FGV EBAPE

RAP
BRAZILIAN JOURNAL OF PUBLIC ADMINISTRATION

Article

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

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 – Brazil
[2] Universidade de São Paulo / Faculdade de Economia, Administração, Contabilidade e Atuária, São Paulo / SP – Brazil

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.

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

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.

DOI: http://dx.doi.org/10.1590/0034-761220220145x
ISSN: 1982-3134
Article received on May 07, 2022 and accepted on January 16, 2023.
[Translated version] Note: All quotes in English translated by this article's translator.
Editor-in-chief:
Alketa Peci (Fundação Getulio Vargas, Rio de Janeiro / RJ – Brazil)
Associate editor:
Gabriela Spanghero Lotta (Fundação Getulio Vargas, São Paulo / SP – Brazil)
Reviewers:
Adilson Giovanini (Universidade do Estado de Santa Catarina, Florianópolis / SC – Brazil)
Teresa Cristina Monteiro Martins (Universidade Federal de Lavras, Lavras / MG – Brazil)
Peer review report: the peer review report is available at this URL.

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.

INTRODUCTION

The smart city has emerged as a new paradigm to dynamically optimize the environment, improve the quality of life of the inhabitants, the use of city resources (Sookhak, Tang, He, & F. R. Yu, 2019), increase sustainability and decrease damage to the environment (Rao & Deebak, 2022). These principles depend on a recipe of technical competence and optimization, technological inventions, and real-time data histories (Bhushan et al., 2020).

In this context, citizens will have continuous and ubiquitous access to information that will allow them to control their lives using collective technological intelligence, through which the city provides innovative and sustainable solutions based on Information and Communication Technology (ICT). Therefore, the objectives of a smart city are multifaceted (Elmaghraby & Losavio, 2014; Haque, Brushan, & Dhiman, 2022; Ismagilova, Hughes, Rana, & Dwivedi, 2020; Javed et al., 2022).

In this way, the proposal of a humanistic look at technical advances raises deeper discussions about the ethical and human aspects inherent in smart city initiatives. It occurs because smart cities evolve from technological innovations that threaten security and privacy expectations while creating new economic and social opportunities (Kasar & Kshirsagar, 2021).

In this sense, data security and privacy emerge as two new significant and complex challenges emerge (Adil & Khan, 2021). Security considers aspects such as illegal access to information and cyber-attacks, which can cause interruptions in the availability of services. Examples of these practices are privacy accounts for, for example, the use of data indiscriminately, without the user's consent or knowledge, as digital citizens are increasingly instrumentalized with available data about their location and activities (Sookhak et al., 2019).

The state-of-the-art literature on privacy and security in smart cities presents challenges that include preserving privacy with data, establishing data-sharing practices, and appropriate use of technology to encourage further exploration of smart city challenges prior to their construction (Braun, Fung, Iqbal, & Shah, 2018; Sookhak et al., 2019). In addition, the lack of privacy can result in social discrimination and enable a fundamentally unequal society (Eckhoff & Wagner, 2018), which requires cities to manage information and communication in the face of urban advances (Hasbini, Eldabi, & Aldallal, 2018; Javed et al., 2022). Thus, for there to be trust and acceptance of smart cities, it is necessary to integrate security mechanisms and preserve the privacy of users, which constitutes a gap that this research sought to explore (L. S. Grandhi, S. Grandhi, & Wibowo, 2021; Habib, Alsmadi, & Prybutok, 2019)the concept of Smart Cities has become an urgent necessity. It refers to an urban transformation which, using latest ICT technologies, makes cities more efficient. Composed of a growing Internet of networks, such as the one connecting humans via cellular systems, computers via broadband connections, or objects and sensors via low-cost data links, the greatest challenge today is to meaningfully manage such systems. Given that these systems will greatly impact human lives, issues related to privacy and security have come into limelight. With a surge in security breaches, not only in the Internet but also with mobile phones and now sensing infrastructures, engineers are very conscious to include privacy and security requirements into architectural designs from the very beginning. This paper summarizes the key challenges, emerging technology standards, and issues to be watched out for in the context of privacy and security in smart cities. A key observations is that privacy can be achieved i.

Thus, this study aims to investigate citizens' perception of security and trust in smart city technology and how it affects their propensity to use it and, consequently, life in the city.

The study is justified because the concept of 'smart cities' is gaining importance due to the exponential growth of urban populations and the need to expand the city's capacity, better manage its resources, increase the quality of life of citizens, and optimize the efficiency and quality of services provided (Habib et al., 2019), mainly by government entities and companies (Kasar & Kshirsagar, 2021). In addition, constructing a smart city depends on the intensive collection of data that can innovatively and creatively be used to create integrated applications that improve city services and the use of its resources. The data-driven culture is becoming increasingly vital as data and information are used more intensely (Bibri, 2021).

Finally, this research seeks to contribute to deepening the topic of security and privacy to understand the concepts and assumptions involved by proposing developing a new theoretical model adapted from the literature related to the topic (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), with components associated with trust and safety (objective and subjective) that affect the propensity to use technologies in smart cities, focusing on citizen behavior. For this purpose, we conducted a survey (n = 601) in the city of São Paulo and used the PLS-SEM to test the formulated hypotheses.

2. THEORETICAL BACKGROUND

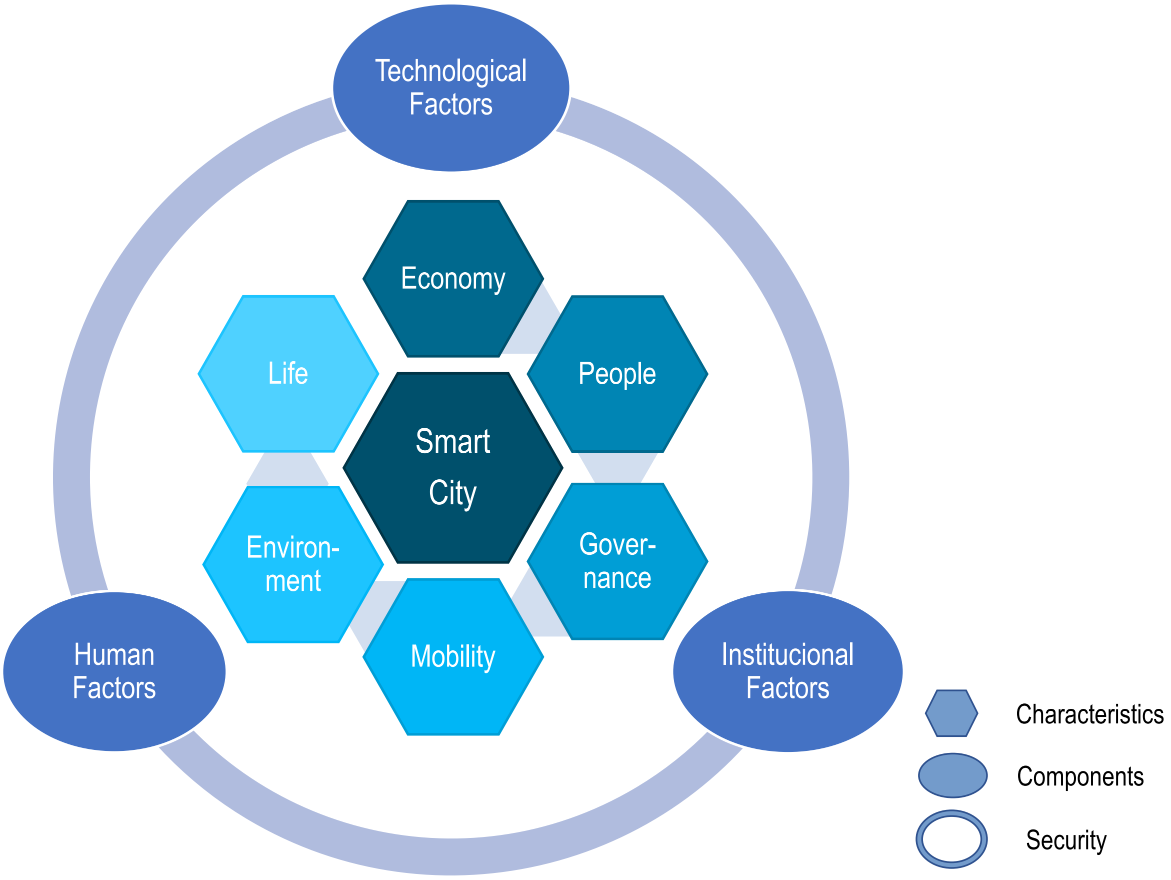
2.1. Smart cities, components, and their characteristics

