INTERNATIONAL SYMPOSIUM ON TECHNOLOGICAL INNOVATION
ISTI 10 YEARS
SEPTEMBER 25TH TO 27TH, 2019
ARACAJU, SERGIPE, BRAZIL

TECNOLOGIAS BIOMÉTRICAS DE CONTROLE DE ACESSO

Raphael Sapucaia dos Santos– raphaelsapucaia.ages@gmail.com
Program of Postgraduate in Intellectual Property Science – Federal University of Sergipe
Jonas Pedro Fabris– jpfabris@hotmail.com
Program of Postgraduate in Intellectual Property Science – Federal University of Sergipe

Resumo - O aumento da concentração de pessoas na zona urbana tem acarretado diversos problemas e um deles é o aumento da criminalidade acarretando em uma maior sensação de insegurança, o que tem levado as pessoas a investirem em sistemas de segurança eletrônica. O avanço na tecnologia e a redução nos preços tem proporcionado uma maior possibilidade de aquisição de equipamentos de segurança eletrônica acarretando em um crescimento do setor. Os controles de acesso por senha e tokens estão cada vez mais sendo substituídos por dispositivos que utilizam autenticação biométrica, garantindo maior praticidade aos usuários por não ter que gravar senhas ou levar algum dispositivo eletrônico para validar a autenticação, podendo ser feita por características fisiológicas e comportamentais. No mercado existem diversos dispositivos de identificação de características biométricas. No artigo é apresentado uma analise dos principais problemas que podem ser apresentados nos diferentes dispositivos de autenticação das características biométricas e uma pesquisa no banco de dados do Instituto Nacional da Propriedade Industrial (INPI), sobre patentes de controle de acesso com utilização de características biométricas para identificar tendências de mercado.
Palavra Chave - Biometria, segurança, eletrônica, patente.

Abstrat - The increasing concentration of people in the urban area has caused several problems and one of them is the increase in crime leading to a greater sense of insecurity, which has led people to invest in electronic security systems. Advances in technology and lower prices have provided a greater possibility of acquiring electronic safety equipment leading to growth in the sector. Password and token access controls are increasingly being replaced by devices that use biometric authentication, ensuring users more convenience by not having to record passwords or carrying an electronic device to validate authentication, which can be done by physiological and behavioral characteristics. . In the market there are several devices for identification of biometric characteristics. The article presents an analysis of the main problems that may be presented in the different authentication devices of biometric characteristics and a search in the database of the National Institute of Industrial Property (INPI), on access control patents using biometric characteristics for identify market trends.
Keywords— Biometrics, security, electronics, patent.

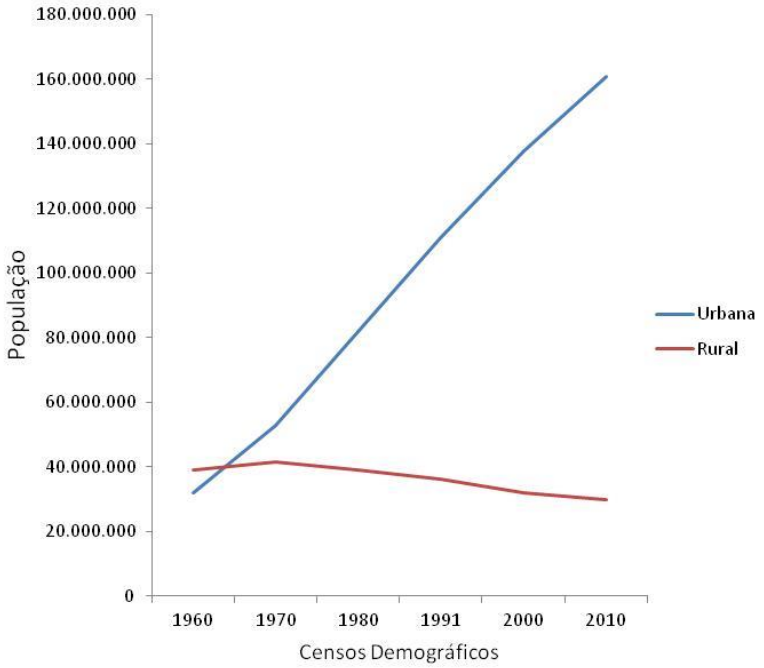
1 INTRODUÇÃO

A violência é um dos principais impulsionadores da inovação espacial, que consiste na oferta de novos locais para a moradia das famílias com condições financeiras de migrarem dos bairros que se tornaram violentos para os novos imóveis que oferecem mais qualidade de vida, que está ligado diretamente com a melhora na percepção de segurança. (PONTES et al., 2011).

