PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ
ESCOLA DE ARQUITETURA E DESIGN
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO URBANA

THIAGO GONÇALVES ROBERTO

NÍVEIS DE VIGILÂNCIA E PRIVACIDADE NA GESTÃO DE DADOS URBANOS: O CASO DE CURITIBA-PR

CURITIBA
2017

THIAGO GONÇALVES ROBERTO

NÍVEIS DE VIGILÂNCIA E PRIVACIDADE NA GESTÃO DE DADOS URBANOS: O CASO DE CURITIBA-PR

Dissertação apresentada ao Programa de Pós-Graduação em Gestão Urbana – PPGTU da Escola de Arquitetura e Design da Pró Reitoria de Graduação, Pesquisa e Pós-Graduação da Pontifícia Universidade Católica do Paraná, - PUCPR, como requisito à obtenção do título de mestre em Gestão Urbana.

Orientador: Prof. Dr. Rodrigo José Firmino

CURITIBA

2017

THIAGO GONÇALVES ROBERTO

NÍVEIS DE VIGILÂNCIA E PRIVACIDADE NA GESTÃO DE DADOS URBANOS: O CASO DE CURITIBA-PR

Dissertação apresentada ao Programa de Pós-Graduação em Gestão Urbana – PPGTU da Escola de Arquitetura e Design da Pró-Reitoria de Graduação, Pesquisa e Pós-Graduação da Pontifícia Universidade Católica do Paraná - PUCPR, como requisito de qualificação de mestrado.

COMISSÃO EXAMINADORA

_____

Prof. Dr. Rodrigo José Firmino

Pontifícia Universidade Católica do Paraná

_____

Prof.ª Dr.ª Samira Kauchakje

Pontifícia Universidade Católica do Paraná

_____

Prof. Dr. Ivan Mizanzuk

Pontifícia Universidade Católica do Paraná

_____

Prof. Dr. Rafael de Almeida Evangelista

Universidade Estadual de Campinas

Curitiba, 04 de setembro de 2017

AGRADECIMENTOS

Agradeço ao meu orientador, o Prof. Dr. Rodrigo José Firmino, pela oportunidade e confiança; pela dedicação nas orientações e correções; e pela disponibilidade e apoio neste período de aprendizado.

Aos demais professores do PPGTU pelas lições e leituras que contribuíram, direta e indiretamente, para o desenvolvimento deste trabalho.

Aos meus colegas do programa pelas discussões proveitosas e pelo incentivo nos momentos de dificuldade.

“O protocolo de acesso da telemática sucede o do portão. Aos tambores das portas sucedem-se os dos bancos de dados, tambores que marcam os ritos de passagem de uma cultura técnica que avança mascarada, mascarada pela imaterialidade de seus componentes, de suas redes, vias e redes diversas cujas tramas não mais se inscrevem no tecido de um espaço construído, mas nas sequências de uma planificação imperceptível do tempo na qual a interface homem/máquina toma o lugar das fachadas dos imóveis, das superfícies dos loteamentos... “

(VIRILIO, 1993, p. 10)

RESUMO

A vigilância tem se colocado como um importante elemento para o entendimento das cidades contemporâneas e como instrumento para as práticas da gestão urbana. O campo de estudo da vigilância compreende uma ampla visão dos mecanismos de controle e exercício de poder associados ao paradigma da modernidade e aos avanços tecnológicos recentes. Atualmente, a coleta de dados pessoais é um mecanismo ubíquo e presente em atividades de rotina das pessoas, tornando os processos de controle inescapáveis, mecanizados e generalizados. As consequências desse cenário podem ser negativas, causando ameaças à privacidade e novas formas de discriminação. Essa configuração tem efeitos nas dinâmicas e formas urbanas, estando associadas ao movimento de globalização e informatização das cidades contemporâneas. Da mesma forma que a gestão pública, a gestão urbana utiliza bancos de dados pessoais com o objetivo de aumentar a segurança pública e melhorar a eficiência dos serviços e processos administrativos, associando tais implementações e práticas à ideia de cidades inteligentes. Porém, as soluções que demandam um maior aporte tecnológico, objetivando um maior controle, acabam se tornando ferramentas de reprodução da ideologia dominante e a manutenção dos problemas urbanos, que são muito presentes no contexto latino-americano. Nesse sentido, objetiva-se com essa pesquisa a apreensão do uso de dados pessoais pela gestão urbana no Brasil e o potencial de vigilância contido nesse processo. O objeto da pesquisa são os cadastros de dados pessoais da Prefeitura Municipal de Curitiba, que foi disponibilizado para o estudo documental dos seus campos de informações. Para a análise dos dados coletados foi elaborada uma metodologia que leva em conta três classificações para esses sistemas cadastrais: informações sensíveis, valor comercial dos dados, e multiplicidade de acesso, que se combinam em uma fórmula para determinação de um “índice de vigilância”. Como resultado, foi descoberto que o tipo de cadastro que contém os maiores potenciais de vigilância, ou seja, que apresentaram os maiores índices, são aqueles que são utilizados por secretarias que trabalham com pessoas em situação de vulnerabilidade social e jovens. Isso pode ser justificado pela demanda de dados sensíveis para que sejam implementadas políticas sociais e serviços direcionados para essa parcela da população.

Palavras-chave: tecnologias de vigilância, privacidade, gestão urbana, cidades e tecnologias, vigilância.

ABSTRACT

Surveillance has become an important constituent for the understanding of contemporary cities and as a tool urban management practices. The surveillance studies field comprehends a broad view of the control and power enforcement mechanisms related to the paradigm of modernity and to the recent technological progress. Currently, the personal data collection is a ubiquitous mechanism present in people's everyday activity, making the control processes unescapable, mechanized and widespread. There might be negative consequences for this prospect, causing threats to privacy and new forms of discrimination. This configuration has effects on the urban forms and dynamics, being associate to the globalizing and informatization of the contemporary city movements. Just as the public management, the urban management relies on personal information databases aiming for the increase of the public security and the improvement of the public services and the administrative processes efficiency, linking such implementation and practices to the idea of smart cities. However, the solutions that demands a greater technological support, aiming a greater control, may become tools to the dominant ideology and the sustenance of the urban problems, which are present on the Latin-American context. In this sense, it aims with this research the apprehension of the personal data use by the urban management in Brasil e the surveillance potential within this process. The subject for this inquiry are the personal data registers hold by the Prefeitura Municipal de Curitiba, which were provided to the documental study of their information fields of registration. For the analysis of the collected data it was elaborated a methodology that takes account on three register system classifications: sensitive information, commercial data value, and multiple access, that are combined in a "surveillance index" expression. As result, it was found that the type of registration that has the greatest potential for surveillance, which is, those with the highest surveillance index, are those that were used by the departments that assists economically vulnerable and young population. That might be justified by the sensible data demanded to be implement social policies and services aimed to this part of the population.

Keywords: surveillance technologies, privacy, urban management, cities and technology, surveillance.

LISTA DE ILUSTRAÇÕES

FIGURA 1: PLANTA, CORTE E ELEVAÇÃO DO PANÓPTICO DE BENTHAM DESENHADO POR WILLIAM REVELEY, 1791 18
GRÁFICO 1: PESQUISA DE SENSIBILIDADE DE INFORMAÇÕES 454
QUADRO 1: CRITÉRIO DE CLASSIFICAÇÃO E FONTE PARA A DEFINIÇÃO DE DADOS SENSÍVEIS. 73
QUADRO 2: VALORES COMERCIAIS PARA DADOS PESSOAIS POR TIPO. 75
QUADRO 3: CADASTROS FORNECIDOS PELA PMC. 79
QUADRO 4: ATIVUS - ACOMPANHAMENTO DE ATIVIDADES FÍSICAS. 81
QUADRO 5: COC.NET - COORDENADORIA DE OBRAS. 82
QUADRO 6: SIC - IDENTIFICAÇÃO DO CIDADÃO. 85
QUADRO 7: SISTEMA: E-SAÚDE - ATENDIMENTO MÉDICO, ODONTOLÓGICO E DE OUTRAS ESPECIALIDADES. 89
QUADRO 8: GESTÃO TRIBUTÁRIA MUNICIPAL. 90
QUADRO 9: GTM - CADASTRO DE COMÉRCIO AMBULANTE. 92
QUADRO 10: 156. 95
QUADRO 11: GED - GESTÃO EDUCACIONAL. 97
QUADRO 12: CONTROLE DE CORRIDAS. 100
QUADRO 13: NCPA - CADASTRO DE PESSOAS ATENDIDAS 103
GRÁFICO 02: NÚMERO DE CAMPOS DE DADOS SENSÍVEIS POR CADASTRO. 104
QUADRO 14: ATIVUS - ACOMPANHAMENTO DE ATIVIDADES FÍSICAS. 106
QUADRO 15: COC.NET - COORDENADORIA DE OBRAS. 106
QUADRO 16: SIC - IDENTIFICAÇÃO DO CIDADÃO. 107
QUADRO 17: SISTEMA: E-SAÚDE - ATENDIMENTO MÉDICO, ODONTOLÓGICO E DE OUTRAS ESPECIALIDADES. 108
QUADRO 18: GTM - CADASTRO DE COMÉRCIO AMBULANTE. 109
QUADRO 19: 156. 109
QUADRO 20: GED - GESTÃO EDUCACIONAL. 110
QUADRO 21: CONTROLE DE CORRIDAS. 111
QUADRO 22: NCPA - CADASTRO DE PESSOAS ATENDIDAS 111
GRÁFICO 03: VALOR COMERCIAL DAS INFORMAÇÕES CADASTRADAS POR SISTEMA. 112
QUADRO 23: CADASTROS QUE PERMITEM O MÚLTIPLO ACESSO. 113
QUADRO 24: PARÂMETROS E ÍNDICE DE VIGILÂNCIA POR SISTEMA. 115
GRÁFICO 04: ÍNDICE DE VIGILÂNCIA POR SISTEMA. 115

SUMÁRIO

1 INTRODUÇÃO 11
1.1 OBJETIVO 15
1.1.1 Objetivo geral 15
1.1.2 Objetivos específicos 15
2 REVISÃO DE LITERATURA 16
2.1 VIGILÂNCIA E SOCIEDADE. 16
2.1.1 O panóptico 17
2.1.2 Para além do panóptico: Controle, Risco e Administração do Medo 22
2.1.3 A “Nova Vigilância” 28
2.1.4 Tecnologias de vigilância e bancos de dados 33
2.1.5 Governo e vigilância 36
2.1.6 Vigilância no Brasil 38
2.1.7 Big Data, Dados Pessoais e Dados Sensíveis 42
2.1.8 Considerações finais 46
2.2 CIDADES E AS TICS 47
2.2.1 A revolução urbana e as redes globais 49
2.2.2 Redes urbanas e espaço público na cidade ampliada 52
2.2.3 Gestão urbana e as TICs 57
2.2.4 Smart Cities 60
2.2.5 Vigilância nas cidades 62
2.2.6 Considerações finais 66
3 METODOLOGIA 67
3.1 UNIDADE-CASO 68
3.2 PROCEDIMENTOS METOLÓGICOS 70
3.2.1 Coleta de dados 70
3.2.2 Análise dos resultados 71
4 DADOS PESSOAIS E POTENCIAL DE VIGILÂNCIA NA GESTÃO MUNICIPAL DE CURITIBA 79
4.1 DADOS SENSÍVEIS 79
4.1.1 ATIVUS - Acompanhamento de atividades físicas 80
4.1.2 COC.Net - Coordenadoria de obras 82
4.1.3 SIC - Identificação do Cidadão 83

4.1.4 E-Saúde - Atendimento médico, odontológico e de outras especialidades ... 85
4.1.5 GTM - Gestão Tributária Municipal ... 89
4.1.6 GTM - Cadastro de Comércio Ambulante ... 90
4.1.7 156 - Atendimento ao Cidadão ... 92
4.1.8 GED - Gestão Educacional ... 95
4.1.9 Controle de Corridas ... 97
4.1.10 NCPA - Cadastro de Pessoas Atendidas ... 100
4.1.11 Comparativo ... 103
4.2 VALOR COMERCIAL ... 104
4.2.1 ATIVUS - Acompanhamento de atividades físicas ... 105
4.2.2 COC.Net - Coordenadoria de obras ... 106
4.2.3 SIC - Identificação do Cidadão ... 106
4.2.4 E-Saúde - Atendimento médico, odontológico e de outras especialidades ... 107
4.2.5 GTM - Gestão Tributária Municipal ... 108
4.2.6 GTM - Cadastro de Comércio Ambulante ... 108
4.2.7 156 - Atendimento ao Cidadão ... 109
4.2.8 GED - Gestão Educacional ... 109
4.2.9 Controle de Corridas ... 110
4.2.10 NCPA - Cadastro de Pessoas Atendidas ... 111
4.2.11 Comparativo ... 111
4.3 MÚLTIPLO ACESSO ... 112
4.4 ÍNDICE DE VIGILÂNCIA ... 113
4.5 DADOS PESSOAIS COMO INSTRUMENTO DE VIGILÂNCIA E CONTROLE NA GESTÃO URBANA ... 115
5 CONCLUSÃO ... 121
5.1 LIMITAÇÕES DA PESQUISA E SUGESTÕES PARA TRABALHOS FUTUROS ... 123
REFERÊNCIAS ... 125
ANEXO I ... 132

1 INTRODUÇÃO

A vigilância tem se tornado um elemento fundamental nas sociedades contemporâneas, sendo objeto de estudo de diversos pensadores atuais (LYON, 2004; 2009; 2010; 2013; 2015; MARX, 2002; 2013; MURAKAMI WOOD et al,. 2006; GANDY, 1993; MATHIESEN, 1997; BOGARD, 1996; HAGGERTY; ERICSON, 1996), que têm levantado importantes questões quanto sua natureza e implicações no panorama global e no paradigma tecnológico atual.

A análise teórica sobre a vigilância, e sua instrumentação para o exercício do poder e do controle, tem origens em autores canônicos como Michel Foucault (2013), Gilles Deleuze (2013) e Paul Virilio (1993). O conceito de panóptico (Bentham, 2008; Foucault, 2013) é o ponto de partida dos estudos que se propõem entender a transformação das práticas de vigilância antigas para o cenário moderno, baseado na racionalização dos processos.

A mudanças no paradigma panóptico, predominante na modernidade clássica, se baseia em uma profunda transformação social e a radicalização dos elementos modernos com os processos de reflexividade (GIDDENS, 1991; BECK, 2010). Além disso, o desenvolvimento tecnológico, especialmente o advento das Tecnologias de Informação e Comunicação (TICs), trouxe novas possibilidades de exercício do poder e configuração social (VIRILIO, 1991; CASTELLS, 1999).

Os novos padrões de vigilância, então, são dependentes das TICs para a execução de seus processos, além de funcionarem em uma rede global de troca de informações, envolvendo instituições públicas e privadas. A vigilância na contemporaneidade está presente no dia-a-dia das pessoas através do uso de sistemas de coleta de dados contidos em dispositivos pessoais, como cartões e aparelhos de comunicação móvel, e pode ser aplicada por corporações e governo com a finalidade de garantir a segurança pública e nacional, ou promover estratégias de marketing direcionado (LYON, 2013). Devido a grande importância das informações pessoais para o setor privado, foi estabelecido um comércio desse tipo de dado, onde há uma cotação para o valor de venda de cada categoria de informação pessoal disponível nas bases informacionais (STEEL *et al*., 2013).

As práticas de vigilância atuais são dependentes de bancos de dados interconectados que armazenam volumes cada vez maiores de informações, o Big

Data (TENE, POLONETSKY, 2013). Dentre os dados armazenados nas bases informacionais, os mais preocupantes no que concerne ao potencial de prejuízo e discriminação são as “informações sensíveis”, que são os tipos de elementos que devem ser processados e divulgados sob cuidados específicos para que não haja invasão ou violação da privacidade dos indivíduos (OHM, 2015).

A cidades são o ambiente próprio para as práticas de vigilância modernos, pois tem experimentado uma transformação nos seus fixos e fluxos a partir da globalização econômica e a adoção das TICs pelo cidadãos contemporâneos (ASCHER, 2010; SANTOS, 2013; CASTELLS, 1999; SASSEN,2001), o que demanda uma infraestrutura tecnológica inédita no meio urbano (GRAHAM; MARVIN, 2001; FIRMINO, 2011). O espaço urbano tem sido infiltrado por informação digital e o mundo virtual, baseado em software, é uma importante ferramenta de movimento e permanência no espaço das cidades atuais (MITCHELL, 2002; DUARTE;FIRMINO, 2008).

A gestão urbana, dessa forma, enfrenta novos desafios relacionados à pervasividade das TICs no meio urbano, que se fazem invisíveis quando embutidas nos sistemas urbanos anteriores, como a infraestrutura de transporte, saneamento, energia e telefonia (CASTELLS, 1999; FIRMINO, 2011). A utilização de TICs também tem sido adotada pela própria administração pública como forma de aumentar a eficiência da gestão urbana e promover a democratização das informações públicas (FIRMINO; FREY, 2014; KITCHIN, 2015).

Dentro da ideia da utilização tecnológica como forma de resolver os problemas das cidades, surgiram os projetos de smart city: um conceito de gestão e propaganda urbanos baseado na ampla aplicação de dispositivos de controle de indicadores urbanos e promoção de uma economia voltada para a inovação tecnológica (CARAGLIU et al., 2009). Porém, apesar de apresentarem um discurso de resolução para as disfunções urbanas, os projetos de smart city, tem se mostrado como uma ferramenta de reprodução da ideologia dominante e manutenção dos problemas urbanos devido à análise superficial dos monitoramentos tecnológicos, levando a um aprofundamento das desigualdades urbanas (RENNÓ, 2016; KAYYALI, 2016, PEÑA; VELASCO, 2016).

O espalhamento das TICs no território urbano trouxe consigo um aparato de vigilância pervasiva presente em grande parte dos processos urbanos. Tecnologias

de coleta de dados pessoais são utilizadas em aparelhos de registro, localização, captura de imagens, bancos de dados integrados e sensores urbanos, tanto nos lugares públicos como privados (LYON, 2004; GRAHAM, 2003; KITCHIN, 2013; BATTY, 2013). A utilização dessas tecnologias pelo poder público tem como objetivo o aumento da segurança pública, face à criminalidade urbana, e a melhora nos serviços públicos junto de um incremento no controle governamental sobre os cidadãos. Tais processos resultam em uma restrição da privacidade e uma ameaça à liberdade de expressão em decorrência do controle concentrado nas mãos de pequenos grupos detentores do poder institucional (KITCHIN, 2013).

Dado o panorama dos estudos sobre vigilância e gestão urbana, se faz necessário os questionamentos sobre como ocorre a prática e a utilização de tecnologias dessa natureza como ferramenta para a administração pública. Mais especificamente, quais os tipos de dados pessoais utilizados para a manutenção dos serviços e implantação de políticas públicas e seu potencial como ferramenta de vigilância.

Ou seja, a pesquisa tem por objetivo entender quais informações são utilizadas por um órgão gestor público municipal nos seus procedimentos diários, pois, a partir da teoria sobre o tema e das informações gerais disponíveis, é pertinente supor que uma prefeitura contemporânea, inserida no paradigma tecnológico e administrativo atual, lance mão de aparatos de vigilância nos seus processos de gestão urbana. A vigilância, muitas vezes, acaba sendo um subproduto do desenvolvimento de políticas e serviços públicos, que se valem de tecnologias de coleta e armazenamento de informações pessoais para seu funcionamento. De acordo com a literatura (LYON, 2013), os fins para essas ferramentas podem ser voltados à melhor eficiência da gestão pública ou à promoção da segurança pública e de Estado, sendo que, neste trabalho, o enfoque é o armazenamento de dados pessoais.

Para que sejam respondidas as questões levantadas anteriormente, foi elaborado um levantamento, utilizando o método de pesquisa documental, dos cadastros que armazenam dados pessoais e são utilizados como instrumento de gestão urbana pela Prefeitura Municipal de Curitiba (PMC). A cidade de Curitiba tem um histórico de vanguardismo e reconhecimento por suas soluções urbanísticas e, com a intenção de retomar sua posição de destaque no planejamento e na gestão

urbana, a prefeitura tem apresentado um discurso muito focado em inovações tecnológicas, que levam ao projeto, pouco definido, Curitiba Smart City.

A pesquisa pretende, através da criação de uma metodologia própria, avaliar o potencial de vigilância contido em cada uma das bases de dados cadastrais utilizadas pela PMC para o aumento da eficiência da gestão, de maneira que foram categorizados e quantificados os campos de dados armazenados. Para a avaliação do potencial de vigilância foi criado um Índice de Vigilância que pretende classificar os cadastros municipais a partir da avaliação de três parâmetros: dados sensíveis, valor comercial dos dados e múltiplo acesso.

A coleta e o armazenamento de informações pessoais são práticas de rotina para a gestão pública de uma cidade, sendo utilizadas para o funcionamento da maior parte dos serviços de atendimento à população. Entretanto, ainda é pouco discutido, no âmbito da gestão pública, sobre a relação desses sistemas de dados pessoais com a invasão de privacidade e as práticas de vigilância tecnológica. Nesse sentido, surge o questionamento sobre que tipos de dados pessoais são gerenciados por uma prefeitura e quais são as possíveis implicações que o armazenamento dessas informações representa para a privacidade e a cidadania plena dos indivíduos cadastrados.

Além de informações de identificação, para a implantação de políticas públicas e a provisão de serviços é mais provável que os dados pessoais utilizados sejam relacionados com o objetivo e o público alvo dessa ação. Os serviços públicos e as políticas mais críticas em termos de invasão de privacidade são aquelas que tratam de populações vulneráveis socialmente, ou seja, que atendem grupos de risco ou lançam mão de dados sensíveis para o seu funcionamento.

A partir dessas premissas, esta dissertação está dividida em seis capítulos. Na sequência da Introdução está o Referencial Teórico, Capítulo 2 dividido em dois subcapítulos: o primeiro aborda o tema da vigilância, a partir de seu desenvolvimento teórico e implicações práticas; enquanto a segunda parte discute a relação das TICs com as cidades contemporâneas, passando de análises sobre a estrutura da rede global de cidades e anulação das distâncias até a problematização da vigilância no meio urbano.

O Capítulo 3 dispõe sobre a metodologia adotada e os procedimentos para a coleta e análise dos dados com a composição de um índice de vigilância, bem como

uma descrição da unidade-caso: a cidade de Curitiba e a PMC. O Capítulo 4 traz a análise dos resultados a partir dos tipos de classificação estudados e do índice de vigilância, e, por fim, as conclusões, limitações da pesquisa e sugestões para trabalhos futuros no Capítulo 5.

1.1 OBJETIVO

1.1.1 Objetivo geral

Analisar o potencial de vigilância dos sistemas de armazenamento de dados pessoais na gestão pública das cidades, considerando o caso da Prefeitura Municipal de Curitiba-PR.

1.1.2 Objetivos específicos

Este trabalho tem como objetivos específicos:

a) Entender a implicação da coleta e armazenamento de dados pessoais como tecnologia de vigilância quando utilizada na gestão urbana.
b) Identificar e classificar os tipos de dados pessoais armazenados pela Prefeitura Municipal de Curitiba.
c) Elaborar metodologia para a construção de um Índice de Vigilância para Bancos de Dados Pessoais a partir de critérios extraídos da revisão de literatura sobre proteção de dados, privacidade e vigilância.

2 REVISÃO DE LITERATURA

2.1 VIGILÂNCIA E SOCIEDADE.

No ano de 1948, o escritor britânico George Orwell (2009) escreveu sua obra mais célebre, o romance 1984 (Nineteen Eighty-four), na qual narra a vida do protagonista Winston Smith em uma sociedade totalitária comandada pelo Grande Irmão, uma instituição onipresente e onisciente. O autor publicou sua distopia como uma crítica aos estados totalitários surgidos na primeira metade do século XX, mas até hoje permeia a imaginação popular como a representação dos medos atrelados a um Estado repressivo e controlador, onde não há privacidade ou liberdade. O regime descrito no livro lança mão de dispositivos de monitoramento constante para atingir o controle total sobre as pessoas, tornando a obra uma referência recorrente quando se fala de estudos sobre vigilância.

O paradigma da vigilância atual não é o mesmo descrito por Orwell, mesmo considerando que hoje vivemos em uma panaceia tecnológica de vigilância ubíqua, pois o Estado não é o único detentor dos dispositivos de controle, além de que os fins e justificativas no mundo contemporâneo não coincidem com a dimensão do autoritarismo do Grande Irmão. Entretanto, a vigilância está mais presente do que nunca e deve ser analisada como um elemento central para o funcionamento da sociedade de hoje.

Atualmente, tecnologias de informação fazem parte do nosso dia-a-dia e compõem uma estrutura de vigilância global da qual é praticamente impossível se manter externo. Por exemplo: câmeras de segurança, bancos de dados, transações bancárias, senhas de acesso, imagens aéreas, dispositivos com GPS, e outros, são algumas das formas de registro das nossas ações. Esses dispositivos onipresentes servem tanto para o controle e a segurança nacional, envolvidos nos discursos antiterror, e a segurança urbana, mas também são ferramentas de manutenção da modernidade, dentro do paradigma da eterna busca pela eficiência máxima, e aos objetivos capitalistas de otimização do comércio através de estratégias de marketing que pressupõem a utilização de dados pessoais.

Dessa forma, as tecnologias de vigilância compõem o rol de tecnologias de informação que são utilizadas em múltiplos e ubíquos processos cotidianos, inclusive

nos governos e órgãos públicos em todas as escalas de domínio, ou seja, do supranacional ao municipal. Nesse contexto, a vigilância faz parte da rotina, do controle e da gestão das cidades, especialmente através de dispositivos tecnológicos que permitem a coleta e o armazenamento de dados em tempo real para a automatização de sistemas e o auxílio nas tomadas de decisão pelos responsáveis pela administração municipal.

Este capítulo traz, através da discussão de autores de referência, a evolução do pensamento, dos conceitos e teorias sobre a vigilância em suas diversas interpretações dentro de um paradigma de modernidade, para que, dessa maneira, possam ser entendidos os problemas e questões associados a emergência de uma vigilância tecnológica global, baseada na coleta e manipulação de dados pessoais, e suas relações com a sociedade contemporânea. O entendimento desses conceitos para o trabalho deve também levar em conta o reconhecimento de suas tecnologias e processos, suas implicações institucionais e governamentais, e também sua manifestação no Brasil.

A discussão inicia-se a partir do conceito central em torno do qual se estabeleceram os principais estudos epistemológicos sobre vigilância: o panóptico; que em essência é um modelo espacial que permite a visibilidade total dos indivíduos controlados. Ou seja, o modelo panóptico, descrito por Jeremy Bentham no século XVIII e analisado por Michel Foucault em 1975, funciona de forma análoga ao narrado no livro de Orwell, onde a tecnologia permite que o cidadão esteja exposto eternamente ao escrutínio de um vigilante invisível.

2.1.1 O panóptico

No final do século XVIII, o filósofo inglês Jeremy Bentham desenvolveu o conceito daquilo que, para ele, seria uma estrutura de vigilância ideal: o Panóptico (BENTHAM et al., 2008). A partir da observação de um projeto de uma prisão, o filósofo expandiu a utilidade de vigilância, ou inspeção, a atividades humanas diversas, com a intenção de:

> [...] punir o incorrigível, encerrar o insano, reformar o viciado, confinar o suspeito, empregar o desocupado, manter o desassistido, curar o

> doente, instruir os que estejam dispostos em qualquer ramo da indústria, ou treinar a raça em ascensão no caminho da educação; [...] (BENTHAM et al., 2008, p. 19).

O Panóptico se constitui de uma estrutura de planta circular em forma de anel com um pátio fechado central. Na circunferência do edifício se localizam as celas dos detentos, ou indivíduos sob inspeção, com aberturas de visibilidade para os dois lados externos do cômodo, permitindo a passagem de ar e luz através desses ambientes até o pátio central, porém sem aberturas entre eles. No centro do pátio circular ficaria uma torre de vigilância, onde os inspetores poderiam observar todas as celas, porém, utilizando-se venezianas e divisões internas, os indivíduos observados não teriam visão da ocupação nessa estrutura. Dessa forma os detentos não poderiam ter certeza se de fato estão sob vigilância (BENTHAN, 2008).

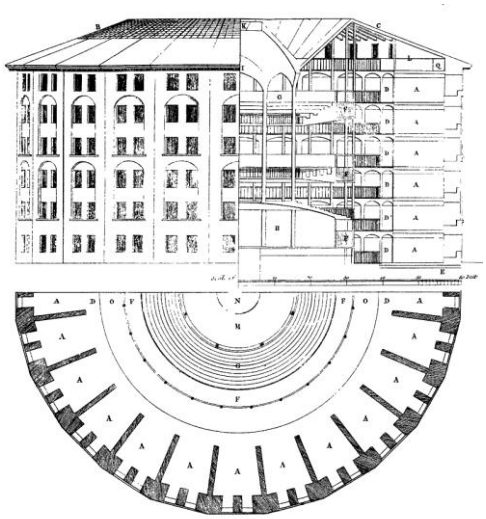

FIGURA 1: PLANTA, CORTE E ELEVAÇÃO DO PANÓPTICO DE BENTHAM DESENHADO POR WILLIAM REVELEY, 1791
FONTE: BENTHAN, 2008

Para o filósofo, quanto mais frequente for a inspeção dos detentos, melhor será o funcionamento do estabelecimento que assim o fizer, sendo o ideal a vigilância individual e constante a cada momento. Como tal nível de observação é impraticável, o desejável, então, é que o indivíduo observado pense que está sendo vigiado todo o tempo, sem razão aparente para acreditar que não se encontra sob o olhar de um inspetor. Dessa forma, o modelo sugerido por Bentham permite a assimetria total da observação entre os encarcerados e os inspetores, criando a incerteza da observação

de fato, estabelecendo estabelece uma realidade potencial de vigilância constante (BENTHAM et al., 2008).

A aplicação desse conceito nos espaços institucionais serviria como instrumento de controle das ações sociais, contendo comportamentos criminosos ou que fossem contrários às normas sociais, sendo assim, nocivos à ordem social e à sociedade como um todo. A agenda do ideal racionalista estava em ascensão com a emergência da industrialização, da economia política e das novas interpretações religiosas presentes na Inglaterra contemporânea aos conceitos de Bentham (BENTHAM et al., 2008).

O conceito do Panótico de Bentham é fundamental para se compreender a vigilância atual, pois baseou estudos posteriores fundamentais sobre o tema, especialmente os escritos publicados sobre a “sociedade disciplinar” do filósofo francês Michel Foucault e teorias derivadas dos conceitos desenvolvidos nesses trabalhos. Foucault em sua obra Vigiar e Punir: O Nascimento das Prisões, de 1975, trouxe uma perspectiva nova sobre a sociedade moderna com a análise da transição da “sociedade do poder soberano” para a “sociedade disciplinar”, onde o modelo panóptico seria a estrutura básica do exercício do poder moderno (FOUCAULT, 2013).

O filósofo francês trata essa transição e suas transformações práticas como mudanças na forma como o poder é exercido. A análise feita por Foucault é fundamental para o entendimento da vigilância enquanto uma ferramenta de exercício do poder e do controle, colocando-a como central na manutenção da ideologia moderna através dos processos de visibilidade e individualização, onde o controle é automático e inerente ao sistema.

O exercício do poder nas sociedades de soberania, que eram a forma dominante na Europa até o final século XVIII, deveria ser visível, a fim de provocar emoções naqueles sobre os quais ele incidia. O controle dos corpos nessa sociedade era através do medo da punição corpórea, ou seja, o suplício. A transição das técnicas de punição aconteceu de forma gradual, de forma que a execução deixa de ser realizada sob o escrutínio público e passa a ser realizada no interior das instituições penais, tornando-se um processo jurídico-administrativo de supressão de um bem ou direito e não uma fonte de sofrimento exemplar. Ou seja, o exercício do poder se transforma, se institucionaliza, compartimentaliza e burocratiza seus processos em uma lógica racionalista moderna (FOUCAULT, 2013).

Com a diminuição gradual da execução de penas capitais, o corpo, então, passa a ser alvo da supressão do direito à liberdade como forma de punição pela prática de crimes e delitos. O encarceramento e o trabalho forçado tornam o corpo dócil, submisso e disciplinado através do controle da mente em um movimento de coerção contínuo. Assim, as disciplinas são as ininterruptas coerções para prática de processos de atividades, de forma a utilizar e otimizar o tempo, o espaço e os movimentos dos corpos, impondo-lhes uma relação de “docilidade-utilidade” (FOUCAULT, 2013).

Para ser efetivo, o poder disciplinar inverte o sentido da visibilidade do poder soberano, onde a ação deve ser demonstrada, pois na disciplina o poder se faz invisível mas torna compulsória a exposição do indivíduo submetido, que se converte em objeto esvaziado de sua subjetividade sob o controle dos mecanismos disciplinares. Essa associação entre a ação do poder e a sujeição em uma relação de visibilidade assimétrica, onde o súdito é sempre observado, é análoga àquele presente nos conceitos e esquemas do Panóptico de Jeremy Bentham. No entendimento de Foucault, o panóptico é o modelo arquitetural da sociedade disciplinar (FOUCAULT, 2013).

A consciência da exposição permanente dos corpos, independente da ação vigilante de fato estar ocorrendo sobre eles em dado momento, é o que mantém a estrutura disciplinar funcionando sem a existência de uma fonte de poder expressa. Assim, a vigilância se manifesta constante em seus efeitos mesmo que sua ação seja intermitente, fazendo com que a relação de poder seja mantida independente de quem o pratica, cuja dinâmica automatiza e desindividualiza o poder (FOUCAULT, 2013).

De acordo com o autor, esse novo modelo de organização representa uma nova economia do poder e é uma invenção da sociedade burguesa, onde ele foi uma das bases do capitalismo industrial e da sociedade moderna (FOUCAULT, 1984). Michael Hardt e Antônio Negri acreditam que o sistema disciplinar conduziu toda da primeira parte de acumulação do sistema capitalista moderno através de sua rede de mecanismos que produzem e regulam costumes, hábitos e práticas produtivas (HARDT; NEGRI, 2000).

A estrutura disciplinar se sustenta através da vigilância, em oposição às taxas e obrigações do sistema de soberania, trazendo por objetivo o aumento da força dominada na nova economia política do poder, característico da sociedade moderna,

a qual o autor chama de “governamentalidade”. Segundo Foucault, saímos de uma era do espetáculo e passamos para a era da vigilância, onde “[...] os faustos da soberania, as manifestações necessariamente espetaculares do poder se apagaram um por um no exercício cotidiano da vigilância [...]” (FOUCAULT, 2013, p. 205).