One of the definitions of a smart city corresponds to a place where Information and Communication Technology (ICT) is combined with infrastructure, architecture, objects, and people to improve processes and address social, economic, and environmental problems. This enables smart devices to connect to the existing infrastructure to optimize the quality of life and productivity in cities, as well as solve problems through solutions based on these technologies and in government partnerships with various stakeholders (Bhushan et al., 2020; Habib et al., 2019; Rao & Deebak, 2022).

The literature review indicates that the main focus of the smart city is the advancement of ICTs. They are a crucial ingredient in smart city development. They are the creators and users of services and technology, the most significant source of ideas and feedback about the city (Elmaghraby & Losavio, 2014; Ismagilova et al., 2020). However, different disciplines are proposing definitions that transcend the idea of the mechanic and encompass more than just this factor, considering a primordial aspect: citizens (Hasbini et al., 2018; Javed et al., 2022).

In short, a smart city is one "that has collective intelligence, environmental responsibility, promotes social development, and stimulates balanced economic growth throughout the city's territory" (Projeto de Lei 01-00830/2017) to minimize the economic and social costs (Câmara Municipal de São Paulo, 2019). In this way, an attempt is made to use ICTs together with human capital to solve urban problems and improve processes within the city, seeking to promote improving citizens' quality of life.

FIGURE 1 COMPONENTS AND CHARACTERISTICS OF SMART CITY



Source: Adapted from Ristvej, Lacinák, and Ondrejka (2020).

There are several ICTs found in smart cities, including Big Data, Cloud and Edge Computing, Artificial Intelligence (AI), the Internet of Things (IoT), Blockchain, and Geospatial Technology. However, more than these emerging technologies can be cited when it comes to applications in smart cities, as many possibilities arise with innovation (Z. Yu, Song, Jiang, & Sharafi, 2021). Given this, it is important to emphasize that there is only a smart city with technology and innovation, as these factors differentiate it from an ordinary city (Eckhoff & Wagner, 2018).

Thus, studying the archetype formulated and adapted by Ristvej et al. (2020) makes it possible to understand the smart city (Figure 1). Three essential components characterize the concept: Technological Factors (ICTs), Human Factors (input from citizens), and Institutional Factors (elements that enable collectivity, such as policies and regulations). These enablers and resources drive the six characteristics (Economy, Mobility, Environment, People, Life, and Governance). Some elements of the components belong to a specific characteristic (such as recycling systems). In contrast, others are horizontal or enablers (such as Big Data and IoT), covering several characteristics, as formulated by Giffinger et al. (2007) and presented in Box 1.

BOX 1 FEATURES OF A SMART CITY

Characteristic	Definition	Author
Smart Economy	[…] knowledge-based economy, promoting creativity […] public-private partnerships and international connections (research exchange). Innovation capacity.	Cunha, Przeybilovicz, Macaya, and Burgos (2016)
Smart People	[…] citizens are the greatest source of urban development and driving force for knowledge creation, better education, social infrastructure, and fostering creativity with collective intelligence.	Gil-Garcia, Pardo, and Nam (2015)
Smart Governance	[…] based on transparency, public participation, interaction with public and private agents, cooperation, and free access to information data through ICTs. The structure allows collaboration, data exchange, service integration, and city administration communication.	Giffinger et al. (2007)
Smart Mobility	[…] transport resources and technological infrastructure of the city to manage the flow of demand and movement of the population. Accessibility is essential to promote greater social inclusion and avoid the isolation of modern urban ghettos.	Benevolo, Dameri, and D'Auria (2016)
Smart Environment	[…] attractive natural conditions, resource management, and environmental protection efforts (sustainability). It seeks to reduce the impacts caused by urbanization with the help of technology, proposing optimized alternatives for environmental management problems. In addition, it is essential to have awareness projects.	Braun et al. (2018); Giffinger et al. (2007)
Smart Life	[…] increased quality of life, accessibility, practicality, and efficiency in the relationship with the city. From the perception of safety and housing conditions to access to health and education resources. Greater focus is on integrating with the city, seeking greater social cohesion and a sense of community belonging.	Cunha et al. (2016); Giffinger et al. (2007)

Source: Elaborated by the authors.

The concept of security permeates all the characteristics proposed by Giffinger et al. (2007) in the context of the smart city and is a crucial component for its entire structure closely linked to technology. Several studies use these characteristics to organize smart cities into analytical categories (Elmaghraby & Losavio, 2014; Ismagilova et al., 2020).

2.2. Security and privacy in the smart city

When analyzing the security and privacy challenges of smart cities, it is important to realize that many of them already exist in everyday reality, although they do not offer as much impact in the present as they would in the fully interconnected context of the smart city (Adil & Khan, 2021; Braun et al., 2018; Javed et al., 2022).

The smart city requires the highest levels of security, as it is mainly composed of digital technology that is intensive in data collection and analysis, a critical element in the infrastructure of this future society. Many innovations related to the concept seek a way to improve and make more services available through technology and applications for stakeholders in the city system (Habib et al., 2019). Thus, it is necessary to have a comprehensive architecture, with security built in from the beginning, to obtain citizens' trust and acceptance of the smart city (Kasar & Kshirsagar, 2021).

L. Cui et al. (2018) state that a smart city's infrastructure comprises thousands of devices and applications that aim to improve processes and provide benefits to citizens, such as smart healthcare and smart home. However, the use of these applications and systems can bring several problems related to security and privacy (Adil & Khan, 2021) due to vulnerabilities in this intelligent system since they not only collect a wide variety of sensitive information from people and their social circles but also control city facilities and influence citizens' lives (Zhang et al., 2017).

