

FUNDAÇÃO GETULIO VARGAS
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

Leonardo Fonseca Netto e Lívio José Lima e Rocha

**GESTÃO DE INFORMAÇÕES DE SEGURANÇA PÚBLICA NO MUNICÍPIO:
DIAGNÓSTICO E PROPOSTAS PARA A SECRETARIA MUNICIPAL DE
SEGURANÇA URBANA DA CIDADE DE SÃO PAULO**

SÃO PAULO - SP

2019

Leonardo Fonseca Netto e Lívio José Lima e Rocha

**GESTÃO DE INFORMAÇÕES DE SEGURANÇA PÚBLICA NO MUNICÍPIO:
DIAGNÓSTICO E PROPOSTAS PARA A SECRETARIA MUNICIPAL DE
SEGURANÇA URBANA DA CIDADE DE SÃO PAULO**

Dissertação apresentada à Escola de Administração de Empresas de São Paulo, da Fundação Getúlio Vargas, como requisito para obter o título de Mestre em Gestão e Políticas Públicas. Campo do Conhecimento: Gestão e Políticas Públicas.

Orientador: Prof. Dr. Renato Sérgio de Lima.

SÃO PAULO - SP

2019

Fonseca Netto, Leonardo.

Gestão de informações de segurança pública no município: diagnóstico e propostas para a Secretaria Municipal de Segurança Urbana da cidade de São Paulo / Leonardo Fonseca Netto, Lívio José Lima e Rocha. - 2019.

137 f.

Orientador: Renato Sérgio de Lima.

Dissertação (mestrado profissional MPGPP) – Fundação Getulio Vargas, Escola de Administração de Empresas de São Paulo.

1. Segurança pública - São Paulo (SP). 2. Gerenciamento da informação. 3. Proteção de dados - Legislação. 4. Políticas públicas - São Paulo (SP). I. Rocha, Lívio José Lima e. II. Lima, Renato Sérgio de. III. Dissertação (mestrado profissional MPGPP) - Escola de Administração de Empresas de São Paulo. IV. Fundação Getulio Vargas. V. Título.

CDU 351.75(816.11)

Ficha Catalográfica elaborada por: Isabele Oliveira dos Santos Garcia CRB SP-010191/O

Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

Leonardo Fonseca Netto
Lívio José Lima e Rocha

GESTÃO DE INFORMAÇÕES DE SEGURANÇA PÚBLICA NO MUNICÍPIO:
DIAGNÓSTICO E PROPOSTAS PARA A SECRETARIA MUNICIPAL DE
SEGURANÇA URBANA DA CIDADE DE SÃO PAULO

Dissertação apresentada à Escola de Administração de Empresas de São Paulo, da Fundação Getúlio Vargas, como requisito para obter o título de Mestre em Gestão e Políticas Públicas.

Campo de Conhecimento: Gestão e Políticas Públicas

Data de Aprovação: _____

Banca Examinadora:

Sandra Helena Peticarrari
Secretaria Municipal de Segurança Urbana da
cidade de São Paulo

Prof. Dra. Carolina de Mattos Ricardo
USP – FDUSP

Prof. Dr. Clóvis Bueno de Azevedo
FGV – EAESP

Prof. Dr. Renato Sérgio de Lima
FGV - EAESP

AGRADECIMENTOS

Leonardo Fonseca Netto

‘Quero agradecer à minha família que sempre me apoiou e suportou a distância neste período de MPGPP, até durante os finais de semana, à minha Esposa Gabriela, meu Filho Lorenzo Gabriel e minha Filha Lais Guilhermina.

Aos meus pais, Sheila e Valter, que sempre estiveram comigo e me ensinaram a importância do estudo na vida de uma pessoa, só estou onde estou graças ao estudo.

Ao meu colega de Mestrado Lívio, que fizemos metade do curso juntos, sempre trabalhando como equipe.

Aos Professores do MPGPP que sempre trabalharam para compartilhar o ensinamento que é o bem mais preciso na educação, e especial do Professor Renato Sérgio de Lima pela dedicação e parceria nesta tese.

Ao Secretário Coronel José Roberto Rodrigues de Oliveira e equipe (principalmente a Sandra Helena Perticarrari) que abriram a porta da Secretaria Municipal de Segurança Pública e nos forneceram todas as informações que foram solicitadas, pensando sempre na melhora do órgão.

Lívio José Lima e Rocha

Aos meus antigos e aos meus pais, Silvino (in memoriam) e Nilce, aqueles que me incentivaram a nunca parar de adquirir conhecimento, o único bem que não pode ser tomado.

À minha esposa Margareth e ao meu filho Cairê, porque família sempre corre junto.

Ao corpo docente da EAESP-FGV, que me ensinaram a entender melhor o mundo e forneceram mais ferramentas para tentar melhorá-lo. Em especial, ao Prof. Dr. Rafael Alcadipani, que me incentivou a cursar o MPGPP, e ao Prof. Dr. Renato Sérgio de Lima, com quem aprendi a enxergar a segurança pública sem viés classista e corporativista.

Não posso deixar de agradecer ao meu sacerdócio: a Polícia Civil do Estado de São Paulo. À todas parcerias que tive, irmãos e irmãs por escolha, que sempre me ajudaram a cumprir a missão principal: voltar, com saúde, para as nossas famílias.

*“(...) a informação é uma grande arma, mais poderosa
que qualquer PT carregada (...)”*

Racionais MC's – Negro Limitado

RESUMO

Este trabalho foi elaborado para entendermos a gestão das informações de segurança pública no âmbito municipal: como são produzidas, quais critérios e outros fatores, em especial, o enquadramento no Sistema Único de Segurança Pública e a adaptação à Lei Geral de Proteção de Dados. Em pesquisa bibliográfica, não encontramos nenhum trabalho com essa abordagem. Para preencher esse espaço, escolhemos a Secretaria Municipal de Segurança Urbana da cidade de São Paulo, pela representatividade de exercer a segurança pública na cidade mais populosa do país e por ter, no seu organograma, a Guarda Civil Metropolitana, a maior guarda civil do Brasil. Uma vez escolhido o órgão público ideal, iniciamos a análise dos setores da Secretaria que cuidam, direta ou indiretamente, do fluxo de informações de segurança pública, através de entrevistas com todos escalões da burocracia, dos tomadores de decisão até a burocracia de nível de rua, bem como pesquisa de campo, observando o cotidiano profissional dos envolvidos. Com os dados coletados, buscamos as teorias aplicáveis à pesquisa e o benchmarking a ser adotado e, assim, conseguimos isolar os problemas principais e propor medidas para aperfeiçoar o uso de informações de segurança pública no órgão estudado.

Palavras-chave: segurança pública – município; segurança urbana; guarda civil; fluxo de informações de segurança pública; gestão em segurança pública; políticas públicas

ABSTRACT

This paper was designed to understand the management of public safety information at the municipal level: how it is produced, what criteria and other factors, the framework of the Unified Public Security System and the adaptation to the General Data Protection Law. In bibliographic research, we did not find any work with this approach. To fill this space, we chose the Municipal Secretariat of Urban Security of the city of São Paulo, for the representativeness of exercising public security in the most populous city in the country and for having in its organization chart the Metropolitan Civil Guard, the largest civil guard in Brazil. Once the ideal public agency has been chosen, we begin to analyse the sectors of the Secretariat that directly or indirectly handle the flow of public safety information through interviews with all levels of bureaucracy, decision makers, and street-level bureaucracy, as well as field research, observing the professional daily life of those involved. With the data collected, we sought the theories applicable to the research and benchmarking to be adopted and, thus, we were able to isolate the main problems and propose measures to improve the use of public safety information.

Keywords: public safety - municipality; urban security; Civil Guard; public safety information flow.

LISTA DE ILUSTRAÇÕES

Figura 1: organograma da SMSU.....	26
Figura 2: níveis hierárquicos dos cargos de DAS do Governo Federal.....	37
Figura 3: despacho do Secretário sobre a doação City Câmeras	44
Figura 4: fluxo de informações de segurança pública da SMSU	52
Figura 5: principais obrigações do LGDP	69
Figura 6: diferentes tipos de dados	84
Figura 7: interconexão.....	90
Figura 8: etapas de Programa.....	90
Figura 9: o secretário municipal de segurança pública José Roberto Rodrigues na sala de monitoramento de câmeras da Guarda Civil Metropolitana	93
Figura 10: diagrama técnico	96
Figura 11: Discovery/Classificação dos Dados/Proteger/Gerenciamento	97
Figura 12: LGPD no mundo.....	97

LISTA DE ABREVIATURAS

COMPSTAT – “compare stats”

CONSEG - Conselho Comunitário de Segurança

DAP – Divisão de Análise e Planejamento

DATASUS - Departamento de Informática do Sistema Único de Saúde

DNI - Documento Nacional de Identidade

DPC – Divisão de Parcerias e Cooperação Técnica

DTIC – Divisão de Tecnologia da Informação e Comunicação

EAD - ensino à distância

FBSP – Fórum Brasileiro de Segurança Pública

GCM – Guarda Civil Metropolitana

IRPF - Imposto de Renda de Pessoa Física

IoT - “Internet of Things” - Internet das Coisas

LGPD – Lei Geral de Proteção de Dados

METRÔ - Companhia do Metropolitano de São Paulo

PNSPDS – Plano Nacional de Segurança Pública e Defesa Social

PRODAM - Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo

SENASP/MJ - Secretaria Nacional de Segurança Pública, Ministério da Justiça

SIG-GCM - Sistema de Gerenciamento da Guarda Civil Metropolitana

SIGPEC - Sistema de Gerenciamento de Pessoal e Competências

SMSU – Secretaria Municipal de Segurança Urbana da Cidade de São Paulo

SPTRANS - São Paulo Transportes S.A.

SUPLAN – Superintendência de Planejamento

SUSP - Sistema Único de Segurança Pública

SUMÁRIO

1	INTRODUÇÃO	13
2	METODOLOGIA	17
3	CONCEITOS	20
3.1	A Administração Pública envolvida	20
3.2	Principais iniciativas da SMSU	21
3.3	A Guarda Civil Metropolitana e a Segurança Pública	22
3.4	Abordagem organizacional	24
3.4.1	A SMSU e a GCM na ótica de Morgan	24
3.4.2	Visão mecanicista	27
3.4.3	Visão culturalista	28
3.4.4	Visão político-sistemática	30
3.5	Aplicação do conceito de burocracia de nível de rua na SMSU e na GCM	31
3.5.1	Elaboração do conceito de burocrata de nível de rua	32
3.5.2	Limitações do burocrata de nível de rua e a burocracia de médio escalão	34
3.5.3	Burocratas na prática: dirigentes da SMSU e guardas civis	36
3.6	Por que analisar uma política pública?	38
3.6.1	Aspectos jurídicos	39
3.6.1.1	<i>Princípios jurídicos</i>	39
3.6.1.2	<i>Aplicação do SUSP e PNSPDS</i>	40
3.6.1.3	<i>Marco Civil da Internet e LGPD</i>	41
3.6.2	Política Pública	45
4	BENCHMARKING	48
5	ACHADOS	52
6	FORMULAÇÃO DE PROPOSTAS	56
6.1	Propostas para o Achado n.1	57
6.1.1	Contratação de terceirizada	57
6.1.2	Solução orgânica	58
6.2	Propostas para achado nº 2	60
6.3	Propostas para o Achado n. 3	61
6.3.1	Setor de TI da SMSU	62
6.3.2	Setor de TI da GCM	62
6.4	Propostas para o achado n. 4	64
6.4.1	Gerenciamento de frota	65
6.4.2	Relatórios de atividades	66
6.5	Propostas para o Achado n. 5	67
7	ANÁLISE DA LGPD	69
7.1	A Lei e o Setor Público	71
7.2	Porque o Setor Público	73
7.3	Tratamento dos dados pelo Setor Público	76
7.4	Definições	78
7.5	Responsabilidade do Órgão Público	79
7.6	Sanções à Administração Pública	80
7.7	Status	81

7.8	O que são os dados?	83
7.9	Preparação para SMSU	84
7.10	Como a Lei identifica um incidente de segurança?.....	88
7.11	Ações Tecnológicas	89
7.12	Softwares SMSU Informação	90
7.13	Responsabilidade e Registros de Acesso	94
7.14	Sugestão de Segurança Técnica	95
7.15	Cases no Mercado Brasileiro e Europeu	98
8	CONSIDERAÇÕES FINAIS.....	103
	REFERÊNCIAS.....	106

1 INTRODUÇÃO

Numa época em que discursos populistas voltam a ter força em matéria de segurança pública, torna-se imperativo ressaltar iniciativas que saiam do mote “tiro-porrada-e-bomba”: aquelas que não priorizam o confronto como prioridade para diminuir a criminalidade.