No Brasil a quantidade de pessoas que vivem na zona Urbana é de 160.925.804 milhões e a quantidade que vivem na zona rural é de 29.829.995 milhões em 2010. Em 1960 os dados eram bem diferentes sendo 32.004.817 milhões na zona urbana e 38.987.526 na zona rural. O crescimento da população na zona Urbana foi de 502,82 %, enquanto na zona rural teve uma queda de 23,49% da população. (IBGE, 2010)

Conforme Guidugli (1985), o crescimento da violência está relacionado com o aumento da concentração espacial devido o fenômeno da metropolização. Conforme apresentado na figura 1 é possível verificar que entre as décadas de 60 e 70 ocorreu uma inversão de domicilio da população brasileira passando da zona rural para a urbana.

Figura 1: População nos Censos Demográficos, segundo a situação do domicílio - 1960/2010.



Fonte: Autoria própria a partir de dados do IBGE (2010)

De acordo com Tamdjian e Mendes (2004), a negligência do poder publico diante dessa nova realidade culminou em uma segregação espacial ocasionando desigualdades socioespaciais.

A segregação acarreta na separação das classes sociais no solo urbano, reduzindo ainda mais as oportunidades das classes desprovidas de recursos financeiros. (KAZITMAN, 2011)

Conforme Pontes et al. (2011), a violência gera a necessidade de mudança para novos produtos de moradia que ofereçam mais segurança. Conforme Cardia (2003), a violência afeta o comportamento das pessoas influenciando-as a investir em segurança de suas moradias.

Segundo Quintana (2013), a violência gera a criação de novos espaços com acesso controlado por tecnologias de segurança e barreiras físicas, ficando isolados dos espaços urbanos.

De acordo com Melgaço (2010), a criação desses novos espaços promove um aumento da desigualdade espacial e privatização dos espaços públicos. Os espaços exclusivos são destinados para uso coletivo, mas com restrição de acesso. Como exemplos: Shopping Center, escolas particulares, parques temáticos etc. A necessidade de segurança passou a alterar a paisagem urbana. Existem diversos filme e livros que mostram como o excesso de vigilância favorece a criação de ambientes opressivos.

A arquitetura e o urbanismo podem ser usados para controlar a criminalidade e reduzir a sensação de insegurança. Essa teoria é conhecida como Defensible Space. (NEWMAN, 1972)

Conforme Melgaço 2010, as pessoas aceitam perder a privacidade passando a ser vigiados constantemente pelas câmeras para poder diminuir a sensação de insegurança ocasionada pelos sistemas de monitoramento que passam a filmar não apenas as atividades criminosas, mas todas as atividades. A resposta a criminalidade tem sido altos investimentos em informatização e privatização dos espaços públicos deixando de lado a causa da criminalidade. A percepção de insegurança ou segurança muda com o tempo e os lugares.

A segurança pública esta ligada a ordem. A segurança privada ligada a proteção de bens e integridade física. A segurança privada pode ser realizada por empresas de segurança eletrônica e armada. A securitização não garante um local seguro. A eficiência da securitização necessita ser mensurada para evitar os recorrentes noticiários de assaltos a edifício. (MELGAÇO, 2010).

Para Bilard, Chevalier, Madoré apud Melgaço (2005), a securitização diminui muito mais o sentimento de insegurança do que a criminalidade real.

Segundo Melgaço (2010), em Curitiba os condomínios horizontais e verticais continuam sofrendo com a violência mesmo possuindo equipamentos de segurança. Geralmente os criminosos rendem os porteiros ou moradores e conseguem entrar nos condomínios. A globalização do medo tem intensificado o crescimento da venda de dispositivos de segurança em todo o mundo. O barateamento desses equipamentos é outro fator que está estimulando a securitização que é uma realidade mundial, mas com objetivos distintos em diferentes Países. Nos Estados Unidos o objetivo é impedir a entrada de Imigrantes e no Brasil impedir a entrada da violência nas residências e empresas.

Conforme Liu; Silverman (2009), o sistema de controle de acesso pode ser dividido em controle de acesso físico e controle de acesso lógico. O foco desse artigo é apresentar as vantagens e desvantagens da implantação do controle de acesso físico utilizando características biométricas. Esse sistema permite a liberação do bloqueio físico e o controle do acesso de pessoas.