Braun et al. (2018) mention that security is dynamic and not stagnant. It is an effort to prevent damage by digital and physical means, both direct and indirect. In a smart city, security can be considered a general component, as it encompasses all the characteristics of the city. It is also included in all aspects that compose it (Ristvej et al., 2020).

Thus, safety is an essential condition that can be seen as a hygiene factor (which leads to dissatisfaction if not contemplated) and is one of the most critical items in technology acceptance surveys (AlHogail, 2018; L. S. Grandhi et al., 2021; Sepasgozar et al., 2019; Urmetzer & Walinski, 2014)cyber security has become a major concern for smart cities adoption, due to interconnectedness of intelligent devices and the use of public networks. Literature presents the significance of security models for the adoption of smart cities, but these are limited to identifying one or few security related factors. To investigate the security determinants by focusing on the user intentions to adopt smart cities, the Security-Unified Theory of Acceptance and Use of Technology (UTAUT). Furthermore, its understanding encompasses much more than just technical factors, having a solid aspect dependent on the human factor in all its functionality (Braun et al., 2018); it also includes subjective facets related to the perception of individuals. Thus, the concept is divided into two dimensions of security, objective and subjective (Ceccato, 2013; Meskaran, Ismail, & Shanmugam, 2013).

Objective security is the 'tangible' aspect of technical protection based on cryptography, the declaration of security policies, and knowledge of 'statistical' risks (Ceccato, 2013). In other words, it means having protection ensured by a technological solution and being rationally aware of what constitutes a threat and the mechanisms that guarantee security. Alternatively, subjective safety is quite 'intangible'. It is the feeling or perception that the user has about their safety in a given environment or situation. It can be easily influenced by external factors, such as trust and the opinion of friends, family, and even third parties. In the context of smart city technology, if this feeling tells the individual there may be a security problem, this potential user will not become a real user, even if it is guaranteed, from a technological point of view (Urmetzer & Walinski, 2014). It means that even with the best approaches and technical solutions, disregarding citizens' perceptions of security can become irrelevant.

It is important to highlight that the two dimensions – objective and subjective safety – are neither disjoint nor independent (Ceccato, 2013; F. Cui et al., 2018). However, the subjective perception of security of individuals does not affect the objective measures of security, while the opposite occurs.

Thus, privacy is a complex concept, initially considered a fundamental right by the European Convention on Human Rights (1950) and established as 'respect for private life' (Council of Europe, 2020). Since then, there have been several attempts to define better the concept of privacy that adapts to each new change in reality. More recently, it has been described as contextual integrity (Eckhoff & Wagner, 2018). That is, there is a need to understand the context in which the concept is inserted so that it is possible to establish the limits of individual integrity.

In the technological context, data privacy is related to how this information is collected, shared, and used, guaranteeing that data manipulation will not occur without the user's authorization (S. E. Chang, Liu, & Shen, 2017). Therefore, this presents as a major challenge in the current context due to the growing flow of information and expanding using monitoring technology, among others (Adil & Khan, 2021).

Many citizens do not realize – or do not know – the risks they run when providing their information online, in applications or websites, and the possibility of having their data sold to third parties. With tools like Big Data and People Analytics, accessing consumer information is a great source of competitive advantage for companies and institutions (Y. Chang, Wong, Libaque-Saenz, & Lee, 2018). However, there needs to be a limit to that freedom to preserve individual integrity.

It is important to point out that Brazil only recently created legislation capable of delimiting and regulating the use of sensitive data by third parties. Thus, in August 2020, the General Data Protection Law (Lei nº 13.709, de 14 de agosto de 2018) established rules and special protection for processing 'sensitive personal data'.

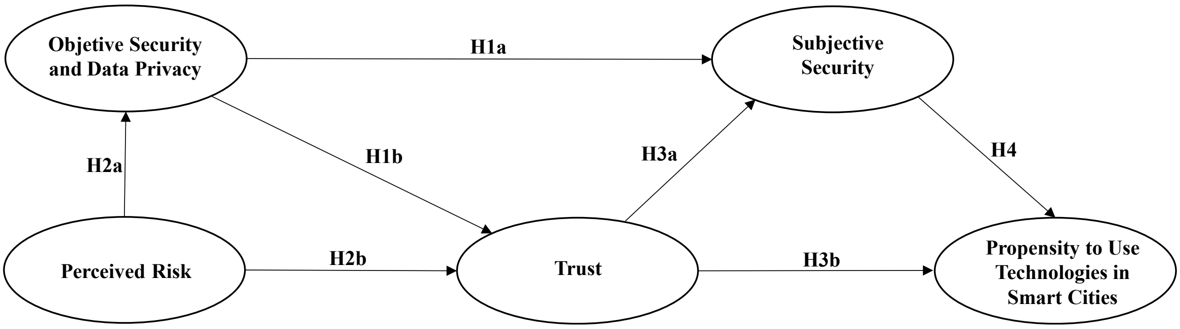
Finally, there are still common threats such as viruses and communication interception, server invasion, and leaking of sensitive information, these being some of the leading causes of privacy violations (L. Cui et al., 2018). Thus, it is necessary to understand the dangers and create barriers to keep users safe (Alraja, Farooque, & Khashab, 2019; L. Cui et al., 2018; Eckhoff & Wagner, 2018).

2.3. Construction of the model and research hypotheses

We formed constructs and hypotheses based on an extensive literature review to identify the key aspects influencing users' behavioral intention to use and continue using smart city technology.

Figure 2 represents the proposed research model with the constructs and formulated hypotheses. The following subsections contemplate the respective definitions.

FIGURE 2 RESEARCH MODEL


Objective Security and Data Privacy
H1a
Subjective Security
H2a
H1b
H3a
H4
Perceived Risk
H2b
Trust
H3b
Propensity to Use Technologies in Smart Cities

Source: Elaborated by the authors.

2.3.1. Objective Security and Data Privacy (OSDP)

Objective security is a tangible technical characteristic because it is strongly related to technical technology issues; it is convenient to combine the concepts of objective security and data privacy. In the smart city context, it is the actual technological solution, such as antivirus and encryption (Urmetzer & Walinski, 2014). Regarding data privacy, structural guarantees are the main factors that influence trust.

In the context of the smart city, the existence of objective security and data privacy is a critical factor for the development of citizens' subjective security and trust (Ortega & Román, 2011), as it is a guarantee that they have safeguards, both in terms of the provision of service or product purchased regarding the leakage or inappropriate use of personal information (S. E. Chang et al., 2017).

Furthermore, the level of technical protection influences the individual's perception of safety or subjective security, as discussed in the literature. In this context, a considerable level of objective security is necessary, capable of influencing the individual's perception of security and trust in the technology so that he can adopt it. Therefore, we established the following hypotheses:

H1a: OSDP has a positive influence on SS.

H1b: OSDP has a positive influence on TR.