Uma das mais importantes abordagens em segurança pública quando se trata dessas iniciativas é o uso de informação. Não o mero uso como fonte de estatísticas criminais. O uso da informação como ferramenta que sirva tanto aos burocratas que estão na linha frente quanto àqueles de nível médio ou mesmo os tomadores de decisão, ou seja, o uso da informação de segurança pública no planejamento do órgão público envolvido.

Para entender o uso de informação de segurança pública no âmbito dos Estados, o Fórum Brasileiro de Segurança Pública (FBSP, 2010 e 2013) elaborou, entre 2010 e 2013, mediante termo de parceria com o governo federal, um diagnóstico dos sistemas que lidam com essa informação, analisando desde os recursos humanos até os recursos materiais envolvidos.

O fato de ter sido elaborado no âmbito dos Estados, e não nos municípios, reflete a abordagem da segurança pública no Brasil ser centralizada nos órgãos estaduais que a legislação determina, sendo a referência mais básica o art. 144 da Constituição Federal (BRASIL, 1989), onde especifica como órgãos de segurança pública apenas as polícias federais (federal propriamente dita, rodoviária federal e ferroviária federal) e as polícias estaduais (civil, militar e bombeiro quando for militar). Para os municípios, em caráter residual, há apenas a menção da possibilidade de constituir guardas municipais, com função somente de vigilância patrimonial de seus bens, serviços e instalações.

Existem motivos históricos, políticos e outros que justificaram essa participação residual dos municípios na segurança pública à época da elaboração da Constituição Federal de 1988. Isso resultou em diversas discussões sobre as guardas municipais serem, ou não, forças policiais e poderem realizar atos privativos de polícia de

segurança pública, e não apenas os atos de polícia administrativa¹. O contexto histórico dessa discussão foi exaustivamente analisado por Lima e Pröghlöff (2013) e, num capítulo próprio, procuraremos verificar quais são as discussões atuais, algumas em andamento no Supremo Tribunal Federal.

Exceto pela segurança pública, Farah (2001) elencou diversos motivos pelos quais o município tem importância crescente quando se fala de políticas públicas sociais: incremento na receita do municípios por participação nos tributos, de acordo com os ditames da Constituição Federal; entre os entes federativos, é o mais próximo das demandas da sociedade, resultando em maior participação; maior descentralização de atribuições do Poder Público, antes focado na União, tanto nas novas teorias de reforma administrativa quanto nos incentivos de instituições financiadoras multilaterais.

Podemos abstrair uma constatação importante desses dois estudos e da legislação citada: o Município, por ser o ente político com maior contato com a sociedade, possui o poder de polícia, no sentido de fiscalização, de todas as áreas (saúde, educação, habitação, meio ambiente....), exceto a segurança pública, o que nos parece um contrassenso.

A reflexão pertinente e atual é a participação efetiva do município na segurança pública hoje. Vista, ainda que brevemente, a importância do uso de informação em segurança pública, faz-se necessário pesquisar como esse uso é abordado em âmbito municipal, contribuindo para tal participação.

Uma vez que não encontramos nenhuma pesquisa com essa abordagem, decidimos analisar o uso de informação de segurança pública no âmbito municipal, tomando como paradigma a Secretaria Municipal de Segurança Pública da Cidade de São Paulo (SMSU).

A SMSU não é um órgão recente, mas foi reorganizada e atualizada pelo Decreto municipal nº 50.388, de 16 de janeiro de 2009 (SÃO PAULO, 2009). O Decreto determina, em seu artigo 2º que compete à SMSU “(..) conduzir ações de segurança urbana, mediante atuação articulada com os órgãos públicos municipais, priorizando, nas políticas públicas urbanas, a prevenção à violência...”. Ao listar extensivamente as competências nos vinte e cinco incisos, destacamos o inciso III,

¹ Temos como polícia administrativa qualquer atividade de fiscalização pelo Poder Público.

que diz que a SMSU deve “estabelecer relação com os órgãos de segurança estaduais e federais, visando ação integrada no Município de São Paulo...”.

Também é importante notar que a Guarda Civil Metropolitana é parte da estrutura da SMSU. Isso atrai a Lei Federal nº 13.675/2018 (BRASIL, 2018) e os Decretos Federais nº 9.489/2018 (BRASIL, 2018) e 9.630/2018 (BRASIL, 2018), onde tivemos a criação e regulamentação da Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e do Sistema Único de Segurança Pública (SUSP). As guardas municipais são citadas expressamente como integrantes operacionais do SUSP.

Complementando esse entendimento, temos o Estatuto Geral das Guardas Municipais², que define atribuições de segurança pública específicas para as guardas municipais, porém, possui conteúdo em discussão no Supremo Tribunal Federal³.

Como um dos fundamentos do trabalho é o conceito de governança democráticas em segurança, onde a segurança é papel de todos, não apenas de polícias, consideramos que a SMSU faz parte da segurança pública, logo, podemos restringir o foco desta pesquisa.

A PNSPDS, entre vários princípios, cita a “promoção da produção de conhecimento sobre segurança pública”. Entre as diretrizes, ela elenca “sistematização e compartilhamento das informações de segurança pública, prisionais e sobre drogas, em âmbito nacional”. Praticamente repete tal diretriz na lista de objetivos quando diz que “integrar e compartilhar as informações de segurança pública, prisionais e sobre drogas”.

Também é necessário incluir a Lei Geral de Proteção de Dados (LGPD) – Lei federal no 13.709, de 14 de agosto de 2018 (BRASIL, 2018), com algumas alterações na redação pela Lei federal no 13.853/2019 (BRASIL, 2019), na discussão. Embora não seja uma lei de segurança pública propriamente dita, ela afeta diretamente o uso de informações na segurança pública.

Aplicando essa legislação federal ao nível municipal, significa que, no caso específico da SMSU, há necessidade de diagnosticar se os processos de produção

² Lei federal nº 13.022, de 8 de agosto de 2014.

³ A ementa sobre a discussão no STF, que está pendente de decisão do pleno, está disponível em <http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verPronunciamento.asp?pronunciamento=4365808>

de estatísticas e informações de segurança pública da Pasta atendem os parâmetros de tais legislações.

Para verificar essas informações, foi informado ao gestor da SMSU⁴, o Secretário Municipal da Segurança Urbana, sobre os questionamentos que faríamos para compreender o órgão dentro do campo da pesquisa. Seriam feitas perguntas como:

- Como é feita a coleta de dados?
- Como são inseridos os dados?
- Como são transmitidos?
- Qual o perfil de quem lida com os dados?
- Como chegam aos tomadores de decisão?
- Qual a pertinência dos dados coletados?
- Como esse processo afeta a gestão pública da Pasta?

De posse das informações obtidas, poderemos cumprir o nosso objetivo principal que é analisar o fluxo de informações de segurança pública na SMSU e como tais informações são afetadas pelos aspectos organizacionais, tecnológicos e finalísticos, de maneira a compreender de que formas os processos podem ser melhorados e quais propostas poderemos fazer para obter essas melhorias nessas informações para, ao final, a SMSU ter um fluxo aperfeiçoado de informações de segurança pública. Com a pretensão de manter a SMSU na vanguarda da aplicação da LGPD, complementaremos o trabalho com a análise e proposta de LGPD para a SMSU.

Como é um trabalho que prioriza a busca de informações para aumentar a qualidade do diagnóstico e das propostas, pretendemos obter essas informações em entrevistas com os tomadores de decisão, burocratas de médio escalão e com os burocratas de nível de rua, sem prejuízo de um levantamento de campo e análise tecnológica dos processos envolvidos.

⁴ O Termo de Referência encontra-se em no Anexo I.

2 METODOLOGIA

Para que haja aperfeiçoamento da gestão e das tomadas de decisões dos dirigentes na SMSU, é preciso elaborar um diagnóstico do uso de informações de segurança pública e, com essa finalidade, fez-se necessário coletar e analisar dados sobre o contexto atual do órgão nesse tema.

A mera leitura da legislação relacionada à SMSU, tanto a sua reformulação como outras portarias e resoluções, não refletiria a realidade.

Considerando os conceitos de pesquisas qualitativas e quantitativas, didaticamente descritos por Minayo (MINAYO & SANCHES, 1993), podemos seguramente afirmar que esta pesquisa foi qualitativa. Não foi fundamental para o trabalho lidar com procedimentos estatísticos, estimação de parâmetros e testes de hipóteses, características de uma pesquisa quantitativa. Como esses autores explicam, “(...) uma análise qualitativa completa interpreta o conteúdo do discursos ou a fala cotidiana dentro de um quadro de referência, onde a ação e a ação objetivada nas instituições permitem ultrapassar a mensagem manifesta e atingir os significados latentes” (MINAYO & SANCHES, 1993, p. 246), ou seja, nos limitarmos às opiniões institucionais dos dirigentes, bem como a mera leitura da legislação relacionada à SMSU, tanto a sua reformulação como outras portarias e resoluções, não refletiria a realidade ser diagnosticada.

Assim, verificamos que, além do levantamento de campo (observação direta), a realização de entrevistas tornaria a aquisição de informações mais completa, afinal, como diz Patton (2002, p. 340), “we interview people to find out from those things we cannot directly observe.” (tradução livre: nós entrevistamos as pessoas para encontrar aquelas coisas que não podemos observar diretamente).

Inicialmente, de acordo com classificação de Patton (2002), realizamos entrevistas abertas (“informal conversational interview”) com os dirigentes da SMSU, com a finalidade de uma noção introdutória de como é a SMSU, como se organiza e quais iniciativas estão em andamento. Cientificamos os entrevistados que poderíamos formular algumas questões via e-mail, para que ficassem registradas as respostas, com a identificação dos entrevistados.

Posteriormente, formulamos uma entrevista mista através do Google Forms⁵. Foram feitas perguntas fechadas com múltiplas escolhas (“closed, fixed-response interview”) para podermos estabelecer um perfil dos entrevistados, sempre focando o uso de informações de segurança pública, e também algumas perguntas com respostas em aberto (“standardized open-ended interview”) quando percebemos que não seria possível prever todas as possibilidades de respostas. Presencialmente, também reforçado no envio do formulário por e-mail, alertamos os entrevistados que as respostas seriam utilizadas de forma desidentificada: somente os autores da pesquisa saberiam a identidade dos entrevistados. Esse alerta teve como objetivo deixar o entrevistado confortável para se manifestar, sem temer uma possível repressão funcional por elaborar críticas à Administração.