2 FUNDAMENTAÇÃO TEÓRICA

O primeiro artigo sobre biometria foi publicado em 1962 na revista Nature por Mitchell Trauring abordando sobre a autenticação através da identificação da impressão digital. Nesta mesma época começaram a surgir equipamentos de autenticação biométrica de outras características como face e assinatura. A biometria evoluiu surgindo outros sistemas biométricos mais precisos como identificação da palma da mão e iris. A autenticação biométrica se tornou uma forma de autenticação para substituir ou usar em conjunto com senha e tokens. Sendo mais recomendada a utilização em conjunto devido a possibilidade de obtenção dos dados biométrico através da solicitação desses dados cada vez mais frequente (JAIN; NANDAKUMAR; ROSS, 2016).

Existem 3 tipos de autenticação: a identificação pode ser feita com algo que a pessoa saiba como exemplo uma senha; a identificação pode ser realizada por algo que a pessoa tenha como um dispositivo que pode ser um token ou um cartão inteligente; o ultimo tipo de identificação é por algo que a pessoa é. Esse ultimo tipo de autenticação é a biometria, considerada a mais segura, pois não pode ser roubada, emprestada ou esquecida. Forjar a autenticação biométrica é muito difícil, pois a biometria mede as características físicas do individuo. Essas características físicas podem ser Iris, retina, mão, características faciais e impressões digitais. (LIU; SILVERMAN, 2009)

No quadro 1 é apresentadas as vantagens e desvantagens da utilização de cada característica física para fazer a autenticação biométrica.

Quadro 1: Vantagens e desvantagens das diversas características físicas para fazer a autenticação biométrica.

Característica biométrica	Vantagem	Desvantagem
Impressões digitais	Grande variedade de dispositivos.	Alguns equipamentos detectam dedos não vivos.
	Redução do custo de implantação e manutenção.	
Geometria da mão	Bom desempenho.	Não é ideal para alta frequência de acesso.
	Fácil de usar.	
	Facilidade de integração em outros sistemas.	
Retina	Padrões únicos da retina.	Necessidade de tirar o óculos e encostar o rosto no dispositivo para olhar o feixe de luz que irá fazer a leitura.
	Bastante preciso.	
Iris	Não precisa de contato próximo entre o leitor e usuário.	Não possui facilidade de uso.
	Desempenho superior a média.	Difícil integração com outros sistemas
Reconhecimento facial	Não necessita contato com o dispositivo.	Precisa de dispositivos com grande capacidade de armazenamento.

Fonte: Elaborado pelos autores (adaptado do artigo LIU, Simon and Silverman, Mark, "A Pratical Guide to Biometric Security Tecnology", IEEE IT Pro, Vol. 1, pp 27-32, Jan-Feb. 2001.

Segundo dados da Associação Brasileira das Empresas de Sistemas Eletrônicos de Segurança (ABESE), deve ser realizado uma analise de risco do imóvel para fazer a elaboração do projeto de sistema de segurança eletrônica, para adequar ao local, usuário e a atividade do imóvel. Devem ser identificados as vulnerabilidades do imóvel e os tipos de ocorrências registrados. (ABESE, 2019)

Um dos cuidados que deve ter no controle de acesso realizado pelas tecnologias de autenticação biométrica é a verificação da vivacidade da característica que está sendo validada. No reconhecimento facial a vivacidade é verificada pela analise do fluxo sanguíneo na face, pela qualidade da imagem, irradiação de calor e batimentos cardíaco. Uma outra forma de verificação da vivacidade seria a utilização de câmeras 3D que possibilita a verificação da profundidade da face. As tecnologias de autenticação biométricas são passiveis de serem violadas por falsificações na autenticação. É possível criar uma impressão digital humana utilizando silicone para enganar o dispositivo de autenticação que não seja capaz de detectar dedo vivo. Para enganar os sistemas de autenticação facial estão utilizando mascaras com o rosto da pessoa autorizada no banco de dados, pois os bancos de dados são de imagens 2D. (ALBAKRI; ALGHOWINEM, 2019)

A autenticação utilizando a técnica de identificação da Iris apresentam as vantagens de não ser invasivo evitando o desconforto do usuário, cada Iris apresenta características distintas facilitando a distinção dos usuários, acarretando maior segurança e devido à estabilidade do padrão da Iris, o processo de autenticação da IRIS torna-se fácil. (JAGADEESH; PATIL, 2017)