Na lógica de Foucault, a vigilância passa a ser um conceito fundamental para que possamos entender os exercícios de poder presentes nas relações sociais, onde a estrutura panóptica sustenta as relações de poder e controle. Mais do que isso, para David Murakami Wood (2003), o trabalho sobre o panopticismo desenvolvido por Foucault foi a pedra fundamental para o crescimento dos estudos e teorias contemporâneos sobre vigilância.

O sociólogo Bart Simon (2005) aponta como uma questão importante a dualidade dos processos panópticos, que podem ser focadas nas técnicas de vigilância invisíveis e contínuas – o ponto de vista do inspetor – ou na auto-disciplina e controle da mente causada sobre o detento. Nesse sentido, apesar de concordar que a metáfora do panóptico pode ser estendida para as relações de poder atuais, o autor ressalta que é importante considerar que a posição de observado por si só não garante o exercício do controle, sendo necessário uma atitude voluntária e um conhecimento das regras para que possam se adequar aos imperativos do sistema. Essa perspectiva garante a agência dos vigiados, que depende de instrumentos além do panóptico para que se crie o desejo pela conformidade e possa reconhecer os locais e momentos em que as regras e protocolos devem ser respeitados (SIMON, 2005).

Por outro lado, os mecanismos de observação, inspeção e diferenciação também são fundamentais para o esquema panóptico, especialmente para as interpretações sobre a vigilância contemporânea. As tecnologias de vigilância atuais – como as câmeras de circuitos internos, bancos de dados pessoais, etiquetas de rastreamento, etc – podem ser entendidas dentro da lógica do panóptico, mas apresentam uma diferença fundamental do modelo clássico: não há enclausuramento espacial. Simon argumenta que essa falta de restrição física torna praticamente impossível o escrutínio ininterrupto, além de que permite ao indivíduo a distração e o esquecimento sobre o estado de monitoramento, enfraquecendo o governo das mentes, a normatização e a disciplina (SIMON, 2005).

A partir do entendimento da sociedade disciplinar identificada e analisada por Foucault, constatamos que a exposição é a posição de sujeição, enquanto o domínio do posto de observação é o que viabiliza a aplicação do poder. De acordo com comentadores contemporâneos (HARDT, NEGRI, 2000; MURAKAMI WOOD, 2003; SIMON, 2005), entendemos que, além de basilar para o desenvolvimento da vigilância enquanto disciplina, tal relação panóptica pode ser transposta a muitos mecanismos de vigilância atuais, mas não encerra suas características, técnicas, processos e efeitos.

2.1.2 Para além do panóptico: Controle, Risco e Administração do Medo

O panóptico é um conceito bastante versátil e adaptável, condição tal que permite inúmeras interpretações e releituras, colocando-o frequentemente como o paradigma central da análise dos mecanismos de controle social. Porém, conforme já comentado, diversos autores argumentam que, apesar de importante no debate sobre vigilância, o panóptico apresenta limitações que não são capazes de se estender aos processos atuais de vigilância e o impacto das tecnologias de informação e comunicação como ferramentas de controle (LYON, 2013; LYON, 2006; BOGARD, 1996; MATHIESEN, 1997).

A sociedade disciplinar descrita por Foucault tem suas origens relacionadas à transição para a era moderna, que se deu a partir das ideias iluministas, do surgimento dos processos industriais e do sistema capitalista. Entretanto, a sociedade contemporânea já não corresponde a esse modelo de fixidez institucional próprio do capitalismo industrial e, por consequência, da estrutura disciplinar da sociedade. De acordo com o filósofo Gilles Deleuze (2013), a partir do final da Segunda Guerra Mundial, as estruturas disciplinares começaram a se desestabilizar. O confinamento deixou de ser um imperativo para o domínio dos corpos, agora ele extravasaria os limites institucionais, permeando a vida dos indivíduos.

A produção disciplinar depende da individualização como forma de separar e hierarquizar os corpos, atribuindo funções específicas de acordo com um conjunto próprio de características desenvolvidas. Já a sociedade de controle atribui aos seus indivíduos valores separados – cifras – que podem ser catalogadas em bancos de dados, tornando-os “dividuos”, pois passam a ser divisíveis em suas características

cifradas. As informações dos “divíduos” são transformadas em estatística, traduzidas em mercados, controles de acesso, amostras, etc. (DELEUZE, 2013).

A distribuição das informações, então, passa a ser um fator de ruptura exemplar entre a sociedade disciplinar e de controle. Enquanto na disciplina as informações são localizadas fisicamente em cada uma das instituições, para o controle os dados são disponíveis em redes de múltiplo acesso. Ou seja, a vigilância passou da escala institucional integral e localizada, agindo diretamente sobre o sujeito dentro da instituição e definindo sua identidade, para a global e espacialmente pulverizada para a gestão dos dados cifrados, promovendo um controle mais sutil, ininterrupto e generalizado sobre as pessoas (DELEUZE, 2013).

Deleuze associa a emergência do controle ao desenvolvimento das tecnologias digitais, que são capazes de armazenar e processar os bancos de dados. As instituições – a família, a escola, a fábrica, a caserna, o hospital e a prisão bem como os próprios Estados – então, deixam de ser espaços fechados e se transmutam em valores cifrados, maleáveis, deformáveis e oscilantes, que são livremente distribuídos nas redes de dados (DELEUZE, 2013).

A disponibilidade em tempo real dos dados, arquivados em uma rede de armazenamento digital ubíqua, permite a observação dos fenômenos independentemente da localização espacial e dimensional dos sujeitos. O filósofo e urbanista Paul Virilio (1993) argumenta que, com o desenvolvimento tecnológico, a ortodoxia ortogonal perde seu sentido frente aos métodos eletrônicos de avaliação do tempo e do espaço.

Partindo da avaliação de Virilio de que a “observação direta dos fenômenos visíveis é substituída por uma teleobservação na qual o observador não tem mais contato imediato com a realidade observada” (VIRILIO, 1993, p. 23), é flagrante a relação entre as tecnologias digitais e a transformação da visibilidade da lógica disciplinar para a lógica do controle. A visibilidade presencial panóptica é potencializada pela observação fragmentada dos “divíduos”, que passam ser pulverizados em redes de dados cifrados.

Tal distribuição reticular é análoga ao conceito de sociedade em rede descrito pelo sociólogo Manuel Castells (1999), onde as redes operam manipulando indivíduos, instrumentos, capital, territórios, e outros atores, a fim de atingir seus objetivos estratégicos. As novas tecnologias exercem um papel decisivo na

construção desse novo padrão, pois têm uma lógica própria, baseada na junção e disseminação de informação em um sistema comum, com uma distribuição cada vez mais abrangente e velocidade de processamento e armazenamento cada vez maiores (CASTELLS, 1999).

A convergência das tecnologias em um sistema integrado e sua penetrabilidade na sociedade são fatores que diferem as ferramentas atuais daquelas das outras revoluções tecnológicas. A integração das ferramentas de informação em um sistema unificado significa que as novas tecnologias estão cada vez mais imbricadas em uma rede de comunicação e processamento de informação comum, entretanto seu paradigma não se desenvolve em um sistema fechado, mas como uma rede aberta em diversos pontos de entrada (CASTELLS, 1999).

Dessa forma, o poder na sociedade de controle é desarticulado, desterritorializado e desmaterializado, estando, de acordo com Hardt e Negri (2000), imanente no campo social. O controle, assim, se faz presente tanto no corpo como na mente dos cidadãos, que agora são gerenciados por máquinas e sistemas tecnológicos. Os autores apontam o controle como a intensificação e generalização da disciplina, podendo se estender para além das limitações espaciais e institucionais para as redes flexíveis de dados (HARDT, NEGRI, 2000).

Cabe o adendo que, de acordo com Foucault (1984), tanto a disciplina como a soberania nunca foram totalmente substituídas, mas atuam conjuntamente na gestão da população. O poder na sociedade de controle, portanto, pode ser exercido na lógica de outros modelos, mas consideramos a exclusividade das ações estabelecidas nas redes globais como próprias dessa estrutura social e de poder conceituada por Deleuze.

A informações cifradas, que podem ser individuais, institucionais ou ambientais, se encontram disponíveis nos bancos de dados globais para escrutínio de atores públicos ou privados e são fundamentais para a prática da vigilância contemporânea. As técnicas de vigilância podem, então, contar com um novo leque de ferramentas e possibilidades de ação, se estendendo por todo o corpo social, trazendo novas formas de lidar com os perigos e os medos em uma sociedade controlada.

A sociedade que sucedeu a Segunda Guerra Mundial tem características próprias que, de acordo com o conceito de sociedade de controle, a especificam em

relação à estrutura disciplinar, ou seja, à modernidade industrial clássica. O desenvolvimento tecnológico, especialmente o advento da informática, o avanço das ciências e a radicalização da racionalização, são marcas distintas desse período ainda atual. A compreensão do panorama no qual estamos trabalhando no escopo dessa conceituação teórica depende, como fator fundamental, da análise da configuração social necessária para o estabelecimento dos processos de vigilância em atividade no mundo contemporâneo.

O sociólogo Ulrich Beck (2010) concebe a realidade da modernidade atual como um conjunto de riscos e perigos inéditos nas sociedades humanas. O paradigma do risco como elemento central para o entendimento da sociedade é próprio da modernidade secundária associada a reflexividade, que é aquela que, segundo o autor, sucede a modernidade industrial primária, cujas premissas foram estabelecidas pelos observadores sociais do século XIX (BECK, 2010).

A modernidade reflexiva é um conceito adotado tanto por Beck como pelo sociólogo britânico Anthony Giddens (1991). De acordo com este, reflexividade se refere a relação entre o pensamento racional e a ação, onde a segunda sempre está dependente da primeira, criando uma quebra com a tradição, que não necessariamente se baseia em princípios de racionalidade. Dessa forma, as práticas modernas estão sempre se transformando à luz dos novos conhecimentos sobre elas próprias. Com a substituição das verdades da tradição pela racionalidade moderna seria de se esperar uma maior certeza sobre os conhecimentos aplicados, porém, com a radicalização da reflexividade na modernidade tardia, nunca é possível se assegurar que dado conhecimento não será revisado (GIDDENS, 1991).

Com a quebra dos valores tradicionais, as instituições modernas também são atingidas, desestruturadas e revistas pelo ciclo da contestação reflexiva. Em 1967, o autor situacionista francês Guy Debord (1997) já reconhecia na sociedade, chamada por ele de “espetáculo”, essa constante baseada na mudança:

> O que o espetáculo oferece como perpétuo é a mudança, e deve mudar com sua base. O espetáculo é absolutamente dogmático e, ao mesmo tempo, não pode chegar a nenhum dogma sólido. Para ele, nada para; este é seu estado natural e, no entanto, o mais contrário à sua propensão. (DEBORD, 1997, p. 47).

Para Beck, a diferença entre a modernidade industrial, ou modernidade primária, e a modernidade reflexiva é que na primeira a produção de bens se sobrepõe à geração de riscos, enquanto que, com radicalização da reflexividade e a acumulação de conhecimento sobre as práticas dela decorrente, a lógica se inverte no desenvolvimento do projeto moderno. As forças de produção não podem mais se acobertar da insciência dos perigos que podem causar, o fundamento passa então a ser o da produção de riscos que vem em decorrência da produção de riquezas, ou seja, de um paradigma de distribuição de bens no primeiro momento da modernidade passamos para outro onde os riscos são partilhados (BECK, 2010).

O risco sempre esteve presente nas atividades humanas, não é uma invenção da modernidade, porém com a modernidade industrial eles passaram ser produzidos em série como um produto, ou subproduto, do desenvolvimento tecnológico e da industrialização, podendo agora ter alcance global e independem da disposição pessoal para assumi-los, sendo reproduzidos e agravados na mesma velocidade em que o progresso avança (BECK, 2010).

Se em civilizações passadas as catástrofes, desastres e infortúnios eram atribuídas a forças divinas ou meras fatalidades, hoje o risco traz o fantasma do perigo conhecido, mas que não foi evitado. Nesse sentido a reflexividade atua como um agente duplo: por um lado produz o conhecimento imanente dos perigos associados a uma determinada prática industrial, por outro provoca a incerteza quanto a credibilidade da avaliação de um risco, que pode ser revogado em uma análise posterior. O indivíduo sob as ameaças modernas encontra-se sempre na questão de como lidar, no campo da ação ou psicologicamente, com os riscos que fazem parte da sua vida (BECK, 2010).

O sociólogo francês Robert Castel (2005) argumenta que com a individualização moderna o sujeito passa a ser responsável pela própria segurança através de sua propriedade privada e, livre da proteção coletiva das instituições tradicionais, cobra do Estado uma demanda virtualmente infinita de segurança, tanto civil como social. Essa reivindicação muitas vezes entra em conflito com os princípios de liberdade e do estado de direito democrático dos países ocidentais, o que gera uma sensação de insegurança generalizada até nas sociedades das nações desenvolvidas – que possuem o ambiente mais seguro já registrado na história, tanto

em relação aos baixos índices de criminalidade, como as altas expectativas de vida associadas a eficiência da medicina moderna (CASTEL, 2005).

A partir do reconhecimento da incapacidade da ciência de gerar segurança, que, pelo contrário, cria novas formas de perigo, Virilio (2012) coloca o medo na sociedade atual como uma ocupação física e mental. Com esse pressuposto, o autor aponta que a administração do medo é utilizada como política de Estado, que busca assegurar a segurança dos seus cidadãos, ao mesmo tempo que, com a militarização da ciência, há o equilíbrio do terror como motor da manutenção dos medos. Nesse sentido, tanto o medo quanto sua administração pelo Estado são dependentes da velocidade e da tecnologia, sendo que a dominação técnico-científica reproduz o próprio medo em sua ocupação física e mental (VIRILIO, 2012).

Os sociólogos Kevin Haggerty e Richard Ericson (1997) analisam a transição das políticas coercitivas e disciplinares para as políticas de gestão dos riscos. As propriedades de mobilidade e individualidade dos cidadãos tem provocado a uma revisão da aplicação do poder do Estado, levando as democracias liberais a adotarem sistemas de governança da segurança descentralizados, desterritorializados e distributivos. Esses sistemas passam de uma distribuição igualitária de segurança e liberdade para uma distribuição onde os riscos são atribuídos de maneira desigual, de forma que seja otimizada a provisão de segurança para as populações atendidas (HAGGERTY; ERICSON, 1997).

Essa administração dos riscos é profundamente dependente de tecnologias de vigilância e gestão de informações. Dentro da lógica reflexividade, Haggerty e Ericson apontam o paradoxo dessa relação com as tecnologias de informação e vigilância: quanto mais desenvolvidas essas ferramentas, maior a capacidade de identificar novos riscos, gerando um movimento contínuo de demanda por tecnologias cada vez mais eficientes em prever e solucionar perigos ao mesmo tempo em que identificam novas ameaças (HAGGERTY; ERICSON, 1997).

Essa dinâmica provoca demandas cada vez maiores por soluções tecnológicas que registrem os deslocamentos das populações no espaço e no tempo, enquanto traça perfis de risco a determinadas populações. Com isso a prioridade dos sistemas de segurança se torna a produção e a rápida disseminação do conhecimento de riscos. Essa condição afere uma relação negativa com o Estado, que outrora provia segurança, agora produz e distribui os riscos (HAGGERTY; ERICSON, 1997).

As noções de comunidade são revistas com os conhecimentos de riscos; comunidades de risco são formadas com a distribuição de informações sobre as ameaças. As classificações de risco não são destinadas a compreender as complexidades culturais dos variados grupos populacionais, mas estabelecem falsas noções de homogeneidade desses grupos. Logo, tais processos são dirigidos por uma racionalidade instrumental que objetiva uma maior governabilidade de populações diversas (HAGGERTY; ERICSON, 1997).

As análises dos riscos sob o paradigma da reflexividade nos levam ao entendimento de um processo ininterrupto de identificação, prevenção e criação de novos riscos. Tais processos dependem de tecnologias que devem coletar e analisar os dados que serão utilizados nesse processo de vigilância constante. A administração dos medos e dos riscos tornaram-se uma agenda política prioritária, onde tanto a sua criação como sua mitigação fazem parte de uma lógica presente no dia-a-dia das pessoas em uma escala global.

2.1.3 A “Nova Vigilância”

Dado o panorama estabelecido pelos teóricos que tratam do paradigma atual da modernidade, compreende-se que o fundamento sociedade contemporânea está intrinsecamente associado à racionalização e ao desenvolvimento tecnológico. Nesse cenário, como elemento definidor, as tecnologias e as práticas de vigilância operam na manutenção do controle social e da hegemonia institucional. A extensão da presença dessas tecnologias, bem como o papel que desempenham na sociedade, caracterizam um modelo de vigilância global distinto dos modelos conceituais que o antecederam. Essa nova configuração da vigilância tem sido caracterizada por alguns pesquisadores da disciplina como “nova vigilância”.

É nessa linha que se coloca a definição de vigilância utilizada para os fins desta pesquisa, conforme estabelecido por David Murakami Wood e outros pesquisadores centrais da disciplina:

> Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement,

> management, influence or protection […]. (MURAKAMI WOOD *et al.*, 2006)

O sociólogo David Lyon (2013) coloca o enfoque de seu discurso acerca da vigilância sobre as tecnologias computadorizadas, que configuram essa “nova vigilância”. Apesar de formas tecnológicas de vigilância terem sido utilizadas em espionagens e operações de inteligência, atualmente os processos de captura digital de dados tem uma extensão global, onde o indivíduo comum se encontra sob esse tipo de escrutínio diariamente (LYON, 2013).

A vigilância, para Lyon, não está somente relacionada às ações do Estado sobre os cidadãos, mas também se encontra na coleta de informações pessoais utilizadas para fins privados. Dados pessoais coletados por organizações privadas ou públicas são trocados ou vendidos para uso comercial: pesquisas de mercado, tendências de consumo e propaganda direcionada. Tais práticas não possuem restrições legais claras e operam em escala mundial, naquilo que o autor caracteriza como “sociedade de vigilância” (LYON, 2013).

A vigilância eletrônica é generalizada a todas as áreas da sociedade, sendo relacionada tanto a fatores de segurança como para a eficiência dos processos modernos e capitalistas. Dessa forma, a vigilância tratada por Lyon é o processamento de dados pessoais com o propósito de cuidar ou controlar, de influenciar ou gerir pessoas e populações, sendo que os processos de poder são intrínsecos ao exercício da vigilância (LYON, 2009a).

De acordo com Gary T. Marx (2002), a “nova vigilância” é composta unicamente por práticas tecnológicas, ou seja, para ele a vigilância é a extração e criação de dados pessoais através de meios tecnológicos. A coleta dos dados é geralmente realizada em tempo real através de um processo remoto, onde a disponibilização dos dados é, geralmente, feita de forma involuntária. As informações coletadas então são armazenadas ou classificadas e podem ser distribuídas em uma rede de dados (MARX, 2002).

Apesar de uma suposta racionalidade associada às tecnologias, do mesmo modo como podem ser percebidos os riscos de Beck, as consequências da vigilância eletrônica podem ser imprevisíveis, pois seus pontos de coleta de dados estão espalhados pela vida das pessoas e muitas vezes são invisíveis. A estrutura de

vigilância se sustenta a partir da coleta e compartilhamento de informações que conectam em um rizoma de transferência de dados e acordos políticos e comerciais praticamente indetectável (LYON, 2003).

Essa estrutura rizomática e instável, dependente dos fluxos que se movem entre os nós e não possuem uma limitação formal, é análoga ao assemblage de vigilância descrito por Haggerty e Ericson (2003). O modelo estabelecido pelos sociólogos é a de uma organização da vigilância a partir de seus componentes conectados em um processo contínuo de estabilização da estrutura, bem como a abstração e desterritorialização dos corpos, com a criação de duplicatas desses indivíduos vigiados em locações distintas, tal qual os divíduos descritos por Deleuze (HAGGERTY; ERICSON, 2003).

A prática rotinizada de coleta e dados pessoais está presente no dia-a-dia de praticamente qualquer indivíduo em uma sociedade ocidental desenvolvida. Todas as transações eletrônicas são registradas, imagens capturadas em câmeras de circuitos fechados de televisão (CFTV), localizações de GPS (Global Position System) anotadas em sistemas georreferenciados; o nível de pervasividade dos processos de vigilância é integral (LYON, 2013). Entretanto, William Bogard (1996) vê o objetivo da vigilância além da omnisciência panóptica. O autor acredita que o objetivo final da vigilância não é saber tudo o que está ocorrendo em tempo real, mas poder prever todas as ações antes que de fato ocorram, evoluindo para a “hipervigilância” (BOGARD, 1996).

Apesar da documentação pessoal associada a um controle governamental ser tão antiga quanto a própria civilização, para Lyon (2009b) sua forma atual, que se apoia em bancos de dados, se diferencia por ser remota, categorizável, interoperacional, fazer análises de riscos, ser físico e comportamental, e exclusivo. O autor aponta para uma forma de governo baseado na identificação e no uso de documentos eletrônicos. Assim, a identificação se sobrepõe e antecede a identidade, reduzindo uma questão complexa e conflituosa a dados abstratos categorizados por sistemas operacionais cujas regras devem se adequar a protocolos de segurança internacionais, que firmam uma divisão social entre aqueles que podem se deslocar livremente e estabelecer cidadania, e aqueles que não podem (LYON, 2009b).

A coleta, processamento e circulação de dados pessoais já era entendido como vigilância por Roger Clarke (1988), que chamou esse processo de “dataveillance”, ou

vigilância de dados. De acordo com Clarke, a dataveillance pode ser individual ou de massa. A primeira se refere ao escrutínio dos dados pessoais de um indivíduo definido, enquanto a segunda mobilidade diz respeito à vigilância de grupos onde há um interesse ou uma suspeita generalizada (CLARKE, 1988). Para tanto, Clarke (1988b) alerta para o fato de que para ter uma situação de vigilância ubíqua, através da análise de dados pessoais e identificação de “perfis de risco”, não é necessário um banco de dados unificado, mas somente a conexão entre diferentes bases processando dados para fins diversos. Dessa forma, a interconexão de informações, em princípio, desassociados pode viabilizar combinações que promovem o melhoramento da segurança pública e fornecimento de serviços, mas também definem a inclusão ou exclusão de pessoas ao acesso da cidadania (LYON, 2009b).

No mundo contemporâneo, grande parte da população se encontra em deslocamentos internacionais e os sistemas de identificação desempenham o papel de classificar as pessoas não somente como cidadãs ou não, mas também quanto ao seu status em um determinado território, definindo um perfil para aqueles que devem ser recebidos ou ter o acesso bloqueado. A exclusão com base em características pessoais atinge principalmente imigrantes provenientes das periferias globais, sendo especialmente categorizados com base na região de origem, cor de pele, religião ou problemas de saúde, apresentando o perfil de um agente de terrorismo ou de potencial abuso de políticas sociais (LYON, 2009b).

A vigilância massificada provoca um fenômeno que Oscar Gandy (1993) chama de “classificação panóptica”. O autor aponta que os indivíduos são classificados pelos sistemas de vigilância tecnológicos de acordo com seu valor econômico ou político, onde a mobilidade física, social e cultural pode ser avaliada dentro da comodificação das informações pessoais. A disponibilidade dessas informações é capaz de traçar perfis a serem escrutinizados e discriminados dentro de um sistema estabelecido para a racionalização e o controle dos seres humanos (GANDY, 1993). Seguindo a mesma linha, Maria Los (2006) atenta que tal poder institucional está nos levando a uma sociedade totalitária, esse processo através da criação de uma norma a ser aferida a partir os dados individuais registrados que separam a população em uma lógica de verdadeiro e falso para as características desejáveis (LOS, 2006).

As classificações dentro dos sistemas de dados podem resultar em exclusão e discriminação de determinados perfis socioeconômicos, raciais ou culturais. A racionalização da discriminação, a partir de dados estatísticos de grupos populacionais, pode conduzir a uma resposta irracional ou desproporcional, caracterizada por Gandy (2006) como “desvantagem cumulativa”. Essa resposta irracional pode ser identificada, por exemplo, no tratamento diferenciado dado a homens negros pela polícia, que são considerados suspeitos preferenciais, ou os preços desproporcionalmente mais altos dos seguros pagos por negros nos Estados Unidos (GANDY, 2006).

As preocupações de Gandy estão relacionadas com a violação da privacidade, que é um conceito que vem sendo revisto ao longo da história, comumente colocado como inexato e de difícil definição nas discussões sobre vigilância. Os limites da privacidade, ou o que deve ser considerado invasão de privacidade, têm sido cada vez mais estreitados dentro das disputas entre os interesses pessoais frente às empresas e governos ocidentais associados à demanda por novas soluções tecnológicas de vigilância (LYON, 2009a).

É importante colocar que a vigilância não é necessariamente uma prática negativa, pois em muitas situações ela é de fato útil e agrega resultados positivos quando aplicadas em determinados contextos, desde a prevenção de crimes até a eficiência e comodidade oferecida por serviços direcionados ou facilitados pela existência prévia de dados pessoais cadastrados. Por outro lado, está colocada a preocupação com questões de segurança, privacidade e vigilância, fazendo necessária uma análise da ética nos processos de vigilância para que se possa minimizar seus danos potenciais (MARX, 2013).

A questão da ética e transparência nas práticas de vigilância institucionais teve uma grande repercussão a partir das denúncias de Edward Snowden, em 2013, acerca de uma rede de vigilância global envolvendo organizações de inteligência dos Estados Unidos e aliados. Snowden apresentou documentos que revelavam a coleta massiva de informações de comunicação privada de cidadãos comuns em um banco de dados unificado. Tais acontecimentos levantaram diversas questões sobre o acesso de informações pessoais por governos e corporações globais, suas vantagens no combate ao terrorismo e o direito à privacidade em uma sociedade democrática (LYON, 2015).

O conceito de vigilância carrega uma forte carga negativa associada ao Big Brother de Orwell ou o Panóptico de Bentham e Foucault, podendo, de fato, ser utilizada como uma ferramenta de controle e invasão de privacidade. As reações contra a implantação e a expansão, bem como o controle e a transparência, de aparatos de vigilância podem ser de dois tipos, de acordo com David Lyon (2013): a) ações legais ou meios tecnológicos de restringir ou tornar mais seguros os sistemas de vigilância; b) e movimentos de mobilização de opinião e de oposição à vigilância.

Para mitigar questões negativas relacionadas a vigilância, Gandy (2006), por exemplo, sugere o fim do uso de definições de raça ou gênero nas classificações estatísticas dos bancos de dados pessoais, enquanto Kristie Ball (2006) propõe uma rejeição aos sistemas de vigilância corporais, como validações biométricas. Além de organizações independentes em diversas partes do mundo que surgem com discursos e ações de resistência a diferentes práticas de vigilância – como monitoramento de imagens de câmeras de segurança, monitoramento espacial, monitoramento de uso da internet e coleta e processamento de dados.

Assim, compreendemos que lidamos diariamente com sistemas de vigilância que podem operar em uma rede de dados global, em uma complexa estrutura formada por pessoas, processos e tecnologias formando uma estabilidade atingida através da associação e o agenciamento desses elementos, uma *assemblage* de vigilância. Tais práticas podem ter efeitos negativos e possibilitam um nível de controle e invasão de intimidade que vão contra direitos como a liberdade e a privacidade, o que levou ao surgimento de movimentos e a criação de leis de regulamentação contrárias à expansão irrestrita dos sistemas de coleta de dados, imagens e outras informações pessoais.

2.1.4 Tecnologias de vigilância e bancos de dados

A tecnologia é um elemento fundamental para que a estrutura de vigilância, ou a própria “sociedade de vigilância”, se sustenta através de conexões digitais e dispositivos cada vez mais sofisticados, que revelam uma necessidade de monitoramento sempre crescente e criando demanda por mais tecnologia e mais controle. Quanto maior o poder de coleta, armazenamento e processamento de

informações pessoais, sustentado tecnologicamente, maiores são as possibilidades de controle e o poder atribuído aos sistemas de vigilância.

O aparecimento da sociedade de vigilância está associado ao desenvolvimento da computação na década de 70, que tem sido responsável por uma transformação dentro das sociedades modernas, pois permite a redução do trabalho mental, enquanto as tecnologias industriais tradicionais facilitavam a manufatura e a produção de bens (LYON, 2013). Outra possibilidade agregada pelos computadores é a capacidade de se comunicar entre si através dos sistemas de telecomunicação, em uma dinâmica chamada de “internet das coisas” (Lemos, 2013). Essa tecnologia trouxe maior facilidade para os controladores dos sistemas de vigilância de coletar informações pessoais, o que torna o sujeito ainda mais transparente sob o escrutínio de um vigilante corporativo invisível (LYON, 2013).

Mesmo com o modelo de coleta computadorizada de dados alfanuméricos sendo o predominante nas práticas de vigilância atuais, a *dataveillance* descrita por Roger Clarke, outros tipos de tecnologia de coleta e criação de informações pessoais também são utilizados nos processos de vigilância. Murakami Wood *et al.* (2006) as classificam em: telecomunicações; vídeo; base de dados; biométricas; e localização, rastreamento e marcação.

A capacidade de armazenar dados é a maior revolução nas práticas de vigilância contemporâneas em comparação a modelos mais antigos. Dados pessoais podem ser tabulados e cruzados em tempo real e com um suporte físico ínfimo em relação ao volume de dados estocado. A análise desse tipo de informações pode revelar padrões e identificar potenciais suspeitos através de uma “vigilância algorítmica”, cujos tipos de dados podem ser: geográficos, demográficos, psicográficos, e comportamento de consumo (MURAKAMI WOOD et al., 2006).

A criação de dados nesse formato pode acontecer de diversas formas: através de “rastros” de transações e conexões, preenchimento de formulários em rede, logins de acesso, pesquisas orientadas, grupos focais, promoções, cookies de sites na internet, call centers, etc. Os dados coletados são cruzados com outros dados disponíveis de outras pesquisas e geram novas informações estatísticas (MURAKAMI WOOD et al., 2006).

A integração entre tecnologias, ou sinergia, potencializa a vigilância dos sistemas e amplia os propósitos de uma mesma ferramenta. Por exemplo, uma

mesma base de dados pode ser utilizada tanto para fins comerciais de direcionamento de consumo como pode auxiliar em investigações criminais; outro exemplo é o uso de câmeras de segurança privadas para restringir crimes ao patrimônio ao mesmo tempo que servem para controle de funcionários. Seguindo nessa lógica, tem-se notado um esforço conjunto para a criação de sistemas integrados de identificação que cruzam dados de diferentes origens e naturezas (MURAKAMI WOOD et al., 2006).

Muitas vezes as tecnologias de vigilância são invisíveis ou, mesmo que sejam reconhecidas, as relações entre elas e seus responsáveis são ocultas e muito difíceis de rastrear. Essa característica, associada ao grande número de dispositivos que registram dados pessoais em operações cotidianas e alimentam bancos de dados globais, nos leva a uma configuração de vigilância pervasiva, em que a combinação dos diversos formatos de informação são associadas sob o discurso de segurança e "sistemas inteligentes". A utilização de cartões de acesso, senhas, transferências monetárias, compras e vendas, preenchimento de formulários, porte de aparelhos móveis com localizador, comunicação através de dispositivos tecnológicos, registro de imagem em câmeras de segurança, etc., são algumas práticas virtualmente inescapáveis para a maior parte dos indivíduos que vivem em sociedades tecnológicas (MURAKAMI WOOD et al., 2006).

É importante ressaltar que tecnologias de vigilância, como qualquer outro tipo de tecnologia desenvolvido, estão sempre sujeitas a falhas e nem sempre suprem sozinhas a função a qual estão designadas. Entretanto, as falhas desses sistemas normalmente provocam uma demanda por tecnologias ainda mais avançadas e com menor potencial de falha, impedindo a análise de outras soluções não-tecnológicas a um determinado problema ou ameaça (MURAKAMI WOOD et al., 2006).

Com isso, temos que as tecnologias de vigilância estão associadas a processos específicos que promovem uma rede global de agentes, tecnologias e ações voltadas ao controle social e acumulação de informações. As informações podem ser utilizadas posteriormente para fins as quais não foram autorizadas ou mesmo que nem existiam quando foram geradas, abrindo um leque de possibilidades infinitas de utilização desses dados pessoais que podem ser cruzados e sobrepostos ao sabor de intenções políticas ou econômicas.

2.1.5 Governo e vigilância

Como visto anteriormente, desde a explanação sobre o modelo panóptico, a vigilância é uma ferramenta de exercício de poder e controle e, como tal, é esperada a relação desta com o Estado e sua utilização como instrumento de governo. É importante lembrar que, como apontado por Murakami Wood et al. (2006), a fronteira entre o público e o privado muitas vezes é difusa nas práticas de vigilância públicas, onde as ações podem ser executadas por agentes públicos ou privados através de agenciamentos híbridos. Mas especificamos agora o papel da vigilância como instrumento de gestão e política pública, bem como sua relação com o Estado.

Sistemas de vigilância se desenvolveram junto dos estados democráticos e dos direitos dos cidadãos, dessa forma, políticas e formas de gestão pública atuais dependem de sofisticados sistemas de vigilância para funcionar e se tornarem cada vez mais eficientes no cumprimento de seus propósitos. Esses sistemas baseados no acúmulo de informação são utilizados como insumo para a tomada de decisões e o desenho de conclusões sobre assuntos públicos (LYON, 2013).

Com as tecnologias atuais, Estados podem armazenar volumes enormes de informação pessoal de seus cidadãos, que podem ser utilizadas para a melhoria do atendimento e individualização das necessidades de cada um. Entretanto, está justamente no uso do poder de vigilância estatal o fantasma orweliano do totalitarismo, da perda de privacidade e do controle total da vida dos indivíduos. Apesar de não haver, empiricamente, uma relação direta entre regimes totalitários e o uso extensivo de tecnologias de informação, não se pode deixar de lado o potencial de autoritarismo que essas práticas carregam, especialmente contra minorias e populações vulneráveis (LYON, 2013).

A vigilância, como instrumento de governo e política, pode ter duas linhas de intenção distintas: a primeira se refere a eficiência e abrangência dos serviços e da administração pública, focando principalmente no bem-estar social e na economia do Estado; a segunda é a manifestação moderna da interpretação comum da “vigilância”, ou seja, associado a segurança e ao tratamento da criminalidade, cujo paradigma mudou da abordagem de coação para a prevenção baseada em informações.

Uma forma comum de vigilância, não-relacionada a segurança pública, utilizada por órgãos estatais é o controle tributário através de cadastros que cruzam

informações econômicas de um cidadão ou empresa e sua atividade fiscal ou recebimento de políticas assistencialistas. Este tipo de ação propõe reduzir o número de inadimplências e injustiças de cobrança e aumentar a arrecadação do Estado. Associado a mecanismos de controle da eficiência no serviço público, a implantação destes sistemas busca a economia e a otimização dos gastos públicos (LYON, 2013).