Simultaneamente, visitamos a sede da SMSU, onde tivemos contato com o próprio Secretário e com os diretores da Divisão de Parcerias e Cooperação Técnica (DPC), da Divisão de Tecnologia da Informação e Comunicação (DTIC) e da Divisão de Análise e Planejamento (DAP). Também visitamos a sede da Guarda Civil Metropolitana (GCM), onde estivemos com a própria Comandante, bem como o responsável pela Superintendência de Planejamento (SUPLAN). Por fim, estivemos na Inspetoria 10, o que denota uma pesquisa com características naturalísticas, onde observamos o uso cotidiano de informações de segurança pública pela GCM, a burocracia de nível de rua da SMSU, onde nos foram cedidos formulários em branco que são preenchidos a cada turno por guardas⁶.

Após coletar e analisar os dados, descobrimos diversos problemas no uso de da informação de segurança pelo órgão analisado, alguns com maior e outros menor nexos com o tema. Aqueles com maior nexo serão abordados ao longo deste trabalho.

Para analisar esses dados e elaborar soluções, foi predominante o método hipotético-dedutivo, conforme os tipos conceituados por Mezzaroba e Monteiro (2009): a necessidade de partir do geral (dados coletados) para o particular (soluções) e a formulação de hipóteses (soluções) caracterizam a maior parte do trabalho. Tomando como base a mesma obra (MEZZAROBA E MONTEIRO, 2009), pode-se afirmar que promovemos uma pesquisa empírica, pois, segundo esses autores “(...) a pesquisa empirista levará em consideração a experiência fática da qual se possam inferir conclusões com alto grau de certeza científica” (MEZZAROBA E MONTEIRO, 2009,

⁵ Perguntas disponíveis no Apêndice I.

⁶ Cópias disponíveis nos Anexos II, III e IV.

p. 99). É necessário ressaltar que nós, os autores deste trabalho, possuímos longa experiência profissional (mais de vinte anos) em temas pertinentes, como segurança pública e tecnologia de informação, o que contribuiu para a qualidade do empirismo empregado.

Caso houvesse mais tempo para entrevistar novamente os dirigentes, seria interessante verificar se eles têm ciência dos problemas apontados e se há previsão para solucioná-los. Devido às ocupações profissionais tanto dos autores da pesquisa quanto dos entrevistados, houve certa dificuldade em coincidir a disponibilidade nas agendas, o que se repetiria se tentássemos entrevistá-los novamente.

Em relação aos burocratas de nível de rua, também sentimos a necessidade uma amostragem válida, pode-se dizer mais rigorosa quantitativamente falando, dos guardas e outros servidores, até mesmo a totalidade deles, para haver uma quantificação precisa das opiniões deles sobre o tema da pesquisa. Conseguimos apenas vinte e três entrevistas, sendo treze na SMSU e 10 na GCM. Para minimizar esse prejuízo, procuramos realizar as entrevistas com pelo menos um “tipo” de burocrata: servidores administrativos na SMSU, burocratas nível médio na SMSU, burocratas nível médio na GCM e burocratas de nível de rua na GCM. Conseguimos realizar com pelo menos um de cada categoria. Tivemos a impressão de que essas poucas entrevistas foram bem significativas.

Consideramos que esses meios foram suficientes para realizar o diagnóstico do uso de informações de segurança pública na SMSU.

Reforçamos que ambos autores desta dissertação têm um longo histórico com o tema de segurança, e vimos na SMSU uma maneira de agregarmos valor técnico à um órgão que tem feito muito pela segurança, mas que precisará se adaptar há uma nova lei que vigorará a partir de Agosto de 2020, a LGPD. Apesar da SMSU ser um órgão relacionado à segurança e contar com certo nível de proteção dos dados, as ações que podem ocorrer à ela por falha de sistemas e processos tendem a repercutir mal se assim acontecer no futuro, lembrando que a SMSU tem se destacado em ações de segurança que estão impactando em índices de segurança na cidade de São Paulo.

3 CONCEITOS

Alguns conceitos são necessários para a correta análise e diagnóstico do tema desta dissertação. Discorreremos neste capítulo sobre alguns conceitos pertinentes e suas aplicações ao caso concreto.

3.1 A Administração Pública envolvida

A cidade de São Paulo⁷ é a nona maior cidade do Brasil em extensão territorial e uma população estimada de mais de 12 milhões de pessoas, sendo a cidade mais populosa do hemisfério sul, sem contar a população flutuante oriunda dos municípios vizinhos.

A Secretaria Municipal de Segurança é um órgão da administração direta municipal da cidade de São Paulo. É umas das Pastas subordinadas à Prefeitura Municipal de São Paulo, encarregada da segurança urbana, defesa social e, por convênio, coordena as Juntas de Serviço Militar. Para a questão de segurança urbana, possui a Guarda Civil Metropolitana como órgão subordinado. Possui 6.465⁸ servidores ativos, dos quais 6.085 são guardas civis metropolitanos e os demais estão nos demais coordenações subordinadas à SMSU ou na Administração da Sede da SMSU.

A Guarda Civil Metropolitana foi criada em 1986 com a proposta de ser uma força de segurança pública cidadã, focada na comunidade, o que a diferenciaria do policiamento militar, de natureza repressiva⁹. Como veremos a seguir, ela antecipou uma resposta à política de segurança interna decorrente do período militar.

⁷ Informações obtidas em: https://pt.wikipedia.org/wiki/S%C3%A3o_Paulo

⁸ Dados obtidos no Portal de Transparência da Prefeitura de São Paulo.

⁹ “GCM completa 30 anos - Criada por Jânio Quadros, corporação iniciou com 150 agentes e armas emprestadas” – disponível em: <http://www.saopaulo.sp.leg.br/apartes-antiores/revista-aptas/numero-18/gcm-completa-30-anos/>

3.2 Principais iniciativas da SMSU

A SMSU, decididamente, não possui uma gestão inerte. Fomos gratamente surpreendidos¹⁰ com iniciativas de qualidade.

O DRONEPOL é o uso de drones por guardas civis. Um grupo de guardas foi treinado e habilitado, de acordo com a legislação vigente, para as diversas aplicações do uso de drones: filmagem e vigilância de áreas de risco, grandes eventos, apoio ambiental, fotografias aéreas e controle de público e trânsito. As equipes DRONEPOL realizam, em média 100 voos por mês, incluindo apoio para outras secretarias e órgãos públicos, mediante solicitação¹¹. A SMSU foi a primeira a usar Drones em suas ações diárias, tendo em sua referência uma ocorrência de repercussão mundial que ocorreu na Represa de Guarapiranga¹².

O City Câmeras é uma ação integrada que visa lidar como emergência de defesa civil e segurança pública, incluindo zeladoria, através de uma rede de câmeras formada por cessão gratuita do acesso de câmeras particulares, somadas com algumas públicas. O sistema possui as câmeras da própria SMSU e câmeras que a população, mediante análise cadastral e requisitos de equipamento, decidir compartilhar com o sistema. Os cidadãos têm acesso às suas câmeras e às câmeras públicas (pertencentes à SMSU), mas não tem acesso às câmeras de outros cidadãos. Somente a SMSU e forças policiais conveniadas tem acesso a todas câmeras compartilhadas pelos cidadãos¹³.

A SP+Segura é uma plataforma que agrega todas as iniciativas anteriores, somando-se às informações coletadas pela GCM e pelos cidadãos (através de aplicativo no celular). É uma forma de apontar a localização de uma ocorrência criminal ou uma situação de zeladoria urbana. O sistema possui módulos que variam de acordo com o usuário. Reunidas em uma Central de Controle, as informações coletadas podem ser destinadas, conforme a triagem, para gestores *online*, GCM, polícia e serviço de ambulância municipal¹⁴.

¹⁰ O fato dos autores serem moradores da cidade e não saberem da existência de tais iniciativas será um dos problemas constatado, em capítulo posterior.

¹¹ Cópia do folheto deste programa encontra-se no Anexo V.

¹² Vídeo da ocorrência disponível em: https://www.youtube.com/watch?v=_04kblukp54. Acessado em 1 nov 2019

¹³ Cópia do folheto deste programa encontra-se no Anexo VI.

¹⁴ Cópia do folheto deste programa encontra-se no Anexo VII.

Voltaremos a abordar essas iniciativas ao longo do trabalho.

3.3A Guarda Civil Metropolitana e a Segurança Pública

Como foi brevemente comentado na Introdução, existe uma celeuma histórica sobre a GCM (como referência para as demais guardas metropolitanas do país) ser uma atividade policial (em sentido estrito) ou não.

Aqueles que defendem que a GCM não pode exercer, em hipótese alguma, qualquer atividade privada de forças policiais alega que o rol do incisos do art.144 da Constituição Federal é taxativo, fazendo uma interpretação literal da redação: se não está nos incisos do art.144, não é força policial¹⁵.

Esse entendimento resulta em diversas complicações.

Somente as forças do incisos do art.144 possuem porte de arma de fogo por prerrogativa de função. O porte das guardas metropolitanas está garantido por liminar no STF dentro da Ação Direta de Inconstitucionalidade 5948. Essa ação versa sobre as limitações impostas ao porte dos guardas metropolitanas de acordo com a quantidade de habitantes dos municípios.

Outra complicação é a busca pessoal¹⁶, popularmente chamada de revista. A Justiça tem entendido, nas instâncias superiores, que um guarda metropolitano, embora possa realizar uma prisão em flagrante como qualquer um do povo¹⁷, não possui o direito de efetuar buscas pessoais e apreensões de objetos suspeito de conexão com atividade criminosa, pois seriam atividades típicas de investigação criminal, atribuição não concedida à guardas metropolitanas. A prisões onde são comprovadas em que foi houve busca pessoal por guardas metropolitanos estão sendo anuladas.

¹⁵ Interessante notar que os incisos do art. 144 também não preveem Polícia Científica, mas 16 Estados aceitam a existência da polícia científica desvinculada da Polícia Civil, mantendo o porte de arma, uso de viaturas e algemas para os policiais científicos, sem qualquer contestação, inclusive São Paulo.

¹⁶ Código de Processo Penal, art. 244. A busca pessoal independerá de mandado, no caso de prisão ou quando houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam corpo de delito, ou quando a medida for determinada no curso de busca domiciliar;

¹⁷ Código de Processo Penal, Art. 301. Qualquer do povo poderá e as autoridades policiais e seus agentes deverão prender quem quer que seja encontrado em flagrante delito.

O Supremo Tribunal Federal decidiu, por maioria, que os guardas metropolitanos, por não estarem nos incisos do art.144, não possuem direito à aposentadoria especial, pois sua atividade não seria essencialmente insalubre ou perigosa^{18,19}

Essa limitada interpretação textual no que se refere a Constituição Federal, deixando os municípios de lado, foi extensivamente estudado por Lima e Pröghlöff (2013), como foi mencionado na introdução.

De forma resumida, esse estudo de Lima e Pröghlöff demonstra que o conceito originário de segurança pública no Brasil, considerando desde o início da República, é subsidiário da segurança nacional, dentro da doutrina militar. Nesse conceito, temos as ameaças e inimigos externos ao país e internos no país. Devemos lembrar que a doutrina militar possui fundamentos, dos quais destacamos a obediência hierárquica absoluta (até hoje, é conduta passível de prisão desobedecer qualquer ordem no ambiente militar) e a necessidade estabelecer um inimigo, logo, a segurança interna, que foi adaptada como segurança pública ao longo das décadas, trata-se de existir um policiamento militar (a Constituição Federal de 1934 já previa polícia militar, para tempos de paz, realizando policiamento ostensivo, subordinada aos governos estaduais) e o infrator da lei ser tratado como inimigo.