A identificação da iris precisa ser realizada de forma estática, mas a identificação do olho humano pode ser utilizado para autenticação da biometria sem precisar que o usuário do sistema tenha que fixar o olhar em algum dispositivo. A validação biométrica pode utilizar a tecnologia de rastreamento ocular que consiste em analisar alguns critérios como: velocidade do olhar, tamanho da pupila, características oculomotoras e tamanho da pupila podendo substituir as senhas digitadas. (CANTONI et al., 2017)

O sistema de autenticação biométrica pode ser usado de duas formas. A primeira forma consiste no cadastramento das características biométricas dos indivíduos que terão passagem liberada pelo sistema. Essas características biométricas ficam associadas a outros dados da pessoa, ficando essas características armazenadas em um banco de dados para futuras comparações quando o usuário precisar realizar a identificação e os sistemas de autenticação biométrica será utilizado na forma de reconhecimento que precisa ser verificado a biometria da pessoa que está solicitando com os dados cadastrados no sistema. Durante o processo de cadastramento e de reconhecimento da característica biométrica pode ocorrer ruídos. Na biometria utilizando uma câmera bidimensional (2D) no reconhecimento facial pode ocorrer algumas limitações do sensor como: baixa resolução espacial e dificuldade devido a baixa iluminação. Outros

problemas no reconhecimento podem estar relacionados à alteração na estrutura facial devido o envelhecimento natural da pessoa. As poses, expressões e acessórios como chapéus e óculos podem atrapalhar o processo de reconhecimento. Diversos problemas podem ser apresentados na leitura da característica biométrica. No quadro 2 são apresentados os diversos problemas relacionados com a característica biométrica que se pretende identificar. (JAIN; NANDAKUMAR; ROSS, 2016)

Quadro 2: Problemas na inscrição e reconhecimento de diferentes características biométricas.

Problemas	Impressão digital	Face	Iris
Sensor	Limpeza do sensor e resolução.	Resolução espacial, taxa de quadros, distância da câmera.	Distância do sensor.
Envelhecimento	Alterações na pele devido a elasticidade.	Mudanças geométricas entre a infância e a adolescência, rugas e flacidez facial.	Contração da pupila.
Interação com o usuário	Pressão e rotação do dedo.	Poses e expressões.	Dilatação da pupila, ângulo do olha e olho parcialmente fechado.
Mudanças no meio ambiente	Interior x exterior.	iluminação e cena de fundo.	Iluminação.
Outros fatores	Cortes e dedos gastos secos e molhados.	Maquiagem, acessórios, oclusão.	Doenças oculares e influência de álcool.

Fonte: JAIN; ROSS, 2016

A redução nos preços das tecnologias de identificação biométrica e o avanço tecnológico que permitiu dispositivos mais seguros, menores e de fácil uso acompanhada de melhores processadores e capacidade de armazenamento de dados foram fatores primordiais para a disseminação da tecnologia de autenticação biométrica. (JAIN; NANDAKUMAR; ROSS, 2016)

3 METODOLOGIA

A pesquisa realizada é de característica exploratória, devido o levantamento bibliográfico realizado em artigos científicos nacionais e internacionais, dissertações e teses. Em conjunto foi realizado uma pesquisa quantitativa através de buscas de Patentes no banco de dados do Instituto Nacional da Propriedade Industrial (INPI), utilizando a palavras chave "Biometria" no campo título. Em seguida foi realizado uma nova busca utilizando as palavras chave "reconhecimento" and "facial" no campo titulo.

Os resultados foram analisados e obtidos dados estatísticos que mostram características biométricas com mais depósitos de patente, comparativo da quantidade de patentes de biometria com característica biométrica de reconhecimento facial e impressão digital e histórico da quantidade de patentes utilizando reconhecimento facial. As prospecções foram realizada entre os dias 25 de junho de 2019 e 25 de julho de 2019.

4 RESULTADOS E DISCUSSÕES

Realizando a pesquisa na base de dados do INPI com a palavra chave "Biometria" no campo título foram localizados 34 resultados. Como dois resultados apareceram em duplicidade o total de dados passou a ser 32 resultados. Os resultados foram analisados para verificar se as patentes realmente se referem a dispositivos de biometria para garantir a segurança do usuário.