Políticas públicas de bem-estar-social demandam cadastros nacionais de cidadãos, que podem ser classificados em grupos preferenciais de atendimento; Sistemas de saúde, educação, previdência, etc., devem ter seus usuários registrados para que possam ser administrados. Para uma maior eficiência dos serviços e um atendimento mais completo, é salutar a unificação de todos os cadastros em um registro único, a fim de evitar desatualizações e informações conflitantes. A partir desse registro único, informações que definem um perfil pessoal podem ser distribuídas entre diversas agências e entidades públicas, cujo propósito é justificado pela eficiência dos processos públicos (LYON, 2013).

Já as práticas de vigilância orientadas à segurança pública são dependentes de registros pessoais e o uso de documentos identificação eletrônica. Redes de informação referentes a indivíduos e veículos são escrutinizados diariamente em ações de comando e controle, onde sistemas de vigilância expandiram as capacidades de informação das organizações policiais. O estado de policiamento total se estende às polícias nacionais dos países desenvolvidos, que detém redes de informações globais não somente sobre indivíduos, mas também sobre outros países, instituições, e seus representantes (LYON, 2013).

Como forma de mitigar seus efeitos e potenciais negativos, a vigilância estatal e privada necessita de regulamentação. A regulamentação de meios de vigilância pode ser feita através de dispositivos legais ou outras técnicas que resultem em efeitos regulatórios. A principal forma de regular a vigilância é a proteção da privacidade dos indivíduos, mas isto somente pode não ser suficiente, então podem ser indicadas outras formas de restrição da vigilância em si (MURAKAMI WOOD et al., 2006).

Governos eletrônicos são modelos de governo que integram nas suas práticas tecnologias de informação em larga escala, tanto nos processos internos como nas interfaces com a população, para que possam prover serviços de maneira mais rápida, confiável e eficiente. Este tipo de governo onde há uma grande dependência de bancos de dados pode ser chamado de “database state”, ou “estado de banco de

dados", e existe uma crescente preocupação com relação a segurança dos dados e a vulnerabilidade da privacidade (HOUSE OF LORDS, 2009).

O discurso do poder público argumenta que é necessária a coleta de informações pessoais para que os serviços públicos sejam mais eficientes e individualizados; para o combate à criminalidade; para reduzir o empenho de cidadãos e empresas; e para reduzir a exclusão social nas suas primeiras manifestações. A gestão pública pode ser mais orientada ao cidadão através da utilização de uma fonte de dados unificada, o que facilita a utilização dos serviços públicos. Entretanto, nem sempre os objetivos se consolidam e muitas vezes os interesses do Estado e dos cidadãos entram em conflito no que tange a coleta e uso dessas informações (HOUSE OF LORDS, 2009).

O Estado tem utilizado cada vez mais tecnologias de vigilância e coleta de dados apoiado em um discurso e maior eficiência dos serviços públicos, redução da criminalidade urbana e combate ao terrorismo global. Esses empenhos trazem a redução da privacidade dos cidadãos, levando a um conflito de interesses entre a modernização cada vez maior do Estado e a manutenção das liberdades e direitos individuais dos cidadãos. Esse paradigma de um Estado de vigilância é predominante nos países do norte desenvolvido, contudo está presente em outras escalas e níveis de integração nos países periféricos.

2.1.6 Vigilância no Brasil

Até hoje o Brasil nunca sofreu um ataque terrorista por agente externo, portanto, a paranoia do inimigo estrangeiro, que envolve a vigilância de fronteiras e bancos de dados para rastreamento de suspeitos, não faz parte do discurso oficial que endossa o uso de ferramentas desta natureza. Apesar disso, há uma grande expansão no uso de tecnologias de vigilância tanto na área do combate à criminalidade, que encabeça os discursos sobre a necessidade deste tipo de intervenção, como na utilização de tecnologias de coleta e monitoramento de dados para fins privados (KANASHIRO et al., 2008; FIRMINO et al., 2013; BRUNO et al., 2013).

Rodrigo Firmino et al. (2013), acreditam que há dois problemas particulares relacionados ao uso de tecnologias de vigilância no Brasil e países da América Latina:

o primeiro seria a falta de leis ou a existência de leis inadequadas que regulamentem a coleta, o armazenamento e a gestão de dados pessoais coletados; a segunda é o debate público insuficiente que não fomenta a participação popular e o interesse na discussão do tema. A justificativa para a adoção de ferramentas de vigilância se apoia na promessa de segurança pública, na possibilidade de eficiência nos processos públicos e privados, ou em um discurso tecnocrático, sendo que dificilmente vem acompanhadas de uma análise crítica que pondere o potencial negativo associado a instalação desses equipamentos (FIRMINO et al., 2013).

O discurso para utilização de equipamentos de vigilância está relacionado à insegurança e ao medo de vitimização criminosa no caso da instalação de câmeras públicas, pois, mais que os cidadãos do norte desenvolvido, os brasileiros vivem sob um risco considerável de sofrer diretamente com a violência. O país registra mais de 58 mil homicídios intencionais e quase 600 mil roubos ou furtos de veículos por ano (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2015), além de uma taxa de vitimização por furtos e roubos em geral que supera 15% da população em um ano (DATAFOLHA; CRISP, 2013).

Popularizadas no setor privado como forma de inibir crimes contra o patrimônio, a demanda para instalação de câmeras de monitoramento no espaço público começou nos anos 80 e se intensificou até os dias atuais. De acordo com Marta Kanashiro et al. (2008), utilização dessas câmeras veio acompanhada da comodificação e da individualização da segurança, associada a consideração do Estado como ineficiente na provisão de proteção aos cidadãos. Com isso, a disposição desses equipamentos e serviços de monitoramento por imagem são vendidos como vantagens em uma lógica de marketing e carregam a promessa higienista de um ambiente livre de indivíduos e situações inadequados (KANASHIRO et al., 2008).

Já no que tange a vigilância no sentido de coleta de dados virtuais, Fernanda Bruno et al. (2013) levantam que os sites e portais brasileiros registram informações pessoais através cookies de navegação. As informações coletadas, com ou sem o consentimento expresso, são enviadas a empresas globais que gerenciam esses dados e os direcionam para serem utilizados em estudos e estratégias de marketing (BRUNO et al., 2013).

Na área da identificação pessoal, Firmino e Murakami Wood (2010) apontam a multiplicidade de sistemas de identificações no Brasil, como a existência do RG, do

CPF, Certidão de Nascimento, Carteira Nacional de Habilitação (CNH), Título Eleitoral e Certificado de Serviço Militar, que são os principais, onde cada um representa um sistema de identificação diferente. Mesmo com essa variedade e a obrigatoriedade de muitos deles para a realização de transações básicas, parte da população ainda não dispõe de nenhum deles, mas pode estar cadastrada no Programa Bolsa Família, que não exige o registro em outro sistema de identificação brasileiro, mas por si só compõe um sistema de informações de famílias de baixa e renda e populações vulneráveis socialmente. Nesse cenário, o governo brasileiro objetiva integrar todos esses sistemas compostos de bancos de dados pessoais, em um sistema único representado por um só documento de identificação nacional (FIRMINO. MURAKAMI WOOD, 2010).

Em suas denúncias em 2013, Edward Snowden apresentou documentos que provavam que o governo dos Estados Unidos estava monitorando a comunicação da presidente Dilma Rousseff. Após o escândalo, a governante brasileira recorreu a instituições internacionais para denunciar o ocorrido e propor regulamentações internacionais que evitem este tipo de invasão, colocando o país a frente de iniciativas de restrição da vigilância em escala mundial. Além disso, internamente, o Brasil reforçou a proteção contra-ataques cibernéticos com investimentos em tecnologia e programas militares de defesa, além de ter aprovado o Marco Civil da Internet, Lei Federal n. 12.965 de 2014, que regulamente o uso e a provisão de serviços de internet no país (ARTIGO 19, 2016).

No âmbito legal, também foi a criada a Lei 12.737 de 2012, conhecida como lei Carolina Dieckmann, que legisla sobre a ilegalidade de invasão de dispositivos e falsificação de acesso. Até recentemente, a legislação brasileira não possuia uma norma geral sobre o uso de dados pessoais, sendo que a matéria é contemplada por provisões constitucionais de caráter geral e normas setoriais, como o Código de Defesa do Consumidor (DONEDA, 2009).

Com o crescimento cada vez maior do acesso à internet e das preocupações sobre sua regulamentação e de proteção das informações pessoais, em 2014, foi aprovado no Brasil o Marco Civil da Internet, Lei 12.965 de 2014, que dispunha sobre a proteção aos registros, aos dados pessoais e às comunicações privadas (BRASIL, 2014). Em 2012 foi encaminhado pelo Poder Executivo ao Congresso Brasileiro o Projeto de Lei 4060 sobre o tratamento de dados pessoais, que em 2016 foi apensado

ao Projeto de Lei 5276. O PL 5276 de 2016 dispõe sobre o tratamento dos dados pessoais para o livre desenvolvimento da personalidade e da dignidade da pessoa natural (BRASIL, 2016) e, até a data presente, encontra-se em tramitação no Congresso Nacional.

O uso governamental de tecnologias de vigilância no país está vinculado a implantação dos governos eletrônicos nas esferas federativas, que é uma forma de gestão associada a tecnologias de informação e comunicação. Este tipo de administração pública tem sido adotado principalmente por municípios e ganhado força e incentivo a partir dos anos 2000. A intenção dos governos eletrônicos é a eficiência dos processos com o aumento da transparência, da participação, do controle e da qualidade da gestão, não sendo relacionados, no discurso, a práticas de vigilância ou controle social (DINIZ et al., 2009).

Recentemente o Brasil tem experimentado um aumento significativo nos investimentos públicos em aparatos de vigilância e controle, além de outros tipos de tecnologia em geral. Tais investimentos são decorrentes dos megaeventos que o país sediou nos anos de 2014 e 2016, a Copa do Mundo e os Jogos Olímpicos, respectivamente. A organização desses megaeventos impulsiona o investimento e a instalação dessas tecnologias que devem se tornar o “legado” deixado por ter sediado esses espetáculos, mas que, segundo Firmino, não encontram debate público sobre as consequências da implantação massiva das ferramentas de controle e exclusão social (FIRMINO, 2012).

Atualmente, a situação brasileira no que tange a implantação de tecnologias de vigilância e coleta de dados tem se mostrado muito significativa. O país tem experimentado um grande aumento na implantação dessas infraestruturas e processos, seja para tentar mitigar a criminalidade urbana; seja como forma de tentar melhorar o insatisfatório serviço público; seja como estratégia de marketing orientado ao mercado brasileiro; seja como legado dos megaeventos e integração em uma política global de antiterrorismo. Apesar disso, o debate público sobre o tema é inexistente, sendo restrito a um limitado debate acadêmico que não possui uma influência política significativa.

2.1.7 Big Data, Dados Pessoais e Dados Sensíveis

A quantidade de dados sendo transferido, armazenado e processado atualmente no mundo é gigantesca, sendo criados como subprodutos de incontáveis ações cotidianas que são registrados por sensores e dispositivos de coleta e são armazenados em diversos servidores espalhados pelo mundo, em um processo que busca sempre a maximização das informações disponíveis. Todo tipo de dado é captado, de produção humana ou não, criando uma rede de bancos de dados e computadores que trocam e processam essas informações a todo tempo, de uma forma que não seria possível de forma centralizada, formando o que é conhecido como Big Data (ANDERSON, RAINIE, 2012).

A recente emergência do Big Data trouxe consigo uma grande especulação sobre seus usos, benefícios e possíveis problemas, que podem estar associados ao armazenamento massivo e disperso e o cruzamento de informações entre bancos de dados. A análise dos dados pessoais, crescentes e autoproduzidos, pode revelar padrões de comportamento, de compra, uso de serviços e respostas a políticas públicas (ANDERSON, RAINIE, 2012).

Omer Tene e Jules Polonetsky (2013), elencam como possíveis benefícios do Big Data o avanço da medicina, tanto no atendimento como identificação de padrões em problemas de saúde; a identificação de padrões sociais através do uso de dispositivos móveis; otimização da distribuição de serviços; controle de tráfego; melhora nas vendas; facilidade e segurança em pagamentos; e personalização de serviços online. Entretanto, as pessoas cujos dados foram utilizados para produzir um conhecimento ou produto positivo através do uso de Big Data nem sempre são contempladas com o benefício gerado.

Já os pontos negativos do Big Data, de acordo com os mesmos autores, seriam o efeito de acumulação dos dados pessoais, onde a associação a uma identificação pode agregar novos dados indefinidamente; a automação da tomada de decisões, que são realizadas a partir da categorização das pessoas em perfis limitados; excessos e injustiças produzidos por análises de previsão de efeitos; a exclusão de pessoas dos benefícios produzidos; a falta de acesso das pessoas às suas próprias informações armazenadas; a falta de parâmetros éticos para o

processamento dos dados; e a sensação de que se está sempre sendo gravado, captado e armazenado em tempo integral (TENE, POLONETSKY, 2013).

Para o funcionamento do Big Data e a produção de seus principais benefícios e problemas, são necessários a coleta e o armazenamento de dados pessoais. De acordo com a definição do Data Protection Act, de 1988, dado pessoal é aquele que um indivíduo vivo pode ser identificado: (i) a partir desses dados; (ii) ou a partir desses dados e outras informações que estão na posse de, ou é susceptível de entrar na posse, do controlador de dados (GRÃ-BRETANHA, 1998). No Brasil, o Projeto de Lei 5276 de 2016, que é o primeiro a tratar exclusivamente sobre a questão da proteção de dados pessoais, dispõe que dado pessoal é: “dado relacionado a pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa” (BRASIL, 2016).

Como já referido, os dados pessoais podem ser comercializados pelas empresas que os controlam, sendo que, de acordo com Emily Steel para o Financial Times (2017), a informação armazenada sobre uma pessoa não deve passar de um dólar americano. Na cotação feita pelo periódico, as informações mais valiosas no mercado de dados pessoais, dentre as analisadas, são referentes à problemas de saúde, seguidas de idade, propriedade de imóvel e e-mail (STEEL *et al.*, 2013).

Dentre os dados pessoais há uma categoria de informações especialmente delicada quanto ao tratamento e distribuição: as informações sensíveis. Segundo Paul Ohm (2015), informações sensíveis são aquelas que podem ser utilizadas para provocar prejuízos de privacidade ou segurança quando em posse de terceiros mal-intencionados. A definição é ampla e pode enquadrar um extenso rol de tipos de dados e, por isso, legislações que tratam do assunto normalmente elencam categorias de informações que devem ser tratadas como sensíveis, muitas vezes ignorando alguns tipos de dados com potencial de prejuízo, como biometria, geolocalização e metadados (OHM, 2015).

Ohm considera as seguintes categorias de informações como potencialmente sensíveis:

- Saúde;
- Vida sexual;
- Finanças;

- Segurança pessoal;
- Registros criminais;
- Registros escolares;
- Informação sobre crianças;
- Opiniões políticas;
- Registros em órgãos públicos;
- Biometria;
- Geolocalização;
- Metadados.

O Pew Reserch Center (2014) levantou que, nos Estados Unidos, as informações que a população considera mais sensível são, respectivamente, o Número da Seguridade Social; seguido de dados de saúde; conteúdo de comunicação por telefone, e-mail e mensagens de texto; localização geográfica; números telefônicos com quem entrou em contato; data de nascimento; e histórico de relacionamentos, conforme o gráfico a seguir[1]:

[1] Para o levantamento os participantes classificaram cada um dos temas sugeridos pelos pesquisadores como: “nada sensível”, “pouco sensível”, “intermediário”, e “muito sensível”.

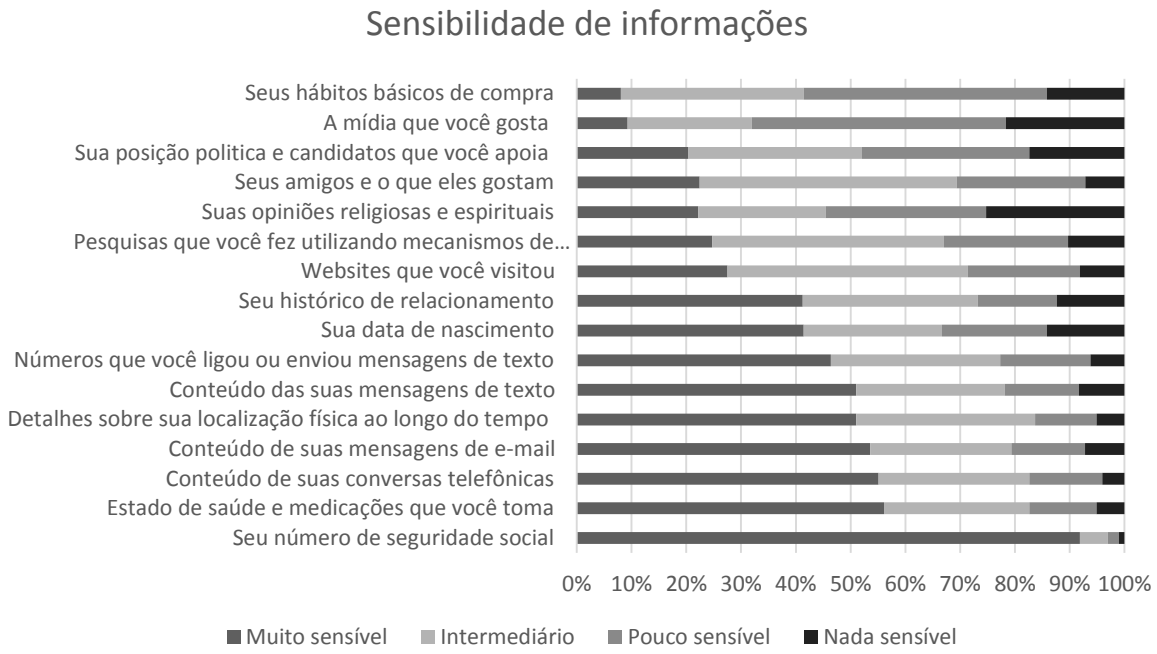

GRÁFICO 1: PESQUISA DE SENSIBILIDADE DE INFORMAÇÕES
FONTE: PEW RESEARCH CENTER, 2014

Foi relatado no levantamento que cidadãos com maior renda e escolaridade tinham maior tendência a classificar as informações com maior grau de sensibilidade. Também foi identificado que os entrevistados que tinham conhecimento sobre os programas governamentais de vigilância ou haviam pesquisado informações relacionadas a si mesmos na internet definiam graus mais altos de sensibilidade, especialmente sobre conteúdo de chamadas telefônicas e mensagens de e-mail (PEW, 2014)[2].

O Information Commisioner's Office (ICO, 2017), caracteriza como informação sensível aquelas que podem ser utilizadas de forma discriminatória, sendo de natureza privada, e precisam ser tratadas com maior cuidado que as demais informações pessoais. Enquanto o Projeto de Lei brasileiro para o tratamento de

[2] Esses dados refletem uma realidade possivelmente diversa da opinião pública sobre o tema no Brasil por se tratar de uma cultura distinta. Entretanto, no Brasil não há pesquisas similares que pudessem ser utilizadas para a consideração da opinião da população sobre o tema.

dados pessoais (PL 5276/2016) estabelece como informações sensíveis aquelas relativas a:

- Origem social ou étnica;
- Convicções religiosas;
- Opiniões políticas;
- Filiação a sindicatos ou organizações de caráter religioso, filosófico ou político;
- Saúde ou vida sexual;
- Dados genéticos ou biométricos.

Com isso, percebemos que dados de saúde são comumente considerados sensíveis ao mesmo tempo em que possuem alto valor comercial para livre troca entre os detentores do dado. Também ficam mais claros os tipos de informações que podem ser utilizados de forma discriminatória e prejudicial, revelando tanto o potencial de vigilância contido nesses bancos de dados, como demonstrando a falta de regulação das trocas comerciais que envolvem dados pessoais sensíveis.

2.1.8 Considerações finais

Com esta análise que traz a evolução dos estudos e conceitos sobre vigilância até chegar nos dias atuais, ansiamos por um entendimento melhor sobre as relações de poder e os perigos ensejados por essas práticas. A vigilância está infiltrada no cotidiano dos indivíduos contemporâneos em uma estrutura complexa de relações de retroalimentação, constantes nas esferas governamentais e privadas, bem como na hibridização destas, levantando questões de privacidade e controle que não são facilmente respondidas.

A utilização de bancos de dados pessoais é uma realidade no mundo todo, e, sendo objeto de análise deste trabalho, o entendimento sobre as formas como pode ser empregado é essencial para o desenvolvimento deste trabalho. Os usos e as implicações relacionadas a aplicação deste tipo de tecnologia são uma realidade que deve ser trazida à luz e discutida pelo corpo social. O contexto brasileiro evidencia uma carência de discussões sobre o tema, bem como regulamentações apropriadas para o tratamento da matéria.

2.2 CIDADES E AS TICS

Em 1984 William Gibson (2008) publicou seu primeiro romance: Neuromancer. A obra é uma ficção científica pertencente ao subgênero cyberpunk, que se baseia na exploração de alta tecnologia em detrimento da vida humana em sociedades futuristas, produzindo ambientações distópicas sobre a utilização de tecnologias avançadas, onde tanto o ambiente como os corpos são transformados e especializados através da hibridização tecnológica.

Em Neuromancer, Gibson situa sua narrativa em um mundo corporativizado, o Spraw, que é uma área urbana contínua que compreende o leste dos Estados Unidos e é protegida por domos que garantem um ambiente completamente artificial e controlado. Nas cidades de Gibson, o abismo social é uma característica dominante, onde nas extensões urbanas predominam periferias e mercados negros pontuados com enclaves de luxo e centros comerciais (GIBSON, 2008).

Além de um mundo material todo artificializado e mecanizado, que se estende para estações espaciais climatizadas voltadas ao turismo e ao consumo, há uma outra dimensão espacial paralela à realidade física, a o ciberespaço. O ciberespaço é acessado através de aparelhos conectados a uma rede de dados global, conformando um universo de sistemas, informações, controles de acesso e meios de deslocamento análogo ao espaço físico. Ou na descrição de Gibson:

> Ciberespaço. Uma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma representação de gráficos abstraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas no não espaço da mente, aglomerados e constelações de dados. Como luzes da cidade, se afastando... (GIBSON, 2008, p. 69).

A ideia de ciberespaço colocada no livro tem analogia à internet como a conhecemos hoje, pois ela somente pode ser acessada através de dispositivos que permitam a conexão. O ciberespaço conecta toda uma rede global de instituições, corporações e pessoas, tal qual as redes de informação se mobilizam no nosso mundo não fictício, permitindo trocas de informações e capital. Além das tecnologias de

informação, o desenvolvimento de outros tipos de redes tecnológicas suporta o deslocamento de pessoas e bens em alta velocidade no mundo todo, em uma revolução urbana característica ao período histórico em que vivemos.

Para que se instale uma situação de vigilância global, conforme o paradigma da “nova vigilância”, é necessária uma infraestrutura tecnológica ubíqua e complexa que permita a coleta e a troca de informações pessoais. Essas infraestruturas atravessam cidades e se cruzam nesses espaços que se tornam polos de comunicação e tecnologia, o que faz do meio urbano o espaço privilegiado para a aplicação dos processos de monitoramento atuais.

Para entender a relação das cidades com essa forma de vigilância tecnológica, é necessário, primeiramente, entender a relação das cidades com as tecnologias e a dimensão virtual que surge com a popularização dos computadores e, principalmente, da internet. Essas novas formas de comunicação impactaram profundamente as cidades, tanto no sentido da sua configuração espacial como nos fluxos e processos cotidianos que tomam forma nos ambientes urbanos conectados e segregados.

A vigilância a nível global depende da conexão das cidades no mundo inteiro para se efetivar, pois é nos pontos de acesso urbano que se controlam os fluxos migratórios e acontecem a maior parte das conexões virtuais. Além disso, a concentração demográfica e de atividades econômicas permitem o rastreio dos indivíduos através de câmeras de segurança e registros de transações comerciais que são predominantes nas áreas urbanas.

Além disso, as cidades enfrentam cotidianamente questões que fazem uso dessas tecnologias como forma de resolvê-los. Aparatos de vigilância são utilizados tanto nas práticas de gestão pública nos municípios, como também são utilizados, pelo poder público e privado, como tentativas de combater a criminalidade urbana. Essa situação se apresenta como uma solução efetiva para os problemas urbanos, mas tem levantado muitas críticas relacionadas a sua efetividade e os efeitos colaterais que pode provocar.

Portanto, para um entendimento mais amplo da relação das práticas e infraestruturas da “nova vigilância” e as cidades, é necessário, antes de tudo, compreender a relação dos espaços urbanos com as tecnologias emergentes, bem como as relações urbanas surgidas dentro do paradigma da globalização. A aplicação

tecnológica na gestão urbana vem em decorrência desse cenário, onde os dispositivos de vigilância se integram em uma composição tecnológica total.

2.2.1 A revolução urbana e as redes globais

Com as transformações na sociedade associadas ao avanço da modernidade, as cidades passaram por mudanças profundas nas suas estruturas e dinâmicas. Isso se deu associado a uma aceleração do processo de urbanização, cujo resultado é que que atualmente a maior parte das pessoas no mundo inteiro vivem em cidades. François Ascher entende as transformações contemporâneas das cidades como a terceira revolução urbana, que seguiu à primeira revolução, do renascimento, e a segunda, associada ao período de industrialização (ASCHER, 2010).

Nessa terceira revolução, iniciada na transição entre as décadas de 60 e 70, apareceram inovações que posteriormente transformaram a paisagem urbana, especialmente as tecnologias de transporte e as tecnologias de informações e comunicação (TICs). A reflexividade, própria da modernidade tardia, traz ainda um processo de individualização, racionalização e diferenciação ao paradigma social atual. Tal condição levou ao desenvolvimento do transporte e da estocagem de bens, de informações e de pessoas, disposição fundamental para a revolução urbana. A transformação, ainda, é encontrada nas atividades das pessoas, nas configurações urbanas, nos deslocamentos, nas comunicações e nas trocas, nos equipamentos e serviços públicos e nas relações com a natureza e o patrimônio (ASCHER, 2010).

Milton Santos (2013) caracteriza o espaço contemporâneo como o meio técnico-científico-informacional, pois, segundo ele, a construção e reconstrução do espaço se dá com uma participação cada vez maior de técnicas e ciências. A partir do meio natural, o espaço se tornou técnico com a industrialização e partir da Segunda Guerra Mundial adquiriu características cientificas, com o avanço das ciências, e informacional, em consequência da informatização crescente a partir da década de setenta (SANTOS, 2013).

A globalização tem um papel fundamental na reestruturação das cidades contemporânea a partir da maior liberação das barreiras aduaneiras e a aceleração nos deslocamentos de pessoas, de bens, de capital e de informações, possibilitados pelo avanço tecnológico nos meios de transporte e comunicação. Essas

infraestruturas conectam as cidades em redes globais, onde há uma interdependência baseada no pertencimento comum, ao mesmo tempo em que impulsiona uma competitividade global para o acúmulo desses insumos (ASCHER, 2010).

Com esse paradigma retomamos a ideia de sociedade em rede de Manuel Castells (1999), que elaborou esse conceito baseado na análise das estruturas que regem os novos padrões observados nos dias de hoje. Sua conclusão foi que estes modelos são análogos às organizações em redes: estruturas topológicas formadas por nós interconectados, onde dois nós pertencentes a mesma rede tem distância igual a zero e dois nós em redes diferentes tem uma distância infinita, conformando, assim, um sistema de “inclusão/exclusão” (CASTELLS, 1999).

Nesse sentido, Saskia Sassen (2001) argumenta que as cidades são nós em uma rede global de transações comerciais e políticas. A própria globalização seria um processo de estruturação dessa rede total de integração econômica, que se faz possível através das conexões tecnológicas providas pelos meios de comunicação dispostos em uma infraestrutura global em que as metrópoles são os terminais (SASSEN, 2001).

A socióloga ainda aponta que esses nós na rede global, bem como os centros de tecnologia de comunicação que sustentam essas conexões, funcionam em áreas financeiras e comerciais saturadas de tecnologias em metrópoles mundiais. Isso se dá pela concentração das elites financeiras nesses espaços e a melhor infraestrutura tecnológica disponível. Assim, instituições financeiras se concentram em cidades como Nova York, Tóquio e Londres, enquanto a demanda por provisão de serviços baratos é terceirizada para grandes cidades nos países periféricos, como acontece com os serviços de atendimento na Índia (SASSEN, 2004).

Anthony Townsend (2004) salienta os riscos da concentração de infraestrutura nas grandes metrópoles globais, pois o colapso dessa infraestrutura, por um ataque terrorista ou problemas técnicos, por exemplo, pode resultar em um prejuízo de milhões de dólares. O risco desse tipo de ocorrência tem levado grandes empresas de telecomunicação a distribuir sua infraestrutura de forma descentralizada, não dependendo de um único polo de convergência (TOWNSEND, 2004).

A sociedade contemporânea, segundo Castells, tem como modelo dinâmico os fluxos, composto de bens, pessoas, informações, capital, etc. Portanto, é necessário um suporte material apropriado para acomoda-los e articula-los em tempo

simultâneo, o qual Castells chama de “espaço de fluxos”. Esse modelo espacial, característico da cidade contemporânea, é composto por três camadas: uma de impulsos eletrônicos, outra de nós interconectados e centros de comunicação, e uma terceira referente a localização das elites dominantes responsáveis pelo direcionamento e decisões estratégicas do sistema, coordenando os fluxos dentro da rede (CASTELLS, 1999).

Apesar dos fluxos se movimentarem em escala global, o impacto das trocas e direcionamentos políticos mundiais são sentidos sempre no âmbito local, na escala dos espaços físicos. As instituições têm a função, nesse contexto, de conciliar as demandas locais e os fluxos de capital e poder que operam nas macro-redes, mesmo sendo muito difícil que manifestações e insurgências locais tenham uma real influência na estrutura global de trocas (CASTELLS, 2004).

Milton Santos (2013) argumenta que essa conjuntura é fruto da demanda do Capital, que impõe como palavras de ordem a fluidez e a competitividade nas dinâmicas socioeconômicas contemporâneas. A demanda pela fluidez, de acordo com o autor, “manda baixar fronteiras, melhorar os transportes e comunicações, eliminar os obstáculos à circulação do dinheiro [...], suprimir as rugosidades hostis ao galope do capital hegemônico [...].” (SANTOS, 2013, p. 31). Santos classifica o espaço de fluxos como um subsistema do espaço global, um subsistema que possui uma maior complexidade tecnológica e uma maior racionalização e intencionalidade nas ações (SANTOS, 2013).

Em oposição a autores que relativizaram o papel das distâncias nesse mundo dominado por fluxos globais em alta velocidade, onde o espaço resultaria homogêneo, Santos aponta para uma heterogeneização, onde se justapõem regiões marcadas pela divisão tradicional e outras dominadas pelos fluxos e objetos da modernidade. No meio urbano, a maior parte da aglomeração populacional e o espaço construído obedece a um tempo lento e tradicional, o qual se contrapõe à cidade informada, às infraestruturas de transporte e à comunicação em alta velocidade (SANTOS, 2013).

Nas cidades brasileiras os recortes entre espaços globalizados e lugares é muito pronunciada. Esse fenômeno é decorrente da urbanização massiva no país nas últimas décadas, em que, de acordo com o autor, houve uma absorção facilitada das estruturas modernas, sem as dificuldades de concepção e assimilação que os países

desenvolvidos que as originaram passaram, mas, ao mesmo, provocou profundas distorções sociais, territoriais, econômicas e políticas (SANTOS, 2013).

Shirin Madon (2004) argumenta que a globalização e a intensificação da presença das TICs nas cidades dos países em desenvolvimento têm como efeito uma ampliação das divisões sociais, geográficas e econômicas. O investimento nessas cidades atrai um grande número de pessoas em busca de empregos e renda que acompanham o desenvolvimento econômico e tecnológico, mas na maior parte das vezes não conseguem dispor dos benefícios trazidos por essa condição, experimentando, inclusive, uma piora na qualidade de vida em relação à condição anterior à globalização (MADON, 2004).

Entendemos que as cidades têm se globalizado em um sistema de redes que integra uma infinidade de trocas materiais e simbólicas. Essas redes são sustentadas por TICs, que permitem a transmissão de dados em tempo real para o mundo todo e influenciam os universos locais que sofrem com o impacto dos fluxos globais. O impacto local, negativo e positivo, é distribuído de maneira desigual nas áreas urbanas, especialmente nos países em desenvolvimento, onde o abismo social aumenta com a concentração dos recursos e tecnologias em áreas delimitadas dominadas pelas elites globais em detrimento das áreas periféricas pauperizadas.

Essa relação das cidades em escala mundial proporciona a troca de informações necessária para a realização da vigilância global, que necessita de uma rede integrada de dados para a análise e cruzamento com a finalidade de coletar, agrupar e classificar pessoas e referências que podem se locomover entre as nações. Além disso, a desigualdade intra-urbana, que ocorre entre as diferentes áreas em relação à integração global e a infraestrutura tecnológica, também tem seu rebatimento em relação às tecnologias de monitoramento, fazendo surgir áreas com presença, escala e qualidade da vigilância global discrepantes em relação umas às outras. Ou seja, são estabelecidas regiões vigiadas e não-vigiadas no território urbano.

2.2.2 Redes urbanas e espaço público na cidade ampliada

Tecnologias sempre fizeram parte das cidades, sendo centrais para as revoluções urbanas. A cidade contemporânea tem como elemento definidor, em

relação aos modelos urbanos passados, as TICs permeando toda a malha urbana e conectando as cidades umas nas outras em tempo real. A presença dessas tecnologias trouxe novas dinâmicas internas para as cidades, bem como é um elemento definidor da morfologia urbana atual.

Alguns dos primeiros teóricos das tecnologias de comunicação sugeriam uma ideia de eliminação do espaço em decorrência da unidade de tempo instantânea das tecnologias. Mais especificamente, o espaço tem perdido suas qualidades tangíveis, onde a percepção fica acondicionada somente ao sentido da visão e a interface passa a ser a referência de distância e profundidade. De acordo com Virilio (1993), o acesso à cidade agora se dá por bancos de dados que acompanham o desenvolvimento de uma cultura da técnica mascarada por suas redes invisíveis no contexto material, redes que só seriam manifestas “nas sequências de uma planificação imperceptível do tempo na qual a interface homem/máquina toma o lugar das fachadas dos imóveis, das superfícies dos loteamentos...” (VIRILIO, 1993, p. 10. Ou ainda:

> “[...] a descentralização assume, sobretudo na França, um sentido totalmente diverso de uma autonomia concedida a regiões, assinalando o fim da unidade de lugar do velho teatro político da Cidade e sua substituição próxima por uma unidade de tempo, uma cronopolítica da intensidade e da interatividade, tecnicidade que sucede à longa duração da Cidade, arquitetura de sistemas substituindo definitivamente os sistemas da arquitetura e do urbanismo contemporâneos. ” (VIRILIO, 1993, p. 99).