Prosseguindo com o mesmo estudo, a maior reação a esse modelo foi ocorrer com a edição da Constituição Federal de 1988, a primeira após o período ditatorial militar de 21 anos. Embora tenha sido um documento exímio em direitos fundamentais e garantias, pecou por não ter, expressamente, exigido uma polícia cidadã e elaborado um conceito distinto de segurança pública. O resultado, que temos até hoje, é “[...] o debate sobre segurança pública é reduzido, mesmo após 1988, quase que exclusivamente ao debate legal e normativo...” nas palavras de Lima e Pröghlöff (2013). Esse é o ponto de partida para discordamos frontalmente dos entendimentos que visam excluir os guardas metropolitanos da segurança pública.

Inicialmente, devemos ressaltar que a segurança pública é mais do que apenas o texto da lei. As melhores iniciativas em segurança pública são transversais, não se limitam a ficar discutindo qual órgão faz o quê, só o órgão “x” pode fazer determinada

¹⁸ Conforme notícia vista em: <https://www.conjur.com.br/2019-set-02/guardas-municipais-nao-direito-aposentadoria-especial>

¹⁹ Opinião dos autores: os ministros do STF consideraram corriqueiro uma pessoa portar material explosivo com detonadores (armas de fogo e munição) junto ao corpo.

atividade. Obviamente, não se está defendendo que qualquer órgão possa fazer qualquer coisa. Estamos defendendo a governança democrática em segurança pública, tal como defendido por Bueno e Lima (in: FBSP, 2018):

Para nós, governança é um termo que nasce da ideia de que o Estado não é o responsável exclusivo pelo sentido da Política e das políticas públicas e, se olharmos em perspectiva, há uma pluralidade de interesses em disputa e que precisam ser administrados (o próprio caput do Artigo 144, da CF, traduz este conceito, ao dizer que segurança é uma responsabilidade de todos). No caso brasileiro, governança em Segurança Pública é responsabilidade difusa de vários atores e que, para ter efetividade, precisa ser coordenada e articulada em torno do que está previsto na nossa Constituição, que diz que segurança é condição basilar para o exercício da cidadania (Art 5º.) e é direito social universal de todos os brasileiros (Art. 6º.).

Posto isso, nota-se que os entendimentos contrários aos guardas metropolitanos como parte da segurança pública se limitam a essa interpretação literal e pobre da legislação. A GCM, bem como a SMSU, não precisam ser as polícias descritas nos incisos do art. 144 da Constituição Federal para serem atores de suma importância da Segurança Pública, tornando tal discussão vencida, mesmo dentro de suas atribuições constitucionais, com ou sem porte de arma de fogo e poder de busca e apreensão.

3.4 Abordagem organizacional

Vamos analisar a SMSU e a GCM sob aspectos de doutrinas organizacionais, com a finalidade de compreender melhor tais órgãos e, posteriormente, conseguirmos elaborar propostas de acordo com suas naturezas.

3.4.1 A SMSU e a GCM na ótica de Morgan

Gareth Morgan, em sua obra “Imagens da Organização” (MORGAN, 2002), propõe o uso de certas metáforas para entendermos melhor as organizações. Trata-

se de um clássico da Administração que, mesmo sendo baseado em exemplos do setor privado, são cabíveis para a análise de órgãos públicos.

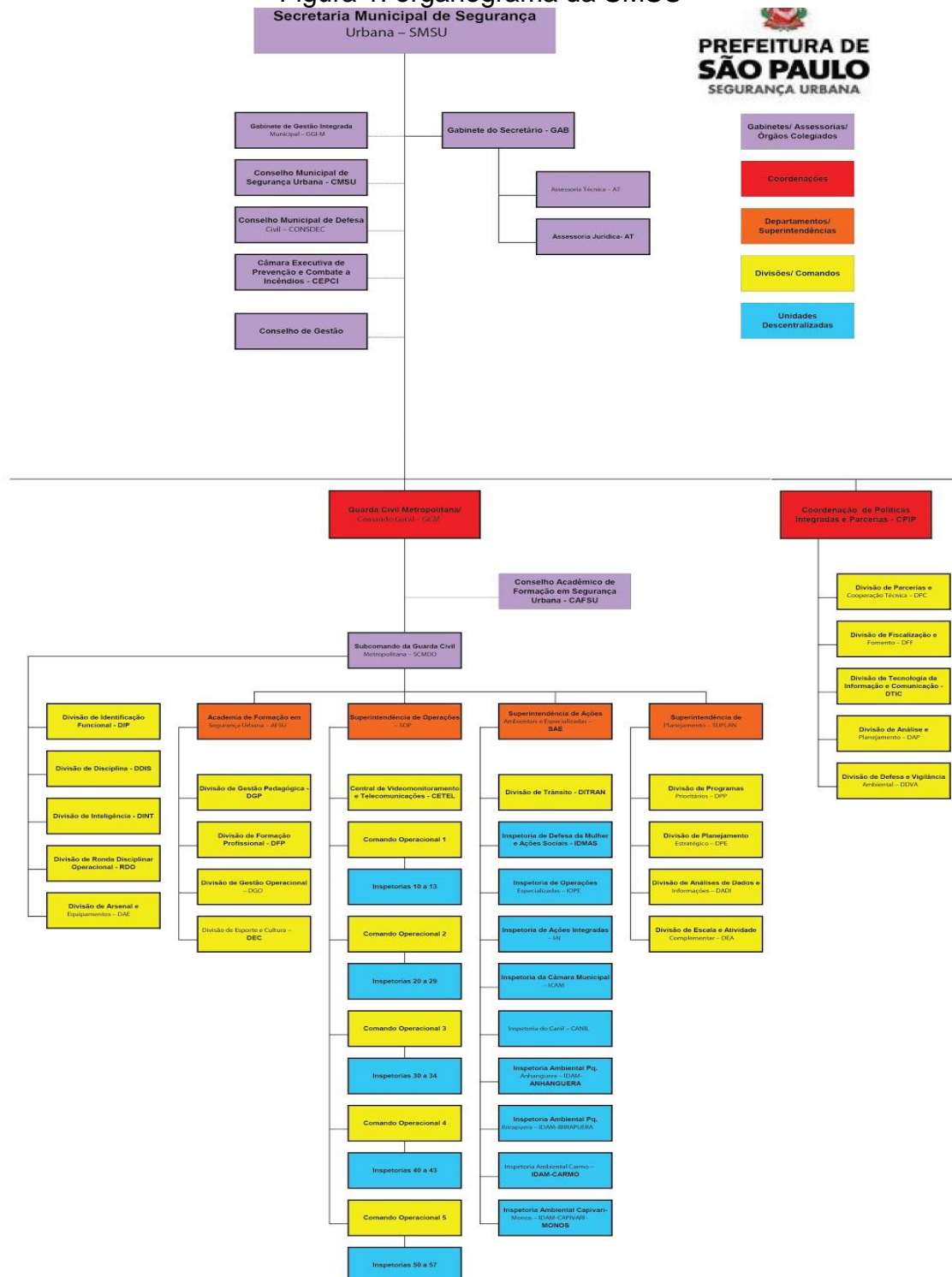
Embora a GCM seja um órgão subordinado à SMSU, é apropriado tratarmos como organizações distintas para termos uma melhor visualização das metáforas de Morgan.

A SMSU é liderada por um gestor político (indicado pelo governante municipal), na figura do Secretário. Suas assistências são compostas por dirigentes e servidores comissionados nos cargos, que podem ou não ser oriundos das carreiras da Pasta, da ativa ou aposentados, como é comum em qualquer órgão público similar. Por si só, esse fato gera diferenças que veremos nas “imagens”. Em regra, não possuem atendimento ao público. Cada divisão hierárquica costuma ter, em média, apenas seis servidores.

A GCM, por sua vez, é liderada por uma pessoa no cargo de Comandante, necessariamente uma servidora de carreira de guarda civil metropolitana, escolhida pelo Secretário entre os guardas no último nível da carreira. Suas assistências são compostas por servidores de carreira comissionados nas funções, necessariamente exercendo atividades-meio. Lida com o público diretamente em suas atividades-fim. Embora tenha poucos servidores em cada divisão da sede, por volta de sete servidores, devemos lembrar que a maior parte do efetivo está na rua, nas inspetorias regionais ou especializadas.

Facilitando a visualização do organograma, temos a figura a seguir, disponível no próprio sítio da SMSU:

Figura 1: organograma da SMSU



Fonte: sítio eletrônico da SMSU.²⁰

²⁰ A imagem está editada. Foram excluídos os setores da SMSU que não lidam diretamente com o fluxo de informações de segurança pública, como a Defesa Civil, a Junta de Alistamento, os setores financeiros-orçamentário e outros. A GCM está na íntegra.

3.4.2 Visão Mecanicista

Quando Morgan discorre sobre o surgimento da organização burocrática, ele comenta (MORGAN, 2002, p.37):

Quando falamos sobre organização, geralmente temos em mente um estado de relações ordenadas entre partes claramente definidas que têm alguma ordem determinada. Embora a imagem possa não ser explícita, estamos falando de um conjunto de relações mecânicas. Falamos sobre organizações como se elas fossem máquinas e, conseqüentemente, tendemos a esperar que funcionem como máquinas: de maneira rotineira, eficiente, confiável e previsível.

Dessa forma, podemos afirmar que, predominantemente, todos os órgãos públicos são mecanicistas, o que por óbvio inclui a SMSU e a GCM. Considerando ainda que o Morgan (2002) cita o exército prussiano como origem da visão mecanicista (uso de equipamento padronizado, aumento de especialização de tarefas, padronização de regulamentos e introdução de uniforme), fica a GCM caracterizada mais ainda.

Temos o taylorismo como forma mais moderna do mecanicismo que o citado exército prussiano do século XVIII, com as seguintes características:

- os gerentes (os dirigentes na SMSU e os chefes na GCM) “(...) devem pensar em tudo que se relaciona ao planejamento e organização do trabalho, deixando os trabalhadores com a tarefa de implementação” (MORGAN, 2002, p.45);
- “planeje a tarefa do trabalhador, especificando com precisão a maneira como o trabalho deve ser feito” (idem) - funções dos servidores na SMSU e guardas na GCM;
- “monitore o desempenho do trabalhador para garantir que os procedimentos de trabalho adequados sejam seguidos e que os resultados apropriados sejam alcançados” (idem) - como nos relatórios dos guardas na GCM.

Uma vez caracterizada a visão mecanicista da SMSU e da GCM, o passo seguinte é lembrar as lições de Morgan (2002) sobre os problemas de organizações mecanicistas.

Tanto na GCM como na SMSU verificamos que, às vezes, a existência de diferentes categorias, divisões, supervisões, assessorias e inspetorias funcionam como uma trava para a discricionariedade e iniciativas criativas dos subordinados.

A mesma hierarquização também compromete a capacidade de lidar com situações novas, visto que dependem de protocolos padronizados, tornando lenta a resposta. Confirmando essa situação, a pessoa E01 declarou que comunicação interna é um problema na SMSU:

(...) desde questões banais mais sérias, como os e-mails “vale este” usados em grande quantidade, até questões mais sérias, como a falta de comunicação entre os funcionários de um mesmo setor, o que dificulta a continuidade e a coletividade das atividades....se estas questões forem resolvidas, outros problemas serão indiretamente sanados.

Os dirigentes na SMSU, mesmo que oriundos da carreira de guarda da GCM, já não possuem mais convívio com quem está na linha de frente, de maneira que acabam isolados dos problemas atuais para quem ainda está.

Como consequência desse quadro, os subordinados acabam aderindo ao comportamento de inércia e passividade, sempre jogando a responsabilidade para os superiores ou para outros setores.

