for mobile shopping applications: an emerging market perspective. *International Journal of Management Science and Business Administration*, *5*(6), 21-28. Recuperado de https://doi.org/10.18775/ijmsba.1849-5664-5419.2014.56.1003

Ortega, J. M. E., & Román, M. V. G. (2011). Explaining physicians' acceptance of EHCR systems: an extension of TAM with trust and risk factors. *Computers in Human Behavior*, *27*(1), 319-332. Recuperado de https://doi.org/10.1016/j.chb.2010.08.010

Oyewo, B., Vo, X. V., & Akinsanmi, T. (2020). Strategy-related factors moderating the fit between management accounting practice sophistication and organisational effectiveness: the global management accounting principles (GMAP) perspective. *Revista Española de Financiación y Contabilidad*, 50(2), 187-223. Recuperado de https://doi.org/10.1080/02102412.2020.1774857

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: problems and prospects. *Journal of Management*, 12(4), 531-544. Recuperado de https://doi.org/10.1177/014920638601200408

Projeto de lei 01-00830/2017. (2017). Dispõe sobre regras para Smart Cities (cidades inteligentes) e da outras providências. São Paulo, SP: Câmara Municipal de São Paulo. Recuperado de http://documentacao.saopaulo.sp.leg.br/iah/fulltext/projeto/PL0830-2017.pdf

Rao, P. M., & Deebak, B. D. (2022). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambiental Intelligence and Humanized Computing*. Recuperado de https://doi.org/10.1007/s12652-022-03707-1

Ristvej, J., Lacinák, M., & Ondrejka, R. (2020). On smart city and safe city concepts. *Mobile Networks and Applications*, *25*(3), 836-845. Recuperado de https://doi.org/10.1007/s11036-020-01524-4

Sepasgozar, S. M. E., Hawken, S., Sargolzaei, S., & Foroozanfa, M. (2019). Implementing citizen centric technology in developing smart cities: a model for predicting the acceptance of urban technologies. *Technological Forecasting and Social Change*, *142*, 105-116. Recuperado de https://doi.org/10.1016/j.techfore.2018.09.012

Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2019). Security and privacy of smart cities: a survey, research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1718-1743. Recuperado de https://doi.org/10.1109/COMST.2018.2867288

Urban Systems. (2021). *Ranking connected smart cities*. São Paulo, SP: Autor. Recuperado de https://www.urbansystems.com.br

Urmetzer, F., & Walinski, I. (2014). User acceptance and mobile payment security. *International Journal of E-Services and Mobile Applications*, *6*(2), 37-66. Recuperado de https://doi.org/10.4018/ijesma.2014040104

Verma, P., & Sinha, N. (2018). Integrating perceived economic wellbeing to technology acceptance model: the case of mobile based agricultural extension service. *Technological Forecasting and Social Change*, *126*, 207-216. Recuperado de https://doi.org/10.1016/j.techfore.2017.08.013

Yamato, N., Hamada, Y., Dustan, P., Jimbo, H., Ward, I., & Isogaya, H. (2021). *Global Power City Index 2021*. Minato-ku, Tokyo: The Mori Memorial Foundation. Recuperado de https://mori-m-foundation.or.jp/pdf/GPCI2021_summary.pdf

Yu, Z., Song, L., Jiang, L., & Sharafi, O. K. (2021). Systematic literature review on the security challenges of blockchain in IoT-based smart cities. *Kybernetes*, *51*(1), 323-347. Recuperado de https://doi.org/10.1108/K-07-2020-0449

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: challenges and solutions. *IEEE Communications Magazine*, *55*(1), 122-129. Recuperado de https://doi.org/10.1109/MCOM.2017.1600267CM

Giulie Furtani Romani

https://orcid.org/0000-0002-4116-0997
Bacharel em Administração pela Escola Paulista de Política, Economia e Negócios (EPPEN) da Universidade Federal de São Paulo (UNIFESP). E-mail: giulieromani@gmail.com