Já Stephen Graham (2004) lembra que o efeito de superação das distâncias e da materialidade não é um processo virtual, na verdade depende de uma ampla rede de infraestrutura física. Essa rede é composta de cabos de fibra óptica transoceânicos, cabos de transmissão de dados na malha urbana, sob a infraestrutura tradicional, servidores localizados, “hotéis de telecomunicação”, locais para armazenamento de dados off-line, e instalações em geral que podem ser invisíveis na paisagem das cidades (GRAHAM, 2004).

Nas últimas décadas houve a invasão das TICs no espaço urbano e a computação se tornou ubíqua e pervasiva, ou seja, atualmente são onipresentes as

redes e dispositivos informáticos no ambiente construído e no cotidiano dos habitantes das cidades contemporâneas. Essas ferramentas de comunicação e acesso às redes informacionais estendem as capacidades e sentidos do corpo humano, adicionando, dessa forma, uma nova camada de experiência ao espaço; uma dimensão virtual que conforma, junto com a realidade física, a realidade ampliada. Fábio Duarte e Rodrigo Firmino (2008) apontam que o espaço urbano foi ampliado pelas TICs e não substituído por um mundo eletrônico, sendo possível transitar nos meios lentos da cidade material ao mesmo tempo em que recebe e envia informações na velocidade instantânea das TICs (DUARTE e FIRMINO, 2008).

Essa qualidade tecnológica e dimensional garante que a vigilância seja realizada em tempo real, de acordo com os fluxos e registros pessoais efetuados no cotidiano dos atores urbanos. Também viabiliza a vigilância invisível através dos dispositivos em escala reduzida e embutidos nas estruturas urbanas tradicionais, característica essa que se opõe ao modelo disciplinar de Foucault, pois na maior parte das vezes a vigilância passa despercebida, deixando o indivíduo alheio a sua realização.

As TICs, e as outras tecnologias no meio urbano, não podem ter seu papel no desenvolvimento das cidades resumidos a um impacto. As infraestruturas tecnológicas estão intrinsecamente associadas a práticas, valores e significações sociais dentro das dimensões materiais, políticas e econômicas das cidades. Ou seja, essa infraestrutura é tanto técnica como social. Stephen Graham e Simon Marvin (2001) classificam o urbanismo atual como um conjunto de paisagens de infraestruturas sobrepostas e justapostas compondo as experiências urbanas e conectando de forma heterogênea lugares, pessoas e edifícios dentro de uma mesma área urbana ou entre cidades distantes (GRAHAM; MARVIN, 2001).

Entre as décadas de 1920 e 1960 houve uma iniciativa massiva para que as cidades, nos países desenvolvidos, fossem providas com infraestruturas de água, eletricidade, transporte e comunicação. Da mesma forma, mais tarde, as infraestruturas de conexão em rede também passaram a ser consideradas bens urbanos garantidos por monopólios estatais e privados, se integrando a malha urbana tradicional. Apesar de tomadas como garantidas e consideradas uma necessidade básica no paradigma da cidade moderna, a disponibilidade dessas infraestruturas nunca foi universal (GRAHAM; MARVIN, 2001).

De acordo com os geógrafos, a concentração de infraestrutura em espaços reduzidos, em consonância com as ideias já referidas de Manuel Castells (1999) e Saskia Sassen (2004), cria espaços de rede (*network*) premium. Essa dinâmica tem criado uma diferenciação nos espaços urbanos que se isolam em enclaves em um meio urbano fragmentado, que somente se tornaram praticáveis com a popularização dos automóveis. Nesse contexto, o planejamento e a gestão urbana se resumem à articulação das demandas por infraestrutura dos variados e conflitantes atores sociais em diferentes áreas das cidades (GRAHAM; MARVIN, 2001).

A conexão em uma dinâmica econômica global desassocia áreas urbanas do restante da cidade através de processos de especialização dentro das demandas do mercado internacional. Essas conexões globais também estão associadas a busca por uma logística cada vez mais eficiente, com a instalação e modernização de portos e aeroportos que muitas vezes estão completamente alheios ao restante dos espaços e processos das cidades. O que está ocorrendo, em certas áreas, é uma conexão global associada a um desligamento do entorno imediato, mesmo que seja impossível a ruptura total com as atividades urbanas locais (GRAHAM; MARVIN, 2001).

Martin Dodge e Rob Kitchin (2004), entendem os elementos que compõem as cidades contemporâneas como “codificados”, ou seja, associados a um software de comunicação e controle. Assim, as redes são codificadas mesmo que os objetos em si não sejam, como, por exemplo, uma rede de água operada através de um software de controle. Objetos, infraestruturas, processos, redes e associações de elementos podem se tornar códigos, estando presentes na vida diária das pessoas através de aparelhos particulares e sistemas públicos de operação (DODGE; KITCHIN, 2004).

Por ser formada por elementos variáveis de propriedades materiais e imateriais, a cidade informacional contemporânea está em constante mudança em uma dinâmica mais acelerada que aquelas do passado devido à velocidade de transporte e transmissão que as TICs possibilitam. Apesar da pouca influência na forma física da maior parte das cidades, as tecnologias transformam a vida urbana, que se torna ampliada pelas extensões humanas tecnológicas utilizadas pelos cidadãos. Essas redes são compostas de diversas formas de tecnologia, incluindo as tecnologias de vigilância, que se organizam em sistemas de sensores, registros, câmeras de segurança, etc., espalhados na área urbana

A modernidade está marcada pela individualidade – termo aqui entendido como uma redefinição na concepção de identidade humana enquanto tarefa e não mais como um estigma dado (BAUMAN, 2001). Contudo, o indivíduo está tirando de cena o cidadão, para ele o espaço público é onde se projetam as questões privadas, não sobrando espaço, assim, para questões que não a exposição da própria liberdade e individualidade. A individualização opõe-se à cidadania na medida em que o cidadão "busca seu próprio bem-estar através do bem-estar da cidade", já o indivíduo tende a ser "morno, cético ou prudente em relação à 'causa comum', ao 'bem comum', à 'boa sociedade' ou à 'sociedade justa'" (BAUMAN, 2001).

O espaço público urbano é onde todos se encontram, locais e estrangeiros; é onde é construída a tolerância e os acordos de civilidade. Para Bauman (2009), um espaço é público quando não exige identificação e não há mecanismos de controle de acesso; é um lugar onde todos são anônimos. Ou seja, o conceito de Bauman pode ser entendido, em certa medida, como referente a um espaço onde a vigilância é limitada ou, pelo menos, invisível e involuntária. São nos lugares públicos que se estabelecem os pactos de diversidade, sendo que este lugar deve reconhecer "o valor criativo das diversidades e sua capacidade de tornar a vida mais intensa, encorajam as diferenças a empenhar-se em um diálogo significativo" (BAUMAN, 2009, p.71).

Nos dias de hoje, passamos por uma redefinição de público e privado por consequência do uso das novas tecnologias de comunicação. Uma transformação comparável, segundo Dana Cuff (2003), às reformas de Haussmann na Paris do século XIX, que, com seus bulevares, permitiram o anonimato e os encontros fortuitos no espaço urbano, propiciando a exibição da intimidade na esfera pública. As transformações atuais, entretanto, se diferem daquelas do século XIX por possibilitarem atitudes privadas no espaço coletivo através do uso de aparelhos portáteis de comunicação. O resultado desse comportamento é uma grande conectividade juntamente a um isolamento crescente; intimidade associada à distância e privacidade exposta em público (CUFF, 2003).

Dessa forma, as narrativas urbanas se deslocam entre as dimensões físicas e virtuais através de aparelhos que estendem as faculdades humanas, como fones de ouvido, lentes, autofalantes e telas eletrônicas – pessoais e portáteis ou em escala urbana. As cidades se duplicam eletronicamente, seus fragmentos se recombinam em incontáveis deslocamentos temporais e espaciais; funções anteriormente localizadas

como o telefone ou o rádio evoluem em aparelhos portáteis, abrindo possibilidades de transformação do espaço urbano. Nessa dinâmica, a dimensão física está ganhando características do ciberespaço, lugares se interconectam e informações online podem ser acessadas a partir de qualquer local (MITCHELL, 2004).

Com o processo de individualização, as fronteiras entre o público e o privado ficaram difusas não somente no sentido do espaço e do patrimônio, mas na concepção daquilo que é de ordem pública e de ordem privada. Transformações profundas ocorreram na relação entre o homem e o ambiente a partir do uso das TICs, especialmente os dispositivos móveis, pois esses aparelhos permitem novas formas de interação com o espaço e também uma conexão permanente com os assuntos de interesse pessoal, que passaram a fazer parte da esfera pública.

Os processos e mecanismos de vigilância também entram nessa situação de indistinção entre o público e privado. Conforme pontuado no subcapítulo anterior, há uma troca constante de informações pessoais entre os setores públicos e privados através de acordos estabelecidos na ausência de regulamentações específicas. Esse sombreamento entre as esferas coletivas e particulares também se apresenta na utilização das câmeras de vigilância particulares que registram imagens do espaço público, mas que, ao mesmo tempo, podem ser requisitadas pelo Estado no caso de uma demanda específica.

2.2.3 Gestão urbana e as TICs

As questões levantadas até esse ponto se concentram nas mudanças na forma e nas relações urbanas decorrentes do desenvolvimento tecnológico das últimas décadas. Tanto as infraestruturas como os softwares são importantes agentes de transformação das cidades em um cenário de globalização econômica. Essa situação trouxe demandas por políticas públicas voltadas ao desenvolvimento e à integração tecnológica nos domínios urbanos, se incorporando, assim, ao campo da gestão pública e urbana.

A introdução das TICs no meio urbano e nos processos de administração trouxeram novas possibilidades e desafios para a gestão urbana. Por um lado, a cidade se transformou com as infraestruturas e os usos das novas tecnologias, impondo cenários inéditos com os quais a gestão urbana tem que trabalhar; por outro

lado, as tecnologias são também novas ferramentas à disposição dos gestores, podendo ser utilizadas para o incremento da eficiência da administração e dos serviços público urbanos.

Clóvis Ultramari (2009) define a gestão ou administração urbana como sendo o processo de decisão entre o planejamento urbano e o urbanismo, ou seja, a escolha ponderada entre o momento de planejar a cidade e o de executar as obras planejadas. A gestão urbana, então, é responsável pela implementação do planejamento urbano, por sua manutenção e por sua fiscalização no âmbito da cidade.

De acordo com Rodrigo Firmino (2011), as redes de informação que permeiam as cidades atuais apresentam uma diferença fundamental em relação aos outros tipos de rede urbana: ao contrário das estruturas precedentes, elas têm um efeito difícil de ser avaliado, pois são suportadas por uma infraestrutura invisível na paisagem, composta por redes de cabos subterrâneos ou sinais de rádio, micro-ondas ou satélite. Por isso, segundo o autor, a implantação de TICs não vem sendo uma política urbana prioritária, visto que os gestores se preocupam especialmente com aspectos e mudanças que apresentam um resultado visível na cidade, cujo efeito se faz mais óbvio para a população (FIRMINO, 2011).

As cidades são palimpsestos de formas e estruturas passadas que se sobrepõem; diversos elementos acumulados ao longo do tempo formam a cena urbana que nós conhecemos. A infraestrutura de informação digital se integra nesse sistema já existente como mais uma camada justaposta às anteriores, porém, como os elementos tradicionais ainda dominam a paisagem das cidades, as tecnologias telemáticas fogem da percepção visual dos habitantes urbanos. Nessa relação está a cidade integrada, “resultado de uma coexistência dialética de pessoas, objetos, territórios, instituições e fluxos oriundos de eras diferentes da história urbana”. (FIRMINO, 2011, p. 18).

Kitchin (2015) reconhece uma tendência atual pela utilização de dados como instrumento de governança municipal, através da análise de indicadores temáticos, classificações comparativas entre cidades, e a utilização de painéis de monitoramento com dados atualizados em tempo real sobre condições temáticas do município. Indicadores e escalas comparativas são tidos em uma lógica de competitividade, onde a gestão pública trata de forma a premiar os setores que atingirem determinados resultados e punir aqueles que ficarem aquém da meta estipulada. Os indicadores

também são utilizados para descobrir se uma estratégia de desenvolvimento ou política pública está dando resultados (KITCHIN, 2015).

Um problema relacionado a essa abordagem está no fato de que a cidade é entendida em termos de números e processos racionalizados traduzidos por computadores, ou seja, um conjunto de sistemas conhecidos e gerenciáveis, o que de forma alguma resume a realidade urbana. Além disso, o autor aponta que esse tipo de iniciativa nem sempre atinge os objetivos esperados e ainda gera questões sobre as intenções e os efeitos de análise associados ao levantamento de dados escolhidos pela administração pública, pois essa escolha nunca é realmente neutra e objetiva. Apesar das preocupações levantadas, a coleta de indicadores e a utilização de painéis de informações urbanas podem ser utilizados em análises mais completas das cidades, pois contribuem com dados espaciais detalhados e com registro continuado em ordem cronológica (KITCHIN, 2015).

Para Firmino (2014), é necessário, primeiramente, reconhecer a necessidade de política públicas voltadas à implantação e ao uso de TICs e seu desenvolvimento nas cidades. Somente com a identificação da necessidade de incorporar essas tecnologias na gestão urbana é que se abre a possibilidade de atingir suas potencialidades desejadas, como a promoção de políticas públicas democráticas e tecnológicas integradas ao desenvolvimento urbano local, em concordância com especificidades e demandas regionais em uma organização político-administrativa mais horizontalizada (FIRMINO; FREY, 2014).

As integrações de políticas e projetos que envolvam TICs e políticas e projetos de desenvolvimento urbano ainda são incipientes, considerando-se o nível de pervasividade tecnológica no espaço urbano. Dessa forma, ainda são identificadas apenas algumas ações isoladas no sentido de reconhecimento e integração desses elementos, mas não há uma observação disciplinar ampla dos estudos urbanos da importância dessa associação (FIRMINO; FREY, 2014)

Essa característica de estar infiltrada no cotidiano das cidades é justamente uma das grandes dificuldades postas a urbanistas e gestores urbanos na identificação e no tratamento do tema. Além disso, os problemas na compreensão das TICs no meio urbano estão, também, relacionados à transição da cidade industrial, com suas práticas de planejamento e gestão urbanas baseadas em padrões fixos de controle e

organização, para a cidade em rede, onde prevalecem os fluxos e o espalhamento heterogêneo da urbanização (FIRMINO,2014).

Klaus Frey (2005) aponta que as TICs têm um grande potencial para promover a interação entre os atores locais, garantir a transparência administrativa e a democracia no âmbito da gestão pública nos municípios. Dada a grande desigualdade de acesso às tecnologias presente nos países latino-americanos, o autor argumenta que as políticas públicas nessas regiões devem objetivar a inclusão das pessoas e das regiões desprovidas nas redes de informação globais e às tecnologias de comunicação, garantindo, dessa maneira, a democratização das vantagens trazidas com a assimilação das TICs na gestão pública. O objetivo, de acordo com Frey, é a criação de um governo eletrônico inclusivo que favoreça a formação de cidadãos e comunidades eletrônicas (FREY, 2005).

As iniciativas de desenvolvimento encontram dificuldades primeiramente na difícil identificação e compreensão da relação das TICs e o meio urbano. Além disso, o desenvolvimento urbano-tecnológico depende de fatores que devem levar em conta estruturas político-administrativas que favoreçam a democracia e a participação na gestão urbana, o que pode ser efetivado através de práticas e tecnologias integradas que considerem as especificidades de cada setor administrativo e as múltiplas visões sobre o tema, incluindo as instituições e a comunidade na discussão.

A vigilância atualmente faz parte da agenda político-administrativa das instituições públicas, incluindo-se as esferas municipais. Os dispositivos e processos de monitoramento, atualmente, fazem parte do aparato tecnológico utilizado pela gestão urbana como forma de administrar o território das cidades em suas relações dinâmicas de fixos e fluxos. A capacidade de coleta e análise de informações pessoais são necessários em um paradigma de gestão baseado no exame de dados e indicadores em tempo real.

2.2.4 Smart Cities

Estratégias integradas de desenvolvimento urbano-tecnológico tem se popularizado na gestão municipal. A utilização de tecnologias e práticas a elas relacionadas para o controle urbano são cada vez mais comuns e o título de “cidade inteligente” ou ”*smart city*” tem sido um objetivo dos governos locais. Portanto, esse

fenômeno, que tem suas implicações locais, mas também está inserido em uma competição global de investimentos e atração de capital humano, é essencial para entendermos o momento atual no que tange as administrações municipais.

O conceito de smart city é muito variado e, por ser ainda muito recente, não existem consensos na área, além de que há uma disputa de interesses pela apropriação do tema, apresentando vieses distintos de acordo com o emissor. Os pesquisadores da área Farnaz Mosannenzadeh e Daniele Vettorato (2014) apontem três tipos de origem para o discurso de smart city: (i) acadêmico, (ii) industrial e (iii) governamental. O ponto de vista acadêmico teria uma abordagem voltada ao entendimento da cidade inteligente como um autômato autorregulado por tecnologias avançadas. Já a visão industrial se refere a produtos e inovações tecnológicas, com um foco maior nas tecnologias em si e nas integrações tecnológicas nas cidades. Por último, o discurso governamental está mais relacionado à gestão e ao planejamento urbano, voltado a um desenvolvimento inteligente (MOSANNENZADEH; VETTORATO, 2014).

Uma definição abrangente pode ser encontrada na de Andrea Caragliu, Chiara del Bo e Peter Nijkamp (2009), que caracterizam que uma cidade é inteligente quando há investimentos em capital humano e social, e existe infraestrutura de comunicação tradicional, por transporte, e moderna, através das TICs, que impulsionam o crescimento sustentável e uma alta qualidade de vida, além de praticar o uso consciente dos recursos naturais e um governo participativo (CARAGLIU *et al.*, 2009). Ou seja, smart cities devem ser uma união entre tecnologias, investimentos e desenvolvimento econômico, sustentabilidade e participação popular.

Neste sentido, então, podemos diferenciar uma cidade imersa em um paradigma tecnológico, ou seja, quase a totalidade das cidades conectadas às redes globais de trocas comerciais, e uma cidade inteligente. Para Marcos Cesar Weiss, Roberto Carlos Bernardes e Flávia Luciane Consoni (2015), a cidade inteligente no Brasil deve lançar mão das TICs com o objetivo de melhorar a vida das pessoas que vivem nos meios urbanos de maneira inovadora e democrática, envolvendo agentes sociais variados na resolução dos problemas decorrentes da intensa urbanização pela qual o país passou nas últimas décadas (WEISS *et al.*, 2015).

Apesar de sua autodeclarada intenção de resolver os problemas e aumentar a eficiência da gestão, a emergência das cidades inteligentes tem gerado críticas

quanto ao seu processo de implantação e seus efeitos na prática. Raquel Rennó (2016) argumenta que na verdade as smart cities se encontram em um paradigma de determinismo tecnológico, onde há a promessa implícita de que as TICs devem salvar a cidade de todos os seus problemas. Ademais, o discurso associado a implantação de projetos de smart city traz consigo o redirecionamento de objetivos próprios do mundo corporativo, como inovação e eficiência, para a gestão pública, resultando em um ambiente que favorece a privatização e o controle dos espaços públicos (RENNÓ, 2016).

Já Dia Kayyali (2016) defende que nem sempre as opções tecnologicamente avançadas são a melhor solução para os problemas urbanos, sendo que projetos para a melhora da qualidade de vida dos habitantes são mais eficientes quando há uma intenção de se resolver um problema através da equidade e inclusão social. Kayyali aponta que sistemas tecnológicos de controle de dados são poderosas ferramentas de reprodução da ideologia dominante, tornando-a inútil, senão contra produtiva, para a resolução dos problemas estruturais urbanos do Brasil (KAYYALI,2016).

Os também ativistas Paz Peña e Francisco Velasco (2016) colocam a implementação de smart cities na América Latina dentro da lógica de manutenção de domínio econômico dos países do norte desenvolvido sobre os países em desenvolvimento, pois quase toda tecnologia empregada nesses sistemas é disponibilizada por grandes empresas das nações mais ricas. Eles ainda afirmam que reduzir os complexos conflitos urbanos a indicadores digitalizados é promover a inteligência das cidades baseado em diagnósticos burros (PEÑA; VELASCO, 2016).

Todos esses autores citados que criticam as cidades inteligentes apontam, além das questões colocadas, o enorme poder de vigilância trazido pela coleta massiva de dados exigida pelos aplicativos e processos envolvidos no controle urbano (RENNÓ, 2016; KAYYALI, 2016, PEÑA; VELASCO, 2016). Portanto, é fundamental analisar a vigilância nas cidades contemporâneas e seu suporte tecnológico para o entendimento da gestão urbana nas cidades contemporâneas.

2.2.5 Vigilância nas cidades

A pervasividade das TICs traz consigo também o espalhamento generalizado de tecnologias de vigilância, tornando o espaço urbano um território intensamente

vigiado. Sensores, cartões de transporte, câmeras de monitoramento, imagens aéreas, bancos de dados, etc., fazem parte da vida urbana, estando embutidos nos espaços públicos e privados das cidades contemporâneas. Além disso, o aumento da capacidade tecnológica também possibilitou o aumento do potencial do controle governamental através de bancos de dados com informações pessoais coletadas dos cidadãos.

David Lyon (2004), aponta que após os ataques terroristas a Nova York em 11 de setembro de 2001, a vigilância nas cidades dos países desenvolvidos sofreu um grande aumento sob a justificativa da proteção contra novos atentados. Assim, o anonimato, marca fundamental da vida urbana durante séculos, tem sido posto de lado em favor do escrutínio público através de tecnologias de informação e quanto maiores as complexidades urbanas, mais se desenvolvem tecnologias capazes de garantir o controle social (LYON, 2003).

A visibilidade nas cidades sempre foi um fator fundamental para a segurança e a manutenção da ordem pública, mas nas cidades modernas sistemas são projetados para garantir a visibilidade máxima e permitir um controle social total. Além do reforço da visibilidade através de dispositivos de coleta de dados e imagens em tempo real, sistemas de segurança baseados em isolamento espacial também são uma característica substancial das desiguais cidades modernas (LYON, 2003).

A utilização de tecnologias de vigilância nas cidades não são somente uma forma de invasão de privacidade e coleta de dados individuais, também tem produtividade e resultados positivos como, por exemplo, redução da velocidade e atividades criminosas em locais controlados por câmeras e sensores. Entretanto, Lyon argumenta que esses benefícios normalmente são sentidos pelos cidadãos privilegiados, que tem meios para adquirir dispositivos de segurança para minimizar seus próprios riscos, aumentando a exclusão das populações periféricas que não podem dispor de proteção tecnológica, mas também através da classificação discriminatória baseada em grupos alvo (LYON, 2003).

Steven Graham (2003) coloca que o espaço urbano tem se comodificado e dividido em fragmentos isolados por limites de exclusão e controles de acesso. A inserção de tecnologias de vigilância nas cidades não serve somente como técnicas para o enfrentamento do medo crescente relacionado à criminalidade, essas

tecnologias servem como formas de atração de empresas e consumidores selecionados em uma dinâmica de competitividade global (GRAHAM; WOOD, 2003).

Sistemas de vigilância são projetados de forma a esconder os julgamentos sociais que este tipo de iniciativa acarreta. Legisladores e gestores públicos enfrentam muita dificuldade em reconhecer e descobrir como utilizar essas tecnologias de controle, além de enfrentar problemas geográficos e de jurisdição que invariavelmente estão associados a legitimidade e o poder político associados a implantação de medidas nesse sentido (GRAHAM; WOOD, 2003).

Graham (2011) ainda denuncia que o urbanismo contemporâneo tem implementado elementos, físicos e simbólicos, e estratégias próprios de ocupações militares nas cidades ocidentais do norte-desenvolvido, o que autor chama de “novo urbanismo militarizado”. Esse movimento acontece com a transferência de modelos e tecnologias para controle social e da violência, aplicadas em áreas de conflito em cidades fora do eixo desenvolvido, a colônia, para as cidades dos países dominantes, a metrópole (GRAHAM, 2011).

O geógrafo coloca como central para o urbanismo militarizado a utilização de tecnologias de controle e vigilância, ou seja, a interposição da aplicação de tecnologias civis e militares como elemento definidor da cidade atual. A aplicação de tecnologias e estratégias militares no urbanismo revela um flagrante estado de guerra contínua, que é justificada de maneiras distinta a depender do contexto, podendo ser contra terror, as drogas, o crime e a insegurança (GRAHAM, 2011).

Michael Batty (2013) e Rob Kitchin (2014) ressaltam que sensores e sistemas coletam dados pessoais de cidadãos em tempo integral nas cidades contemporâneas, sendo que toda a informação coletada é armazenada em grandes bancos de dados, ou Big Data. Esse processo pode gerar vantagens à população, ao governo e à iniciativa privada, porém os dados, que são produzidos em larga escala e fornecem os indicadores urbanos de imediato, podem mudar o paradigma do planejamento a longo prazo para uma gestão tecnocrática de cada instante da vida urbana (BATTY, 2013; KITCHIN, 2014).

Kitchin (2014) classifica três tipos de forma de coleta de dados pessoais utilizados na gestão urbana:

- *Direto*: é o modelo de vigilância tradicional, ou seja, é a coleta de dados individualizada de um alvo pré-determinado e cujo processo é dependente de um operador humano.
- *Automatizado*: são dados resultantes de processos automáticos de um sistema ou dispositivo tecnológico, tais como registros de chamadas em celulares, transações monetárias automatizadas, registros de acesso virtual, registros de compras, atividade de sensores, etc.
- *Voluntário*: são dados fornecidos conscientemente e de forma voluntária através de interações em rede sociais, respostas de pesquisas, adições em mapas virtuais colaborativos, etc.

O autor argumenta que o tipo de coleta e produção de dados mais destacado para a formação do Big Data é o automatizado, pois, apesar de os outros dois tipos serem fontes de informações valiosas sobre a condição de uma cidade, é a coleta automática que garante a atualização permanente dos índices urbanos, dos movimentos das pessoas e das coisas. A abundância de informações sobre as atividades e processos urbanos, que podem ser levantadas por iniciativas governamentais ou privadas, permitem uma gestão urbana adaptativa às mudanças no panorama das cidades em tempo real (KITCHIN, 2014).

Kitchin também levanta questões quanto a validade das iniciativas de controle inteligente das cidades às custas de direitos à privacidade, confidencialidade e liberdade de expressão da população, onde o poder de monitoramento está somente nas mãos de círculos específicos, formando um oligóptico, ou seja, um panóptico cujo controle é distribuído em grupos de observação. O problema se agrava ainda mais quando levamos em conta que o aparato tecnológico empregado nesses projetos é desenvolvido por empresas privadas, resultando em uma situação de corporativização da administração pública municipal (KITCHIN, 2014).

Chegamos então em um paradigma urbano em que as tecnologias de vigilância estão presentes em todo o território das cidades, sendo utilizados pela gestão pública e pela iniciativa privada para o controle dos espaços públicos e os fluxos intraurbanos. Apesar de trazer benefícios e resolver pragmaticamente certas adversidades pontuais, o emprego dessas tecnologias tem levado a um governo tecnocrático que não reconhece os problemas em suas origens para então

desenvolver uma resposta adequada, simplesmente se contentando com medidas paliativas de gerenciamento imediato das situações críticas. Além disso, questões de discriminação estatística, privatização da gestão pública, invasão da privacidade e cerceamento da livre expressão, são apontamentos importantes para o entendimento das consequências associadas à adoção desse tipo de agenda.

2.2.6 Considerações finais

Redes de conexão e as TICs de maneira geral tem impulsionado uma transformação urbana que reflete nas – e é impulsionada por – práticas, movimentos e apropriações dos cidadãos urbanos. A cidades, e seus cidadãos, agora estão conectados e uma rede global de trocas de bens, capital, informação e pessoas, mudando a dinâmica local através de influências dos fluxos globais e imperativos de competitividade e eficiência.

As tecnologias estão imbricadas em infraestruturas urbanas, o que torna seu suporte material praticamente invisível no dia-a-dia das cidades, conferindo uma qualidade de difícil apreensão e compreensão a essa nova realidade. Essa característica complica a elaboração de políticas públicas adequadas que valorizem e regulem a utilização das TICs, de propriedade pública ou privada, dentro do meio urbano. Apesar disso, projetos têm sido elaborados e implantados com foco na utilização desses dispositivos como forma de melhorar a gestão urbana.

Mesmo trazendo certos resultados imediatos, a utilização dessas tecnologias traz um grande potencial de vigilância associado à coleta e ao armazenamento de informações pessoais, recurso tido como necessário para o funcionamento dos processos de gestão tecnológica das cidades. Além de não reconhecer e resolver estruturalmente os problemas urbanos, as tecnologias de vigilância acarretam ainda a perda da privacidade e um potencial de controle social desproporcional nas mãos das instituições públicas, que, dentro desse paradigma neoliberal, pode estar associada aos interesses privados e corporativos.

3 METODOLOGIA

O método escolhido para uma pesquisa deve definir um caminho a ser trilhado para se atingir os objetivos definidos no trabalho. A partir do entendimento dos objetivos esperados do trabalho, esta deve ser uma pesquisa descritiva. De acordo com Antônio Carlos Gil (2002), uma pesquisa de objetivo descritivo é aquela que “tem como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis”, sendo que “[...] uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática” (GIL, 2002, p. 42),

Devido ao objetivo descritivo e com modelo de análise quantitativo, este trabalho foi conduzido como uma pesquisa documental. Para Gil (2002), uma pesquisa documental se caracteriza por seu embasamento em documentos de natureza diversa, que podem ser de “primeira mão”, quando o material não recebeu tratamento analítico, ou de “segunda mão”, que seriam as informações que já foram analisadas de alguma forma.

Este modelo de pesquisa foi escolhido porque o material coletado, ou seja, a relação dos campos cadastrais do Bancos de Dados utilizados pela Prefeitura Municipal de Curitiba (PMC), é de natureza documental de primeira mão. O tipo de análise que foi desenvolvida é a partir da classificação dos campos cadastrais, resultando em uma comparação quantitativa das características consideradas mais críticas quanto ao potencial de vigilância encontrado em cada cadastro.

Os parâmetros de análise para classificação do potencial de vigilância levam em conta os tipos de dados armazenados pela PMC, o múltiplo acesso ao banco de dados, a classificação de sensibilidade e risco de prejuízo, e a estimativa de valor comercial. Tais valores devem ser analisados em todos os cadastros disponíveis, conformando um índice de vigilância a partir da avaliação comparativa entre eles.

Após essa introdução, nesse capítulo será, então, justificada e descrita, em seus aspectos relevantes para o trabalho, a unidade-caso da pesquisa, ou seja, a Prefeitura Municipal de Curitiba. Na sequência foram estabelecidos e especificados os procedimentos metodológicos que deverão ser aplicados na coleta dos dados, bem como será esclarecido como foram efetuadas as análises dos resultados coletados.

3.1 UNIDADE-CASO

O estudo de caso que elaborado nesta pesquisa tem como unidade-caso a Prefeitura Municipal de Curitiba (PMC). A cidade tem um histórico muito associado à vanguarda e à inovação no planejamento e na gestão urbana. Recentemente, no período da última gestão municipal, o paradigma e os sistemas tecnológicos da gestão pública em Curitiba têm sido contestados em favor da modernização tecnológica. Nesse contexto, a gestão vem trazendo uma proposta de smart city que está profundamente associada às tecnologias de vigilância para sua operação. Dessa forma, Curitiba foi escolhida tanto por seu valor simbólico no âmbito do urbanismo brasileiro, mas, principalmente, por ser um município em processo de implantação do projeto de cidades inteligentes, um dos únicos no país.

Curitiba é a capital do estado do Paraná, no sul do Brasil, e abriga 1.879.355 habitantes (IBGE, 2015), chegando a 3.732.642 habitantes em sua região metropolitana (IBGE, 2013). Assim como as demais grandes cidades brasileiras, Curitiba passou por um grande aumento populacional acompanhado um intenso processo de urbanização na segunda metade do século XX. Tal condição trouxe problemas urbanísticos associados ao rápido processos e crescimento urbano, como a periferização e a metropolização de parte da população da cidade (MOURA; ULTRAMARI, 1994).

Curitiba se destacou com reconhecimento internacional pelo seu planejamento urbano, que tem uma característica de ser voltada para as pessoas e o meio ambiente. A cidade sofreu transformações radicais com as intervenções propostas no Plano Preliminar de Urbanismo, também conhecido como Plano Serete, de 1965. A partir do reconhecimento da efetividade das estratégias urbanas implantadas na capital, Curitiba assumiu uma posição de vanguarda na proposição de novas formas de aplicar o urbanismo, tornando esse reconhecimento em uma estratégia de marketing inserida em uma competição global (SANCHEZ, 2010).

A unidade-caso poderia ser uma das grandes cidades brasileiras com projetos de modernização da gestão, dentre as quais Curitiba se coloca como um exemplo pertinente e cujo estudo se encaixa na linha pesquisa em que se estabelece esse trabalho. Assim, como qualquer outra grande cidade brasileira, Curitiba está inserida dentro de um padrão de globalização, sofrendo com os problemas associados às

questões de diferenciação e causalidade que existem na oposição entre os fatores globais e os locais. Nesse paradigma de globalização, as TICs fazem parte da cidade, como elemento presente no meio urbano, na utilização de tecnologias móveis pelos cidadãos, pelo meio da comunicação e da mídia digital que tem a cidade como assunto, e pelo meio da gestão urbana que utiliza tecnologias em seus processos.

De acordo com Tamiris Cunha Vaz (2015), a assimilação de tecnologias digitais na Prefeitura de Curitiba se iniciou com a instalação do Centro de Processamento de Dados (CPD) no ano de 1970, passando por diversas adições, alterações e realocações nas décadas seguintes. Em 1996, o CPD se transformou no Instituto Curitiba de Informática (ICI), uma Organização Social (OS), ou seja, de direito privado, que levou a uma segunda mudança no paradigma informacional da instituição. Com a eleição do prefeito Gustavo Fruet, em 2013, o domínio informacional do ICI sobre a prefeitura passou a ser contestado e foi criada a Secretaria de Informação e Tecnologia (SIT), que busca reaver o controle público sobre os dados municipais (CUNHA VAZ, 2015).