Isso não quer dizer que estejamos defendendo a ausência de hierarquia e divisões hierárquicas ou mesmo a falta de protocolo para o trabalho dos servidores da SMSU e guardas da GCM. A visão mecanicista serve para alertar a Administração sobre os ajustes que podem ser feitos nesses fatores, de maneira que não afetem negativamente o nível de discricionariedade necessário para o trabalho e não acabem vedando inovações oriundas dos servidores “chão de fábrica”.

3.4.3 Visão culturalista

Das ideias que compõem essa visão, destacamos a própria organização como fenômeno cultural e, nas palavras do próprio Morgan, “explorar padrões de cultura e subcultura corporativas entre e dentro de organizações” (MORGAN, 2002, p.138). Em linha gerais, às vezes o órgão é unificado em relação aos outros órgãos e, em outras, possui seus grupos culturais internos, com suas próprias regras, valores, condutas e afins. Sendo assim, é mais uma oportunidade para fundamentarmos a necessidade de separação entre a SMSU e a GCM para análise como órgãos distintos.

Na SMSU, observamos a cultura corporativa semelhante à de uma empresa segmentada: diversos setores independentes, que não possuem necessidade de se comunicarem, fazendo com que os servidores também não se comuniquem, que respondam somente à diretoria. Como possuem diversas origens e não atendem o público, não apresentam comportamento uniforme (os servidores de setores diferentes) e, individualmente, não apresentam sinais de “pertencimento” à SMSU: poderiam estar executando as mesmas funções em outros órgãos, não faria diferença. Corroborando com isso, temos o depoimento da pessoa E06:

Deveríamos ter mais treinamento e acompanhamento de um servidor mais antigo que possa nos orientar na atuação da função. E que pudéssemos ter conhecimento da função que cada servidor realiza nos outros setores. E conhecimento de todos os produtos que os servidores trabalham para um melhor atendimento.

A GCM, onde há uma carreira única, obrigando todos os servidores a começarem pela rua, em contato direto com o público, e, conforme as ascensões profissionais, vão se distanciando, mas não muito, das ruas, a cultura é diferente da SMSU. O fato de todos, do novato ao comando, terem passado por experiências semelhantes nas ruas, terem trabalhado em equipe, usarem o mesmo uniforme, faz com que os membros da GCM tenham a sensação de pertencimento ao mesmo time: mesmo que não tenham as melhores condições de trabalho existentes, o cargo de guarda exige certa vocação. Dependendo da missão passada para os guardas do turno, alguns chegam a passar oito horas confinados na mesma viatura, obrigando, no mínimo, a terem uma boa convivência, sendo mais comum a geração de vínculos de amizade.

A contrapartida da visão culturalista é, por vezes, a incapacidade dos dirigentes de entenderem que culturas pode até ser influenciadas, valores desejáveis serem reforçados, mas, mesmo que alguns autores defendam tal tese, não é possível controlar culturas.

3.4.4 Visão político-sistemática

Pensando de maneira simplista, seria óbvio dizer que órgãos públicos, como a SMSU e a GCM, são sistemas políticos.

Ocorre que a explicação dessa metáfora pelo Morgan (2002) é bem mais elaborada do que o nome indica. A política nas organizações, segundo o autor, é enxergar “(...) as organizações por meio das lentes da política, os padrões de interesses concorrentes, conflitos e jogos de poder...” (MORGAN, 2002, p.177), logo, “(...) aceitamos o fato de que a política é um aspecto inevitável da vida corporativa” (idem).

Novamente, é importante lembrar que não há pretensão de esgotar toda a metáfora, mas apenas verificar os aspectos dela que são mais pertinentes para este trabalho.

Ao comparar os tipos de comandos com tipos de governo, autor cita, entre outros, a burocracia e a tecnocracia.

A burocracia, presente tanto na SMSU quanto na GCM, é o tipo de poder exercido, nas palavras do autor:

(...) por burocratas que se sentam atrás de seus bureaux ou mesas, criando e administrando as regras que orientam a atividade organizacional. O poder e a responsabilidade em tais organizações estão intimamente ligados ao conhecimento e uso de regras e à forma legal de administração” (MORGAN, 2002, p.181).

Aplicando ao caso concreto, verificamos isso na SMSU, e na maioria dos órgãos públicos, quando o servidor, mesmo comissionado, está há muito tempo incumbido de determinada rotina administrativa que, embora ninguém tenha interesse em absorver e não seja complexa, é imprescindível. Não tivemos oportunidade de pesquisar quem seriam os servidores comissionados mais antigos na SMSU, porém, se tiver o mesmo perfil de outros órgãos públicos, costumam ser os servidores envolvidos em recursos humanos e assuntos financeiros, por não serem funções cobiçadas para terem as pessoas trocadas quando há mudanças eleitorais, momento em que é comum as pessoas em cargos comissionados serem trocadas.

Já na GCM, onde as mudanças não são tão frequentes, visto que todos os servidores são concursados e de carreira, temos mais visível os indícios de tecnocracia: quando poder e a influência são consequências do conhecimento técnico do autor. São aqueles casos, que também são comuns em outros órgãos públicos, em que o servidor que domina determinada tecnologia, tranca tal conhecimento consigo e dificulta que outros a aprendam. Essa situação pode chegar ao cúmulo de o “especialista” ter regalias que os demais não têm, porque o superior hierárquico, mesmo que mude o titular, continuará dependente do “especialista”. Durante o levantamento de campo, algumas pessoas, pedindo o completo anonimato, comentaram conosco sobre servidores que detinham o código-fonte de determinado sistema de TI e, ao aposentarem, levaram-no consigo, obrigando a Administração a adaptar o sistema existente ou criar outro.

Concluindo a metáfora, Morgan (2002) nota que os conflitos que ocorrem nela são oportunidades para estimular a autoavaliação da organização, gerando, possivelmente, inovações, enquanto a ausência de conflitos costuma resultar em conformidade e perda de eficácia.

3.5 Aplicação do conceito de burocracia de nível de rua na SMSU e na GCM

A formulação de propostas para os problemas encontrados requer que a política pública que falhou (as falhas são os problemas, observe-se) seja analisada.

Neste ponto, Secchi adianta que “um problema é a discrepância entre o status quo e uma situação ideal possível” (SECCHI, 2017, p. 44).

Dentro do ciclo de política públicas didaticamente demonstrado pelo mesmo autor (SECCHI, 2017), temos, após diversas fases como, por exemplo, a formação da agenda e tomada de decisão, a fase de implementação de políticas públicas.

Nessa fase, segundo o mesmo autor, é onde temos o “(...) arco temporal que são produzidos os resultados concretos das políticas pública” (SECCHI, 2017, p. 55). É a fase em que a sociedade percebe (ou não) a política pública como ela é, não como foi teorizada.

Ocorre que, no momento de avaliar a falha de uma política pública, os formuladores ou tomadores de decisão procuram os motivos dessa falha em diversos pontos da política pública: indicadores, variáveis, cenário, erros de formulação...

Alguns autores começaram a perceber que havia um elemento fundamental para a implementação que, frequentemente, é deixado de fora em todas as fases antecessoras da implementação: o burocrata de nível de rua.

As políticas públicas dificilmente são formuladas adequadamente. Elas costumam ter objetivos e significados vagos, dúbios e contraditório porque, entre outras coisas, os legisladores preferem redações de efeito e/ou populistas. Como consequência, o administrador fica com o problema de aplicar a política, da maneira que for entendida, e aumenta a discricionariedade dos executores.

LIPSKY (2019) foi pioneiro em sistematizar a influência do burocrata do nível de rua na implementação da política pública.

Em sua obra seminal, aprendemos como essa variável é importante para a aplicação de uma política pública: como ela vai lidar com os funcionários que vão ser a “cara” da Administração Pública perante o cidadão pode ser decisivo para seu sucesso.

3.5.1 Elaboração do conceito de burocrata de nível de rua

Inicialmente, Lipsky²¹ comentou que foi um livro sobre policiais que o inspirou a formular o conceito de burocrata de nível de rua, ou seja, um burocrata que precisa tomar decisões enquanto está em serviço, sem ter oportunidade de consultar os superiores sobre tais decisões.

Lipsky (2019) foi o primeiro a fazer análise sistemática da burocracia do nível de rua:

(...) essas arenas decisórias são importantes, é claro, mas elas não representam a imagem completa. É preciso adicionar à variedade de lugares onde as políticas são feitas os escritórios lotados e os encontros diários dos trabalhadores de nível de rua” (LIPSKY, 2019, p.17-8).

²¹ A fonte desse comentário do Lipsky é anotação de aula em que os autores estavam presente, durante o Curso de Inverno da FGV-SP em 2018.

O burocrata de nível de rua, por estar em contato com o público, não tem o conforto do tempo, informação e outros recursos para tomar a decisão como o formulador ou administrador gostaria sobre a política pública. As regras não dão conta da dinâmica do atendimento ao público, por isso ele precisa de certa discricionariedade.

Lipsky²² também comentou que o cenário acadêmico da época era o estouro de estudos sobre implementação, com destaque para Wildavski, com quem tinha amizade.

Como definir quem são os burocratas de nível de rua? Existem algumas discussões sobre isso, todas necessárias para definir o conceito.

Inicialmente, o serviço precisa ser público, o que, por si só, exclui as atividades privadas, pois estas visam lucro, enquanto o serviço público está dentro do “welfare state”, logo, é mais típico, embora não seja exclusivo, em serviços de segurança (policiais), saúde (enfermagem), educação (professores) e sociais (assistentes sociais). No geral, são aqueles serviços públicos onde dificilmente o cidadão pode ter acesso sem pagar à parte. Essa natureza da procura por lucro afeta diretamente o burocrata de nível de rua: quando o cidadão está pagando por serviço, ele pode procurar por outro que o atenda melhor, e o serviço terá esse prejuízo da perda do cliente. Enquanto isso, para aqueles que não podem pagar por tais serviços, não há a opção de procurar outro prestador do mesmo serviço. Por exemplo, a escola que o estudante de escola pública vai estudar está cruzado com o endereço residencial do aluno, sendo necessariamente a escola mais próxima, variando pela existência de vagas ou excesso de alunos. Simplesmente não tem como escolher.

A característica mais fundamental dos burocratas de nível de rua é a discricionariedade. Embora caiba uma extensa discussão sobre a definição de discricionariedade, Lipsky mantém ela simples. A discricionariedade envolve:

- poder do burocrata de categorizar os clientes (cidadãos) ou circunstâncias;
- possibilidade do burocrata de empregar suas habilidades, conhecimento ou experiência no serviço público, como ele vai gerenciar determinada dificuldade encontrada. Ex.: é o professor quem decide como vai lidar com um aluno

²² Idem.

difícil; é o guarda metropolitano quem decide como lidar com uma situação para o qual não foi treinado, mesmo tendo parâmetros éticos e jurídicos.

Os burocratas de nível de rua precisam ser espertos, inventivos e criativos. Além da falta de tempo comum em quase todas oportunidades (sem tempo para consultar superiores hierárquicos), os burocratas também precisam lidar com a falta de recursos: sempre estão aquém do necessário. De maneira resumida, a base teórica do conceito de burocracia de nível de rua é tentar fazer o melhor com os recursos que estão disponíveis.

3.5.2 Limitações do burocrata de nível de rua e a burocracia de médio escalão

Uma vez notada a importância do burocrata do nível de rua, faz-se necessário verificar os limites dos mecanismos de regulação deles.