2.3.2. Perceived Risk (PR)

According to Alraja et al. (2019), perceived risk is the subjective judgment people make about the characteristics and severity of a risk, which are generally associated with a product or service. In the context of smart cities, perceived risks are primarily related to technology due to its substantial presence in products and services, such as IoT, which forms the basis of city life (AlHogail, 2018; Ismagilova et al., 2020; Z. Yu et al., 2021).

The feeling of lack of control, whether over data or technology, is one of the aggravating factors of a greater perception of risk, causing an incompatibility between the actual risk level, objective security, and data privacy, as well as the individual trust in technology observed in the 'objective security and data privacy' construct (AlHogail, 2018). Furthermore, several studies mention perceived risk as a predictor of a strong negative influence on trust (Meskaran et al., 2013). Thus, we formed the following hypotheses:

H2a: PR has a negative influence on OSDP.
H2b: PR has a negative influence on TR.

2.3.3. Trust (TR)

Trust corresponds to the expectations of what other people will do in the future based on previous experiences and is a crucial factor for establishing relationships, especially in environments with uncertainty and risk, such as online transactions (Mittendorf, 2016). In this way, it is mainly applied in the context of relations between user and technology since there are not always clear rules and regulations, as trust is decisive for this link to be established. In the context of technology, trust is consolidated in the personal guarantee that the institution behind the service (or product) will fulfill its obligations, will behave as expected (it will not take advantage of vulnerabilities), and will value the satisfaction and well-being of the customer (the user's expectations will be delivered) (Mushtaq, Jingdong, Ahmed, & Ali, 2019). In this way, it is considered that trust plays an essential role in subjective security and the adoption of technology in smart cities, so we formulated the following hypotheses:

H3a: TR has a positive influence on SS.
H3b: TR has a positive influence on PUTSC.

2.3.4. Subjective Security (SS)

Subjective security is the intangible aspect of security, the user's perceived feeling about security in general, which is influenced by social opinion and already established beliefs, in addition to the objective security factor and data privacy (Urmetzer & Walinski, 2014). Research indicates that safety is not just a technical issue but a human and organizational one (Meskaran et al., 2013). By recognizing the impact of subjective safety on the individual's propensity, many studies investigated the influence of perceived safety (subjective) rather than objective safety (F. Cui et al., 2018).

In the context of the smart city, it is the perceived feeling that the user (potential or not) has about how secure the technology is, regardless of the technical safeguards (i.e., encryption) that it has (Urmetzer & Walinski, 2014). Furthermore, especially in the case of developing countries, there is a stronger need for the perception of security so that there is acceptance and use of new technologies (AlHogail, 2018; Sepasgozar et al., 2019). Therefore, we generated the following hypothesis:

H4: SS has a positive influence on PUTSC.

2.3.5. Propensity for the Use of Technology in Smart Cities (PUTSC)

Behavioral intention is one of the critical constructs of technology acceptance models derived from the theory of Reasoned Action (L. S. Grandhi et al., 2021; Sepasgozar et al., 2019; Verma & Sinha, 2018). Such models seek to explain and anticipate individuals' disposition about accepting information technology. Thus, this construct represents the user's intention to act on the object of study affected by a set of proposed variables.

In the context of this research, this construct was defined as the 'propensity to use technology in smart cities' (Al-Sharafi et al., 2016; Sepasgozar et al., 2019), being the dependent variable of the study, which is influenced by the variables: trust (Abu-Shanab, 2017; Mittendorf, 2016), subjective security (F. Cui et al., 2018; Urmetzer & Walinski, 2014), objective security and data privacy (Abu-Shanab, 2017; Sepasgozar et al., 2019), and perceived risk (Hansen et al., 2018).

3. METHOD

3.1. Sample choice and characterization

This study is classified as empirical exploratory-descriptive, and the research approach adopted was quantitative with a cross-section. The sample is non-probabilistic and was constituted by convenience (Duhamel, Langerak, & Schillewaert, 1998).

In exploratory-descriptive empirical studies, the sample's representativeness becomes a secondary concern since the main objective is to analyze the phenomenon and not to extrapolate the results to the population (Churchill, 1999). In addition, heterogeneity is important so that the research is not restricted to a specific group of technology users. That is, it encompasses greater diversity within the characterization of the sample.

Thus, as a criterion, we only selected individuals who would be able to carry out a more accurate assessment of the consumption of technology offered by the city of São Paulo due to their level of digital literacy and access to technology. Therefore, respondents would need to be smartphone and app users, which would make them potential users searching for information about services provided by the city to serve citizens (Oyewo, Vo, & Akinsanmi, 2020).

We chose São Paulo because, in the Connected Smart Cities rankings, Urban Systems ranked it the most innovative city in Brazil (Urban Systems, 2021); it occupies the 42nd position globally, according to the Global Power City Index 2021 (Yamato et al., 2021).

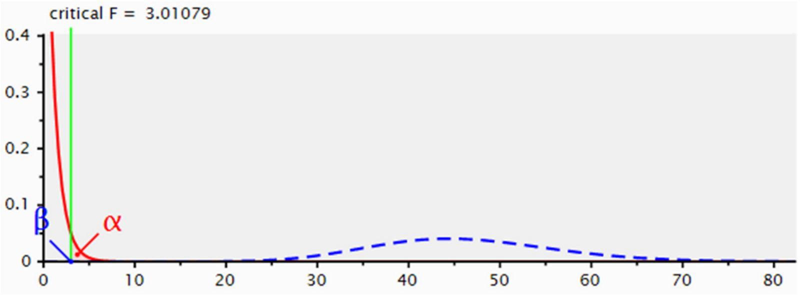
We conducted the survey between December 2022 and January 2023 using an online questionnaire distributed by the QuestionPro service. Before that, the research instrument underwent a reverse translation analyzed by specialists. Next, we performed a pre-test with 40 respondents to validate the instrument.

We performed the data purification step on the 631 complete responses using the Mahalanobis distance criterion (D^2) to identify outliers. This process eliminated 30 records, resulting in 601 valid questionnaires tabulated in a spreadsheet, which we subsequently analyzed using SPSS 25 and R Studio Build 353 software (see Appendix 2).

3.2. Sample calculation

We used the G*Power 3.1.9 software (Faul, Erdfelder, Buchner, & Lang, 2009) to estimate the minimum sample size for this research. The construct that receives the highest number of relationships (arrows) or has the highest number of predictors is evaluated in the proposed model. For the a priori calculation, before data collection, it should be noted that there are two parameters: the test power ($Power = 1- \beta_{erro\ prob\ II}$) and the effect size ($f^2$). Cohen (1998) and Hair, Hult, Ringle, and Sarstedt (2014) recommend using the power of 0.80 and the f^2 median = 0.15. Therefore, a minimum sample to be used is suggested. Figure 3 shows the result of the software. However, in a post hoc test, it is possible to observe the ideal sample with the sample power at 100%. The proposed model brings the number of predictors to 2, making conducting the research with only 68 respondents possible. However, in a post hoc analysis, it was observed that, with 601 respondents, the parameters obtained were $F_{critical}$ = 3.010 and sample power 100% (Figure 3).