De acordo com o secretário municipal responsável, a criação da SIT veio acompanhada de uma intenção de reestruturação tecnológica no município, que pretende uma maior utilização de tecnologias inteligentes como instrumentos para melhorar a gestão urbana. A situação atual do uso de sistemas informacionais na administração da cidade apresenta defasagem tecnológica e, mais importante, uma grande falta de integração entre as informações produzidas pelos diferentes órgãos municipais (MIRANDA, 2015).

A diretriz de renovar os sistemas tecnológicos vem acompanhada do projeto de tornar Curitiba uma *smart city*, que pode ser entendido do ponto de vista da gestão pública em si, mas também da publicidade associada ao termo. Para levar a cabo o projeto Curitiba Smart City a prefeitura efetuou um empréstimo de 94 milhões de reais junto ao BNDES para investir em tecnologias – software e infraestrutura – e capacitação de pessoas voltada a sua utilização (MIRANDA, 2015).

O cenário tecnológico atual dentro da prefeitura é de descentralização e falta de integração entre os setores, bem como a existência da disputa entre os interesses públicos e os contratos ainda em vigor com o ICI, que controla as bases de dados da cidade. Dessa forma, podemos entender a Curitiba de hoje como uma cidade tentando

recuperar sua posição pioneira em termos de soluções urbanas através da evolução e integração informacional na gestão pública.

Para o funcionamento das atividades e prestação de serviços, a PMC possui diversos cadastros armazenados no Instituto Curitiba de Informática (ICI). O acesso aos cadastros é compartimentalizado de acordo com as necessidades de cada secretaria e departamento da prefeitura, sendo alguns deles utilizados por mais de um órgão. No sistema de Dados Abertos da prefeitura é possível encontrar alguns cadastros com temas públicos para a acessibilidade de informação e prestação de contas com a população, entretanto, para o tema desta pesquisa, o material necessário são os cadastros que possuem informações pessoais, que são sigilosas e não são abertas para consulta. Dessa forma, o objeto de análise da pesquisa são os dados pessoais armazenados pelos cadastros municipais.

3.2 PROCEDIMENTOS METOLÓGICOS

3.2.1 Coleta de dados

Os procedimentos metodológicos adotados para a coleta de dados aconteceram em duas etapas: a primeira foi um levantamento documental e contato com técnicos e envolvidos na Secretaria de Urbanismo da prefeitura, onde foram feitos os primeiros direcionamentos para o encaminhamento da pesquisa. Em seguida foi realizada uma entrevista com um técnico designado da Secretaria de Informação e Tecnologia (SIT), sobre a forma como os cadastros das diferentes secretarias estavam armazenados e estruturados.

Nessa etapa inicial, descobriu-se que os cadastros da PMC estão todos contidos e operacionalizados pelo ICI, ou seja, centralizados em um mesmo lugar, apesar de não unificados. Os dados são armazenados em servidores armazenados no Data Center da empresa que disponibiliza para a prefeitura através dos sistemas que ela também fornece. O ICI também presta o serviço de segurança de toda a rede da prefeitura, incluindo os servidores dos bancos de dados cadastrais. O técnico da PMC informou, em entrevista, que os dados cadastrais, de propriedade da administração pública, são legalmente protegidos por contrato.

A partir desta informação foi encaminhado um ofício para a PMC, através da SIT, solicitando uma listagem dos campos de todos os cadastros da prefeitura que contivessem dados pessoais, bem como a identificação dos campos e a secretaria que faz uso do cadastro. Após análise jurídica da solicitação, os dados foram entregues em formato analógico, contendo as tabelas com os cadastros e os campos de informações armazenadas (ANEXO I). Foram disponibilizados os campos de onze cadastros da PMC, dos quais dez contém dados pessoais, e são utilizados pelas diversas secretarias da prefeitura. Foram utilizados na análise somente os cadastros que possuem dados pessoais.[3]

3.2.2 Análise dos resultados

Para o funcionamento das atividades e prestação de serviços, a PMC possui diversos cadastros armazenados no Instituto Curitiba de Informática (ICI). O acesso aos cadastros é compartimentalizado de acordo com as necessidades de cada secretaria e departamento da prefeitura, sendo alguns deles utilizados por mais de um órgão. No sistema de Dados Abertos da prefeitura é possível encontrar alguns cadastros com temas públicos para a acessibilidade de informação e prestação de contas com a população, entretanto, para o tema desta pesquisa, o material necessário são os cadastros que possuem informações pessoais, que são sigilosas e não são abertas para consulta. Dessa forma, o objeto de análise da pesquisa são os dados pessoais armazenados pelos cadastros municipais.

[3] No período em que os dados seriam coletados a Prefeitura de Curitiba sofreu uma troca de gestão, onde o prefeito Gustavo Fruet (PDT) foi substituído após seu primeiro mandato por Rafael Greca (PMN), que faz parte do grupo político de oposição. Com isso, a Secretaria de Informação e Tecnologia teve que se preparar a transição e, após a posse do novo prefeito, foi transformada em superintendência. Tais fatos ocorridos dificultaram o contato, pois já se contava com a cooperação secretário substituído, o Sr. Paulo Roberto Miranda, e a disponibilização dos dados, o que atrasou a conclusão do relatório.

As informações foram analisadas a partir do levantamento quantitativo de acordo com a classificação dos campos dados pessoais contidos nos cadastros da prefeitura, bem como a partir da interpretação dos resultados baseada na literatura sobre o assunto. A avaliação foi feita a partir da classificação dos campos cadastrais quanto a sensibilidade da informação, o valor comercial dos dados e multiplicidade de acesso por mais de uma secretaria. Os campos foram tabulados e possuem um valor atribuído de acordo com cada parâmetro.

Sensibilidade dos dados

A questão da sensibilidade foi analisada a partir da classificação dos dados coletados em sensíveis ou não, utilizando de fontes de origem diversa. Para ser considerado sensível o dado deve: a) se encaixar nas tipologias definidas por Paul Ohm (2015), que traz uma análise metodológica do assunto; b) informações predominantemente consideradas “muito sensíveis” no levantamento do Pew Research Center (2014), que demonstra a opinião pública sobre o que é considerado mais privado; c) se enquadrar nas definições legais do Projeto de Lei 5276/2016, que estabelece parâmetros legais para a matéria.

O prejuízo potencial inerente ao uso deste tipo de dado é coincidente com a discriminação panóptica e acúmulo de desvantagens explanadas nas teorias de vigilância (LYON, 2009b; GANDY, 2006). Dados dessa natureza possuem uma relação mais estreita com a privacidade individual, pois sua divulgação e mal-uso pode resultar em dano para aqueles que possuem características que fogem do padrão ideal. Assim, informações sensíveis podem ser classificadas como aquelas que podem causar algum tipo de dano, invasão de privacidade, risco à segurança pessoal ao sujeito e, frequentemente, são coletadas de forma privada (OHM, 2015).

O tipo mais de informação sensível mais reconhecida é a de saúde, que pode ser exemplificada pelo estabelecimento do sigilo médico, pois a divulgação de dados de condição de saúde e tratamentos podem causar uma série de prejuízos à pessoa identificada. Outros campos são considerados, como vida sexual, conteúdos de comunicação privada, histórico de relacionamento, registros criminais, opiniões políticas, origem social ou étnica e convicções religiosa, que estão ligadas ao constrangimento e marginalização social, risco de segurança e discriminação profissional e pública, como exclusão e perseguição oficial.

Os valores para os dados considerados sensíveis são equivalentes por não haver indicação na literatura de uma hierarquia de sensibilidade, de forma que não foram consideradas medidas diferentes entre eles. Ao final da classificação foram elaboradas gráficos e quadros comparativos entre os cadastros obtidos. A seguir está apresentada a tabela com os tipos de dados destacados e a fonte do critério adotado:

	Paul Ohm	**Pew Reserch Center**	**PL 5276/2016**
Saúde	■	■	■
Vida sexual	■		■
Finanças	■		
Segurança pessoal	■		
Registros criminais	■		
Registros escolares	■		
Informação sobre crianças	■		
Opiniões políticas	■		■
Registros em órgãos públicos	■		
Seguridade social		■	
Conteúdo de conversas telefônicas		■	
Conteúdo de mensagens de e-mail		■	
Localização física	■	■	
Conteúdo de mensagens de texto		■	
Números contatados		■	
Data de nascimento		■	
Histórico de relacionamento		■	
Origem social ou etnica			■
Convicções religiosas			■
Filiação a sindicatos ou organizações de caráter religioso, filosófico ou político			■
Dados genéticos ou biométricos	■		■

QUADRO 1: CRITÉRIO DE CLASSIFICAÇÃO E FONTE PARA A DEFINIÇÃO DE DADOS SENSÍVEIS.
FONTE: O AUTOR.

Assim, foram considerados sensíveis os dados que forem de:

- Saúde;
- Vida sexual;
- Finanças;
- Segurança pessoal;
- Registros criminais;
- Registros escolares;

- Informação sobre crianças;
- Opiniões políticas;
- Registros em órgãos públicos;
- Seguridade social;
- Conteúdo de conversas telefônicas;
- Conteúdo de mensagens de e-mail;
- Localização física;
- Conteúdo de mensagens de texto;
- Números contatados;
- Data de nascimento;
- Histórico de relacionamento;
- Origem social ou étnica;
- Convicções religiosas;
- Filiação a sindicatos ou organizações de caráter religioso, filosófico ou político;
- Dados genéticos ou biométricos.

Valor comercial

O segundo critério adotado para a construção do Índice de Vigilância é o valor comercial que as informações possuem. Atualmente, há um mercado global para dados pessoais, dos quais o tipo deles é um fator que determina a variação do valor entre eles. Essas trocas fazem parte do modelo de negócios de diversas organizações, caracterizando uma vigilância mercantil, que se dedica menos ao escrutínio individual do que na análise de massa baseada voltada para publicidade comportamental (EVANGELISTA, VIEIRA, 2017).

Além do setor privado, a venda de informações também pode envolver o setor público. A terceirização de serviços e parcerias público-privadas, muitas vezes pressupõe a transferência de dados pessoais de cidadãos para as empresas que gerenciam o serviço, sem que haja uma regulamentação sobre a venda dessas informações. Isso pode acontecer, por exemplo, na implantação de wi-fi gratuito, na concessão do transporte público, no gerenciamento de bilhetes únicos, programas de nota fiscal associada ao CPF, e outros (MONTAGNER, 2017; DIAS, 2017; LIMA,

2017). A administração pública, muitas vezes, argumenta que a concessão de venda dos dados pessoais é um fator que viabiliza financeiramente esses projetos e programas públicos (LIMA, 2017).

Portanto, foi considerado que valor comercial de um dado é um critério importante para o estabelecimento de um potencial de vigilância que pode estar associada ao armazenamento de dados de cidadão pela gestão pública municipal. O valor comercial dos dados foi atribuído diretamente, em dólar (US$), de acordo com os preços levantados por Emily Steel *et al.* para o Financial Times. Os pesquisadores basearam a definição dos preços a partir da análise da atribuição de preços de dados pessoais de diversas fontes nos Estados Unidos (STEEL *et al.*, 2013). Os tipos de dados que não possuírem valor estimados foram considerados com valor US$ 0,00.

Ao final da valoração dos cadastros, foram demonstrados gráficos e quadros comparativos entre os bancos de dados com o valor estimado de venda para a informações de um indivíduo cadastrado.

Os valores cotados pelo Financial Times são:

Campo	Valor (US$)
Idade	0,092
Sexo	0,0004
Raça/cor	0,0045
Ocupação	0,066
Estado civil	0,092
Dado de saúde	0,23
Filhos	0,03
Endereço	0,0004
Possui casa	0,094
E-mail	0,0713
Telefone	0,004
Navegação web	0,0018
Posição geográfica	0,0004

QUADRO 2: VALORES COMERCIAIS PARA DADOS PESSOAIS POR TIPO.
FONTE: FINANCIAL TIMES, 2013.

Múltiplo acesso

O múltiplo acesso a bancos de dados pode ser um fator de potencialização da vigilância sobre os cidadãos, pois essa condição aumenta as possibilidades de um mesmo cadastro, que passa a poder ser utilizado para finalidades diversas (MURAKAMI WOOD et al., 2006). Portanto, um cadastro que não esteja atrelado

formalmente a uma finalidade específica pode ter o controle sobre sua aplicação dificultado e, assim, ser utilizado para propósitos que causem dano ou discriminação de indivíduos. Dessa forma, o acesso de um banco de dados por mais de uma secretaria é uma situação que representa um maior alcance a dados pessoais, inclusive dados que podem não ser necessariamente relacionados ao trabalho de determinados departamentos que possuem a permissão de dispor das informações.

A definição de múltiplo acesso para este trabalho foi estabelecida de forma a classificar os cadastros que são exclusivos de determinadas secretarias e aqueles que servem a mais de uma repartição pública. Assim sendo, quando um cadastro não é de acesso a uma única secretaria ele foi considerado com maior potencial de vigilância. Entretanto, apesar de sua importância, esse parâmetro foi considerado de menor relevância que os anteriores por se tratar de acessos internos de uma organização pública.

Ao final da classificação dos cadastros, foram demonstrados quadros comparativos entre os bancos de dados.

Índice de Vigilância

A vigilância contida em determinadas práticas e tecnologias, na maior parte das vezes, é derivada de múltiplos fatores que somados redobram o dano potencial e a invasão de privacidade dos indivíduos. Além disso, a análise da vigilância pode ser feita a partir de diversas perspectivas temáticas e teóricas, o que demonstra a multidisciplinaridade do tema e a abrangência dos fatores envolvidos na construção de um aparato de vigilância global, ou a assemblage de vigilância de Haggerty e Ericson (2003).

Assim sendo, foram considerados os três critérios acima explanados para a elaboração de uma fórmula que pudesse classificar o nível de vigilância contido em cada um dos sistemas cadastrais disponibilizados pela PMC. Esses fatores foram escolhidos por se tratarem da classificação de dados pessoais e de bancos de dados, além de serem compatíveis com o tipo e o conteúdo do material coletado, de forma que tornasse possível uma classificação comparativa entre os sistemas.

De acordo com o Ministério do Planejamento (2009), um indicador deve ter os seguintes componentes básicos:

- Medida: são as grandezas a serem consideradas;

- Fórmula: que expressa o padrão do cálculo;
- Índice: o indicador em determinado momento;
- Padrão de comparação: um índice arbitrário para comparação do resultado;
- Meta: um índice a ser alcançado em relação ao “padrão de comparação”.

Para este trabalho o “padrão de comparação” e a meta não são considerados pois se trata de uma primeira tentativa de construção do indicador, ou seja, sem progressão temporal, resultando somente em um índice a ser considerado em suas propriedades presentes. Além disso, este tipo de indicador pretende medir resultados e definir objetivos de desempenho, enquanto que, para esta pesquisa, a intenção é a avaliação da situação atual do tema.

As medidas são relativas aos temas já explanados: dados sensíveis, valor comercial e múltiplo acesso. Assim, a fórmula foi elaborada com base no maior peso identificado nos critérios de sensibilidade e valor comercial dos dados e, por isso, os dois valores são multiplicados. Além disso, os valores comerciais por usuário cadastrado são de grandezas, em sua maioria, menores que um, fazendo com que a soma simples dos fatores resultasse em uma prevalência desproporcional dos dados sensíveis. Já o múltiplo acesso é definido pelo padrão binário de sim ou não, ou seja, a multiplicação de um item sem múltiplo acesso seria zero, por isso foi definido que esse critério seria somado aos demais, com peso 1 de acordo com a proporcionalidade em relação à importância dos demais itens.

Dessa forma, após a análise de cada um dos critérios, é elaborado um índice geral de vigilância, que também pode ser entendido como índice de invasividade do Estado, composto dos três critérios acima dispostos. A composição do índice foi feita a partir do número de dados sensíveis identificados por cadastro multiplicado pelo valor comercial das informações de um usuário registrado e adicionado um aos cadastros que forem de múltiplo acesso entre as secretarias municipais.

A formula é a seguinte:

$$IV = [DS \,.\, VC] + MA$$

IV = Índice de vigilância

DS = Somatório dos dados sensíveis

VC = Valor comercial

MA = Múltiplo acesso (0/1)

Ao final da classificação dos cadastros, foram demonstrados gráficos e quadros comparativos entre os bancos de dados afim de classifica-los em seu potencial de vigilância.

4 DADOS PESSOAIS E POTENCIAL DE VIGILÂNCIA NA GESTÃO MUNICIPAL DE CURITIBA

Os cadastros fornecidos pela Prefeitura Municipal de Curitiba, por solicitação formal e avaliação jurídica, foram os seguintes:

Sistema	Secretaria
ATIVUS – Acompanhamento de atividades físicas	Esporte Lazer e Juventude – SMELJ
COC.Net – Coordenadoria de obras	Trânsito – SETRAN
NCPA – Cadastro de Pessoas Atendidas	Fundação de Ação Social – FAS
SIC - Identificação do Cidadão	Diversos órgãos e secretarias
E-Saúde - Atendimento médico, odontológico e de outras especialidades	Saúde - SMS
GTM - Gestão Tributária Municipal	Diversos órgãos e secretarias
GTM / Cadastro de Comércio Ambulante	Diversos órgãos e secretarias
GTM - Localiza Lotes	Diversos órgãos e secretarias
156 - Atendimento ao Cidadão	Todos os órgãos e secretarias
GED - Gestão Educacional	Educação - SME
Controle de Corridas	Esporte Lazer e Juventude - SMELJ

QUADRO 3: CADASTROS FORNECIDOS PELA PMC.
FONTE: PMC, 2017.

O sistema GTM – Localiza Lotes foi desconsiderado por não possuir dados pessoais em seus campos cadastrais.

4.1 DADOS SENSÍVEIS

Conforme descrito na metodologia (3.2.2), os dados sensíveis foram analisados a partir da classificação dos campos cadastrais disponíveis no material fornecido pela prefeitura.

4.1.1 ATIVUS - Acompanhamento de atividades físicas

Este cadastro é de uso exclusivo da Secretaria de Esporte, Lazer e Juventude (SMELJ), que trabalha principalmente com jovens. Neste sistema cadastral foram identificados oito campos que armazenam dados potencialmente sensíveis, sendo os mais destacados aqueles relacionados a saúde, como o hábito de fumar ou beber.

Sistema: ATIVUS - Acompanhamento de atividades físicas			
Secretaria: Esporte Lazer e Juventude - SMELJ			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
ALUNO	ALU_QTDPESSOA	Quantidade de pessoas que moram na residência	Não
	ALU_ATIVIDADE	Atividade do aluno	Não
	ALU_FUMA	Indica se o aluno fuma	Sim
	ALU_BEBE	Indica se o aluno bebe	Sim
	ALU_DTACADASTRO	Data de cadastro do aluno	Não
	ING_IDF	Identifica o ingresso	Não
	SOB_IDF	Identifica a sobrevivência	Não
	AME_IDF	Identifica a assistência médica	Sim
	REN_IDF	Identifica a renda	Sim
	ESC_IDF	Identifica a escolaridade	Sim
	PES_IDF	Identifica a pessoa	Não
	NAT_IDF	Identifica a naturalidade	Sim
	PRO_IDF	Identifica a profissão	Não
	ALU_PAI	Nome do pai do aluno	Não
	ALU_MAE	Nome da mãe do aluno	Não

	ALU_NIS	Número de identificação social do aluno	Não
	ESCO_IDF	Identifica a escola	Não
PESSOA	PES_IDF	Chave primária da tabela	Não
	SIC_IDF	SIC da pessoa	Não
	PES_NOME	Nome da pessoa	Não
	PES_NASC	Data de nascimento da pessoa	Sim
	PES_CIVIL	Estado civil da pessoa	Não
	PES_CPF	CPF da pessoa	Não
	PES_RG	RG da pessoa	Não
	PES_SEXO	Sexo da pessoa	Não
	PES_FONE	Telefone da pessoa	Não
	END_IDF	Identifica o endereço	Não
	PES_EMAIL	Email da pessoa	Não
	PES_FONE_PRINCIPAL	Telefone principal da pessoa	Não
	PES_FONE_ALTERNATIVO	Telefone alternativo da pessoa	Não
	PES_CONTAT_PRINCIPAL	Nome do contato principal	Não
	PES_CONTAT_ALTERNATIVO	Nome do contato alternativo	Não
	PES_DEFICIENCIA	Tipo de deficiência que a pessoa pode possuir	Sim
	PES_MATRICULA	Matrícula da pessoa	Não

QUADRO 4: ATIVUS - ACOMPANHAMENTO DE ATIVIDADES FÍSICAS.
FONTE: PMC, 2017.

4.1.2 COC.Net - Coordenadoria de obras

O Sistema de Coordenadoria de Obras é acessado pela Secretaria de Trânsito (SETRAN) e não armazena qualquer dado considerado sensível.

Sistema: COC.Net - Coordenadoria de obras			
Secretaria: Trânsito - SETRAN			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
USUÁRIO_ EXTERNO	UEX_CODIGO	Chave primária da tabela	Não
	EMP_CODIGO	Vínculo empresa e login de usuários externos	Não
	UEX_LOGIN	Login utilizado para acesso via aplicação web	Não
	UEX_SENHA	Senha utilizada para acesso via aplicação web	Não
	UEX_NOME	Nome do usuário externo	Não
	UEX_EMAIL	Email do usuário externo	Não
	UEX_TELEFONE	Número do telefone do usuário externo	Não
	UEX_CELULAR	Número do celular do usuário externo	Não
	UEX_STATUS	Indica se o usuário externo está ativo ou não na aplicação web	Não
	UEX_DATA_ATUALIZACAO	Data em que ocorreu a última atualização do cadastro	Não

QUADRO 5: COC.NET - COORDENADORIA DE OBRAS.
FONTE: PMC, 2017.

4.1.3 SIC - Identificação do Cidadão

O Sistema de Identificação do Cidadão (SIC) é um cadastro que serve como chave para outros cadastros da prefeitura, como um código de acesso a informações pessoais de pessoas associadas a outros bancos de dados. Dessa forma, o SIC é utilizado por diversas secretarias municipais.

Quanto ao armazenamento de dados sensíveis, o SIC possui seis campos assim classificados, onde os pontos mais críticos são os dados de nacionalidade e raça, ou seja, quanto a origem étnica e social dos indivíduos.

SIC - Identificação do Cidadão			
Secretaria: Diversos órgãos e secretarias			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
PESSOA	Pes_Cod	Chave primária da tabela	Não
	Dom_Cod	Código do domicílio	Não
	Pes_Cod_DomicilioGF	Código do domicílio, do Sistema do Governo Federal	Não
	Pes_Num_OrdemDom	Número de ordem da pessoa no domicílio	Não
	Pes_Nme	Nome	Não
	Pes_Nme_Pai	Nome do pai	Não
	Pes_Nme_Mae	Nome da mãe	Não
	Pes_Dta_Nascimento	Data de nascimento	Sim
	Pes_Tp_Dta_Nascimento	Data de nascimento (informada ou comprovada)	Não
	Pes_sexo	Sexo da pessoa	Não
	Pes_Nacionalidade	Nacionalidade	Sim
	Cod_Pais	Código do País, vindo do Logradouro Serviço	Não

	Pes_Dta_ChegadaBrasil	Data de chegada ao Brasil, se brasileiro naturalizado ou estrangeiro	Sim
	Pes_Cod_IBGEMunicipio	Código do IBGE do município	Não
	Cod_Unid_Federacao	Código da Unidade da Federação	Não
	Cod_Cidade	Código da cidade	Não
	Est_Cod	Código do estado civil	Não
	Pes_Num_OrdemConjuge	Número de ordem do cônjuge, dentro do domicílio	Não
	Pes_Deficiência	Indica se a pessoa possui deficiência	Sim
	Cor_Cod	Código da Cor / Raça	Sim
	Pes_Provedor_Fin	Código do provedor financeiro	Não
	Pes_Responsavel	Indica se a pessoa é responsável pelo domicílio	Sim
	Pes_ProgramaGoverno	Participação de Programa do Governo Federal	Não
	Pes_Eml	Email	Não
	Pes_Dta_Cadastro	Data de cadastro	Não
	Pes_Dta_Atualizacao	Data da última atualização de cadastro	Não
	Pes_CadastroGF	Indica se a pessoa tem cadastro no Governo Federal	Não
	Pes_Num_SIC	Número do SIC	Não
	Pes_Fig_EmissaoCartao	Indica a emissão de cartão que possua o número do SIC	Não
	Pes_Fig_PossivelDelecao	Indica possível deleção do cadastro	Não

	Pes_Fig_Falecido	Indica se a pessoa é falecida	Não

QUADRO 6: SIC - IDENTIFICAÇÃO DO CIDADÃO.
FONTE: PMC, 2017.

4.1.4 E-Saúde - Atendimento médico, odontológico e de outras especialidades

O sistema E-Saúde é utilizado pela Secretaria de Saúde (SMS) e é o cadastro de usuários da rede municipal de saúde. Foram identificados doze campos com informações sensíveis das quais, apesar de ser um sistema de saúde, a maior parte se refere a origem étnica ou social. Além disso, este foi o único cadastro que apresentou indicação de sexualidade com a inclusão do campo “nome social”, que é utilizado por pessoas transgêneras.

Sistema: E-Saúde - Atendimento médico, odontológico e de outras especialidades			
Secretaria: Saúde - SMS			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
USUÁRIO	cdusuario	Código do usuário (chave primária)	Não
	nmusuario	Nome do usuário	Não
	nmmae	Nome da mãe	Não
	nmpai	Nome do pai	Não
	cdnacionalidade	Código da nacionalidade	Sim
	cdnatmunicipio	Código do município de naturalidade	Sim
	cddomicilio	Códigodo domicílio	Não
	tpsexo	Tipo de sexo	Não
	dtnascimento	Data de nascimento	Sim
	idsituacao	Código da situação	Não
	cdfaixarenda	Código da faixa de renda	Sim

	cdracacor	Codigo da raça / cor	Sim
	cdescolaridade	Código de escolaridade	Sim
	cdestadocivil	Código do estado civil	Não
	cdsituacaoconjugal	Código da situação conjugal (referência)	Não
	cdocupacao	Código da profissão conforme código brasileiro de ocupação	Não
	nmusuariofonetico	Nome fonético	Não
	nmmaefonetico	Nome fonético da mãe	Não
	idfrequentaescola	Se o usuáro frequenta a escola	Não
	idbolcaalimentacao	Se o usuário possui bolsa alimentação	Sim
	nrimpessoesetiquetas	Número de impressão de etiqueta de usuário	Não
	dtcadastro	Data de cadastro	Não
	dtatualizacao	Data de atualização dos dados	Não
	cdusuariopai	Código de usuário do pai	Não
	cdusuariomae	Código de usuário da mãe	Não
	cdcidcobito	Código de CID do óbito	Não
	dtobito	Data do óbito	Não
	dscomplementoobito	Informações complementares do óbito	Não
	nrtempoestudo	Tempo de estudo	Sim
	cdtipodocumentocad	Código do tipo de documento cadastrado	Não
	cdmotivocadastramento	Código do motivo de cadastramento	Não

	cdcontratocadastrador	Código do contrato que cadastrou	Não
	nmpaifonetico	Nome fonético do pai	Não
	dsjustifisemcbo	Descrição da justifiva do cadastro sem ocupação CBO	Não
	cdusurespnaoident	Código do usuário responsável quando não identificado	Não
	dscomplusunaoident	Cognome do usuário quando não identificado	Não
	nrcnsmae	Número do cartão nacional de saúde da mãe	Não
	dtunificacao	Data de nunifiaçaõ do cadastro	Não
	nrdeclaracaoobito	Número da declaração de óbito	Não
	dsjustifreativcancobito	Descrição da justificativa de reativação de cancelamento de óbito	Não
	cdloginatividade	Código do login atividade	Não
	nmusuariosocial	Nome social	Sim
	cdesusuario	Código do usuário no ESUS	Não
	cdetnia	Código da etnia indígena	Sim
DOMICILIO	cddomicilio	Código do domicílio do usuário (chave primária)	Não
	cdcontrato	Código do estabelecimento responsável pelo domicílo	Não
	cdcontrolecep	Código do CEP	Não
	dscomplementoobito	Descrição do complemento	Não

	nrresidencia	Número da residência	Não
	dspontoreferencia	Descrição do ponto de referência	Não
	nrcomodos	Número de cômodos no domicílio	Não
	idenergia	Se o domicílio possui energia elétrica	Sim
	idcadastrosiab	Se o domicílio pertence à área de abrangência atendida por equipe SIAB	Não
	idsituacao	Situação do domicílio (ativo ou inativo)	Não
	dtcadastro	Data de cadastro do domicílio	Não
	dtatualizacao	Data de atualização do domicílio	Não
	idcalassificacaoriscofamilia	Código de classificação de risco da família	Sim
	nrlatitudeutm	Número da latitude da localização geográfica	Não
	nrlongitudeutm	Número da longitude da localização geográfica	Não
	cdtipocomplemento	Código do tipo de complemento do domicílio	Não
	cdsetorcensitario	Código do setor censitário do domicílio	Não
	cdendereco	Código do endereço do domicílio	Não
	cdquadra	Código da quadra do domicílio	Não
	cdmicroarea	Código da micro área do domicílio	Não

	cdesusdomicilio	Código do domicílio no cadastro ESUS	Não

QUADRO 7: SISTEMA: E-SAÚDE - ATENDIMENTO MÉDICO, ODONTOLÓGICO E DE OUTRAS ESPECIALIDADES.
FONTE: PMC, 2017.

4.1.5 GTM - Gestão Tributária Municipal

O sistema de Gestão Tributária Municipal é o cadastro de pessoas e sociedades para fins tributários. O sistema não possui dados sensíveis armazenados.

Sistema: GTM - Gestão Tributária Municipal			
Secretaria: Diversos órgãos e secretarias			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
GTMPESPessoa	Cod_Pessoa	Identifica uma pessoa no cadastro de pessoas	Não
	Nme_Pessoa	Nome do Municipio	Não
	Dta_Cadastro_Pessoa	Data do cadastro da pessoa no sistema	Não
	FIg_Ind_Pessoa_Fora	indica que pessoa não é de Curitiba	Não
	Ind_Interessado_Municipe		Não
	lnd_Origem_Migracao_Pessoa	Origem da migragao dos dados do mainframe	Não
	lnd_Tipo_Pessoa		Não
	Cod_Pessoa_Grup03_MF	Código existente no mainframe, para pessoas eventuais do grupo 3	Não
	Dta_Ultima_Atualizacao	Data da última atualização	Não
	Dta_Atualizacao_Geral_Cadastro	Data da atualização geral do cadastro	Não
	Fig_Ativo		Não

	Cod_Pessoa_Oficial	Referência ao registro oficial da pessoa, em casos de duplicidade de documento	Não
GTMSOCSociedade	Cod_Pessoa_Juridica	Identifica uma pessoa no cadastro de pessoas	Não
	Cod_Socio	Identifica uma pessoa no cadastro de pessoas	Não
	FIg_Ind_Socio_Responsavel		Não
	Ind_Nivel_Socio	Indica o nivel de instrução do sócio	Não
	Ind_Socio_Conj		Não
	Cod_Qualificacao_Pessc as	Indica a qualificação	Não
	Cod_Pessoa_Empresa		Não

QUADRO 8: GESTÃO TRIBUTÁRIA MUNICIPAL.
FONTE: PMC, 2017.

4.1.6 GTM - Cadastro de Comércio Ambulante

O sistema de Gestão Tributária Municipal também possui o cadastro de comerciantes ambulantes. Nesse cadastro, os três campos de informações que podem ser consideradas sensíveis são relacionadas a saúde, deficiências, e origem social.

Sistema: GTM / Cadastro de Comércio Ambulante			
Secretaria: Diversos órgãos e secretarias			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
GTMAMBAmbulante	Cod_Ambulante	Identifica o código do ambulante	Não
	Cod_Pessoa	Identifica o código da pessoa	Não
	Cod_End_Generico	Endereço	Não

	Cod_Desc_Motivo_Canc_CCA	Descrição do motivo do cancelamento CCA	Não
	Cod_Protocolo	Código do protocolo	Não
	Ano_Protocolo	Ano do protocolo	Não
	Cod_Docto_Protocolo	Código do documento do protocolo	Não
	Dta_Cancelamento	Data do cancelamento	Não
	Num_Carteira_Motorista	Número da carteira de motorista	Não
	Num_Carteira_Profissionai	Número da carteira profissional	Não
	Num_Titulo__leitor	Número titulo de eleitor	Não
	lnd_Estado_Civil	Estado civil	Não
	Nme_Conjuge	Nome do conjuge	Não
	Fot_Ambulante	Foto do ambulante	Não
	Des_Profissao_Conjuge	Profissão do conjuge	Não
	Num_Telefone	Número do telefone	Não
	Qtd_Anos_Residencia	Anos de residência	Não
	Qtd_Anos_Atividade	Anos de atividade	Não
	Ind_Condicoes_Moradia	Condições de moradia	Sim
	Ind_Deficiente_Fisico	Caso possui alguma deficiência	Sim
	Des_Deficiencia	Descrição da deficiência	Sim
	Num_Filhos_Menores	Quantidade de filhos menores	Não
	Num_Filhos_Escola	Quantidade de filhos na escola	Não
	Dta_Cadastramento	Data do cadastramento	Não
	Vir_Peso_Total		Não

	Cod_Usuario	Código do usuário	Não
	Fig_Proibido_Preposto		Não
	Des_Motivo_Proib_Prepost o		Não
	Txt_Observacao_Cracha		Não
	Txt_Observacao_Geral		Não
	Ind_Sit_Ambulante		Não

QUADRO 9: GTM - CADASTRO DE COMÉRCIO AMBULANTE.
FONTE: PMC, 2017.

4.1.7 156 - Atendimento ao Cidadão

O 156 é o sistema de atendimento ao cidadão da PMC e é utilizado por todas as secretarias da prefeitura. Este cadastro armazena como dado sensível apenas a data de nascimento da pessoa.