Com base em WILSON (1967, apud OLIVEIRA, 2013), verifica-se que o burocrata do nível de rua precisa, ao mesmo tempo:

- cumprir os objetivos da política pública (“accountability”);
- tratar todos do público igualmente, dentro das regras (equidade);
- por senso de justiça, abrir exceções aos objetivos e regras, improvisando (“responsiveness”);

Esse conflito de metas é chamado pelo LIPSKY (2019) de paradoxo do burocrata do nível de rua. Diante desse paradoxo, como avaliar o burocrata? Como monitorar o burocrata? Observa-se ainda que o burocrata do nível de rua tem percepção de que a Administração não tem noção da realidade cotidiana, gerando abalo da legitimidade da hierarquia.

O sistema que costuma ser o preferido para o burocrata que cumpre a tarefa é de recompensa. No entanto, Oliveira alerta que:

(...) os sistemas de recompensa são efetivos quando podem medir acuradamente as contribuições individuais e a produção da organização. Se os índices para avaliar os resultados forem inapropriados, seja porque eles não têm como identificar os acréscimos individuais para o produto, seja

porque não medem as variáveis corretas, então o sistema de recompensas pode ser ineficiente ou até mesmo contraproducente (OLIVEIRA, 2013, p. 1558).

Tal sistema pode falhar de várias maneiras, entre elas, incentivar o “alvo errado”: a política ter um alvo mas a má interpretação ou “gaming” fazer com que o burocrata foque em outro; ou permitir o caronista (“free rider”): por causa de um indicador mal planejado, um grupo de burocratas pode não aderir à política pública e, mesmo assim, receberem a recompensa.

Fora o problema no desenho da política pública, cuja falta de clareza já dificulta o monitoramento da execução pelo burocrata, existem limites que mesmo uma política pública bem desenhada dificilmente conseguirá superar outros limites: a expectativa dos pares e as normas profissionais.

A expectativa dos pares está dentro da cultura organizacional da burocracia. Ela dita o comportamento médio que um burocrata espera do outro. Essa expectativa é verificável quando, ao ser determinada uma meta, percebe-se um comportamento médio dos burocratas, fazendo com que aqueles que saem da média, seja produzindo acima da média ou abaixo da média, sejam prejudicados pelos pares de alguma maneira. Os burocratas que sobem a média fazem com os demais pareçam ineficientes, enquanto aqueles produzem abaixo da média prejudicam a imagem de toda a categoria.

Já as normas profissionais são os limites regulamentares da atividade burocrática. Esses limites valem tanto para políticas públicas que, para o cumprimento, exigiriam que os burocratas operassem na “área cinzenta” da legalidade, na melhor das hipóteses, e o uso do regulamento para cumprir parcialmente, ou não cumprir, a política pública, como na comentada “operação-padrão”: com finalidade de protestar pelo atendimento de reivindicações classistas, os burocratas de nível de rua usam a burocracia para travar ela, seja pela inatividade, redução do ritmo de trabalho ou aumento do ritmo e observação de mínimos detalhes. Por exemplo, não é comum o policiamento apreender veículos automotores que não sejam produtos de crime, mas estejam com algumas irregularidades. Numa “operação-padrão”, o policiamento pode decidir não ter tolerância com irregularidades, mas com finalidade de se ocuparem e não ficarem à disposição da Administração – entre a espera do serviço de reboque e o fluxo de procedimento até o veículo ficar apreendido no pátio de depósito, os policiais ficam 3 a 4 horas indisponíveis para

atender outras ocorrências. Se todos policiais do turno decidirem fazer isso ao mesmo tempo, como forma de protesto, a região ficará sem policiais durante esse período.

A percepção da discricionariedade do burocrata de nível de rua não significa que haja um vácuo institucional. Para tal espaço, existe a burocracia de médio escalão, que tem como características:

- traduzir regras, procedimentos e esclarecer objetivos para os executores finais;
- são aqueles que tem a maior chance de identificar os erros e de intervir antes dos resultados indesejados ocorrerem;
- possuem ferramentas como: promoção, local de trabalho, tipo de tarefa, suavizar ou piorar o trabalho do burocrata. Ex. punição geográfica ou “bonde” (transferência involuntária de local de serviço).

Segundo Lotta, a burocracia de médio escalão “trata-se dos atores que desempenham função de gestão e direção intermediária (como gerentes, diretores, coordenadores ou supervisores) em burocracias públicas e privadas” (LOTTA et al, 2015, p.23).

Dentro ainda desse encontro de burocratas de nível e burocratas de médio escalão, também importa notar que é uma relação de conflito pela dependência mútua, onde os dirigentes precisam que servidores cumpram suas tarefas e os servidores desejam recompensas e evitar punições.

3.5.3 Burocratas na prática: dirigentes da SMSU e guardas civis

Analisar os burocratas é analisar as pessoas que estão cumprindo suas funções dentro de um órgão público, logo, enquanto dividimos a SMSU e GCM na abordagem organizacional, aqui caberá, para melhor entendimento, falarmos em burocratas de médio escalão, tanto na SMSU quanto na GCM, e burocratas de nível de rua, somente na GCM.

Estamos excluindo, propositalmente, os servidores administrativos da SMSU do conceito de burocrata de nível de rua. A “rua” do conceito é ter contato com o

público, ser a presença do Estado para a população, ter a discricionariedade para decidir quem receberá e como receberá a política pública. Isso não ocorre com os servidores administrativos da SMSU que, como já foi dito, não atendem o público e estão sob supervisão direta e imediata dos dirigentes (exemplo de burocratas de médio escalão), o que, por óbvio, impede a discricionariedade de “rua”, onde não há tempo ou oportunidade de consultar superiores para tentar sanar uma urgência.

Começando pelos burocratas de médio escalão, como definiremos quem faz parte?

LOTTA et al (2015), ao analisar os cargos “DAS” (Direção e Assessoramento Superior) do governo federal, definiu como burocrata de médio escalão os cinco primeiros níveis, descartando o sexto e maior nível, que é do próprio dirigente político:

Figura 2: níveis hierárquicos dos cargos de DAS do Governo Federal

DAS-101.6	Secretário de órgão finalísticos Dirigente de autarquias e fundações Subsecretário de órgãos da Presidência da República
DAS-102.6	Assessor especial
DAS-101.5	Chefe de gabinete de ministro de Estado Diretor de departamento Consultor jurídico Secretário de controle interno Subsecretário de planejamento, orçamento e administração
DAS-102.5	Assessor especial de ministro de Estado
DAS-101.4	Coordenador-geral
DAS-102.4	Assessor
DAS-101.3	Coordenador
DAS-102.3	Assessor técnico
DAS-101.2	Chefe de divisão
DAS-102.2	Assistente
DAS-101.1	Chefe de seção, assistência intermediária
DAS-102.1	Assistente técnico

Fonte: Art. 4º do Decreto nº 4.567, de 1º de janeiro de 2003.

Fonte: LOTTA et al, 2015, p. 16

Traçando uma analogia com esse quadro, podemos excluir o Secretário Municipal, pois ele exerce o cargo político, no âmbito da SMSU, bem como os assessores diretos dele. Mantendo-se o nexo entre a função exercida e o uso de informações de segurança, podemos afirmar que, no âmbito da SMSU, somente os dirigentes da Divisão de Parcerias e Cooperação Técnica (DPC), Divisão de Tecnologia da Informação e Comunicação (DTIC) e Divisão de Análise e Planejamento (DAP) podem ser considerados burocratas de médio escalão.

Enquanto isso, na GCM, considerando o grau de autonomia em relação à SMSU, mesmo sendo um órgão subordinado a esta, podemos excluir o comando geral da burocracia de médio escalão, restando o dirigente da Superintendência de

Planejamento (SUPLAN) e seus divisionários como médio de escalão, além dos inspetores regionais²³.

Os guardas civis metropolitanos preenchem todas as características de um burocrata de nível de rua: após uma preleção na Inspetoria, cumprem o horário de trabalho integralmente tendo contato com o público. Tomando como exemplo a “Operação Redenção”, a política pública implantada na região conhecida como Cracolândia, o guarda pode receber a missão de patrulhar a pé, permanecer numa base fixa ou patrulhar numa viatura. Como ele vai realizar essas missões, como ele vai lidar com os obstáculos que aparecerem, como ele vai atender os munícipes, como suas ações afetarão, ou não, os destinatários da políticas de segurança urbana são atividades que, mesmo com treinamento e protocolos, dependerão do guarda como serão realizadas.

Somando essas análises, percebemos que uma política pública que afete o público, seja ela proveniente da SMSU ou da própria GCM, dependerá da adesão dos guardas à não-ocorrência de falhas na implantação.

3.6 Por que analisar uma política pública?

Como fase preparatória ao diagnóstico e propostas para o uso de informações de segurança pública no âmbito da SMSU, estabeleceremos alguns pressupostos para analisar o que está acontecendo e como deveria estar acontecendo. Nas palavras de Arretche, “por análise de políticas públicas, entende-se o exame da engenharia institucional e dos traços constitutivos dos programas”. (ARRETCHE, 1998, p.2).

Começamos com os aspectos jurídicos, para termos noção de quais leis em vigor são mais pertinentes ao tema, não havendo necessidade de aprofundar.

Posteriormente, verificar o que a doutrina recomenda para análises de políticas públicas.

²³ Estivemos realizando levantamento de campo na Inspetoria 10, como paradigma de unidade territorial.

3.6.1 Aspectos jurídicos

Existe um repertório jurídico que possui relação direta com o tema deste trabalho, servindo de parâmetro e fundamento para análise de políticas públicas. Começando do documento mais fundamental de qualquer país, a Constituição Federal, o repertório inclui a legislação do Sistema Único de Segurança Pública (SUSP) e da Política Nacional de Segurança Pública e Defesa Social (PNSPDS). Sendo o uso de informação o liame das análises, é imperativo incluir a Lei Geral de Proteção de Dados Pessoais (LGPD) em tal repertório.

A LGPD é o marco legal que regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil, a norma pretende garantir maior controle dos cidadãos sobre suas informações pessoais, a mesma exige consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados.

3.6.1.1 *Princípios jurídicos*

A Constituição Federal de 1988 inovou ao abordar a Administração Pública, estabelecendo princípios que devem nortear todos os atos administrativos. Até então, as Constituições pretéritas se ocuparam apenas em estabelecer regras específicas, principalmente em relação aos servidores públicos.

Quando se adotam princípios, tanto o servidor quanto o gestor público possuem noção dos limites da discricionariedade de suas ações, sem precisar consultar algum rol taxativo do que podem ou não fazer.

O art. 37, caput, da Constituição de 1988 (BRASIL, 1990), com redação alterada pela Emenda Constitucional n. 19/98, definem como princípios que devem nortear a Administração Pública: legalidade, impessoalidade, moralidade, publicidade e eficiência. A redação não exclui a existência de outros princípios administrativos tidos como implícitos e aqueles expressos na legislação infraconstitucional

Para fazer o diagnóstico dos problemas que forem encontrados, alguns desses princípios tem papel fundamental.

O Princípio da Legalidade limita a Administração a fazer somente o que estiver previsto em lei. Embora a maioria dos gestores entenda tal princípio como uma camisa-de-força, é apenas um parâmetro para não ocorrer abusos na gestão.

O Princípio da impessoalidade trata de a impossibilidade de um ato administrativo ter a intenção de beneficiar ou prejudicar alguém especificamente. Todos os atos precisam ter como objetivo beneficiar ou prejudicar determinado perfil ou comportamento. O perfil que cumprir os requisitos da lei tem direito à aposentadoria. Quem cometer as condutas previstas na parte especial do Código Penal Brasileiro, em regra, está cometendo um crime. Todos os servidores públicos são vedados de realizar atos que beneficiem somente a si mesmos. Obviamente, se o ato do servidor for para um perfil em que ele se enquadra, em tese, não há problema. Um servidor que trabalhe em setor de pessoal, dando andamento em procedimentos de férias de outros servidores, também tem direito a usufruir de férias.