FIGURE 3 POST HOC SAMPLE EFFECT SIZE TEST



Source: G*Power software.

3.3. Research Instrument

The research instrument was composed of adapted psychometric scales (see Appendix 1) and also had introductory questions and a sociodemographic part to identify the respondent's profile. We built the model with 18 questions anchored on a five-point Likert scale (1 – 'totally disagree' to 5 – 'totally agree'). To test the hypothesis, the analysis used the multivariate data technique through structural equation modeling, with estimation by partial least squares (PLS-SEM).

3.4. The choice of method

We identified PLS-SEM as the most suitable analysis method for four main reasons: first, to maximize the variance of endogenous variables explained by exogenous variables. Second, it does not require normality for data distribution to be met, which is ideal in applied social sciences that tend to have distortions due to asymmetry and/or kurtosis. Third, it is ideal for estimating new and complex models. Finally, it is preferred for interaction tests since it does not inflate the measurement error (Hair, Risher, Sarstedt, & Ringle, 2019). To operationalize the method, we used the R software (SEMinR).

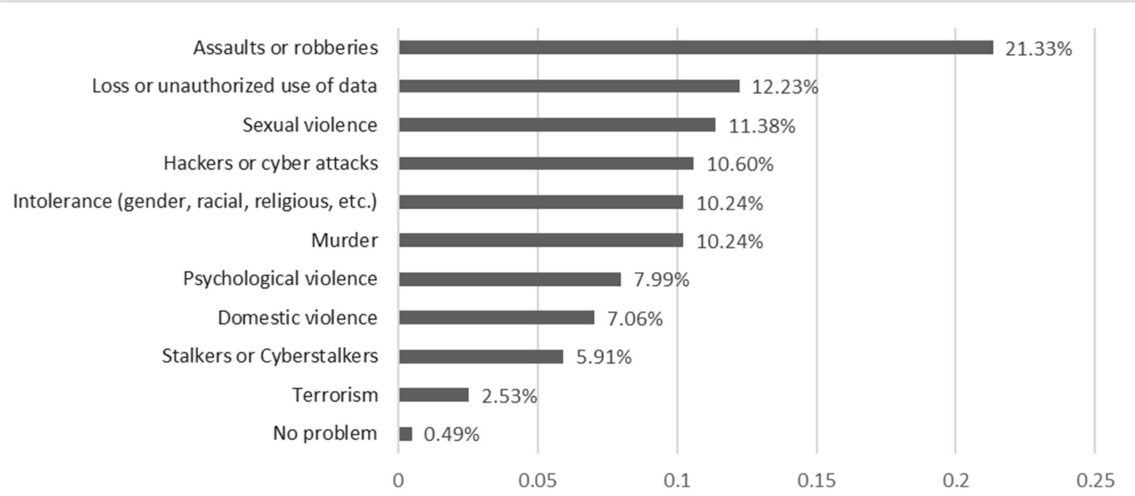
4. DATA PRESENTATION AND ANALYSIS

4.1. Characterization of respondents

When analyzing the sociodemographic data of the sample, a slight predominance of females (57.9%/n = 348) is evident compared to male respondents (42.1%/n = 253). Furthermore, in terms of age group, a large part of the sample is between 18 and 27 years old (61.04% /n = 367).

This study notes that citizens' reality shapes security concerns. In the city of São Paulo, there is concern about the high rates of primary violence. That is, people, for the most part, still have the basic need to protect their physical integrity, which is a characteristic arising from the sociocultural scenario of the country, which the smart city concept seeks to alleviate and, ideally, mitigate.

GRAPH 1 SECURITY ISSUES IN THE CITY



Source: Elaborated by the authors.

Among the five main problems in city security (Graph 1) is the 'loss or unauthorized use of data,' an issue more related to the smart city scenario, which came in second place compared to public safety issues. Thus, this concern has been growing and is relevant because of the scenario of technological evolution, which cannot only cause harm in itself but can facilitate and contribute to other crimes. In addition, the four main items mentioned can also be linked to data and information from citizens on mobile devices.

4.2. Normality, common method bias, non-response bias, and collinearity

Mardia's multivariate test verified data normality. The results obtained for the indicators were highly significant, with $p < 0.001$, indicating no normality, which was expected and necessary for the use of PLS-SEM.

Since the data are primary, it was necessary to ensure that no systematic bias influenced the collected information. Thus, applying Harman's single-factor test verified the common method bias (Podsakoff & Organ, 1986) in the 15 items. The variance extracted from the first component was 39.75%, below the minimum of 50%, which validates the test. In addition, we performed the non-response bias analysis, which sought to compare two subsamples in a t-test to verify whether there was a difference between the means, which was not found, so it was possible to carry out the research with the total sample.

Concerning the predictor variables related to the dependent variable 'propensity to use technologies in a smart city,' it was possible to verify there was no multicollinearity in the model since all the values of the Variance Inflation Factors (VIFs) of the constructs were below 3.3, with the respective values: OSDP = 1.820; PR = 1.950; PUTSC = 1.993; SS = 2.276; and TR = 1.690.

4.3. Structural equation modeling

After adjusting the model in the first iteration, we presented the results of the factor loadings and the analysis of the measurement model to adjust the discriminant validity. We excluded variables with factor loadings < 0.7 (SS1, TR4, and PUTSC4) to obtain more adequate results (Malhotra, 2012). The analysis of the measurement model must precede the analysis of the relationships between the constructs or latent variables. The next step was to examine the measurement model (Table 1): Cronbach's alpha (CA), composite reliability (CR), average variance extracted (AVE), and determination coefficients (R^2) (Hair, Hult, Ringle, & Sarstedt, 2017).

TABLE 1 CONVERGENT AND DISCRIMINANT VALIDITY

Constructs					Discriminant				
	CA	CR	AVE	R²	(1)	(2)	(3)	(4)	(5)
(1) Objective Security and Data Privacy	0.837	0.902	0.754	0.032	0.868				
(2) Perceived Risk	0.782	0.873	0.696		-0.178	0.834			
(3) Propensity to Use Technologies in Smart Cities	0.820	0.893	0.736	0.232	0.322	-0.190	0.858		
(4) Subjective Security	0.812	0.889	0.727	0.576	0.618	-0.262	0.474	0.853	
(5) Trust	0.856	0.912	0.777	0.314	0.540	-0.242	0.53	0.705	0.881

*CA: Cronbach's alpha (> 0.6); CR: composite reliability (> 0.7); AVE: average variance extracted (> 0.5).
Note: the highlighted diagonal shows the square roots of the AVE by the Fornell-Larcker Criterion.
Source: Software R (SEMinR).

Since all variables in a questionnaire use the same measurement scale, the coefficient is calculated based on the variance of individual items. CAs were considered moderate; CRs and AVEs were very good and acceptable. Thus, the CA coefficients indicated high internal consistency of the scales used, as well as the CRs (Hair et al., 2017) and the AVEs (Chin, 1998), for indicating the existence of convergent validity. In addition, we added the heterotrait-monotrait ratio (HTMT) criterion. According to Henseler, Ringle, and Sarstedt (2015), the HTMT value must be below 0.90, which means that discriminant validity has been established between two reflective constructs. In Table 2, it is observed that this criterion was also met.