Sistema: 156 - Atendimento ao Cidadão			
Secretaria: Todos os órgãos e secretarias			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
Central 156 - Solicitação de Serviços	Cadastrador	Nome do usuário que cadastrará o protocolo	Não
	Protocolo	Numérico, seguindo uma ordem crescente	Não
	Origem	Sigla do órgão ao qual cadastrador pertence	Não
	Data de Criação	Data e hora do registro do protocolo	Não
	Tipo	Tipo de registro que será realizado	Não

	Dados do Solicitante	Caso solicitante seja Pessoa Física	Não
	Nome do Solicitante	Nome completo do solicitante	Não
	Tipo de Solicitante	Tipo de solicitante	Não
	Sexo	Gênero masculino ou feminino	Não
	Nome da Mãe	Nome da mãe do solicitante	Não
	Aspecto Emocional	Utiliza quando constatado que o cidadão está alterado	Não
	Telefone	Número de telefone para contato com cidadão	Não
	CPF	Número do CPF do cidadão	Não
	Data de Nascimento	Data de nascimento do cidadão	Sim
	E-mail	Se o meio de resposta selecionado for e-mail	Não
	Número do RG	Documento do cidadão	Não
	Órgão Emissor	Órgão emissor do Documento RG	Não
	Data	Data emissão do Documento RG	Não
	Unidade Federativa	UF do Documento RG	Não
	Unidade Federativa (UF) e Localidade	Estado e a cidade do solicitante	Não
	Logradouro	Logradouro do solicitante	Não
	Número	Número de endereço do solicitante	Não
	Complemento	Complemento de endereço do solicitante	Não
	CEP	Número de CEP de endereço do solicitante	Não

	Pessoa Jurídica	Caso solicitante seja Pessoa Jurídica	Não
	Razão Social	Razão social da empresa	Não
	Ramo de Atividade	Segmento que a empresa atende	Não
	Nome Fantasia	Nome comercial da empresa, caso possua	Não
	Website	Site da empresa	Não
	CNPJ	Número completo do CNPJ da empresa	Não
	Inscrição Estadual	lnscrição estadual da empresa, caso possua	Não
	Contato	Nome de contato na empresa	Não
	Telefone	Telefone para contato	Não
	Setor	Setor em que o contato trabalha	Não
	E-mail	E-mail do contato	Não
	Endereço	Endereço da empresa	Não
	Número	Número de endereço da empresa	Não
	Complemento	Complemento de endereço da empresa	Não
	CEP	Número de CEP de endereço da empresa	Não
	Dados do Assunto	Descrição; Assunto; Subdivisão; Texto Explicativo; Manter Sigilo (opcional)	Não
	Endereço do Assunto	Local do Assunto lgual ao Endereço do Solicitante	Não

	Meio de Resposta	Meio de resposta que cidadão será informado	Não
	Tipo de Documento Externo	Utilizado pelos Orgãos externos para identificar o tipo de protocolo que está sendo criado	Não
	Número do Documento Externo	Utilizado pelos órgãos externos para inserir o número do documento que foi registrado	Não
	Observações	Acrescentar informações adicionais ao pedido do cidadão	Não
	Dados Importantes	São dados que os órgãos consideram importantes para atender o protocolo	Não
	Enviar ao Responsável	Enviar o protocolo ao Órgão responsável	Não

QUADRO 10: 156.
FONTE: PMC, 2017.

4.1.8 GED - Gestão Educacional

O sistema de Gestão Educacional é utilizado exclusivamente pela Secretaria de Educação. O cadastro possui dez campos de dados considerados sensíveis, com predominância de dados de origem étnica ou social. Além disso, este foi o único sistema a apresentar convicção religiosa em seus dados cadastrados.

Sistema: GED - Gestão Educacional			
Secretaria: Educação SME			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
TBO137PESSOA	TB0137_COD_PESSOA	Código que identifica unicamente uma pessoa física	Não

	TB0137_NOME_PESSOA	Nome da Pessoa Física	Não
	TBO137_IND_SEXO	Sexo Feminino ou Masculino	Não
	TBO137_IND_RACA	Indica a raça da pessoa	Sim
	TBO137_IND_NACIONALIDADE	Indica se a pessoa tem a naturalidade brasileira	Sim
	T30092_COD_FUNCAO	Código sequencial para cadastro das funções	Não
	TBO137_DATA__NASCIMENTO	Data de nascimento da pessoa	Sim
	TBO137_IND_ESTADO_CIVIL	Estado Civil da pessoa	Não
	TB0137_NOME_PESSOA_REDUZIDO	Nome reduzido da pessoa	Não
	TBO137_IND_GRAU_ESCOLARIDADE	Grau de escolaridade da pessoa	Sim
	TBO137_QTDE_FILHOS	Quantidade de filhos da pessoa	Não
	TB0137_COD_UF_NASC	Código da UF de nascimento da pessoa	Não
	TBO137_COD_MUNICIPIO_NASC	Código do município de nascimento da pessoa	Não
	TBO140_COD_PAIS	Código do país	Sim
	TBO137_DATA__ENTRADA_PAIS	Data em que a pessoa entrou no país	Não
	TBO137_NOME_LOCALIDADE_NASC	Nome da Iocalidade de nascimento da pessoa	Sim
	TBO137_OPCAO_RELIGIAO	Religião da pessoa	Sim
	TBO137_VLR_RENDA_MENSAL	Valor da renda da pessoa	Sim
	TB0137_EMAIL_PESSOA	Endereço eietrônico da pessoa	Não

	DOM_COD	Código do domicílio da pessoa	Não
	PES_COD	Código do Sistema de Identificação do Cidadão	Não
	TB0137_NOME_PESSOA_MODI	Nome modificado da pessoa para busca por nome similar	Não
	TB0137_PORTARIA_NATURALIZAÇÃO	Número da portaria da naturalização	Não
	TB0137_VLR_DESPESA_MORADIA	Valor da despesa corn moradia que família tem	Sim
	TBO137_VLR_AJUDA_CUSTO	Valor da ajuda de custo que familia tem	Sim
	TBO137_DUPLA_CIDADANIA	Identifica existência de dupla cidadania	Não
	TB0137_IND_ZONA_RESID	Indicativo da zona residência do aluno	Não
	TBO137_TIPO_PESSOA	Tipo de pessoa	Não
	TBO137_NOME_PESSOA_SOCIAL	Nome da pessoa social	Não
	TBO137_NOME_PESSOA_CENSO	Nome usado para o Censo	Não
	TBO137_NOME_PESSOA_RESP1_CENSO	Nome RESP1 usado para o Censo	Não
	TBO137_NOME_PESSOA_RESP2_CENSO	Nome RESP2 usado para o Censo	Não

QUADRO 11: GED - GESTÃO EDUCACIONAL.
FONTE: PMC, 2017.

4.1.9 Controle de Corridas

O Controle de Corridas é um sistema da Secretaria de Esporte, Lazer e Juventude (SMELJ) e serve para gerenciar as corridas de rua municipais, com

cadastros dos atletas e de provas. Como dado sensível foi identificado somente a data de nascimento dos atletas.

Sistema: Controle de Corridas			
Secretaria: Esporte, Lazer e Juventude SMELJ			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
ATLETA	ATL_COD	ID Atleta	
	ATL_NOME	Nome completo	
	ATL_RG	RG	
	ATL_CPF	CPF	
	ATL_NASC	Data de nascimento	Sim
	ATL_SEXO	Sexo	
	ATL_FONE	Telefone	
	ATL_RESP	Nome do responsável pelo atleta	
	ATL_RESP_RG	RG do responsável pelo atleta	
	ATL_RESP_FONE	Telefone responsável pelo atleta	
	ATL_INSC	Antigo código identificador	
	END_COD	Código do Endereço	
	ATL_INSCPENDENTE	Inscrição pendente (Sim / Não)	
	ATL_CHIP	Chip Pendente (Sim / Não)	
	ATL_CEL	Telefone Celular	
	ATL_EMAIL	Email	
	EQU_COD	Código da equipe	

	ATL_IMPORTADO	Cadastro importado (Sim / Não)	
PROVAS	PRO_COD	ID Provas	
	PRO_DESC	Descrição	
	PRO_DATA_REALIZACAO	Data de realização	
	PRO_RANK	Se prova tem pontuação	
	PRO_OBS	Observação/ Informação sobre a prova	
	PRO_PERCURSO	Imagem do percurso da prova	
	PRO_INSC_INICIO	Data de início da inscrição	
	PRO_INSC_FIM	Data de encerramento da inscrição	
	PRO_MOSTRA	Mostrar provas (Sim / Não)	
	PRO_INSCINI_SMEL	Data de início da inscrição - SMELJ	
	PRO_INSCFIM_SMEL	Data de encerramento da inscrição - SMELJ	
	PRO_TIPO	Tipo de prova (Revezamento / Individual)	
	PRO_LIMITE	Limite de inscrições	
	CAM_COD	Código do campeonato	
	PRO_ONIBUS	Solicita confirmação de ônibus	
	PRO_INT_MINIMO_PARTIC	Quantidade minima do Grupo	
	PRO_INT_MAXIMO_PARTIC	Quantidade máxima do grupo	
	CLA_COD	Código da classe	
	EXE_COD	Código do exercício	

	PRO_CATEGORIAWEB	Mostrar categoria na Web (Sim / Não)	
	PRO_PREINSCRICAO	Pré-inscrição (Sim / Não)	
	PRO_LIMITEEQUIPE	Limite de equipes	
	PRO_EMAIL	Email / Boleto	
	PRO_LIMITE_ATLETA_TRECHO	Limite de trechos por atleta	

QUADRO 12: CONTROLE DE CORRIDAS.
FONTE: PMC, 2017.

4.1.10 NCPA - Cadastro de Pessoas Atendidas

O NCPA é o cadastro das pessoas atendidas pela Fundação de Ação Social (FAS), ou seja, em sua maioria, os cadastrados se encontram em situação de vulnerabilidade social, o que justifica a presença de campos de informações relacionadas à condição social e econômica. As informações sensíveis armazenadas pelo sistema contemplam dezesseis campos, sendo compostas principalmente por fatores de origem social, financeira e parâmetros biométricos.

Sistema: NCPA - Cadastro de Pessoas Atendidas			
Secretaria: Fundação de Ação Social - FAS			
Tabela	**Coluna**	**Descrição**	**Dado Sensível**
PESSOA_ATENDIDA	CNT_COD	Identifica a condição de trabalho	
	PCA_NOME	Nome da pessoa	
	PCA_DTNASCIMENTO	Data de nascimento	Sim
	PCA_TIPODTNASCIMENTO	Data de nascimento (informada ou comprovada)	
	PCA_SEXO	Sexo	

	CID_NATURALIDADE	Código da cidade de naturalidade	
	PCA_FOTO	Nome do arquivo de foto da pessoa	Sim
	ECI_COD	Identifica o estado civil	
	CID_PROCEDENCIA	Código da cidade de procedência	
	PCA_DATACHEGADA	Data de chegada da pessoa	
	PCA_ACOMPFAMILIA	Acompanhada de um familiar no momento do cadastro	
	PCA_POSSUIVINCFAM	Indica se a pessoa possui vínculo com a família	
	PCA_TEMPOPERDAVINC	Unidade de tempo da perda do vínculo	
	PCA_DESEJOTRATARDEPEND	Indica se a pessoa deseja tratar dependência	Sim
	PRF_PROFISSAO	Identifica uma profissão	
	PRF_OCUPACAO	Identifica uma ocupação	
	PCA_DATACONDTRAB	Data da condição de trabalho	
	PCA_TEMPORUA	Indica o tempo que a pessoa mora na rua	Sim
	PCA_UNIDTMPRUA	Unidade de tempo de moradia na rua	
	CDP_COD	Identifica uma cor de pele	Sim
	CDC_COD	Identifica uma cor de cabelo	Sim
	TPCAB_COD	Identifica um tipo de cabelo	Sim
	CDO_COD	Identifica a cor dos olhos	Sim

	PCA_TRACOS	Traços marcantes da pessoa	Sim
	USU_COD	Identifica o usuário que cadastrou a pessoa atendida	
	PCA_DATA_CADASTRO	Data de cadastro da pessoa atendida	
	PCA_RENDAINDIVIDUAL	Valor da renda individual da pessoa atendida	Sim
	PCA_RENDAFAMILIAR	Valor da renda familiar da pessoa atendida	Sim
	PCA_LOG		
	REG_COD	Identifica a regional	
	PCA_ALTURA	Altura da pessoa atendida	
	PCA_PESO	Peso da pessoa atendida	
	ID	Coluna não utilizada	
	CD_NACIONALIDADE	Código da cidade de nacionalidade	Sim
	PCA_PROVFINANC	Indica se a pessoa atendida sustenta a família	
	PCA_DT_ATUALIZA	Data de atualização dos dados	
	USU_ATUALIZA	Identifica o usuário que atualizou os dados	
	PES_COD	Coluna não utilizada	
	PCA_NMEMAE	Nome da mãe	
	PCA_NMEPAI	Nome do pai	
	PES_NUM_SIC	Número do SIC	
	PCA_FLAGRUA	Indica se a pessoa atendida é moradora de rua	Sim
	PCA_ANOCONCLUSAOESC	Ano de conclusão	

	FAM_INT_CODDOM	Identifica um domicílio	
	ESC_COD	Identifica a escolaridade	Sim
	PCA_COD	Chave primária da tabela	
	NUM_CARTEIRINHA_SMAB	Número da carteirinha da SMAB	
	DESCRICAO_PROGRAMASOCIAL	Descrição do programa social	Sim
	PROG_COD	Programa social ao qual a pessoa está associada	Sim
	PCA_NOMEFONETICO3	Fonética do terceiro nome	
	PCA_NOMEFONETICO2	Fonética do segundo nome	
	PCA_EMAIL	Email da pessoa	
	GPA_CODIGO	Identifica um grau de parentesco	
	PCA_NOMEFONETICO1	Fonética do primeiro nome	

QUADRO 13: NCPA - CADASTRO DE PESSOAS ATENDIDAS
FONTE: PMC, 2017.

4.1.11 Comparativo

Ao comparar os dez sistemas levantados, o com mais registro de dados sensíveis é o NCPA utilizado pela FAS, com 16 campos. O fato de lidar com pessoas em situação de vulnerabilidade social é o fator mais destacado para este resultado. O NCPA é seguido pelo E-Saúde, com doze campos contendo informações sensíveis, e o GED, com dez resultados, ambos, também com dados predominantemente de natureza socioeconômica ou de origem étnica. Assim, notamos que para os cadastros municipais, os tipos mais comuns de dado sensíveis armazenados dizem respeito à origem social, étnica e financeira das pessoas atendidas.

Esse padrão para os dados armazenados é justificado pelo modelo de políticas públicas que demanda, para sua efetivação, classificações sobre fatores socioeconômicos para ações que atendam a população que se encontra em situação de vulnerabilidade social e políticas afirmativas. Entretanto, a exclusão baseada em

características sociais e étnicas é uma realidade da qual os governos também são promotores, além de que, com o registro de informações dessa natureza, a aplicação de potenciais políticas de segregação é facilitada.

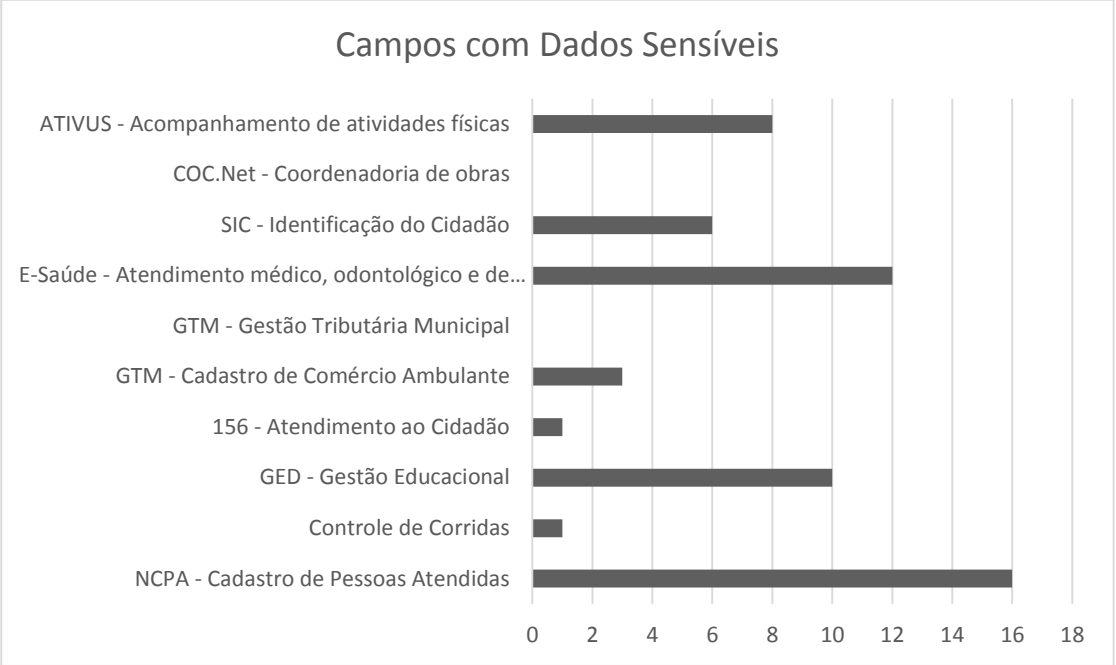

GRÁFICO 02: NÚMERO DE CAMPOS DE DADOS SENSÍVEIS POR CADASTRO.
FONTE: O AUTOR.

4.2 VALOR COMERCIAL

Conforme descrito na metodologia (3.2.2), os valores comerciais de dados pessoais foram atribuídos a partir da cotação dos valores (STEEL *et al.*, 2013), em dólares (US$) e analisados a partir da classificação dos campos cadastrais disponíveis no material fornecido pela prefeitura.

O tipo de dado com valor comercial mais alto é relacionado a saúde do indivíduo, pois no mercado de dados pessoais, as informações mais difíceis de serem encontradas possuem um preço mais alto por ser uma informação de natureza mais privada e específica, não sendo facilmente encontrada em muitos bancos de dados, como dados básicos e de identificação, que são padrão em praticamente qualquer cadastro eletrônico.

Nesse subcapítulo os campos não precificados dos quadros dos sistemas cadastrais foram suprimidos, de forma que somente os dados que possuem valor atribuído sejam mostrados.

4.2.1 ATIVUS - Acompanhamento de atividades físicas

O sistema ATIVUS da SMELJ possui como estimativa de valor comercial um total de US$ 1,2541 por cada usuário cadastrado, sendo este valor proveniente, principalmente, dos dados de saúde contidos neste sistema.

Sistema: ATIVUS - Acompanhamento de atividades físicas			
Secretaria: Esporte Lazer e Juventude - SMELJ			
Tabela	**Coluna**	**Descrição**	**Valor (US$)**
ALUNO	ALU_FUMA	Indica se o aluno fuma	0,23
	ALU_BEBE	Indica se o aluno bebe	0,23
	AME_IDF	Identifica a assistência médica	0,23
	PRO_IDF	Identifica a profissão	0,066
PESSOA	PES_NASC	Data de nascimento da pessoa	0,092
	PES_CIVIL	Estado civil da pessoa	0,092
	PES_SEXO	Sexo da pessoa	0,0004
	PES_FONE	Telefone da pessoa	0,004
	END_IDF	Identifica o endereço	0,0004
	PES_EMAIL	Email da pessoa	0,0713
	PES_FONE_PRINCIPAL	Telefone principal da pessoa	0,004
	PES_FONE_ALTERNATIVO	Telefone alternativo da pessoa	0,004

	PES_DEFICIENCIA	Tipo de deficiência que a pessoa pode possuir	0,23
Total			1,2541

QUADRO 14: ATIVUS - ACOMPANHAMENTO DE ATIVIDADES FÍSICAS.
FONTE: PMC, 2017.

4.2.2 COC.Net - Coordenadoria de obras

O sistema COC.Net utilizado pela SETRAN tem um valor de US$ 0,0793, de onde todos dados com preço estimado são de contato do usuário.

Sistema: COC.Net - Coordenadoria de obras			
Secretaria: Trânsito - SETRAN			
Tabela	**Coluna**	**Descrição**	**Valor (US$)**
USUÁRIO_EXTERNO	UEX_EMAIL	Email do usuário externo	0,0713
	UEX_TELEFONE	Número do telefone do usuário externo	0,004
	UEX_CELULAR	Número do celular do usuário externo	0,004
Total			0,0793

QUADRO 15: COC.NET - COORDENADORIA DE OBRAS.
FONTE: PMC, 2017.

4.2.3 SIC - Identificação do Cidadão

O Sistema de Identificação do Cidadão possui um valor de venda, por pessoa cadastrada, de US$ 0,4902, resultado do armazenamento de informações de natureza variada, desde dados de saúde a informações pessoais.

Sistema: SIC - Identificação do Cidadão
Secretaria: Diversos órgãos e secretarias

Tabela	Coluna	Descrição	Valor (US$)
PESSOA	Pes_Dta_Nascimento	Data de nascimento	0,092
	Pes_sexo	Sexo da pessoa	0,0004
	Est_Cod	Código do estado civil	0,092
	Pes_Deficiência	Indica se apessoa possui deficiência	0,23
	Cor_Cod	Código da Cor / Raça	0,0045
	Pes_Eml	Email	0,0713
Total			0,4902

QUADRO 16: SIC - IDENTIFICAÇÃO DO CIDADÃO.
FONTE: PMC, 2017.

4.2.4 E-Saúde - Atendimento médico, odontológico e de outras especialidades

O cadastro individual de um usuário do E-Saúde, da SMS, vale US$ 0,2553, sendo valorizados, em sua maioria dados de identificação.

Sistema: E-Saúde - Atendimento médico, odontológico e de outras especialidades			
Secretaria: Saúde - SMS			
Tabela	**Coluna**	**Descrição**	**Valor (US$)**
USUARIO	cddomicilio	Código do domicílio	0,0004
	tpsexo	Tipo de sexo	0,0004
	dtnascimento	Data de nascimento	0,092
	cdracacor	Codigo da raça / cor	0,0045
	cdestadocivil	Código do estado civil	0,092

	cdocupacao	Código da profissão conforme código brasileiro de ocupação	0,066
Total			0,2553

QUADRO 17: SISTEMA: E-SAÚDE - ATENDIMENTO MÉDICO, ODONTOLÓGICO E DE OUTRAS ESPECIALIDADES.
FONTE: PMC, 2017.

4.2.5 GTM - Gestão Tributária Municipal

O sistema da Gestão Tributária Municipal não possui informações cadastradas com valor comercial.

4.2.6 GTM - Cadastro de Comércio Ambulante

O Cadastro de Comércio Ambulante do GTM possui um valor comercial de US$ 0,7184 por pessoa registrada, com registro de natureza diversa, mas principalmente dados de saúde, que possuem um valor de venda maior.

Sistema: GTM / Cadastro de Comércio Ambulante			
Secretaria: Diversos órgãos e secretarias			
Tabela	**Coluna**	**Descrição**	**Valor (US$)**
GTMAMB Ambulante	Cod_End_Generico	Endereço	0,0004
	Num_Carteira_Profissionai	Número da carteira profissional	0,066
	lnd_Estado_Civil	Estado civil	0,092
	Des_Profissao_Conjuge	Profissão do conjuge	0,066
	Num_Telefone	Número do telefone	0,004
	Ind_Deficiente_Fisico	Caso possui alguma deficiência	0,23
	Des_Deficiencia	Descrição da deficiência	0,23

	Num_Filhos_Menores	Quantidade de filhos menores	0,03
Total			0,7184

QUADRO 18: GTM - CADASTRO DE COMÉRCIO AMBULANTE.
FONTE: PMC, 2017.

4.2.7 156 - Atendimento ao Cidadão

O preço de venda de um solicitante do sistema 156 - Atendimento ao Cidadão é US$ 0,1677, compostos principalmente por valores de identificação e contato.

Sistema: 156 - Atendimento ao Cidadão			
Secretaria: Todos os órgãos e secretarias			
Tabela	**Coluna**	**Descrição**	**Valor (US$)**
Central 156 - Solicitação de Serviços	Sexo	Gênero masculino ou feminino	0,0004
	Telefone	Número de telefone para contato com cidadão	0,004
	Data de Nascimento	Data de nascimento do cidadão	0,092
	E-mail	Se o meio de resposta selecionado for e-mail	0,0713
Total			0,1677

QUADRO 19: 156.
FONTE: PMC, 2017.

4.2.8 GED - Gestão Educacional

O sistema de Gestão Educacional apresenta um valor de US$ 0,2902 para cada usuário cadastrado, cujas informações precificadas são predominantemente de identificação.

Sistema: GED - Gestão Educacional	

Secretaria: Educação SME			
Tabela	**Coluna**	**Descrição**	**Valor (US$)**
PESSOA	TBO137_IND_SEXO	Sexo Feminino ou Masculino	0,0004
	TBO137_IND_RACA	Indica a raça da pessoa	0,0045
	TBO137_DATA__NASCIMENTO	Data de nascimento da pessoa	0,092
	TBO137_IND_ESTADO_CIVIL	Estado Civil da pessoa	0,092
	TBO137_QTDE_FILHOS	Quantidade de filhos da pessoa	0,03
	TB0137_EMAIL_PESSOA	Endereço eietrônico da pessoa	0,0713
Total			0,2902

QUADRO 20: GED - GESTÃO EDUCACIONAL.
FONTE: PMC, 2017.

4.2.9 Controle de Corridas

O sistema de Controle de Corridas, da SMELJ, apresenta um valor de US$ 0,1761 por cada atleta cadastrado. Os dados com valores são, em sua maioria, de contato.

Sistema: Controle de Corridas			
Secretaria: Esporte, Lazer Juventude SMELJ			
Tabela	**Coluna**	**Descrição**	**Valor (US$)**
ATLETA	ATL_NASC	Data de nascimento	0,092
	ATL_SEXO	Sexo	0,0004
	ATL_FONE	Telefone	0,004
	ATL_RESP_FONE	Telefone Responsavel pelo Atleta	0,004

	END_COD	Código do Endereço	0,0004
	ATL_CEL	Telefone Celular	0,004
	ATL_EMAIL	Email	0,0713
Total			0,1761

QUADRO 21: CONTROLE DE CORRIDAS.
FONTE: PMC, 2017.

4.2.10 NCPA - Cadastro de Pessoas Atendidas

O NCPA, da FAS, tem um valor por pessoa atendida de US$ 0,6984, cuja natureza dos dados com valorização é variada.

Sistema: NCPA - Cadastro de Pessoas Atendidas			
Secretaria: Fundação de Ação Social - FAS			
Tabela	**Coluna**	**Descrição**	**Valor (US$)**
PESSOA_ATENDIDA	PCA_DTNASCIMENTO	Data de nascimento	0,092
	PCA_SEXO	Sexo	0,0004
	ECI_COD	Identifica o estado civil	0,092
	PCA_DESEJOTRATARDEPEND	Indica se a pessoa deseja tratar dependência	0,23
	PRF_PROFISSAO	Identifica uma profissão	0,066
	CDP_COD	Identifica uma cor de pele	0,0045
	PCA_EMAIL	Email da pessoa	0,0713
Total			0,6984

QUADRO 22: NCPA - CADASTRO DE PESSOAS ATENDIDAS
FONTE: PMC, 2017.

4.2.11 Comparativo

Na comparação dos valores comerciais por pessoa cadastrada por sistema, o maior preço foi o do sistema ATIVUS, US$ 1,2541, de uso da SMELJ que, por ser

uma secretaria que trabalha com a promoção do esporte e inclusão dos jovens em práticas saudáveis, possui o maior número de campos relacionados a uso de álcool e drogas, bem como a presença de deficiências. Na sequência aparecem o sistema de Cadastro de Comércio Ambulante e o Cadastro de Pessoas Atendidas da FAS, ambos com campos valorizados de origem mista, mas com algumas informações de saúde, que é tipo de informação de valor comercial mais elevado.

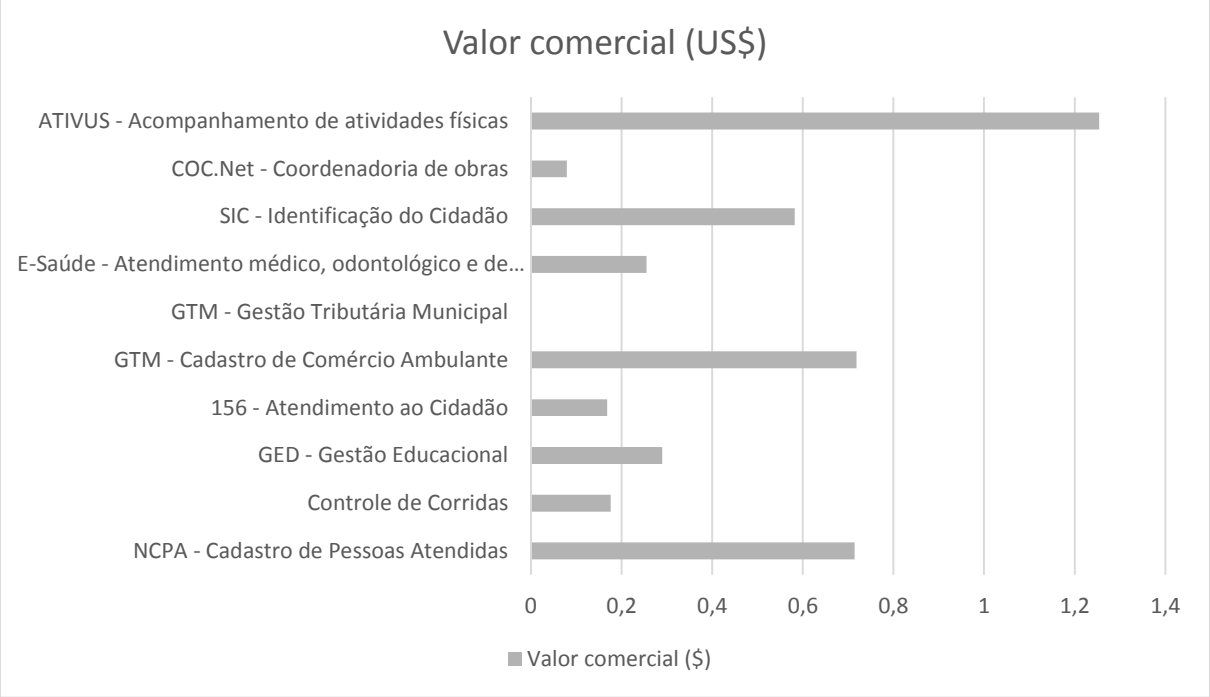

GRÁFICO 03: VALOR COMERCIAL DAS INFORMAÇÕES CADASTRADAS POR SISTEMA.
FONTE: O AUTOR.

4.3 MÚLTIPLO ACESSO

Conforme descrito na metodologia, a multiplicidade de acesso a um banco de dados por mais de um departamento aumenta as questões relacionadas à quebra e invasão de privacidade associada a um cadastro. Dentre os sistemas levantados, quatro possuem acesso de mais de uma secretaria: o SIC, o GTM, o GTM – Cadastro de Comércio Ambulante, e o Atendimento ao Cidadão – 156. Esses sistemas possuem dados de finalidade genérica e identificação, servindo de apoio a diversas secretarias da prefeitura.

Sistema	Múltiplo Acesso
ATIVUS - Acompanhamento de atividades físicas	**Não**
COC.Net - Coordenadoria de obras	**Não**
SIC - Identificação do Cidadão	**Sim**
E-Saúde - Atendimento médico, odontológico e de outras especialidades	**Não**
GTM - Gestão Tributária Municipal	**Sim**
GTM - Cadastro de Comércio Ambulante	**Sim**
156 - Atendimento ao Cidadão	**Sim**
GED - Gestão Educacional	**Não**
Controle de Corridas	**Não**
NCPA - Cadastro de Pessoas Atendidas	**Não**

QUADRO 23: CADASTROS QUE PERMITEM O MÚLTIPLO ACESSO.
FONTE: PMC, 2017.

4.4 ÍNDICE DE VIGILÂNCIA

Dentre os sistemas levantados, o NCPA, utilizado pela FAS, possui o índice de vigilância mais alto, 11,4336. O fato desse cadastro servir a políticas de assistência e inclusão social justifica o armazenamento de dados sensíveis e relacionados a saúde dos usuários. Entretanto, é justamente a vulnerabilidade social dos cadastrados o fator que evidencia o prejuízo potencial que a quebra da privacidade dessas informações pode provocar, principalmente no que concerne à exclusão da cidadania plena. Um tipo de dado particularmente importante desse sistema é o que trata de características físicas, que ajuda no reconhecimento de beneficiários das políticas de atendimento, mas também pode estabelecer perfis para suspeitos potenciais.

O dano potencial que vigilância governamental exerce sempre vem acompanhado de benefícios que podem ser relacionados à segurança ou a eficiência da prestação de serviços e efetividade das políticas públicas. Nesse sentido, as pessoas que são o público alvo de práticas de auxílio e acolhimento também são aquelas que, por outro lado, são consideradas indesejáveis ou suspeitas em outros

contextos de ação, fazendo com que a simples identificação de características pessoais em um banco de dados possa causar prejuízo aos indivíduos cadastrados.

Já o sistema ATIVUS, operado pela SMELJ, foi o segundo colocado para o Índice de Vigilância, com 10,0328 pontos. O cadastro armazena os dados de pessoas atendidas por programas de atividade física e possui muitas informações relacionadas a saúde dos cidadãos beneficiados, que tem alto valor comercial e cuja quebra de sigilo pode causar prejuízo na vida das pessoas que sofrem com algum problema dessa natureza. O ATIVUS, por se tratar de uma iniciativa pública de promoção do esporte, também trabalha predominantemente com pessoas de baixa renda, sobrepondo, assim, fatores de juventude, saúde e origem social para o funcionamento do sistema.

O Sistema de Identificação do Cidadão vem na sequência dos maiores índices, com 4,4032. O SIC funciona como uma chave comum para vários sistemas da prefeitura e armazena informações de identificação, cujos dados sensíveis são, principalmente, relativos à origem social e étnica, que podem colocar indivíduos com determinados perfis em situação de risco, especialmente imigrantes que podem ser limitados em seu direito à cidadania plena.

Sistema	**Campos com Dados Sensíveis**	**Valor (US$)**	**Acesso Múltiplo**	**Índice de Vigilância**
ATIVUS - Acompanhamento de atividades físicas	8	1,2541	0	10,0328
COC.Net - Coordenadoria de obras	0	0,0793	0	0
SIC - Identificação do Cidadão	6	0,4902	1	4,4932
E-Saúde - Atendimento médico, odontológico e de outras especialidades	12	0,2553	0	3,0636
GTM - Gestão Tributária Municipal	0	0	1	1
GTM - Cadastro de Comércio Ambulante	3	0,7184	1	3,1552
156 - Atendimento ao Cidadão	1	0,1681	1	1,1681

GED - Gestão Educacional	10	0,2902	0	2,902
Controle de Corridas	1	0,1761	0	0,1761
NCPA - Cadastro de Pessoas Atendidas	16	0,7146	0	11,4336

QUADRO 24: PARÂMETROS E ÍNDICE DE VIGILÂNCIA POR SISTEMA.
FONTE: O AUTOR.