Considerando que este trabalho foi realizado visando a gestão pública, o princípio mais pertinente é o da eficiência. Di Pietro (2014, p.84) define com perfeição a aplicação deste princípio na gestão pública:

O princípio da eficiência apresenta, na realidade, dois aspectos: pode ser considerado em relação ao modo de atuação do agente público (grifado na redação original), do qual se espera o melhor desempenho possível de suas atribuições, para lograr os melhores resultados; em relação ao modo de organizar, estruturar, disciplinar a Administração Pública (idem), também com o mesmo objetivo de alcançar os melhores resultados na prestação do serviço público.

Essa definição da autora também fundamenta a análise de políticas públicas: se encontrarmos servidores/gestores que não estão desempenhando suas funções da melhor maneira; projetos que não foram bem elaborados, processos com falhas e tais coisas, de inopino, por desrespeito ao princípio da eficiência, teremos a justificativa para questionar e propor melhorias.

3.6.1.2 *Aplicação do SUSP e PNSPDS*

O Sistema Único de Segurança Pública (SUSP) foi instituído pela Lei federal n. 13.675/2018 (BRASIL, 2018), publicada em 11 de junho de 2018 e entrado em vigor

no dia de 11 julho de 2018. É uma lei com uma proposta inovadora em segurança pública, contrastando com histórico de ser uma área conhecida por ter legislações arcaicas. O mesmo diploma cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS).

O SUSP aborda diversos pontos, mas destacamos aqueles mais pertinentes com uma política pública de uso de informação da segurança pública.

O art. 9o, na seção em que aborda a composição do SUSP, atualiza o art. 144 da Constituição ao dizer que é “(...) integrado pelos órgãos de que trata o art. 144 da Constituição Federal, pelos agentes penitenciários, pelas guardas municipais (grifo nosso) ...” (BRASIL, 1990)

Ao falar da diretrizes da PNSPDS, em seu artigo 5o, percebemos a pertinência dos incisos que mencionam, como diretrizes, a coordenação e cooperação das instituições de segurança pública desde o planejamento até a avaliação de ações (inc.); sistematização de compartilhamento das informações de segurança pública (inc. VII) e uso de sistema integrado de informações e dados eletrônicos (inc. XXIII).

No art.10, quando discorre sobre o funcionamento da integração e a coordenação dos órgãos integrantes do SUSP, especifica que um dos meios é a “integração das informações e dos dados de segurança pública por meio do Sinesp” (inc. VI).

O financiamento, no que concerne a receber recursos da União, só ocorrerá se o município elaborar e implantar os seus planos correspondentes ao PNSPDS (art. 22, §5o).

3.6.1.3 *Marco Civil da Internet e LGPD*

A evolução das telecomunicações vem ocorrendo de forma exponencial. Em menos de vinte anos, saímos de uma internet “discada” e já estamos falando em internet 6G.

Isso fez com que os legisladores tivessem que correr em um ritmo não-natural para não deixar esses avanços tecnológicos ocorrerem em um ambiente caótico desregulamentado.

Diante disso, tivemos a publicação do Marco Civil da Internet (MCI), Lei federal n. 12.865/2014, em 23 de abril de 2014 (BRASIL, 2014), que estabeleceu diversos parâmetros para o uso da Internet no Brasil, consolidando legislações esparsas que existiam. Ela aborda questões de privacidade de usuários, na condição de consumidores dos serviços de internet, mas sem aprofundar a questão de dados.

Para regulamentar o tratamento de dados, protegendo os direitos de qualquer cidadão que tenha seus dados pessoais registrados por quaisquer meios, inclusive por meios digitais, foi elaborada a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei federal 13.709/2018 (BRASIL, 2018), com diversas alterações pela Lei federal n. 13.853/2019 (BRASIL, 2019).

Se depender de uma interpretação simplista do art. 4º, inc. II, “a”, que declara que a LGPD não se aplica quando o fim exclusivo do tratamento de dados for segurança pública, parecerá estranho ao tema deste trabalho mencionar a LGPD.

No entanto, a própria LGPD menciona em seu art. 1º, parágrafo único, que “as normas gerais (grifo nosso) contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios”.

Aplicando ao caso concreto, isso significa que o tratamento de dados elaborado pela SMSU e GCM devem seguir a LGPD, exceto quando for exclusiva para a segurança pública.

Bobbio (1995), quando elenca os diversos tipos de interpretação das leis, explica que a interpretação por meio teleológico é aquele baseado “(...) no motivo ou finalidade para os quais a norma foi posta” (BOBBIO, 1995, p. 214). Isso significa que ao falar da não-aplicabilidade da LGPD para informações de segurança pública, mas ao determinar que entes federativos devem seguir as normas gerais, a intenção do legislador é que as informações para fins de segurança pública não deveriam sofrer as restrições de tratamento das demais informações, pois a segurança pública está dentro do princípio da supremacia do interesse público sobre o privado.

Também temos uma situação fática que sustenta essa interpretação: considerando o fluxo de informações, nem sempre ela é coletada como segurança pública, podendo assim ser classificada posteriormente, logo, a coleta “genérica” inicial é regida pela LGPD e deixa de sê-lo quando é classificada como legislação de segurança pública.

Saindo da abstração, tomemos como base uma hipótese do SP+Segura: um cidadão, na opção de zeladoria urbana, e não de segurança pública, denuncia um

muro pichado. Isoladamente, é um caso de zeladoria urbana, indiretamente de segurança pública, logo, é uma informação regida pela LGPD. Porém, com o mapeamento permitido “Compstat”, é possível que seja possível identificar um padrão nas denúncias de pichação, levando a operações que visem prevenir a pichação, que, penalmente, é considerado um ato criminoso (Art.65 da Lei de Crimes Ambientais - pichar ou por outro meio conspurcar edificação ou monumento urbano). Em suma, as informações passaram a ser de segurança pública, saindo das restrições da LGPD, pois geraram uma atividade de policiamento preventivo pela proteção dos bens públicos, um dever constitucional expresso das guardas civis (art.144, §8 da Constituição Federal - os municípios poderão constituir guardas municipais destinadas à proteção de seus bens, serviços e instalações, conforme dispuser a lei).

Não menos importante, ressaltamos que, por diversos motivos, temos, cada vez mais, entidades da administração indireta e privada atuando em conjunto com os órgãos públicos da administração direta, através de convênios, doações e outras formas.

Na administração pública indireta da cidade de São Paulo, temos uma empresa de economia mista que atua com soluções de tecnologia da informação para toda a Prefeitura chamada PRODAM (Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo). A SMSU é um dos órgãos atendidos pelo contrato da PRODAM com a Prefeitura, não havendo a menor dúvida que a PRODAM, mesmo lidando com vários tipos de informações da SMSU, deve observar integralmente a LGPD.

Como exemplo de empresa privada, temos a empresa Vejo ao Vivo que, conforme publicação no Diário Oficial da Cidade de São Paulo de 20 de junho de 2017, foi autorizada a doar criação de website e pacote de sete dias de gravação em nuvem para a SMSU. Foi o ato inicial do City Câmeras:

Figura 3: despacho do Secretário sobre a doação City Câmeras

DESPACHOS DO SECRETÁRIO

6013.2017/0000849-5 - Secretaria Municipal de Segurança Urbana.- Proposta de doação de pacote de gravação nos termos do Edital de Chamamento Público 01/2017 – SMG.G. - À vista dos elementos contidos no presente, com fulcro no artigo 538 e seguintes da Lei Federal 10.406/02 (Código Civil), Decreto Municipal 40.384/01 alterado pelo Decreto Municipal 55.152/14 e no Edital de Chamamento Público 02/2017 – SMG.G, **AUTORIZO**, observadas as formalidades legais e cautelas de estilo, a doação da criação de website para o uso da Secretaria Municipal de Segurança Urbana, e pelo período de 02 (dois) anos contados da assinatura do Termo de Doação o pacote de 07 (sete) dias de gravação em nuvem para conexão de 1.000 (mil) câmeras e a liberação de acesso via aplicativo para os sistemas operacionais IOS e ANDROID para o uso Secretaria Municipal de Segurança Urbana – SMSU, serviços oferecidos em regime de doação, a ser firmado com a empresa **VEJO AO VIVO PUBLICIDADE E MONITORAMENTO LTDA.(9CL)**, inscrita no CNPJ sob o nº 05.818.541/0001-45.

Fonte: Diário Oficial da Cidade de São Paulo.

Não há a menor dúvida de que esse serviço doado precisará ser regido futuramente pela LGPD.

Em suma, a legislação, quando declara que tratamento de informações de segurança pública não estão sujeitos à LGPD, apenas desejou que a LGPD não fosse um obstáculo para a prevenção e repressão de crimes.

Apenas para complementar, em um estudo comparado tivemos a oportunidade de conhecer a legislação europeia que regulamentou a LGPD no âmbito dos países-membros da União Europeia, inclusive com menção aos casos de segurança pública.

O Regulamento (UE) 2016/679, de 27 de abril de 2016, publicado no Jornal Oficial da União Europeia em 4 de maio de 2016, possui conteúdo similar à LGPD, provavelmente tendo sido uma das inspirações do legislador. Em seu item 19, diz que:

A proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção (sic) e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos.

Tal conteúdo coincide com o dispositivo da LGPD que exclui a segurança pública.

Porém, na mesma data e jornal, também foi publicado o Regulamento (UE) 2016/680, que trata, numa análise breve, de todas as questões de LGPD quando for situação de segurança pública. Por exemplo, em seu artigo 6o, o Regulamento distingue as categorias de titulares de dados:

Os Estados-Membros preveem que o responsável pelo tratamento estabeleça, se aplicável, e na medida do possível, uma distinção clara entre os dados pessoais de diferentes categorias de titulares de dados, tais como:

a) Pessoas relativamente às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal;

b) Pessoas condenadas por uma infração penal;

c) Vítimas de uma infração penal ou pessoas relativamente às quais certos factos levam a crer que possam vir a ser vítimas de uma infração penal; e

d) Terceiros envolvidos numa infração penal, tais como pessoas que possam ser chamadas a testemunhar em investigações penais relacionadas com infrações penais ou em processos penais subsequentes, pessoas que possam fornecer informações sobre infrações penais, ou contactos (SIC) ou associados de uma das pessoas a que se referem as alíneas a) e b) ”.

Caberia aprofundar a reflexão sobre a existência de uma “LGPD - Segurança Pública” em andamento no Congresso Nacional ou projeto de lei de conteúdo similar ao Regulamento (UE) 2016/680, mas não é o alvo desta pesquisa. Esse art. 6o, embora não aplicável no Brasil, torna expresso o que a União Europeia considera informações de segurança pública e qual deve ser o seu tratamento específico, o que cobriria um vácuo deixado pela legislação nacional de LGPD. Esse vácuo de uma lei unificada resulta, novamente, em uma legislação esparsa e sem padrão, como decretos, resoluções e portarias dos entes federativos e seus órgãos.

3.6.2 Política Pública

Secchi (2017) trata de maneira completa o conceito de política pública: começa discorrendo sobre ser uma solução de um problema de repercussão coletiva, passa pelos nós conceituais (abordagem estatista, orientações persuasivas ou dissuasivas e questão de macrodiretrizes) até chegar na síntese que queremos: “(...) o problema

público é a diferença entre a situação e uma ideal possível para a realidade pública.” (SECCHI, 2017, p. 10).

De uma maneira simplista, poderíamos dizer que essa definição é o cerne deste trabalho: tendo o uso de informações de segurança pública no âmbito da SMSU como política pública, precisamos descobrir como ela está, através de observação direta e entrevistas; verificar o que impede que ela esteja ideal e, por fim, propor maneiras dela atingir esse ideal.