Luis Hernan Contreras Pinochet

https://orcid.org/0000-0003-2088-5283
Professor doutor do Departamento Acadêmico de Administração (DAA) da Escola Paulista de Política, Economia e Negócios (EPPEN) da Universidade Federal de São Paulo (UNIFESP).
E-mail: luis.hernan@unifesp.br

Vanessa Itacaramby Pardim

https://orcid.org/0000-0003-0893-7271
Doutoranda em Administração pela Universidade de São Paulo, Faculdade de Economia, Administração, Contabilidade e Atuária (FEA-USP); Professora de Administração da Universidade Nove de Julho (UNINOVE).
E-mail: vanessa.itacaramby@usp.br

Cesar Alexandre de Souza

https://orcid.org/0000-0001-8941-8582
Professor doutor da Universidade de São Paulo, Faculdade de Economia, Administração, Contabilidade e Atuária (FEA-USP); Membro permanente do Programa de Pós-graduação stricto sensu em Administração.
E-mail: calesou@usp.br

CONTRIBUIÇÃO DOS AUTORES

Giulie Furtani Romani: Conceituação (Igual); Curadoria de dados (Liderança); Análise formal (Igual); Metodologia (Igual); Administração do projeto (Suporte); Recursos (Igual); Supervisão (Igual); Validação (Igual); Visualização (Igual); Escrita - rascunho original (Liderança); Escrita - revisão e edição (Igual).

Luis Hernan Contreras Pinochet: Conceituação (Igual); Curadoria de dados (Suporte); Análise formal (Igual); Metodologia (Liderança); Administração do projeto (Liderança); Recursos (Igual); Supervisão (Igual); Validação (Igual); Visualização (Igual); Escrita - rascunho original (Suporte); Escrita - revisão e edição (Igual).

Vanessa Itacaramby Pardim: Conceituação (Igual); Curadoria de dados (Suporte); Análise formal (Igual); Metodologia (Igual); Administração do projeto (Suporte); Recursos (Igual); Supervisão (Igual); Validação (Igual); Visualização (Igual); Escrita - rascunho original (Suporte); Escrita - revisão e edição (Igual).

Cesar Alexandre de Souza: Conceituação (Igual); Curadoria de dados (Suporte); Análise formal (Igual); Metodologia (Igual); Administração do projeto (Suporte); Recursos (Igual); Supervisão (Igual); Validação (Igual); Visualização (Igual); Escrita - rascunho original (Suporte); Escrita - revisão e edição (Igual).

APÊNDICE 1

QUADRO A1 DETALHAMENTO DO MODELO ESTRUTURAL

Constructo	Item	Assertiva	Referências
Propensão ao uso de Tecnologia de Cidades Inteligentes (PUTCI)	PUTCI1	Supondo que tenha acesso à tecnologia da cidade inteligente, eu planejo usá-la no cotidiano (p. ex.: aplicativos de carona, banco on-line, pagamento digital, entre outros).	Adaptado de Al-Sharafi et al. (2016)
	PUTCI2	Se na cidade em que moro tivesse disponível tecnologia de cidade inteligente, com certeza a usaria.	Adaptado de Al-Sharafi et al. (2016)
	PUTCI3	Eu encorajaria outras pessoas a usar tecnologia de cidade inteligente (p. ex.: aplicativos de carona, banco on-line, pagamento digital, entre outros).	Adaptado de Sepasgozar et al. (2019)
	PUTCI4*	Mesmo se eu tiver a opção de usar tecnologia de cidade inteligente (p. ex.: banco on-line, entre outros), ainda prefiro o atendimento físico dos serviços urbanos.	
Confiança (CO)	CO1	Soluções tecnológicas e aplicativos no geral são confiáveis.	Adaptado de Mittendorf (2016)
	CO2	Eu confio em soluções tecnológicas e aplicativos.	
	CO3	Eu penso que as soluções tecnológicas e os aplicativos são eficientes e confiáveis.	Adaptado de Mittendorf (2016)
	CO4*	Eu tendo a confiar na tecnologia da cidade inteligente, mesmo sabendo pouco sobre elas.	Abu-Shanab (2017)
Segurança Subjetiva (SS)	SS1*	Eu acho que a instituição ou empresa responsável pela tecnologia da cidade inteligente se preocupa com a segurança nas transações de informações.	Adaptado de L. Cui et al. (2018)
	SS2	Sinto-me confortável em usar tecnologia de cidade inteligente (p. ex.: banco on-line, aplicativos de transporte, veículos elétricos, entre outros).	Adaptado de Urmetzer e Walinski (2014)
	SS3	Acredito que a tecnologia de cidade inteligente (p. ex.: banco on-line, aplicativos de transporte, veículos elétricos, entre outros) é segura.	Adaptado de Urmetzer e Walinski (2014)
	SS4	Acredito que usar tecnologia de cidade inteligente para realizar tarefas no cotidiano (p. ex.: fazer compras) é seguro.	Adaptado de L. Cui et al. (2018)