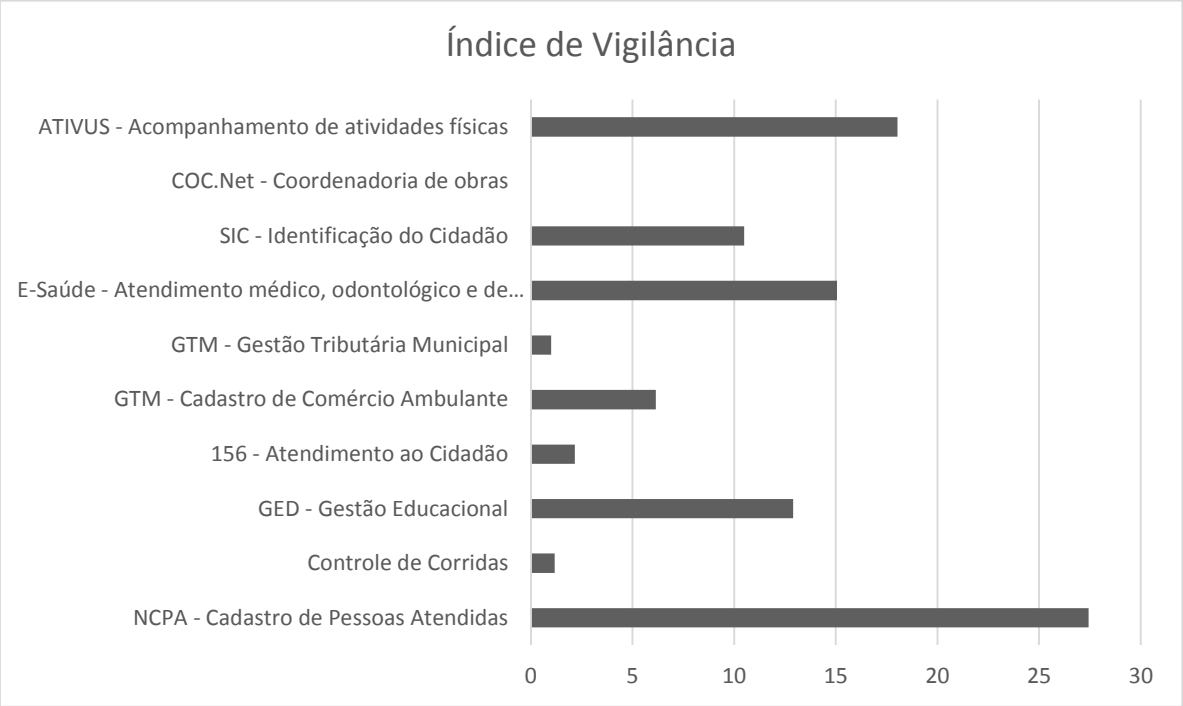

GRÁFICO 04: ÍNDICE DE VIGILÂNCIA POR SISTEMA.
FONTE: O AUTOR.

4.5 DADOS PESSOAIS COMO INSTRUMENTO DE VIGILÂNCIA E CONTROLE NA GESTÃO URBANA

Apoiado no levantamento realizado para este trabalho, foi identificado que a Prefeitura Municipal de Curitiba possui, e busca expandir, um modelo de gestão urbana que lança mão de tecnologias da informação, especificamente bancos de dados cadastrais, para a implementação de suas políticas públicas e provisão de serviços para a população. Essa realidade, evidentemente, não é exclusividade de Curitiba, mas sim um movimento global de incorporação tecnológica que se intensificou com a informatização dos sistemas e processos (LYON, 2013).

A invasão das TICs nas cidades veio acompanhada de um sistema integrado de vigilância que faz parte de grande parte dos processos de rotina das pessoas, onde

a utilização dessas ferramentas pelo governo busca a melhoria da segurança pública e serviços em geral. Esse fenômeno fez com que as cidades se tornassem palco das práticas de vigilância atuais, pois é onde se concentra a maior parte das pessoas e da tecnologia, bem como são os polos que se articulam nas dinâmicas globais (ASCHER, 2010; SANTOS, 2013; SASSEN,2001). Com a infiltração das TICS no meio urbano, seu uso vem sendo incentivado pela administração pública como forma de melhorar a gestão e o atendimento aos cidadãos (FIRMINO, 2001; FIRMINO; FREY, 2014; KITCHIN, 2015).

A variedade de secretarias com cadastros de cidadãos demonstra que a gestão municipal de Curitiba realiza cadastramentos, com o objetivo de melhor fiscalizar e servir a população, em praticamente todos os temas de responsabilidade da prefeitura. Apesar de não ser o propósito dessa pesquisa, é possível inferir que esses sistemas auxiliam, de fato, na execução dos processos, reduzindo o tempo demandado pela burocracia analógica.

O projeto da prefeitura é incrementar ainda mais a sua base tecnológica, visando a modernização da gestão (CUNHA VAZ, 2015). Essa tendência objetiva a consolidação de Curitiba como uma smart city, que é um modelo de gestão apoiado em tecnologias de informação e pretende o desenvolvimento inteligente e sustentável da cidade, fornecendo insumos de informação simultânea para a otimização da tomada de decisões. Para implementação desse projeto são necessários um aporte e uma integração tecnológica ainda maior do que hoje está implantado na PMC.

Entretanto, as tecnologias de vigilância e o Big Data, além dos benefícios, também trazem consigo para a administração pública uma tendência à gestão tecnocrática e oligóptica da cidade. Ou seja, um modelo onde as informações são controladas por um grupo de pessoas que tomam decisões baseadas em dados estatísticos. O problema desse padrão é que ficam alheios os outros aspectos não computáveis da realidade urbana, bem como não são identificadas e analisadas a origem dos problemas das cidades, ficando restrito à resolução dos conflitos de maneira pontual e não definitiva (BATTY, 2013; KITCHIN, 2014).

Aliado a isso, ainda há a preocupação com a privatização da administração pública, já que as tecnologias normalmente são fornecidas e geridas por empresas privadas, comprometendo ainda mais a privacidade dos cidadãos (KITCHIN, 2014). Essa realidade faz parte da administração pública de Curitiba, visto que a maior parte

dos sistemas municipais são geridos pelo Instituto Curitiba Informática, uma empresa privada que controla informações públicas e o desenvolvimento tecnológico da prefeitura.

A vigilância atualmente está presente na vida dos indivíduos através do uso de sistemas de coleta de dados e pode ser aplicada por instituições privadas e governos com a finalidade de melhorar serviços prestados, aumentar as vendas através de marketing direcionado, garantir a segurança pública urbana e de fronteiras, e implementar políticas públicas (LYON, 2013). Assim, a coleta e armazenamento de dados pessoais é uma forma de vigilância que vem sendo utilizada pela gestão pública, inclusive pela Prefeitura Municipal de Curitiba.

Atualmente o que se entende por “nova vigilância” são processos que dependem exclusivamente de um aparato tecnológico para que funcione, sendo que tipo tecnológico de vigilância mais comum e notável para a análise do cenário atual é a coleta e armazenamento de dados (MURAKAMI WOOD *et al*., 2006). O levantamento realizado demonstrou que a Prefeitura Municipal de Curitiba utiliza esse tipo de tecnologia, que se baseia em armazenamento, análise e processamento de bases de dados, a dataveillance de Roger Clarke, e pode ser feita sobre o indivíduo ou sobre grupos de indivíduos (CLARKE, 1988).

A vigilância praticada pela administração pública em Curitiba pretende, a princípio, melhorar o atendimento aos usuários dos serviços municipais e os processos internos da prefeitura. Entretanto, implicado nessas intenções está o controle do governo sobre os indivíduos, convertendo-se em problemas de privacidade e prejuízos a pessoas pertencentes a certos grupos sociais ou étnicos (LYON, 2004; LYON, 2009b; KITCHIN, 2013).

A prática de vigilância se estabelece através do controle comportamental dos indivíduos desde a transição da modernidade e a instituição da lógica disciplinar do poder. A disciplina é uma ferramenta para a otimização do uso do tempo através de um controle da mente que objetiva a docilidade e a utilidade (FOUCAULT, 2013). Tal qual esse exercício de poder moderno, nós ainda vivemos sob o paradigma de uma estrutura que utiliza a dominação dos indivíduos através do governo da mente, que hoje se faz com a coleta massiva de informações pessoais, atualmente utilizadas para o direcionar o marketing de produtos e serviços, incentivando o consumo, e fiscalizar os cidadãos em suas práticas de rotina.

Porém, diferente da disciplina, hoje a supervisão do indivíduo não pressupõe a individualização do sujeito, mas sim a pulverização das características individuais em categorias de informações cifradas e armazenadas em bancos de dados, os “divíduos”. Essas informações são descoladas do sujeito e não são coincidentes com a sua localização física e dimensional, podendo ser transformada em estatísticas e amostras para o controle dos riscos (DELEUZE, 2013; BECK, 2010).

Essa dinâmica, segundo Tobias Matzner (2016), coloca o indivíduo contra esses construtos, ou cópias de dados, em uma relação em que as identidades codificadas se tornam uma imposição para o sujeito original. A análise de Matzner denuncia uma consequência importante da identificação e o cálculo de risco associados a indivíduos a partir da análise de perfis, pois coloca a própria categorização individual baseada em determinadas características como um reforço para a construção da identidade. O problema, ainda, tem relação com a realidade que esses perfis codificados opõem uma identidade criada indiretamente em bancos de dados com um padrão formado a partir de outros sujeitos, servindo para o estabelecimento de vereditos algorítmicos (MATZNER, 2016).

A automação do processo decisório baseado em cálculos de risco faz com que a definição de perfis associados a ameaças, ou privilégios, seja utilizada como forma de execução de ações da parte do poder público. Assim, a discriminação baseada em características pessoais armazenadas em bancos de dados passa a ser um regime de rotina nos processos públicos, nos levando a um sistema de “classificação panóptica”, que pode implicar em práticas totalitárias de governo (GANDY, 1993; LOS, 2006; LYON, 2009b).

Os tipos de dados que, de maneira geral, mas não somente, podem representar uma maior ameaça à privacidade e potencial de dano dependendo da forma como forem utilizados ou divulgados, são chamados de “informações sensíveis”. Esse tipo de informação deve ser tratado e processado de maneiras específicas para que não provoquem prejuízo ao indivíduo registrado, ainda que atualmente sejam comercializadas entre as empresas de tecnologia (OHM, 2015).

No levantamento realizado foi identificado que a Prefeitura Municipal de Curitiba armazena diversas informações sensíveis de seus cidadãos, podendo essas informações ser de vários tipos classificados. Entretanto, dentre os tipos de dados sensíveis mais recorrentes eram os que identificavam a origem étnica ou social dos

usuários dos sistemas cadastrais, que são um tipo de informação que podem também ser utilizadas para os processos de exclusão e discriminação, assim como para a inclusão e identificação de padrões sociais negativos.

Os sistemas com maior número de dados sensíveis dessa natureza foram justamente os que trabalham com populações em situação de vulnerabilidade social e juventude, o que justifica a coleta e o armazenamento desses dados para que o atendimento e a promoção das políticas públicas sejam efetivados. Assim, é fundamental que a proteção e processamento dessas informações sejam feitos com responsabilidade de forma a proteger a privacidade, evitando que elas prejudiquem de alguma forma os sujeitos atendidos.

Hoje em dia, há um mercado multibilionário que lucra com o comércio de informações pessoais registradas em bancos de dados. Apesar da movimentação de altos valores financeiros, os dados pessoais de um único indivíduo normalmente não passam de um dólar americano. Os valores mais altos para as informações pessoais são as que se referem a condições de saúde, pois essa são dificilmente encontradas em cadastros comuns, como as informações de identificação e contato (STTEL, *et al.*, 2017).

Esse tipo de dado, considerado também sensível, muitas vezes tem como uma de suas únicas fontes os cadastros de instituições públicas, como a Prefeitura Municipal de Curitiba. Na pesquisa foi identificado que o sistema cadastral que teria o maior de venda é o que trata do atendimento à juventude e incentivo à prática esportiva, pois esse banco de dados abriga mais informações que dizem respeito à condição de saúde dos beneficiários.

Por deter informações privadas com valor comercial, é especialmente importante que o controle da administração pública sobre o uso dessas informações seja sempre alto, visto que uma empresa privada que gerencie esses dados tem formas de lucrar com essa situação. Além disso, a própria gestão pública pode ganhar com a venda desses dados, tornando também imprescindível um controle democrático sobre o aproveitamento das informações pessoais.

Mesmo com o potencial de totalitarismo, discriminação e exclusão, a demanda por sistemas cada vez mais inteligentes e vigilantes só cresce, demanda essa que vem em decorrência do desejo por mais segurança e eficiência; resultado esse nem sempre alcançado através dos dispositivos tecnológicos (KAYYALI,2016; PEÑA,

VELASCO,2016). Como já referido, a Prefeitura Municipal de Curitiba está inserida nessa dinâmica, com planos e projetos de investimento cada vez maiores em sistemas de vigilância.

Por se tratar de uma realidade tecnológica que não parece que vai retroceder, e que ainda apresenta alguns resultados positivos importantes em muitas áreas nas quais são utilizadas, inclusive na gestão urbana, cabe, como alternativa mais viável e recomendada, a regulamentação e o controle das práticas de vigilância pelo poder público e privado. Foi sugerido, por exemplo, que não sejam utilizados classificação de raça e gênero, bem como validações biométricas nos bancos de dados pessoais (GANDY, 2006; BALL, 2006).

Outros tipos de restrição e regulamentação podem ser impostos aos gestores dos dados pessoais coletados, como as próprias leis que tratam do tema, além de uma rígida fiscalização dos processamentos e movimentação das informações pessoais. Entretanto, ainda mais importante que isso, é que o debate sobre as implicações desse tipo de uso da tecnologia pode trazer seja difundido na sociedade, para que os cidadãos tomem o conhecimento e controle sobre o destino de suas informações pessoais.

5 CONCLUSÃO

Esta pesquisa teve por objetivo estudar e categorizar o uso de dados pessoais utilizados pela gestão pública de cidades, através do exemplo da Prefeitura Municipal de Curitiba, em suas implicações como tecnologia de vigilância. Portanto, este trabalho vem acompanhado do debate sobre a emergência de um sistema de vigilância cada mais integrado e pervasivo, que abrange as esferas públicas e privadas, trabalhando com informações de natureza diversa. O campo analisado neste trabalho possui bases teóricas muito vastas, envolvendo diversas áreas de conhecimento distintas, como a filosofia, a sociologia, o direito, o urbanismo, entre outros.

Porém, apesar da rica disponibilidade conceitual entre os temas trabalhados, ainda são poucos os autores que analisam a relação da vigilância no âmbito do urbanismo e, mais especificamente, da gestão urbana. Nesse sentido, a Revisão de Literatura desta pesquisa buscou estabelecer as correlações e narrativas teóricas e contribuir para o debate acadêmico na área, além da análise prática sobre o uso de dados pessoais pela gestão urbana municipal.

Para podermos observar e entender a utilização de dados pessoais como instrumento de vigilância na gestão urbana, foi elaborada uma metodologia específica para a avaliação do potencial de vigilância contido nos bancos de dados que contivessem dados pessoais da Prefeitura Municipal de Curitiba. As informações representaram dez sistemas de dados e foram disponibilizadas em formato analógico. A metodologia de análise estabeleceu a classificação dos campos de informações coletadas e uma fórmula para a criação de um Índice de Vigilância construído para determinar uma categorização do material coletado para análise.

O primeiro critério utilizado para a classificação dos dados foi a sensibilidade das informações, considerada a partir do entendimento teórico, jurídico e de opinião pública sobre o tema (OHM, 2015; PEW RESEARCH CENTER, 2014, BRASIL, 2016). Foi feita uma classificação dos cadastros municipal em relação à quantidade de informações sensíveis armazenadas, em que o NCPA, utilizado pela Fundação de Ação Social (FAS), foi o com maior número. Esse cadastro possui em seus dados cadastrados um grande número de informações sensíveis sobre origem étnica, social

e financeira dos usuários, por se tratar de uma secretaria que lida com pessoas em situação de vulnerabilidade social.

O segundo ponto analisado foi a valorização comercial dos dados, que determina um preço de venda para alguns tipos de dados pessoais, em que o com maior valorização são informações de saúde. (STEEL *et al.*, 2013). O cadastro com maior valor por indivíduo cadastrado foi o sistema ATIVUS, da Secretaria de Esporte, Lazer e Juventude (SMELJ), que armazena mais tipos de informações de saúde, por ter como objetivo a promoção de práticas esportivas e a inclusão social de jovens através de atividades físicas.

O terceiro ponto verificado foi se o sistema cadastral possuía múltiplo acesso, ou seja, podia ser acessado por mais de uma secretaria, pois esse fator pode representar uma maior ameaça à privacidade dos usuários (MURAKAMI WOOD *et al.*, 2006). Nessa análise foi verificado que o Sistema de Informações do Cidadão, o sistema de Gestão de Tributária Municipal, o Cadastro de Comércio Ambulante, e o Sistema de Atendimento ao Cidadão – 156, foram os bancos de dados que podem ser acessados por mais de uma secretaria. Isso é justificado pelo caráter mais genérico das informações contidas neles.

Por fim, esses três fatores foram combinados em uma fórmula que calcula um Índice de Vigilância para cada sistema estudado, visto que a sobreposição de agentes potenciais de vigilância faz amentar o risco de prejuízo ou discriminação para os usuários cadastrados. Nessa análise foi encontrado que o sistema com maior potencial de vigilância é o NCPA, da FAS, por contar com o maior número absoluto de dados sensíveis cadastrados e um alto valor comercial para os dados armazenados. Os sistemas ATIVUS, da SMELJ, e o E-Saúde, da SMS, vem na sequência com uma alta possibilidade de exercício de vigilância.

A pesquisa como um todo buscou discutir a relação dos governos municipais com as práticas de vigilância, bem como entender quais são os tipos de dados pessoais utilizados pela gestão urbana. É necessário evidenciar os problemas associados à invasão tecnológica do meio urbano e da administração pública no contexto da vigilância ubíqua, demonstrando a interconexão dos elementos em uma rede global de bancos de dados e práticas de catalogação.

Neste trabalho verificamos que a utilização de dados pessoais perpassa diferentes áreas da administração pública municipal, onde cada tema de interesse

possui um rol específico de informações das quais lança mão para o funcionamento dos serviços. Ou seja, para o funcionamento da gestão urbana contemporânea, do governo eletrônico à smart city, se tornou um imperativo o uso desse tipo de dado e a criação de bancos de dados cada vez mais integrados.

Foi demonstrado que o maior número de informações sensíveis armazenadas nos bancos de dados diz respeito à origem étnica e social das pessoas, o que torna a vulnerabilidade social dos indivíduos um fator de risco que pode causar exclusão ou limitação da cidadania plena. O cuidado e a ética na finalidade do uso dessas informações são cruciais para que o potencial de dano criado por essa tecnologia de vigilância não se concretize.

Evidentemente, o desenvolvimento tecnológico e o uso de dados pessoais não são uma realidade exclusivamente negativa, já que, de fato, muitos dos processos de gestão urbana são otimizados e as categorização das pessoas em perfis pode ser crucial para a efetivação de políticas públicas de inclusão social. Além disso, a ubiquidade tecnológica e o desenvolvimento do Big Data são processos que já estão consolidados, então devemos nos voltar para a implantação de ações de regulação e controle da parte da sociedade sobre a gestão dos dados pessoais.

5.1 LIMITAÇÕES DA PESQUISA E SUGESTÕES PARA TRABALHOS FUTUROS

Um primeiro desafio enfrentado para desenvolvimento desta pesquisa foi a falta de um fundamento conceitual aprofundada para a construção da metodologia, bem como sistemas de classificação de dados pessoais além do fator de sensibilidade. A falta de uma base teórica que pudesse embasar a definição de tipos de dados pessoais impôs a criação de uma metodologia experimental para a definição de um Índice de Vigilância.

Outro fator que se mostrou um limitador para o desenvolvimento da pesquisa foram os processos burocráticos para o fornecimento dos dados solicitados da parte da administração pública. A sucessão de mal-entendidos e análises jurídicas levou ao atraso da pesquisa, bem como a incerteza sobre o material que seria disponibilizado, que impacta na definição da metodologia de análise definida.

O caráter descritivo e quantitativo do trabalho, sugere que se façam pesquisas em termos similares em outras cidades a fim de se estabelecer um comparativo e

identificar padrões sobre o tema, assim como que se façam outros estudos futuros de caráter mais explicativo, abrangente e holístico do fenômeno. Além disso, também se propõem que sejam feitas análises sobre o tema em outros geográficos e níveis de governo.

Outra sugestão é que se façam estudos relativos a outros tipos de tecnologias de vigilância utilizadas na gestão urbana, não somente os bancos de dados, para que se expanda o conhecimento sobre o assunto e amplie o entendimento sobre o uso dessas ferramentas.

Pode-se, ainda, realizar uma pesquisa sobre a convergência entre o discurso e a prática associada ao uso de tecnologias de vigilância pelo poder pública, bem como averiguar se os interesses do governo e do governo estão alinhados no que tange a coleta e o uso desses dados.

REFERÊNCIAS

ASCHER, F. **Os novos princípios do urbanismo.** Tradução de Somekh, N. São Paulo: Romano Guerra, 2010.

AMIN, A.; THRIFT, N. **Cities:** reimagining the urban. Cambridge: Polity Press, 2002.

ARTIGO 19. **Da cibersegurança à ciberguerra:** o desenvolvimento de políticas de vigilância no Brasil. ARTIGO 19, 2016. Disponível em: http://artigo19.org/wp-content/blogs.dir/24/files/2016/03/Da-Ciberseguranc%CC%A7 a-a%CC%80-Ciberguerra-WEB.pdf. Acessado em: 28/04/2016.

BALL, K. Organization, surveillance and the body: towards a politics of resistance *In:* LYON, D. **Theorizing surveillance:** the panopticon and beyond. Cullompton: Willam Publishing, 2006.

BATTY, M. **Big data, smart cities and city planning.** London: Dialogues in Human Geography, v. 3, n. 3, p. 274-279.

BAUMAN, Z. **Modernidade líquida.** Tradução de Dentzien, P. Rio de Janeiro: Zahar, 2001.

_____. **Confiança e medo na cidade.** Tradução de Dentzien, P. Rio de Janeiro: Zahar, 2001.

BECK, U. **A sociedade de risco:** rumo a uma outra modernidade**.** Tradução de Nascimento, S. São Paulo: Ed. 34, 2010.

BENTHAM, J.; MILLER, A. PERROT, M. **O panóptico.** Organização de Tomaz Tadeu; traduções de Guacira Lopes Louro, M. D. Magno, Tomaz Tadeu. Belo Horizonte: Autêntica Editora, 2008.

BOGARD, W. **The simulation of surveillance:** hypercontrol in telematic societies. Cambridge: Cambridge University Press, 1996.

BRASIL. Projeto de Lei N. 5.276, de 2016 (do Congresso Nacional). Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. **Diário do Congresso Nacional**, Brasília, 13 maio 2016.

_____. Projeto de Lei N. 4.060, de 2012 (do Congresso Nacional). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. **Diário do Congresso Nacional**, Brasília, 13 de Junho de 2012.

BRUNO, F.; NASCIMENTO, L.; FIRMINO, R.; KANASHIRO, M.; EVANGELISTA, R. **Rastros humanos en internet:** privacidad y seguimiento online en sitios web populares del Brasil. Novática, Madrid, n. 217, p. 27-33, 2012.

CARAGLIU, A; BO, C; NIJKAMP, P. **Smart cities in Europe.** *In:* Central European Conference in Regional Science – CERS, 3., 2009, Slovak Republic.

CASTEL, R. **A insegurança social:** o que é ser protegido? Tradução de Orth, L. M. E. Petrópolis: Vozes, 2005.

CASTELLS, M. **A sociedade em rede** (A era da informação: economia, sociedade e cultura : v. 1). São Paulo: Paz e Terra, 1999.

CLARKE, R. **Information technology and dataveillance.** Disponível em: http://www.rogerclarke.com/DV/CACM88.html. Acessado em 15/03/2016.

CRISP; DATAFOLHA. **Pesquisa Nacional de Vitimização.** Disponível em: http://www.crisp.ufmg.br/wp-content/uploads/2013/10/Sumario_SENASP_final.pdf. Acessado em: 28/04/2016.

CUFF, D. **Immanent domain:** pervasive computing and the public realm. Disponível em <http://www.eesc.usp.br/nomads/tics_arq_urb/ImmanentDomain.pdf>. Acessado em 17/04/2016.

CUNHA VAZ, T. **A construção sociotécnica da cidade informacional:** o caso do Instituto Curitiba de Informática. 2015. Dissertação (Mestrado em Gestão Urbana) - Programa de Pós-graduação em Gestão Urbana, Pontifícia Universidade Católica do Paraná, Curitiba, 2015.

DEBORD, G. **A sociedade do espetáculo.** Tradução de Santos Abreu, E. Rio de Janeiro: Contraponto, 1997.

DELEUZE, G. **Conversações (1972-1990).** Tradução de Pal Pelbart, P. São Paulo: Editora, 34, 2013.

DELEUZE, G.; GUATTARI, F. **Mil platôs:** capitalismo e esquizofrenia, vol. 1.São Paulo: Ed. 34, 1995.

DIAS, T**. Por que programas de nota fiscal podem violar sua privacidade**. Nexo Jornal, 2017. Disponível em: https://www.nexojornal.com.br/expresso/2017/01/09/ Por-que-programas-de-nota-fiscal-podem-violar-sua-privacidade. Acessado em: 25/07/2017.

DINIZ, E. H.; BARBOSA, A. F.; JUNQUEIRA, A. R. B,; PRADO, O. **O governo eletrônico no Brasil:** perspectiva histórica a partir de um modelo estruturado de análise. Rev. Adm. Pública, v.43, n.1, p. 23-48, 2009.

DUARTE, F.; FIRMINO, R. **Cidade infiltrada, espaço ampliado:** as tecnologias de informação e comunicação e as representações das espacialidades contemporâneas.

2008. Disponível em <www.vitruvius.com.br/revistas/read/ arquitextos/ 08.096/3408>. Acesso em 18/04/2016.

EVANGELISTA, R; VIEIRA, M. **A máquina de exploração mercantil da privacidade e suas conexões sociais**. III Simpósio Internacional da LAVITS. Vigilância, Tecnopolíticas, Territórios, Vol. 1, pp.524-533, Rio de Janeiro, 2015.

FIRMINO, R. **Cidade ampliada:** desenvolvimento urbano e tecnologias da informação e comunicação. São Paulo: Hedra, 2011.

_____. **Cidade conectada, movimentos controlados:** tecnologia, espaço e megaeventos. Ciência e Cultura, v. 64, p. 4-5, 2012.

FIRMINO, R.; FREY, K. **A cidade e a construção sociopolítica do planejamento urbano-tecnológico.** Santiago: Eure, v. 40, n. 119, p. 99-118, 2014.

FIRMINO, R.; KANASHIRO, M.; BRUNO, F.; EVANGELISTA, R.; NASCIMENTO, L. **Fear, security, and the spread of CCTV in brazilian cities:** legislation, debate, and the market. Journal of Urban Technology, v. 20, p. 65-84, 2013.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Públlica 2015.** 2015. Disponível em: http://www.forumseguranca.org.br/ storage/download//anuario_2015.retificado_.pdf. Acessado em: 28/04/2016.

FOUCAULT, M. **Vigiar e punir**: o nascimento da prisão. Tradução de Ramalhete, R. Rio de Janeiro: Editora Vozes, 2013.

_____. **Microfísica do poder.** Organização e tradução de Machado, R. Rio de Janeiro: Edições Graal, 1984.

FREY, K. **Gobernanza electrónica urbana y inclusión digital: experiências en ciudades europeas y brasileñas**. Nueva Sociedad, v. 196, p. 109-124, 2005.

GANDY, O. H. **The panoptic sort:** a political economy of personal information. Boulder: Westview Press, 1993.

_____. Quixotics unite! Engaging the pragmatists on rational discrimination. *In:* LYON, D. **Theorizing surveillance:** the panopticon and beyond. Cullompton: Willam Publishing, 2006.

GIBSON, W. **Neuromancer.** São Paulo: Aleph, 2008.

GIDDENS, A. **As consequências da modernidade.** Tradução de Filker, R. São Paulo: Editora Unesp, 1991.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Editora Atlas, 2002.

GRAHAM, S. Excavating the material geographies of cybercities. *In:* GRAHAM, S. **The cybercities reader**. Londres: Routledge, 2004.

GRAHAM, S.; MARVIN, S. **Splintering urbanism:** network infrastructures, tecnological mobilities and the urban condition. Londres: Routledge, 2001.

GRAHAM, S; WOOD, D. **Digitizing surveillance:** categorization, space, inequality. Critical Social Policy, v.23, n. 2, p. 227-248, 2003.

GREAT BRITAIN. **Data Protection Act**. London. The Stationery Office, 1998. Disponível em: http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf. Acessado em: 20/10/2016.

HAGGERTY, K. ERICSON, R. **Policing the risk society.** Toronto: University of Toronto Press, 1997.

_____. **The surveillant assemblage.** British Journal of Sociology, v. 51, n.4, p. 605-622, 2000.

HARDT, M; NEGRI, A. **Empire.** Cambridge: Harvard University Press, 2000.

HARRIS, N. **The use of surveillance technologies in planning enforcement**. Routledge: Planning Practice & Research, v. 30, n. 5,p. 528-547, 2015.

HOUSE OF LORDS. **Surveillance:** citizens and the State. 2nd Repor of session 2008-9. HL Paper 18-I, Londres, vol. 1, p. 2009.

INFORMATION COMMISSIONER'S OFFICE. **The Guide to Data Protection**. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-9.pdf. Acessado em: 09/07/2017.

KANASHIRO, M. **Surveillance cameras in Brazil:** exclusion, mobility regulation, and the new meanings of security. Surveillace & Society, Ontario, v.5, n.3, p. 270-289, 2008.

KITCHIN, R. **The real-time city? Big data and smart urbanism.** GeoJournal, v. 79, n. 1, p. 1-14, 2014.

KITCHIN,R; LAURIAULT, T. P.; MCARDLE, G. **Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards**. Regional Studies, Regional Science, Maynooth, v. 2, n. 1, p. 6-28, 2015.

KAYYALI, D. **Cidades inteligentes:** conectadas para a injustiça. Disponível em: https://antivigilancia.org/pt/2016/03/cidades-inteligentes-conectadas-para-a-injustica/. Acessado em 24/05/2016.

LATOUR, B. **Jamais fomos modernos: ensaio de antropologia simétrica.** Tradução de Costa, C. I. São Paulo: Ed. 34, 2009.

LÉVY, P. **As tecnologias da inteligência.** Tradução de Costa, C. I. Rio de Janeiro: Ed. 34, 1993.

LIMA, J. **O que está em jogo na expansão do wi-fi público em São Paulo**. Nexo Jornal, 2014. Disponível em: https://www.nexojornal.com.br/expresso/2017/07/19/O-que-est%C3%A1-em-jogo-na-expans%C3%A3o-do-wi-fi-p%C3%BAblico-em-S%C3%A3o-Paulo. Acessado em 25/03/2017.

LUKE, T. The co-existence of cyborgs, humachines and enviroments in posmodernity: getting over the end of nature. *In:* GRAHAM, S. **The cybercities reader**. Londres: Routledge, 2004.

LYON, D. **Surveillance after Snowden**. Cambridge: John Wiley & Sons Inc., 2015. [E-BOOK]

_____. **The electronic eye:** the rise of surveillance society. Cambridge: Polity Press, 2013. [E-BOOK]

_____. 11 de setembro, sinóptico e escopofilia: observando e sendo observado. *In:* BRUNO, F.; KANASHIRO, M.; FIRMINO, R. **Vigilância e visibilidade:** espaço, tecnologia e identificação. Porto Alegre: Sulina, 2010.

_____. Surveillance, power and everyday life. *In:* MANSEL, R. **The Oxford hand2009book of information and communication technolgies.** Oxford: Oxford University Press, 2009a.

_____. **Identifying Citizens**. Cambridge: Polity Press, 2009b.

_____. **Theorizing surveillance:** the panopticon and beyond. Cullompton: Willam Publishing, 2006.

_____. Surveillance technology and surveillance society. *In:* MISA, T.J.; PHILIP, B.; FEENBERG, A. **Modernity and technology.** Cambridge: MIT Press, 2003.

_____. **Everyday surveillance:** personal data and social classification. Information, Communication & Society, v.5, n.2, p. 242-257, 2002.

LOS, M. Looking into the future: surveillance, globalization and the totalitarian potential. *In:* LYON, D. **Theorizing surveillance:** the panopticon and beyond. Cullompton: Willam Publishing, 2006.

MADON, S. Bangalore: internal disparities of a city caught in the information age. *In:* GRAHAM, S. **The cybercities reader**. Londres: Routledge, 2004.

MARX, G.T. **Ethics for the new surveillance.** Information Society, jul-ago, vol 14, Issue 3, p: 171- 186, 1998.

_____. **What´s new about the "new surveillance"?** Classifying for change and continuity. Surveillance & Society, Ontario, v. 1, n. 1, p. 9-29, 2002.

_____.An Ethics for the New (and Old) Surveillance. *In*: FLAMMINI, F; SETOLA, R; FRANCESCHETTI, G. Effective Surveillance for Homeland Security: Balancing Technology and Social Issues. Boca Raton: CRC Press, 2013.

MATHIESEN, T. **The viewer society:** Michel Foucault's "Panopticon" revisited. Theoretical Criminology: an international journal, Londres. v. 1, n.2. p. 215-232, 1997.

MATZNER, T. **Beyond data as representation**: The performativity of Big Data in surveillance. Surveillance and Society, v. 14, n. 2, p. 197-210, 2016.

MCLUHAN, M. **Os meios de comunicação como extensões do homem.** Tradução de Pignatari, D. São Paulo: Ed. Cultrix, 2007.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. **Guia Referencial para medição de Desempenho e Manual para construção de indicadores.** Brasília: MPOG, 2009.

MITCHELL, W. J. **City of bits:** space, place and the infobahn. Cambridge: MIT Press, 1996.

_____. **E-topia:** a vida urbana, mas não como a conhecemos. São Paulo: Editora Senac São Paulo, 2002.

_____. **Me++:** the cyborg self and the networked city. Cambridge: MIT Press, 2004.

MONTAGNER, C. **Investimentos públicos, dados privatizados.** Lavits, 2017. Disponível em: http://lavits.org/investimentos-publicos-dados-privatizados/?lang=pt. Acessado em: 01/08/2017.

MOSANNENZADEH, F; VETTORATO, D. **Defining Smart City: A Conceptual Framework Based On Keyword Analysis.** Naples: TeMa, Special Issue, p. 683-694, 2014.

MURAKAMI WOOD, D. (ed), **A report on the surveillance society.** Disponível em: https://ico.org.uk/media/about-the-ico/documents/1042390/surveillanc e-society-full-report-2006.pdf. Acessado em 17/03/2016.

OGURA, T. Electronic government and surveillance-oriented society. *In:* LYON, D. **Theorizing surveillance:** the panopticon and beyond. Cullompton: Willam Publishing, 2006.