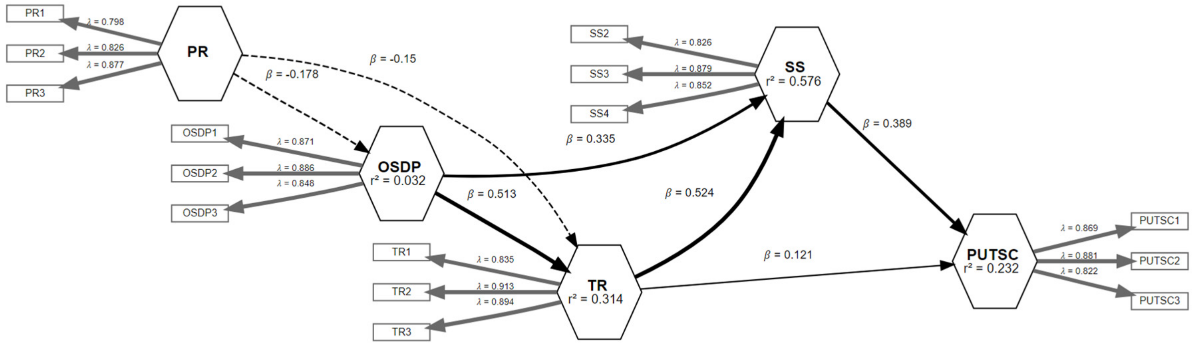
TABLE 2 PRESENTATION OF THE HTMT CRITERION

	OSDP	PR	PUTSC	SS	TR
OSDP	.	.	.	.	.
PR	0.218	.	.	.	.
PUTSC	0.387	0.235	.	.	.
SS	0.748	0.325	0.583	.	.
TR	0.639	0.290	0.468	0.841	.

Source: Software R (SEMinR).

In the practical application of structural equation modeling for the proposed research model (Figure 4), the measurements performed individually for each construct are observed to verify its validity and internal and external consistency, as well as the results obtained in its paths and hypotheses.

FIGURE 4 RESULTS OF THE PROPOSED RESEARCH MODEL



Note: solid lines, positive relationship; dashed lines, negative relationship.
Source: Software R (SEMinR).

The model was estimated using the bootstrapping technique (Table 3), and this process compared the original sample with the generated samples (Chin, 1998). The results of the path significance analysis supported all hypotheses. In addition, we found that all three mediations proposed in the model were partial. That is, both the direct and the indirect relationship had similar significant results.

TABLE 3 PATH AND HYPOTHESES

Hypotheses	β	*Bootstrapping* (n = 5000)	Standard deviation	T Test	P Value	CI 2.5% 97.5%
Direct relationship						
H1a: OSDP SS	0.335	0.335	0.038	8.887	0.000	0.262 0.409
H1b: OSDP TR	0.513	0.513	0.037	13.906	0.000	0.437 0.582
H2a: PR OSDP	-0.178	-0.181	0.044	-4.097	0.000	-0.266 -0.096
H2b: PR TR	-0.150	-0.152	0.035	-4.337	0.000	-0.219 -0.085
H3a: TR SS	0.524	0.524	0.036	14.540	0.000	0.452 0.591

Continue

Hypotheses	β	*Bootstrapping* (n = 5000)	Standard deviation	T Test	P Value	CI 2.5% 97.5%
H3b: TR PUTSC	0.121	0.121	0.053	2.277	0.023	0.014 0.224
H4: SS PUTSC	0.389	0.389	0.059	6.629	0.000	0.275 0.504
Indirect relationships (mediators)						
M1: PR OSDP TR	-0.091	-0.092	0.022	-4.080	0.000	-0.136 -0.049
M2: OSDP TR SS	0.268	0.268	0.026	10.265	0.000	-0.218 0.320
M3: TR SS PUTSC	0.204	0.203	0.035	5.802	0.000	0.137 0.276

Source: Elaborated by the authors.

5. DISCUSSION OF THE RESULTS

When analyzing the hypotheses formulated (Table 3), we observed that the proposed model was able to identify, based on the literature, a robust pattern for the theme of propensity to use (Boon-itt, 2019) widely used in technology acceptance surveys (L. S. Grandhi et al., 2021). In addition, this research contributes to the perception of citizens that, when using smart city technology, they will gain an advantage over traditional systems, showing an understanding that technology has the potential to facilitate life in the urban environment.

Since technology is basically what moves the city, for greater adherence to the smart city concept, promoting this perception of value is necessary. By observing the collected sample, it is possible to notice that the ease of access and the frequency of use reinforce a strong perception of the usefulness of the technology.

Hypothesis H1a with the path 'SOPD → SS' was supported ($\beta = 0.335$; $p < 0.001$), corroborating Linck's (2006) concept that the technical protection of a system has a strong influence on the user's perception of security. It is because a large part of the formation of individuals' conception of security, in general, is based on physical and tangible issues, which, in the technological context, are translated as cryptography, antivirus, and authentication, among others.

Similarly, when analyzing the characteristics of the sample, a strong perception of the value of personal information was identified, as well as a significant concern with the loss and misuse of data. The same happened with hypothesis H1b with the path 'SOPD → CO' ($\beta = 0.513$; $p < 0.001$), which presented the second most significant effect of all hypotheses. In this case, the safeguards must be evident so that the potential user can feel more confident and, consequently, prone to expose their vulnerabilities and give the technology a chance.

The negative relationship of hypothesis H2a with the path 'PR→OSDP' ($\beta = -0.178$; $p < 0.001$) was also supported. It occurred because it comprises two opposing ideas; that is, when high technical security against possible threats and inappropriate use of information is found, the tendency is to minimize the perception of the existence of risks. Thus, by preventing counterattacks and establishing rules for using the information obtained, institutions are more likely to increase adherence to their products and services (Habib et al., 2019).

Likewise, the negative relationship of hypothesis H2b with the path 'PR→TR' ($\beta = -0.150$; $p < 0.001$) was supported, as expected, corroborating the idea that it is a predictor of significant influence on the confidence variable that has a negative and inverse relationship (Meskaran et al., 2013). In the context of smart cities, it is a concern mostly related to the availability of information on the network, even on well-known websites or applications. Such apprehension is due to the uncertainty regarding the use of personal data by the institution and third parties in the event of a possible leak, considering that this can cause various damages to the individual.

Hypothesis H3a with path 'TR→SS' ($\beta = 0.524$; $p < 0.001$) was supported with the most significant effect among all hypotheses. It shows that the perception of security is an essential element for trust, especially given the technological context of the smart city, which brings risks and insecurity. This is evident in the case of data loss or unauthorized use, as highlighted by respondents (Graph 1). Negligence in this regard can lead to a loss of confidence in the institutions that perform this type of service due to the exposure of registration data of individuals and companies (Adil & Khan, 2021; Kasar & Kshirsagar, 2021; Meskaran et al., 2013). Thus, to obtain and maintain users' trust, the institutions behind technology services need to be attentive to the opinion of their users and society about it to maintain a good reputation so that they can, thus, conquer a positive perception of safety.