Continua

Constructo	Item	Assertiva	Referências
Segurança Objetiva e Privacidade de Dados (SOPD)	SOPD1	Tecnologia de cidade inteligente possui estrutura legal e tecnológica (p. ex.: criptografia, sistemas atualizados de segurança, entre outros) que protege meus dados adequadamente.	Adaptado de Abu-Shanab (2017) e Sepasgozar et al. (2019)
	SOPD2	Tecnologia de cidade inteligente possui salvaguardas (proteções) suficientes para que eu me sinta confortável em usá-la.	Adaptado de Sepasgozar et al. (2019)
	SOPD3	Tecnologia de cidade inteligente tem capacidade de proteger minhas informações pessoais.	Adaptado de Abu-Shanab (2017)
Risco Percebido (RP)	RP1	Eu não me sinto seguro(a) para fornecer informações pessoais e dados confidenciais para a tecnologia da cidade inteligente.	Adaptado de Hansen et al. (2018)
	RP2	Existe um alto potencial de perda associado ao fornecimento de informações para a tecnologia da cidade inteligente.	
	RP3	No geral, seria arriscado fornecer informações para a tecnologia da cidade inteligente.	

Nota: *Itens excluídos no processo de ajuste do modelo (SEM-PLS).
Fonte: Elaborado pelos autores.

APÊNDICE 2

Programação Utilizada no Software R (Seminr)

```
library(seminr)
require(seminr)
measurements = constructs(
  composite("PUTCI", c("PUTCI1", "PUTCI2", "PUTCI3")),
  composite("CO", c("CO1", "CO2", "CO3")),
  composite("SS", c("SS2", "SS3", "SS4")),
  composite("SOPD", c("SOPD1", "SOPD2", "SOPD3")),
  composite("RP", c("RP1", "RP2", "RP3"))
)
structure = relationships(
  paths(from = "SOPD", to = c("SS")),
  paths(from = "SOPD", to = c("CO")),
  paths(from = "RP", to = c("SOPD")),
  paths(from = "RP", to = c("CO")),
  paths(from = "CO", to = c("SS")),
  paths(from = "CO", to = c("PUTCI")),
  paths(from = "SS", to = c("PUTCI")))
plot(structure)
pls__sem_model=estimate_pls(data=rap_r,
                            measurements,
                            structure,
                            inner_weights=path_weighting)
p3=summary(pls__sem_model, theme=t)
print(p3$descriptives,digits=3)
print(p3$reliability,digits=3)
print(p3$validity,digits=3)
print(p3$loadings,digits=3)
print(p3$paths,digits=3)
print(p3$fSquare,digits=3)
print(p3$composite_scores,digits = 3)
plot(pls__sem_model)
p4=bootstrap_model(pls__sem_model,nboot = 5000)
s2=summary(p4)
s2$bootstrapped_paths
# Inspect indirect effects
#specific_effect_significance(p4, from = "CO", through = "SS", to = "PUTCI", alpha = 0.05)
#specific_effect_significance(p4, from = "RP", through = "SOPD", to = "CO", alpha = 0.05)
#specific_effect_significance(p4, from = "SOPD", through = "CO", to = "SS", alpha = 0.05)
#find p-value
#p_value=2*pt(q="t score", df=599, lower.tail=FALSE)
#p_value
```