OHM, P. **Sensitive Information**. Southern California Law Review, v. 88, n. 5, p. 1133-1196, 2015.

ORWELL, G. **1984.** Tradução de Hubner, A. São Paulo: Companhia das Letras, 2009.

PEÑA, P; VELASCO, P. **Santiago, Smart City:** em defesa das cidades estúpidas. Disponível em: https://antivigilancia.org/pt/2016/03/santiago-smart-city-em-defesa-das-cidades-estupidas/. Acessado em 24/05/2016.

RENNÓ, R. **Smart cities como estratégia discursiva:** o caso brasileiro. Disponível em: https://antivigilancia.org/pt/2016/03/smart-cities-como-estrategia-discursiva-o-caso-brasileiro/. Acessado em 18/05/2016.

SANTOS, M. **Técnica, espaço, tempo:** globalização e meio técnico-científico-informacional. São Paulo: Editora da Universidade de São Paulo, 2013.

SASSEN, S. **The global city:** New York, London, Tokyo. Princeton: Princeton University Press, 2001.

_____. Agglomeration in the digital era? *In:* GRAHAM, S. **The cybercities reader**. Londres: Routledge, 2004.

SIMON, B. **The return of panopticism:** Supervision, Subjection and the New Surveillance. Surveillace & Society, Ontario, v.3, n.1, p. 1-20, 2005.

STEEL, E.; LOCKE, C.; CADMAN, E.; FREESE, B. **How much is your personal data worth?**. The Financial Times, 2013. Disponível em: http://ig.ft.com/how-much-is-your-personal-data-worth/. Acessado em: 11/05/2016.

TOWNSEND, A. Learning from September 11th: ICT infrastructure collapses in a "global cibercity". *In:* GRAHAM, S. **The cybercities reader**. Londres: Routledge, 2004.

ULTRAMARI, C. **Significados do urbanismo.** Pós, São Paulo, v.16, n. 25, p. 166-184, 2009.

VIRILIO, P. **O espaço crítico.** Tradução de Pires, P. R. Rio de Janeiro: Ed. 34, 1993.

_____. **Administration of fear.** Tradução de Hodges, A. London: Semiotext(e), 2012.

WEISS, M; BERNARDES, R; CONSONI, F. **Cidades inteligentes como nova prática para o gerenciamento dos serviços e infraestruturas urbanos: a experiência da cidade de Porto Alegre.** Urbe, v. 7, n. 3, p. 310-324, 2015.

ANEXO I

Tabelas de bases de dados com informações relacionadas à pessoas

Sistema: ATIVUS - Acompanhamento de atividades físicas

Secretaria: Esporte Lazer e Juventude - SMELJ

Tabela	Colunas	Descrição dos campos
ALUNO *Tabela que armazena os dados dos alunos*	ALU_QTDPESSOA	Quantidade de pessoas que moram na residência
	ALU_ATIVIDADE	Atividade do aluno
	ALU_FUMA	Indica se o aluno fuma
	ALU_BEBE	Indica se o aluno bebe
	ALU_DTACADASTRO	Data de cadastro do aluno
	ING_IDF	Identifica o ingresso
	SOB_IDF	Identifica a sobrevivência
	AME_IDF	Identifica a assistência médica
	REN_IDF	Identifica a renda
	ESC_IDF	Identifica a escolaridade
	PES_IDF	Identifica a pessoa
	NAT_IDF	Identifica a naturalidade
	PRO_IDF	Identifica a profissão
	ALU_PAI	Nome do pai do aluno
	ALU_MAE	Nome da mãe do aluno
	ALU_NIS	Número de identificação social do aluno
	ESCO_IDF	Identifica a escola
PESSOA *Tabela que armazena os dados às pessoas*	PES_IDF	Chave primária da tabela
	SIC_IDF	SIC da pessoa
	PES_NOME	Nome da pessoa
	PES_NASC	Data de nascimento da pessoa
	PES_CIVIL	Estado civil da pessoa
	PES_CPF	CPF da pessoa
	PES_RG	RG da pessoa
	PES_SEXO	Sexo da pessoa
	PES_FONE	Telefone da pessoa
	END_IDF	Identifica o endereço
	PES_EMAIL	E-mail da pessoa
	PES_FONE_PRINCIPAL	Telefone principal da pessoa
	PES_FONE_ALTERNATIVO	Telefone alternativo da pessoa
	PES_CONTAT_PRINCIPAL	Nome do contato principal
	PES_CONTAT_ALTERNATIVO	Nome do contato alternativo
	PES_DEFICIENCIA	Tipo de deficiência que a pessoa pode possuir
	PES_MATRICULA	Matrícula da pessoa

Sistema: COC.Net - Coordenadoria de Obras Secretaria: Trânsito - SETRAN		
Tabela	**Colunas**	**Descrição dos campos**
USUARIO_EXTERNO *Armazena os dados dos usuários que podem acessar o módulo web do sistema*	UEX_CODIGO	Chave primária da tabela
	EMP_CODIGO	Vínculo empresa e login de usuários externos
	UEX_LOGIN	Login utilizado para acesso via aplicação web
	UEX_SENHA	Senha utilizada para acesso via aplicação web
	UEX_NOME	Nome do usuário externo
	UEX_EMAIL	Email do usuário externo
	UEX_TELEFONE	Número do telefone do usuário externo
	UEX_CELULAR	Número do celular do usuário externo
	UEX_STATUS	Indica se o usuário externo esta ativo ou não na aplicação web
	UEX_DATA_ATUALIZACAO	Data em ocorreu a última atualização do cadastro

Sistema: NCPA - Cadastro de Pessoas Atendidas		
Fundação de Ação Social - FAS		
Tabela	**Colunas**	**Descrição dos campos**
PESSOA_ATENDIDA	CNT_COD	Identifica a condição de trabalho
	PCA_NOME	Nome da pessoa
	PCA_DTNASCIMENTO	Data de nascimento
	PCA_TIPODTNASCIMENTO	Data de nascimento (Informada ou Comprovada)
	PCA_SEXO	Sexo
Tabela que armazena os dados das pessoas atendidas	CID_NATURALIDADE	Código da cidade de naturalidade
	PCA_FOTO	Nome do arquivo de foto da pessoa
	ECI_COD	Identifica o estado civil
	CID_PROCEDENCIA	Código da cidade de procedência
	PCA_DATACHEGADA	Data de chegada da pessoa
	PCA_ACOMPFAMILIA	Acompanhada de um familiar no momento do cadastro
	PCA_POSSUIVINCFAM	Indica se a pessoa possui vínculo com a família
	PCA_TEMPOPERDAVINC	Quanto tempo foi perdido o vínculo com a família
	PCA_UNIDTMPPERDAVINC	Unidade de tempo da perda do vínculo
	PCA_DESEJOTRATARDEPEND	Indica se a pessoa deseja tratar dependência
	PRF_PROFISSAO	Identifica uma profissão
	PRF_OCUPACAO	Identifica uma ocupação
	PCA_DATACONDTRAB	Data da condição de trabalho
	PCA_TEMPORUA	Indica o tempo que a pessoa mora na rua
	PCA_UNIDTMPRUA	Unidade de tempo de moradia na rua
	CDP_COD	Identifica uma cor de pele
	CDC_COD	Identifica uma cor de cabelo
	TPCAB_COD	Identifica um tipo de cabelo
	CDO_COD	Identifica a cor dos olhos
	PCA_TRACOS	Traços marcantes da pessoa
	USU_COD	Identifica o usuário que cadastrou a pessoa atendida
	PCA_DATA_CADASTRO	Data de cadastro da pessoa atendida
	PCA_RENDAINDIVIDUAL	Valor da renda individual da pessoa atendida
	PCA_RENDA_FAMILIAR	Valor da renda familiar da pessoa atendida
	PCA_LOG	
	REG_COD	Identifica a regional
	PCA_ALTURA	Altura da pessoa atendida
	PCA_PESO	Peso da pessoa atendida
	ID	Coluna não utilizada
	CD_NACIONALIDADE	Código da cidade de nacionalidade
	PCA_PROVFINANC	Indica se a pessoa atendida sustenta a família
	PCA_DT_ATUALIZA	Data de atualização dos dados
	USU_ATUALIZA	Identifica o usuário que atualizou os dados
	PES_COD	Coluna não utilizada
	PCA_NMEMAE	Nome da mãe
	PCA_NMEPAI	Nome do pai

PES_NUM_SIC	Número do SIC
PCA_FLAGRUA	Indica se a pessoa atendida é moradora de rua
PCA_ANOCONCLUSAOESC	Ano de conclusão
FAM_INT_CODDOM	Identifica um domicílio
ESC_COD	Identifica a escolaridade
PCA_COD	Chave primária da tabela
NUM_CARTEIRINHA_SMAB	Número da carteirinha da SMAB
DESCRICAO_PROGRAMASOCIAL	Descrição do programa social
PROG_COD	Programa social ao qual a pessoa está associada
PCA_NOMEFONETICO3	Fonética do terceiro nome
PCA_NOMEFONETICO2	Fonética do segundo nome
PCA_EMAIL	E-mail da pessoa
GPA_CODIGO	Identifica um grau de parentesco
PCA_NOMEFONETICO1	Fonética do primeiro nome

Sistema: SIC -Identificação do Cidadão		
Secretarias: Diversos órgãos e secretarias da Prefeitura Municipal de Curitiba		
Tabela	**Colunas**	**Descrição dos campos**
PESSOA	Pes_Cod	Chave primária da tabela
	Dom_Cod	Código do domicilio
	Pes_Cod_DomicilioGF	Código do domicílio, do sistema do Governo Federal
	Pes_Num_OrdemDom	Número de ordem da pessoa no domicilio
	Pes_Nme	Nome
	Pes_Nme_Pai	Nome do pai
	Pes_Nme_Mae	Nome da mãe
Tabela que armazena os dados das pessoas.	Pes_Dta_Nascimento	Data de nascimento
	Pes_Tp_Dta_Nascimento	Data de nascimento (Informada ou Comprovada)
	Pes_Sexo	Sexo da pessoa
	Pes_Nacionalidade	Nacionalidade
	Cod_Pais	Código dos Pais, vindo do Logradouro Serviço
	Pes_Dta_ChegadaBrasil	Data de chegada ao Brasil, se brasileiro naturalizado ou estrangeiro
	Pes_Cod_IBGEMunicipio	Código do IBGE do município
	Cod_Unid_Federacao	Código da Unidade da federação
	Cod_Cidade	Código da cidade
	Est_Cod	Código do estado civil
	Pes_Num_OrdemConjuge	Número de ordem do cônjuge, dentro do domicílio
	Pes_Deficiencia	Indica se a pessoa possui deficiência
	Cor_Cod	Código da cor / raça
	Pes_Provedor_Fin	Código do provedor financeiro
	Pes_Responsavel	Indica se a pessoa é responsável pelo domicílio
	Pes_ProgramaGoverno	Participação de programa do Governo Federal
	Pes_Eml	E-mail
	Pes_Dta_Cadastro	Data de cadastro
	Pes_Dta_Atualizacao	Data da última atualização de cadastro
	Pes_CadastroGF	Indica se a pessoa tem cadastro no Governo Federal
	Pes_Num_SIC	Número do SIC
	Pes_Flg_EmissaoCartao	Indica a emissão de cartão que possua o número SIC
	Pes_Flg_PossivelDelecao	Indica possível deleção do cadastro
	Pes_Flg_Falecido	Indica se a pessoa é falecida

Sistema: E-Saúde / Hospitalar - Atendimento médico, odontológico e de outras especialidades		
Secretaria: Saúde - SMS		
Tabela	**Colunas**	**Descrição dos campos**
USUÁRIO	cdusuario	Código do usuário (chave primária)
	nmusuario	Nome do usuário
	nmmae	Nome da mãe
	nmpai	Nome do pai
	cdnacionalidade	Código da nacionalidade
	cdnatmunicipio	Código do município de naturalidade
	cddomicilio	Código do domicílio
	tpsexo	Tipo de sexo
	dtnascimento	Data de nascimento
	idsituacao	Código da situação
	cdfaixarenda	Código da faixa de renda
	cdracacor	Código da raça / cor
	cdescolaridade	Código de escolaridade
	cdestadocivil	Código do estado civil
	cdsituacaoconjugal	Código da situação conjugal (referência)
	cdocupacao	Código da profissão conforme código brasileiro de ocupação
	nmusuariofonetico	Nome fonético
	nmmaefonetico	Nome fonético da mãe
	idfrequentaescola	Se o usuário frequenta a escola
	idbolsaalimentacao	Se o usuário possui bolsa alimentação
	nrimpressoesetiquetas	Número de impressão de etiqueta de usuário
	dtcadastro	Data de cadastro
Registros das informações dos usuários	dtatualizacao	Data de atualização dos dados
	cdusuariopai	Código de usuário do pai
	cdusuariomae	Código de usuário da mãe
	cdcidobito	Código de CID do óbito
	dtobito	Data do óbito
	dscomplementoobito	Informações complementares do óbito
	nrtempoestudo	Tempo de estudo
	cdtipodocumentocad	Código do tipo de documento cadastrado
	cdmotivocadastramento	Código do motivo de cadastramento
	cdcontratocadastrador	Código do contrato que cadastrou
	nmpaifonetico	Nome fonético do pai
	dsjustifsemcbo	Descrição da justificativa do cadastro sem ocupação CBO
	cdusurespnaoident	Código do usuário responsável quando não identificado
	dscomplusunaoident	Cognome do usuário enquanto não identificado
	nrcnsmae	Número do cartão nacional de saúde da mãe
	dtunificacao	Data de unificação do cadastro
	nrdeclaracaoobito	Número da declaração de óbito
	dsjustifreativcancobito	Descrição da justificativa de reativação de cancelamento de óbito
	cdloginatividade	Código do login atividade

	nmusuariosocial	Nome social
	cdesususuario	Código do usuário no ESUS
	cdetnia	Código da etnia indígena
DOMICILIO	cddomicilio	Código do domicílio do usuário (chave primária)
	cdcontrato	Código do estabelecimento responsável pelo domicílio
	cdcontrolecep	Código do CEP
	dscomplemento	Descrição do complemento
	nrresidencia	Número da residência
	dspontoreferencia	Descrição do ponto de referência
	nrcomodos	Número de cômodos no domicílio
	idenergia	Se o domicílio possui energia elétrica
	idcadastrosiab	Se o domicílio pertence a área de abrangência atendida por equipe SIAB
Registros do domicílio dos usuários	idsituacao	Situação do domicílio (ativo ou inativo)
	dtcadastro	Data de cadastro do domicílio
	dtatualizacao	Data de atualização do domicílio
	idclassificacaoriscofamilia	Código da classificação de risco da família
	nrlatitudeutm	Número da latitude da localização geográfica
	nrlongitudeutm	Número da longitude da localização geográfica
	cdtipocomplemento	Código do tipo de complemento do domicílio
	cdsetorcensitario	Código do setor censitário do domicílio
	cdendereco	Código do endereço do domicílio
	cdquadra	Código da quadra do domicílio
	cdmicroarea	Código da micro área do domicílio
	cdesusdomicilio	Código do domicílio no cadastro ESUS

Sistema: GTM - Gestão Tributária Municipal		
Secretarias: Diversos órgãos e secretarias da Prefeitura Municipal de Curitiba		
Tabela	**Colunas**	**Descrição dos campos**
GTMPESPessoa *Qualquer pessoa física ou jurídica. Pode ser um munícipe, caso tenha sido proprietário de imóvel no Município, ou um interessado, no caso de necessitar de informações sobre imóveis.*	Cod_Pessoa	Identifica uma pessoa no cadastro de pessoas
	Nme_Pessoa	Nome do Munícipe
	Dta_Cadastro_Pessoa	Data do cadastro da pessoa no sistema
	Flg_Ind_Pessoa_Fora	Indica que a pessoa não é de Curitiba
	Ind_Interessado_Municipe	
	Ind_Origem_Migracao_Pessoa	Origem da migração dos dados do mainframe
	Ind_Tipo_Pessoa	
	Cod_Pessoa_Grupo3_MF	Código existente no mainframe, para pessoas eventuais do grupo 3
	Dta_Ultima_Atualizacao	Data da última atualização
	Dta_Atualizacao_Geral_Cadastro	Data da atualização geral do cadastro
	Flg_Ativo	
	Cod_Pessoa_Oficial	Referência ao registro oficial da pessoa, em casos de duplicidade de documento
GTMSOCSociedade *Identifica os sócios ou proprietário de uma empresa*	Cod_Pessoa_Juridica	Identifica uma pessoa no cadastro de pessoas
	Cod_Socio	Identifica uma pessoa no cadastro de pessoas
	Flg_Ind_Socio_Responsavel	
	Ind_Nivel_Socio	Indica o nível de instrução do sócio
	Ind_Socio_Conj	
	Cod_Qualificacao_Pessoas	Indica a qualificação
	Cod_Pessoa_Empresa	

Sistema: GTM / Cadastro de Comércio Ambulante		
Secretarias: Diversos órgãos e secretarias da Prefeitura Municipal de Curitiba		
Tabela	**Colunas**	**Descrição dos campos**
GTMAMBAmbulante *Tabela com vínculo ao cadastro de pessoas, especializando-o para manter informações específicas do comércio ambulante com atividade no município*	Cod_Ambulante	Identifica o código do ambulante
	Cod_Pessoa	Identifica o código da pessoa
	Cod_End_Generico	Endereço
	Cod_Desc_Motivo_Canc_CCA	Descrição do motivo do cancelamento CCA
	Cod_Protocolo	Código do protocolo
	Ano_Protocolo	Ano do protocolo
	Cod_Docto_Protocolo	Código do documento do protocolo
	Dta_Cancelamento	Data do cancelamento
	Num_Carteira_Motorista	Número da carteira de motorista
	Num_Carteira_Profissional	Número da carteira profissional
	Num_Titulo_Eleitor	Número título de eleitor
	Ind_Estado_Civil	Estado civil
	Nme_Conjuge	Nome do conjugue
	Fot_Ambulante	Foto do ambulante
	Des_Profissao_Conjuge	Profissão do conjugue
	Num_Telefone	Número do telefone
	Qtd_Anos_Residencia	Anos de residência
	Qtd_Anos_Atividade	Anos de atividade
	Ind_Condicoes_Moradia	Condições de moradia
	Ind_Deficiente_Fisico	Caso possui alguma deficiência
	Des_Deficiencia	Descrição da deficiência
	Num_Filhos_Menores	Quantidade de filhos menores
	Num_Filhos_Escola	Quantidade de filhos na escola
	Dta_Cadastramento	Data do cadastramento
	Vlr_Peso_Total	
	Cod_Usuario	Código do usuário
	Flg_Proibido_Preposto	
	Des_Motivo_Proib_Preposto	
	Txt_Observacao_Cracha	
	Txt_Observacao_Geral	
	Ind_Sit_Ambulante	

Sistema: GTM / Localizador de Lotes - Informações de imóveis da cidade		
Secretarias: Diversos órgãos e secretarias da Prefeitura Municipal de Curitiba		
Tabela	**Colunas**	**Descrição dos campos**
GTMLOTLote *Qualquer imóvel, que contenha ou não edificação, de propriedade de pessoa física ou jurídica, de direito público ou privado, sujeito à tributação pelo Município*	Cod_Lote	Identifica os lotes gerados a partir da implantação do sistema
	Num_Lote_Inscr_Imob	Metragem do Lote na Inscrição Imobiliária
	Ind_Compl_Inscr_Imob	Complemento da Inscrição Imobiliária
	Nme_Registro_Imoveis	Identifica uma planta não aprovada, no registro de imóveis
	Ind_Mot_Canc_Padrao	Origem do cancelamento do lote
	Ano_Lanc_Terreno	Ano de Lançamento do Terreno
	Ano_Exercicio_Lote	Ano em que o IPTU será tributado para o Lote
	Des_Especie_Lote	Classificação do lote quanto à espécie
	Sta_Sit_Lote	Quando o lote estiver em um processo de unificação, subdivisão ou cadastramento
	Mtr_Area_Terreno	Área total do lote, sem parcelamentos
	Mtr_Distancia_Lote_Esquina	Distância em metros do lote até a esquina mais próxima
	Ind_Primeiro_Lancamento_Lote	Lotes que não possuem uma inscrição imobiliária de origem
	Flg_Lote_Doado	Indicativo de Lote Doado para a Prefeitura
	Flg_Unidade_Preservacao	Identifica se o lote é uma unidade de interesse de preservação
	Flg_Ating_Bosque	Informado se o lote é atingido por bosque ou áreas verdes
	Flg_Atualizacao_Cadastral	Identificado os lotes que sofrerão alterações
	Mtr_Cone_Aeronautica	Altura máxima permitida para o lote em relação ao nível do mar
	Mtr_Referencia_Nivel_Lote	Posição do lote (altura), expressa em metros em relação ao nível do mar
	Num_CEP_Especial	CEP Especial
	Dta_Cadastramento_Lote	Data (dia/mês/ano) em que o lote foi incluído no cadastro
	Dta_Ultima_Alteracao_Lote	Data (dia/mês/ano) da mais recente alteração em quaisquer dados do lote
	Dta_Cancelamento_Lote	Data em que o lote foi cancelado
	Dta_Recadastramento	Data em que foram atualizados os dados cadastrais através de um programa de recadastramento
	Num_Indicacao_Fiscal	Número da indicação fiscal do lote
	Obs_Lote	Observações sobre o Lote
	Cod_Logradouro_Esq_Proxima	Código do Logradouro da esquina mais próxima
	Cod_Bairro	Código do Bairro
	Cod_Quadra	Código da Quadra da Inscrição Imobiliária
	Cod_Micro_Bairro	Código do micro-bairro
	Cod_Caracteristica	Característica do Lote
	Cod_Regional	Código identificador da regional a qual o lote está vinculado
	Cod_Mot_Canc_Lote_Sublote	Motivo de cancelamento de lote ou sub-lote

	Cod_Posicao_Lote_Quadra		
	Cod_Versao		
	Des_Inf_adic_Certidao_End		
GTMSUBSublote *Convenção ou codificação adotada para identificar parcelas do lote e/ou construções edificadas sobre o mesmo*	Cod_Lote		Código do lote
	Cod_Sublote		Código do sub-lote
	Ano_Exercicio_Sublote		Este campo indica o Ano em que o IPTU será tributado
	Tip_Natureza_Sublote		Identifica a Natureza do sub-lote
	Des_Reg_Imoveis		Informações sobre o Registro de Imóveis feito em cartório
	Tip_Patrimonio		Identifica se o imóvel é de patrimônio particular ou público
	Tip_Imposto_Sublote		Indica o tipo de incidência de impostos no sub-lote
	Tip_Taxa_Sublote		Indica o tipo de incidência de taxas no sublote
	Ind_Utilizacao_Sublote		Finalidade em que o sub-lote está sendo utilizado (Residencial, Comercial ou Misto)
	Ind_Cohab		Identifica se o imóvel pertence a COHAB
	Ind_Lote_Foreiro		Informa a situação atual do sublote com relação ao foro
	Ind_Abrangencia		
	Txa_Coef_Propor		Coeficiente de Proporcionalidade
	Dta_Cadastramento_Sublote		Armazena a data (dia/mês/ano) em que o sublote foi cadastrado no sistema
	Dta_Ultima_Alteracao_Sublote		Data (dia/mês/ano) em que o sublote sofreu alteração em quaisquer dos seus dados
	Dta_Canc_Sublote		Data de Cancelamento do sub-lote
	Cod_Mot_Canc_Lote_Sublote		Código sequencial que identifica um motivo de cancelamento de lote ou sub-lote
	Cod_Lote_Condominio		Este campo irá identificar os lotes gerados a partir da implantação do sistema
	Num_Bloc_Condominio		Número de Blocos do Condomínio
	Cod_Versao		
	Mtr_Area_Total_Sublote		
	Mtr_Area_Privat_Sublote		
	Obs_Sublote		Observações pertinentes ao sub-lote
	Mtr_Area_Territ_Privat_Sublote		Área territorial privativa do sub-lote para condomínios horizontais.
GTMLOGLogradouro *Via pública destinada ao trânsito em geral (ruas, avenidas, praças, alamedas, largos, rios etc.)*	Cod_Logradouro		Código sequencial do Logradouro, que será implementado via sistema
	Cod_Tip_Logradouro		Tipo do Logradouro
	Cod_Sit_Logradouro		Descrição da situação do logradouro
	Cod_Posicao_Logradouro		Indica a existência de um único registro de posição do lote
	Cod_Mot_Canc_Diretriz_Projeto		
	Cod_Logradouro_Inicio		Logradouro onde inicia determinado logradouro que esta sendo trabalhado
	Cod_Logradouro_Fim		Logradouro onde termina determinado logradouro que esta sendo trabalhado
	Cod_Identificacao_Logradouro		Código de Identificação do Logradouro

Nme_Logradouro	Nome do Logradouro
Mtr_Extensao_Logradouro	Extensão em m2 que o logradouro possui
Tip_Origem_Criacao_Logradouro	Relacionamento com o atributo que denominou o logradouro
Num_Origem_Criacao_Logradouro	Número Origem Criação Logradouro
Dta_Criacao_Logradouro	Data em que foi criado o logradouro
Dta_Denom_Logradouro	Data em que foi denominado o logradouro
Tip_Origem_Denom_Logradouro	Relacionamento com o atributo que denominou o logradouro
Num_Denom_Logradouro	Número Denominação Logradouro
Ano_Docto_Aprov_Denom_Logradou	Ano em que foi aprovado o documento de aprovação da denominação de um logradouro
Dta_Canc_Logradouro	Data em que o logradouro foi cancelado
Dta_Ultima_Alteracao	
Ind_Let_Com_Logradouro	A Letra Complemento serve para indicar que duas ou mais ruas estão próximas
Nme_Popular_Logradouro	Pseudônimo atribuído à rua
Ano_Docto_Criacao_Logradouro	Ano de Origem do Logradouro
Des_Historico_Cultural	Contém o histórico da origem do nome do logradouro e outras informações importantes
Nme_Logradouro_Planta	Nome pelo qual o logradouro aparece na planta de loteamento
Ano_Docto_Alter_Logradouro	Ano Documento Alteração Logradouro
Num_Docto_Alter_Logradouro	Número do documento que oficializou a alteração do logradouro
Tip_Docto_Alter_Logradouro	Tipo do documento que oficializou uma alteração nos dados do logradouro
Des_Historico_Origem_Rua	
Cod_Ocupacao	

Sistema: 156 - Atendimento ao Cidadão		
Secretarias: Todos os órgãos e secretarias da Prefeitura Municipal de Curitiba		
Tabela	**Colunas**	**Descrição dos campos**
Central 156 – Solicitação de Serviços *Formulário onde são inseridas as informações necessárias para o envio de solicitações de serviço e informações aos órgãos da administração municipal.*	**Cadastrador**	Nome do usuário que cadastrará o protocolo
	Protocolo	Numérico, seguindo uma ordem crescente
	Origem	Sigla do órgão ao qual o cadastrador pertence
	Data de Criação	Data e hora do registro do protocolo
	Tipo	Tipo de registro que será realizado
	Dados do Solicitante	Caso solicitante seja Pessoa Física
	Nome do Solicitante	Nome completo do solicitante
	Tipo de Solicitante	Tipo de solicitante
	Sexo	Gênero Masculino ou feminino
	Nome da Mãe	Nome da mãe do solicitante
	Aspecto Emocional	Utilizar quando constatado que o cidadão está alterado
	Telefone	Número de telefone para contato com o cidadão
	CPF	Número do CPF do cidadão
	Data de Nascimento	Data de nascimento do cidadão
	E-mail	Se o meio de resposta selecionado for e-mail
	Número do RG	Documento do cidadão
	Órgão Emissor	Órgão emissor do Documento RG
	Data	Data de emissão do Documento RG
	Unidade Federativa	UF do Documento RG
	Unidade Federativa (UF) e Localidade	Estado e a cidade do solicitante
	Logradouro	Logradouro do solicitante
	Número	Número de endereço do solicitante
	Complemento	Complemento de endereço do solicitante
	CEP	Número de CEP de endereço do solicitante
	Pessoa Jurídica	Caso solicitante seja Pessoa Jurídica
	Razão Social	Razão social da empresa
	Ramo de Atividade	Segmento que a empresa atende
	Nome Fantasia	Nome comercial da empresa, caso possua
	Website	Site da empresa
	CNPJ	Número completo do CNPJ da empresa
	Inscrição Estadual	Inscrição estadual da empresa, caso possua
	Contato	Nome de contato na empresa
	Telefone	Telefone para contato
	Setor	Setor em que o contato trabalha
	E-mail	E-mail do contato
	Endereço	Endereço da empresa
	Número	Número de endereço da empresa
	Complemento	Complemento de endereço da empresa
	CEP	Número de CEP de endereço da empresa

Dados do Assunto	Descrição; Assunto; Subdivisão; Texto Explicativo; Manter Sigilo (opcional)
Endereço do Assunto	Local do Assunto é Igual ao Endereço do Solicitante
Meio de Resposta	Meio de resposta que o cidadão será informado
Tipo de Documento Externo	Utilizado pelos órgãos externos para identificar o tipo de protocolo que está sendo criado
Número do Documento Externo	Utilizado pelos órgãos externos para inserir o número do documento que foi registrado
Observações	Acrescentar informações adicionais ao pedido do cidadão
Dados Importantes	São dados que os órgãos consideram importantes para atender o protocolo
Enviar ao Responsável	Enviar o protocolo ao órgão responsável

Sistema: GED - Gestão Educacional Secretaria: Educação - SME		
Tabela	**Colunas**	**Descrição dos campos**
TB0137PESSOA *Tabela que contém os dados de pessoas*	TB0137_COD_PESSOA	Código que identifica unicamente uma pessoa física
	TB0137_NOME_PESSOA	Nome da Pessoa Física
	TB0137_IND_SEXO	Sexo Feminino ou Masculino
	TB0137_IND_RACA	Indica a raça da pessoa
	TB0137_IND_NACIONALIDADE	Indica se a pessoa tem a naturalidade brasileira
	TB0092_COD_FUNCAO	Código sequencial para o cadastro das funções
	TB0137_DATA_NASCIMENTO	Data de nascimento da pessoa
	TB0137_IND_ESTADO_CIVIL	Estado Civil da pessoa
	TB0137_NOME_PESSOA_REDUZIDO	Nome reduzido da pessoa.
	TB0137_IND_GRAU_ESCOLARIDADE	Grau de escolaridade da pessoa
	TB0137_QTDE_FILHOS	Quantidade de filhos da pessoa
	TB0137_COD_UF_NASC	Código da UF de nascimento da pessoa
	TB0137_COD_MUNICIPIO_NASC	Código do município de nascimento da pessoa
	TB0140_COD_PAIS	Código do país
	TB0137_DATA_ENTRADA_PAIS	Data em que a pessoa entrou no país
	TB0137_NOME_LOCALIDADE_NASC	Nome da localidade de nascimento da pessoa.
	TB0137_OPCAO_RELIGIAO	Religião da pessoa
	TB0137_VLR_RENDA_MENSAL	Valor da renda da pessoa
	TB0137_EMAIL_PESSOA	Endereço eletrônico da pessoa
	DOM_COD	Código do domicilio da pessoa
	PES_COD	Código do Sistema de Identificação do Cidadão
	TB0137_NOME_PESSOA_MODI	Nome modificado da pessoa para busca por nome similar
	TB0137_PORTARIA_NATURALIZACAO	Numero da portaria da naturalização
	TB0137_VLR_DESPESA_MORADIA	Valor da despesa com moradia que a família tem
	TB0137_VLR_AJUDA_CUSTO	Valor da ajuda de custo que a família tem
	TB0137_DUPLA_CIDADANIA	Identifica a existência de dupla cidadania
	TB0137_IND_ZONA_RESID	Indicativo da zona residência do aluno
	TB0137_TIPO_PESSOA	Tipo de pessoa
	TB0137_NOME_PESSOA_SOCIAL	Nome da pessoa social.
	TB0137_NOME_PESSOA_CENSO	Nome usado para o Censo
	TB0137_NOME_PESSOA_RESP1_CENSO	Nome RESP1 usado para o Censo
	TB0137_NOME_PESSOA_RESP2_CENSO	Nome RESP2 usado para o Censo

Sistema: Controle de Corridas		
Secretaria: Esporte, Lazer e Juventude - SMELJ		
Tabela	**Colunas**	**Descrição dos campos**
ATLETA	ATL_COD	ID Atleta
	ATL_NOME	Nome Completo
	ATL_RG	RG
	ATL_CPF	CPF
	ATL_NASC	Data de Nascimento
	ATL_SEXO	Sexo
	ATL_FONE	Telefone
	ATL_RESP	Nome Responsável pelo Atleta
	ATL_RESP_RG	RG Responsável pelo Atleta
Cadastro de Atletas	ATL_RESP_FONE	Telefone Responsável pelo Atleta
	ATL_INSC	Antigo codigo identificador
	END_COD	Código do Endereço
	ATL_INSCPENDENTE	Inscrição Pendente (Sim/ Não)
	ATL_CHIP	Chip Pendente (Sim/ Não)
	ATL_CEL	Telefone Celular
	ATL_EMAIL	Email
	EQU_COD	Código da Equipe
	ATL_IMPORTADO	Cadastro Importado (Sim/ Não)
PROVAS	PRO_COD	ID Provas
	PRO_DESC	Descrição
	PRO_DATA_REALIZACAO	Data de Realização
	PRO_RANK	Se prova tem pontuação
	PRO_OBS	Observação/ Informação sobre a Prova
	PRO_PERCURSO	Imagem do Percurso da Prova
	PRO_INSC_INICIO	Data de Início da Inscrição
	PRO_INSC_FIM	Data de Encerramento da Inscrição
	PRO_MOSTRA	Mostrar Provas (Sim/ Não)
	PRO_INSCINI_SMEL	Data de Início da Inscrição – SMELJ
	PRO_INSCFIM_SMEL	Data de Encerramento da Inscrição – SMELJ
	PRO_TIPO	Tipo de Prova (Revezamento/ Individual)
Cadastro de Provas	PRO_LIMITE	Limite de Inscrições
	CAM_COD	Código do Campeonato
	PRO_ONIBUS	Solicita confirmação de ônibus
	PRO_INT_MINIMO_PARTIC	Quantidade Mínima do Grupo
	PRO_INT_MAXIMO_PARTIC	Quantidade Máxima do Grupo
	CLA_COD	Código da Classe
	EXE_COD	Código do Exercício
	PRO_CATEGORIAWEB	Mostrar Categoria na Web (Sim/Não)
	PRO_PREINSCRICAO	Pré-Inscrição (Sim/Não)
	PRO_LIMITEEQUIPE	Limite de Equipes
	PRO_EMAIL	Email/ Boleto
	PRO_LIMITE_ATLETA_TRECHO	Limite de Trechos por Atleta