Foi verificado que 7 resultados não se aplicam sendo: 1 relacionado a métodos e sistemas para gestão de atividade de rede usando biometria, 2 resultados se referem a equipamentos médico de diagnostico ocular, 1 a método de medição de objetos, 1 a câmera que faz contagem de pessoas, 1 a cartão magnético que pode ser caracterizado como um dispositivo físico de controle de acesso, mas não pode ser considerado como controle de acesso com uso de biometria e 1referente a cadeira que pode ser liberada por senha, ingresso, biometria ou cartão eletrônico.

O total de registros válidos relacionados à biometria de controle de acesso passa a ser de 25 registros sendo divido por características biométricas conforme apresentado na tabela 1. O maior percentual de patentes encontradas no banco de dados do INPI com a palavra chave "biometria" foi de dispositivos de controle de acesso que utiliza como característica biométrica o reconhecimento facial representando 40 %. As que utilizam a impressão digital como característica biométrica representa 32% dos resultados validos.

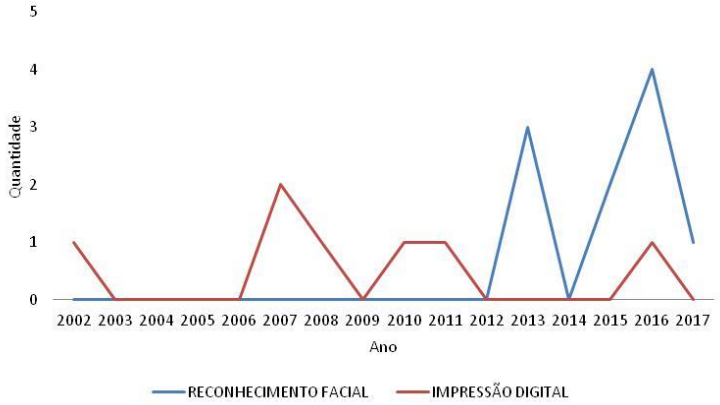
Tabela 1: Características biométricas dos resultados da pesquisa no INPI utilizando a palavra chave "biometria".

CARACTERÍSTICAS BIOMÉTRICAS	QUANTIDADE
RECONHECIMENTO FACIAL	10
IMPRESSÃO DIGITAL	8
MULTIMODAL	2
ASSINATURA	2
VOZ	1
CORNEA	1
RETINA	1
Total	25

Fonte: Adaptado de INPI (2019)

Na figura 2 é possível verificar um crescimento na quantidade de patentes de autenticação biométrica por reconhecimento facial e uma queda do pedido de patente do controle de acesso por impressão digital conforme pesquisa realizada na base de dados do INPI.

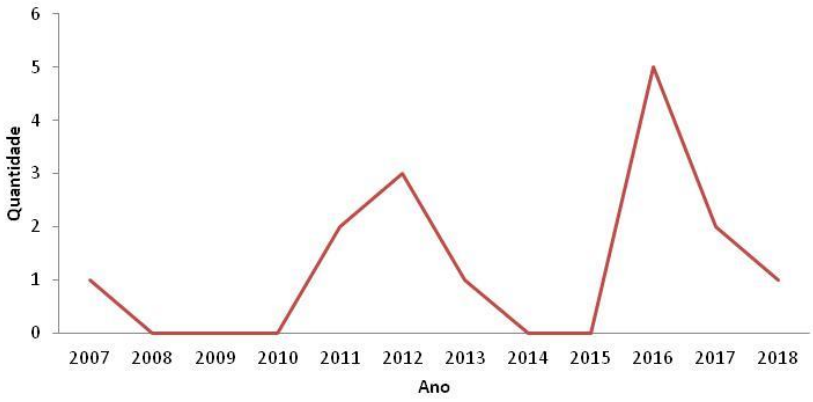
Figura 2: Comparativo da quantidade de patentes de dispositivos de controle de acesso de Reconhecimento facial e impressão digital entre os anos de 2002 e 2017 localizados no banco de dados do INPI utilizando como palavra chave "biometria".



Fonte: Adaptado de INPI (2019)

Uma nova pesquisa foi realizada utilizando as palavras chave "reconhecimento facial" no campo título e foram localizadas 15 patentes podendo ser analisado na figura 3 o seguinte histórico de depósito de patente. Em 2007 ocorreu o primeiro depósito via PCT e o ano que mais teve depósito de patente foi 2016.