Next, hypothesis H3b with the path 'TR→PUTSC' ($\beta = 0.121$; $p = 0.023$), was supported. It shows that the citizens' perception is that technology should bring the expected confidence and that this does not happen just by its presence. The effect of technology in smart cities can boost its value and advantages and make its intention to use stronger. However, as observed by mediation (M3; $\beta = 0.204$; $p < 0.001$), the perception of technology's subjective security of individuals is what enables greater confidence in the propensity to use technology in smart cities (Mushtaq et al., 2019).

Thus, subjective security proved to be a construct of fundamental importance in this study to establish relationships in the context of the smart city, which is still an environment with a certain degree of uncertainty and risk. It indicates that an individual's perception of technology security in the smart city varies according to society's view (Kaushik, Agrawal, & Rahman, 2015; Meskaran et al., 2013), especially what they think the people consider important to the individual. It also confirms that trust in the technology can be built based on positive feedback from other users.

Hypothesis H4 supported the relationship 'SS→PUTCI' ($\beta = 0.389$; $p < 0.001$), indicating that subjective safety is a predictor that explains the propensity to use technology in smart cities, for example, to carry out transactions, use services urban mobility, and believe in platform safety.

Finally, the relationships involving the construct 'objective security and data privacy' confirmed the strong influence of 'tangible' barriers in reinforcing the 'intangible' perception of 'subjective security'.

The results confirmed that the proposed model demonstrated consistency, with adequate adjustments, so it can be replicated in future research. The article brings as a contribution an important discussion about the need for the privacy standards inserted in the 'subjective security' construct to be incorporated into the aspects of 'trust', as they are crucial for the management of smart cities (Braun et al., 2018). In addition, it generates a discussion of the benefits of citizens more broadly participating in using digital systems to build 'trust' in 'propensity to use'.

In general, this study brought results that can serve to direct actions in public policies for society, to make citizens aware of how their data and information are used by governments and partner companies to offer public services (Habib et al., 2019). Given this, there is a concern with the control and management of the different levels and resources of the systems in smart cities, which are normally distributed among different entities. It can bring a layer of concern and security limitations through networks (public and/or private) (Rao & Deebak, 2022).

Furthermore, it is perceived that the relationship with data privacy also changes, as it is easier to lose control over it, which becomes more vulnerable due to several factors, such as lack of care on the part of individuals (by not reading terms of the consent), lack of barriers (which allow easy access by malicious third parties), and lack of choice (as it is an essential requirement for using particular services or applications).

Regarding the issue of the lack of limitations, some advances have been observed by government institutions over the years and, in Brazil, with the new General Data Protection Law (Lei nº 13.709, de 14 de agosto de 2018), which aims to remedy some related issues, such as the power of treatment agents (controllers and information operators) over the individual's data.

It is expected that changes will occur in digital relations from now on. Therefore, future studies must analyze this topic and its impact on the smart city in depth.

6. CONCLUSIONS AND IMPLICATIONS

The main objective of this study was to investigate the perception of security and trust in smart city technology by citizens to understand its relationship with the propensity to use it and, consequently, with life in the city. This objective was successfully achieved by analyzing the proposed model and validating the formulated hypotheses.

In addition, the results of the research indicated, above all, the need for collective work to be completed in the city of São Paulo with greater dissemination of information regarding issues related to information security so that citizens can individually demonstrate greater confidence in the acceptance and propensity to use technology in smart cities and, consequently, experience them. Likewise, we confirmed that information security is a theme that strongly influences the use of technology in smart cities. More broadly, it is also necessary to understand the subjective and objective aspects observed in this study that demonstrated a strong impact.

Modern urbanization depends on different devices analyzed for better strategic management of the city. In this context, people in smart cities are monitored, for example, for social security purposes. Thus, as smart cities thrive by collecting and processing local, personal, and confidential information from citizens, any breach of privacy threatens both individuals and society.

In this sense, the study argues that the 'trust' in the technology system of São Paulo is still a worrying factor from the point of view of security and that it can be conquered with the expansion of digital education for citizens, based on data-driven security measures. Unfortunately, in any system, many security risks arise from human error. This effect is amplified by many users, as well as the discrepancy in their skills and levels of security awareness.

However, in Brazil, 'smart city' is still an unknown concept for most of the population because, despite the term gaining more visibility over time and appearing in newspapers and magazines, there is a lack of understanding of the subject. In addition, it is a term that still seems confusing and distant, especially for citizens with little knowledge of basic technology. However, as presented by Bibri (2021), the data-driven culture can be a promising solution, as data and information are used more intensively.

Public managers in the city of São Paulo, in the context of a smart city, can benefit from a data-based security policy that can measure facts, behavior patterns, correlations, insights, and knowledge of its population. This knowledge can be used to develop or revise processes, activities, systems, policies, and strategies.

Smart city initiatives have been moving slowly but gradually in many Brazilian regions. A very prominent example is the city of São Paulo, which, as one of the leading centers of technological advancement, is the recipient of a large number of projects in this regard and is considered the most innovative city in the country by the IESE Cities in Motion Index 2020 and 2021 (Berrone & Ricart, 2020).

Therefore, although the capital of São Paulo stands out in terms of mobility and accessibility due to the various possibilities of transportation, it still worries about the most common problems associated with privacy, such as access or use of data for unauthorized purposes, failures and/or instability in systems/applications, and malicious use of private information, among others present in the literature (Bélanger & Crossler, 2011; S. E. Chang et al., 2017).

As such, leaders of smart city initiatives need to be able to promote this perception of value, be aware of mass trends, and cultivate a strong culture of user, customer, or citizen feedback and support so that continuous improvements are made.

Finally, for the government and leaders of smart city initiatives, it is essential to pay attention to the issue of security not only technologically, but in all aspects of the city, considering how technology can help solve these problems. In the specific case of Brazil, observing the issue of intolerance, which was the second major concern of the research sample, it can be concluded that part of this problem is due to lack of information and lack of questioning and that it can be addressed using technology not only to monitor transgressors but to promote debates but also disseminate content and information to the population.

Given the above considerations, it is important to conduct studies that assess citizens' acceptance, potential problems, and barriers to the effective implementation of smart city solutions, and the advancement of improvements. Furthermore, it is understood that the subjective issues of perception and the environmental context strongly influence collective or individual opinion and exploring them in future studies is relevant.