Figura 3: Histórico dos depósitos de patentes do banco de dados do INPI utilizando as palavras chaves "reconhecimento" and "facial"



Fonte: Adaptado de INPI (2019)

5 CONCLUSÃO

De acordo com o estudo desenvolvido foi constatado que a autenticação biométrica está cada vez mais sendo utilizada pelas pessoas em diversas situações, como a autenticação para entrar nas edificações,

nas transações bancárias, nos automóveis e no uso de dispositivos pessoais como celular e notebook. A biometria é uma forma prática de realizar a autenticação, pois a autenticação realizada com PIN ou token pode ocorrer problemas como: o usuário esquecer o código PIN ou esquecer o dispositivo token que autoriza a entrada do usuário nas edificações.

O número de depósitos de tecnologias de autenticação biométricas de reconhecimento facial foi o que apresentou maior crescimento e maior número de deposito de patentes, possuindo ligação com a redução do preço da tecnologia de processadores e armazenamento de dados, acarretando na redução do preço da tecnologia, permitindo maiores precisões de reconhecimento devido a possibilidade de realizar diversas analises em imagens mais nítidas e em 3 demissões, permitindo verificação da profundidade do rosto. O avanço da tecnologia está tornando a autenticação biométrica mais segura e confiável.

REFERÊNCIA

ABESE - Associação Brasileira das Empresas de Sistemas Eletrônicos de Segurança, Disponível em: < https://abese.org.br/index.php/consumidor-final/cuidados>. Acesso em: 17 jul. 2019.

ALBAKRI, G.; ALGHOWINEM, S. The Effectiveness of Depth Data in Liveness Face Authentication Using 3D Sensor Cameras. **Sensors.** 2019, 19, 1928.

CANTONI, V.; NUGRAHANINGSIH, N.; PORTA, M.; WANG, H. Biometric Authentication to Access Controlled Areas Through Eye Tracking. **Human Recognition in Unconstrained Environments**, M. De Marsico, M. Nappi, H. Proença (Eds.), Academic Press-Elsevier, 2017,

CARDIA, N. Exposição à violência: seus efeitos sobre valores e crenças em relação a violência, polícia e direitos humanos. **Revista Lusotopie**, p. 299-328, 2003.

Censo Demográfico 2010. Rio de Janeiro: IBGE, 2010. Disponívelem:<https://www.ibge.gov.br/estatisticas/sociais/populacao/9662-censo-demografico 2010.html?edicao=10503&t=destaques >. Acesso em: 15 ago. 2018.

GUIDUGLI, O. S. Crime Urbano e Geografia Aplicada. **Geografia**, 10(19), p. 232-233, 1985.

JAGADEESH N.; CHANDRASEKHAR M. PATIL. A Brief Review of the Iris Recognition Systems for Developing a User-Friendly **Biometric Application**. ICECDS, 2017.

JAIN, A. K.; NANDAKUMAR, K.; ROSS, A. 50 years of biometric research: accomplishments, challenges, and opportunities. **Pattern Recogn Lett**, v. 79, p. 80–105, 2016.

KAZTMAN, R. Seducidos y abandonados: el aislamiento social de los pobres urbanos. **Revista de CEPAL**, v. 75, n. 1, p. 171-189, 2001.

LIU, S; SILVERMAN, M.. Technology-savvy organizations looking to develop a competitive advantage should carefully watch developments in biometrics. **T Professional**, v. 3, n. 1, p.27-32, 2001.

MELGAÇO, L. **Securitização urbana**: Da psicosfera do medo à tecnosfera da segurança. São Paulo: Edusp, 2010.

NEWMAN, O. Defensible Space: People and Design in the Violent City. **Architectural Press,** London, 1973.

PONTES, E., PAIXÃO, L. A.; ABRAMO, P. O mercado imobiliário como revelador das preferências pelos atributos espaciais: uma análise do impacto da criminalidade urbana no preço de apartamentos em BH, **Revista de Economia Contemporânea,** v. 15, n. 1, p. 171–197, 2017.

QUINTANA, E. **Influência de características físicoespaciais na ocorrência de crimes e na percepção de segurança em áreas residenciais com condomínios fechados.** Dissertação (Mestrado em Planejamento Urbano e Regional.). Universidade Federal do Rio Grande do Sul, Porto Alegre, 2013.

TAMDJIAN, James Onnig; MENDES, Ivan Lazzari. **Geografia Geral e do Brasil: estudos para compreensão do espaço**. James & Mendes. São Paulo: FTD, 2004.