REFERENCES

Abu-Shanab, E. A. (2017). E-government familiarity influence on Jordanians' perceptions. *Telematics and Informatics*, *34*(1), 103-113. Retrieved from 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. Retrieved from 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. Retrieved from https://doi.org/10.36478/jeasci.2016.545.552

AlHogail, A. (2018). Improving IoT technology adoption through improving consumer trust. *Technologies*, *6*(3), 64. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from https://doi.org/10.1016/j.scs.2018.02.039

Câmara Municipal de São Paulo. (2019, July 16). *Regras para adequar São Paulo ao conceito de cidade inteligente são tema de projeto*. Retrieved from 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. Retrieved from 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. Retrieved from 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*. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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 Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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*. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from https://doi.org/10.1109/COMST.2018.2867288

Urban Systems. (2021). *Ranking connected smart cities*. São Paulo, SP: Author. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from https://doi.org/10.1109/MCOM.2017.1600267CM

Giulie Furtani Romani

https://orcid.org/0000-0002-4116-0997
Bachelor in Business Administration from the Paulista School of Politics, Economics and Business (EPPEN) of the Federal University of São Paulo (UNIFESP). E-mail: giulieromani@gmail.com

Luis Hernan Contreras Pinochet

https://orcid.org/0000-0003-2088-5283
Professor of the Academic Department of Administration (DAA) of the Paulista School of Politics, Economics and Business (EPPEN) of the Federal University of São Paulo (UNIFESP). E-mail: luis.hernan@unifesp.br

Vanessa Itacaramby Pardim

https://orcid.org/0000-0003-0893-7271
Doctoral student in Administration at the University of São Paulo, Faculty of Economics, Administration, Accounting and Actuarial Science (FEA-USP); Professor of Administration at the Nove de Julho University (UNINOVE). E-mail: vanessa.itacaramby@usp.br

Cesar Alexandre de Souza

https://orcid.org/0000-0001-8941-8582
Professor at the University of São Paulo, Faculty of Economics, Administration, Accounting and Actuarial Science (FEA-USP); Permanent member of the stricto sensu Graduate Program in Administration.
E-mail: calesou@usp.br

AUTHOR'S CONTRIBUTION

Giulie Furtani Romani: Conceptualization (Equal); Data curation (Lead); Formal Analysis (Equal); Methodology (Equal); Project administration (Supporting); Resources (Equal); Supervision (Equal); Validation (Equal); Visualization (Equal); Writing - original draft (Lead); Writing - review & editing (Equal).

Luis Hernan Contreras Pinochet: Conceptualization (Equal); Data curation (Supporting); Formal Analysis (Equal); Methodology (Lead); Project administration (Lead); Resources (Equal); Supervision (Equal); Validation (Equal); Visualização (Equal); Writing - original draft (Supporting); Writing - review & editing (Equal).

Vanessa Itacaramby Pardim: Conceptualization (Equal); Data curation (Supporting); Formal Analysis (Equal); Methodology (Equal); Project administration (Supporting); Resources (Equal); Supervision (Equal); Validation (Equal); Visualization (Equal); Writing - original draft (Supporting); Writing - review & editing (Equal).

Cesar Alexandre de Souza: Conceptualization (Equal); Data curation (Supporting); Formal Analysis (Equal); Methodology (Equal); Project administration (Supporting); Resources (Equal); Supervision (Equal); Validation (Equal); Visualization (Equal); Writing - original draft (Supporting); Writing - review & editing (Equal).

APPENDIX 1

BOX A1 DETAILING OF THE STRUCTURAL MODEL

Construct	Item	Assertive	References
Propensity to Use Technologies in Smart Cities (PUTSC)	PUTSC1	Assuming I have access to smart city technology, I plan to use it in everyday life (e.g., ride-hailing apps, online banking, digital payment, etc.).	Adapted from Al-Sharafi et al. (2016).
	PUTSC2	If the city where I live had smart city technology available, I would definitely use it.	Adapted from Al-Sharafi et al. (2016).
	PUTSC3	I would encourage others to use smart city technology (e.g., ride-hailing apps, online banking, digital payment, and so on).	Adapted from Sepasgozar et al. (2019)
	PUTSC4*	Even if I have the option of using smart city technology (e.g., online banking, etc.), I still prefer the physical presence of urban services.	
Trust (TR)	TR1	Technological solutions and applications, in general, are reliable.	Adapted from Mittendorf (2016)
	TR2	I trust technology solutions and applications.	
	TR3	I think the technology solutions and applications are efficient and reliable.	Adapted from Mittendorf (2016)
	TR4*	I tend to trust smart city technology even though I know little about it.	Adapted from Abu-Shanab (2017)
Subjective Security (SS)	SS1*	I think that the institution or company responsible for smart city technology is concerned about the security of information transactions.	Adapted from Cui et al. (2018)
	SS2	I am comfortable using smart city technology (e.g., online banking, transportation apps, electric vehicles, etc.).	Adapted from Urmetzer and Walinski (2014)
	SS3	I believe smart city technology is safe (e.g., online banking, transport apps, electric vehicles, etc.).	Adapted from Urmetzer and Walinski (2014)
	SS4	I believe using smart city technology to perform everyday tasks (e.g., shopping) is safe.	Adapted from Cui et al. (2018)

Continue

Construct	Item	Assertive	References
Objective Security and Data Privacy (OSDP)	OSDP1	Smart city technology has a legal and technological framework (e.g., encryption, updated security systems, etc.) that adequately protects my data.	Adapted from Abu-Shanab (2017) and Sepasgozar et al. (2019)
	OSDP2	Smart city technology has enough safeguards (protections) for me to feel comfortable using it.	Adapted from Sepasgozar et al. (2019)
	OSDP3	Smart city technology can protect my personal information.	Adapted from Abu-Shanab (2017)
Perceived Risk (PR)	PR1	I feel unsafe providing personal information and confidential data to smart city technology.	Adapted from Hansen et al. (2018)
	PR2	There is a high potential for loss associated with providing information for smart city technology.	
	PR3	Overall, it would be risky to provide information for smart city technology.	

Note: *Items excluded in the model fitting process (SEM-PLS).
Source: Elaborated by the authors.

APPENDIX 2

Programming Used in Software R (Seminr)

```
library(seminr)
require(seminr)
measurements = constructs(
  composite(“PUTSC”, c(“PUTSC1”, “ PUTSC2”, “ PUTSC3”)),
  composite(“TR”, c(“TR1”, “TR2”, “TR3”)),
  composite(“SS”, c(“SS2”, “SS3”, “SS4”)),
  composite(“OSDP”, c(“OSDP1”, “ OSDP2”, “ OSDP3”)),
  composite(“PR”, c(“PR1”, “PR2”, “PR3”))
)
structure = relationships(
  paths(from = “OSDP”, to = c(“SS”)),
  paths(from = “OSDP”, to = c(“TR”)),
  paths(from = “PR”, to = c(“OSDP”)),
  paths(from = “PR”, to = c(“TR”)),
  paths(from = “TR”, to = c(“SS”)),
  paths(from = “TR”, to = c(“PUTSC”)),
  paths(from = “SS”, to = c(“PUTSC”)))
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 = “TR”, through = “SS”, to = “PUTSC”, alpha = 0.05)
specific_effect_significance(p4, from = “PR”, through = “SOPD”, to = “TR”, alpha = 0.05)
specific_effect_significance(p4, from = “OSDP”, through = “TR”, to = “SS”, alpha = 0.05)
```