Seguindo o ciclo de políticas, temos em SECCHI (2017) a versão mais enxuta dele: identificação do problema, formação de agenda, formulação de alternativas, tomada de decisão, implementação, avaliação e extinção.

Sobre a fase de identificação de problema, no caso deste trabalho, podemos afirmar que é a fase que o precedeu: tínhamos conhecimento prático²⁴ de uso de informações na segurança pública e de aplicação²⁵ da LGPD, lei recém aprovada e com prazo para entrar em vigor, e suas consequências para empresas privadas e órgãos públicos; depois, pela experiências dos autores deste trabalho, os órgãos da segurança pública seriam os preferenciais, mas só haviam duas opções de fácil acesso: a Secretaria estadual de Segurança Pública (SSP) e a SMSU. Como haveria chance de ocorrerem conflitos éticos por um dos autores ser servidor público concursado da SSP²⁶, optou-se pela SMSU. Bastaram poucos contatos iniciais para haver a ampliação da abordagem para a análise e diagnóstico do fluxo de informações de segurança pública na SMSU e quais fatores favorecem, ou não, não somente a aplicação da LGPD em tal fluxo.

Em relação à formação de agenda, pode-se dizer que o tema deste trabalho está antecipando a agenda.

Brasil e Capella (2015) sintetizam a história e os modelos de agenda-setting. Nesses modelos, nota-se que a repercussão, seja na mídia, seja no público interno, seja nas instâncias políticas superiores, é uma das formas mais comuns para o problema merecer a atenção e obrigar os gestores a formularem alternativas. Não se espera que os problemas no uso de informações de segurança pública pela SMSU estejam no noticiário ou nos debates populares ou acadêmicos. Porém, a crise

²⁴ O autor Lívio José Lima e Rocha é investigador de polícia na Polícia Civil do Estado de São Paulo há mais de 20 anos.

²⁵ O autor Leonardo Fonseca Netto é engenheiro eletrônico e trabalha há anos na empresa multinacional NEC.

²⁶ Idem 18.

econômica, que gera problemas de arrecadação dos Poder público, desaguando na diminuição do orçamento de seus órgãos; a cobrança, cada vez maior, por diminuição dos gastos públicos, e a cobrança também de transparência, accountability e participação social, resultam no tema deste trabalho estar perfeitamente encaixado na “systemic agenda”, parte do conceito de agenda em níveis Birkland (BIRKLAND, 2005, apud BRASIL e CAPELLA, 2015): esse rol, com conceitos mais amplos, porém conexos com o tema, está tendo atenção da opinião pública atualmente.

Esta dissertação se trata da formulação de alternativas a serem entregues ao tomador de decisão, não sendo possível, pelo alcance reduzido, ir além dessa fase.

4 BENCHMARKING

A melhor referência para SMSU da Cidade de São Paulo é a Cidade de New York (EUA) que chegou a ter números altíssimos de criminalidade, como furtos, roubos, vandalismos e outros. No entanto, houve comprometimento de todos os níveis que tinham poder para agir e fazer algo diferente; partindo do Prefeito, chegando ao novo chefe de polícia e principalmente dos cidadãos que mais ganharam com uma cidade mais segura e respeitosa.

O chefe de Polícia foi realmente uma pessoa de destaque na qual sabia que aumentar o número de policiais não seria o jeito para resolver a criminalidade, por isto a liderança é fundamental, o chefe trabalhou para que houvesse investimento em tecnologia, pois sabia que sem a mesma seria difícil chegar a redução da criminalidade.

Com um grupo de trabalho foram definidas ações para que a tecnologia fosse empreendida de acordo com a maturação do trabalho dos policiais e assim usufruir o máximo e conseguir chegar às metas estabelecidas com o prefeito.

Uma das soluções adotadas foi o COMPSTAT (acrônimo para “compare stats”) é um sistema tecnológico de gerenciamento que adquiriu fama quando fez parte da política pública “Tolerância Zero”, implantada na Cidade de Nova Iorque, durante a gestão do prefeito Rudolph Giuliani e o então Comissário Bratton, chefe da polícia local. Ele combina uma avançada análise estatística com informações geográficas e o que há de melhor de princípios de gestão.

Segundo WILLIS et al (2007), o sistema, elaborado para direcionar a capacidade da polícia de reduzir a criminalidade, possui quatro fundamentos (WILLIS et al, 2007, p.148):

- Informação precisa e disponível para todos os setores do órgão;
- As táticas mais efetivas para problemas específicos;
- Emprego veloz e focado dos recursos para implementar as táticas;
- “follow-up” e monitoramento sem intervalos para compreender a ocorrência e elaborar ajustes;

WILLIS et al (2004) também identificaram outros seis fatores-chaves que se destacaram para os desenvolvimento de sistema como o COMPSTAT:

a-) clareza na missão: a burocracia de nível alto, incluindo o gestor político, são responsáveis por esclarecer e valorizar a função do órgão e o motivo de sua existência, o que inclui ter metas específicas as quais os membros do órgão e sua direção acreditam ser alcançáveis;

b-) “accountability” interna: o COMPSTAT torna a burocracia de médio escalão responsáveis por combater e reduzir a criminalidade e, quem falhar, sofrerá as consequências na carreira, por exemplo, ser removido do cargo de chefia;

c-) organização geográfica do comando operacional: o sistema é apropriado para unidades territoriais de policiamento (no Brasil, o que conhecemos como batalhões, delegacias e inspetorias regionais) e não para unidades especializadas. Estas deverão ser o comando das territoriais ou serão feitas alterações para que atendam às necessidades desse comando;

d-) flexibilidade organizacional: o órgão precisa desenvolver a possibilidade de mudar rotinas e recursos quando e onde forem necessários para a aplicação da estratégia;

e-) análise de problemas baseada em dados e avaliação dos esforços em resolução dos problemas pelos departamentos: os dados coletados e produzidos precisam servir para identificar e resolver problemas e monitorar as respostas dos departamentos;

f-) táticas inovadoras de resolução de problemas: é esperado dos policiais que, estimulados pelo COMPSTAT, procurem além de sua experiência, somando o conhecimento adquirido por outros departamentos, e do que houver de novas teorias sobre o crime.

A “Tolerância Zero” foi composta por outros elementos, principalmente zeladoria urbana, não só policiamento. Mesmo no policiamento, por exemplo, houve a contratação para dobrar efetivo. Além disso HAMMER & CHAMPY (apud WILLIS et al, 2007, p. 151), especialistas em desenvolvimento organizacional, à época contratado pelo comissário Bratton, acrescentam que a “reengenharia” de processos, para uma organização como a Polícia, que opera em cenários incertos, também requer: um compromisso da gestão e sua capacidade de estabelecer prioridades;

assegurar o apoio dos servidores; achar maneiras inovadoras de cumprir as missões e usar informações para direcionar o processo decisório, seguindo uma metodologia científica.

Essa abordagem sobre o COMPSTAT é o “benchmarking” mais apropriado para a análise do uso de informação de segurança pública na SMSU, por diversos motivos.

Inicialmente, no pacto federativo americano, o município possui as maiores responsabilidades dentro de sua circunscrição, incluindo o policiamento, sendo residual as competências estaduais (políticas públicas que afetem mais de uma cidade ou as fronteiras do Estado) e competências federais (políticas públicas que afetem mais um Estado, soberania e assuntos internacionais enquanto nação).

Como vimos, no Brasil, o município possui o poder de polícia, exceto pela atividade policial preventiva (polícias militares) e repressiva (polícias civis). No entanto, pela atuação na municipalidade e observação da zeladoria urbana, são as guardas civis brasileiras que mais se aproximam do modelo de policiamento americano regular.

Também temos uma questão atual: o COMPSTAT é adotado tanto pela Secretaria de Segurança Pública de São Paulo (SSP), órgão que subordina a polícia civil, militar e técnico-científica no âmbito do Estado, na forma do sistema conhecido como “Detecta”, o qual baseou o projeto Radar, exclusivo da Polícia Militar do Estado de São Paulo. Já foi comentado que o COMPSTAT também é a base das iniciativas da SMSU.

O COMPSTAT é uma ferramenta que tem como princípio ajudar, mas se não tivesse tido um desenho de solução e com processos definidos não teria a serventia na qual seria necessário para a Polícia de Nova York, pois não adianta ter a tecnologia se não souber usufruí-la ao máximo.

O COMPSTAT é um “framework” (“workflow” ou barramento) com a estratégia interna definida que interagir será essencial para as resoluções dos problemas que existiam; e o interessante que o sistema foi implementado independentemente do tamanho da polícia e as suas localidades (postos, delegacias ...) ou seja, a ferramenta veio para ajudar a todos os níveis mas precisa estar acessível à todos os níveis, a missão dos “gerenciadores” eram deixar uma ferramenta fácil com acesso e que os dados criados pudessem ajudar os policiais nas investigações.

O sistema foi criado para alterar os processos que existiam e que não funcionavam mais, pelo menos não de acordo com os números apresentados. Quando um sistema deste começa a ser implementado também existe um período de ajustes e adaptações, pois não se alteram processos e ações de um dia para outro, por isso é fundamental trabalhar desde cedo e muito bem com as alterações que virão para que não causem impactos desejados num processo existente.

Em suma, o COMPSTAT novaiorquino é um paradigma adequado para a aplicação da LGPD e reengenharia dos processos da SMSU e da GCM.

5 ACHADOS

A **gestão de informação de segurança pública** pela SMSU e pela GCM é uma linha condutora que está relacionada com diversos setores e servidores. É um processo com várias fases: **coleta, tratamento, encaminhamento, compartilhamento e uso da informação**.

Através da observação direta e entrevistas, encontramos diversos **problemas** que, em maior ou menor escala, estão relacionados com o tema desta pesquisa, ou seja, **afetam alguma (ou mais de uma) fase do fluxo de informação de segurança pública pela SMSU/GCM**. Chamaremos esses problemas de “**achados**”.

Começamos as pesquisas de campo conversando com o próprio Secretário da SMSU. Na oportunidade, foi-nos apresentados os principais produtos da Pasta: Dronepol, City Câmeras e SP+Segura²⁷.

É interessante notar que, ainda que de maneira simplificada, no folheto do “SP+Segura” possui um desenho aproximado do fluxo de informações de segurança pública:

Figura 4: fluxo de informações de segurança pública da SMSU



Fonte: folheto padrão do “SP+Segura”²⁸.

Logo tivemos o contato com o primeiro problema: nenhum dos autores da pesquisa, ambos moradores e trabalhadores de longa data na cidade de São Paulo,

²⁷ Vistos no item 3.2.

²⁸ Disponível na íntegra no Anexo VII.

inclusive com vivência na segurança pública estadual, sequer ouviram falar dessas louváveis iniciativas, exceto o City Câmeras. A pessoa E14, mesmo que se referindo apenas à GCM, disse que “(...) deveriam ser mais divulgadas para conhecimento da população, e demais órgãos de segurança”.

Essa situação nos leva ao **Achado nº 1: falta de divulgação das iniciativas**. Isso afeta diretamente a **coleta** e o **uso** de informações de segurança pública.

Vimos na introdução que as guardas municipais são parte integrante do Sistema Único de Segurança Pública (SUSP)²⁹. Mesmo assim, a realidade mostra que essa integração está deficitária.

Nesse sentido, verificamos que a SMSU não possui integração com a SPTRANS e o METRÔ, mesmo a SPTRANS sendo uma empresa de economia mista controlada pela Prefeitura Municipal de São Paulo. Os dados de segurança pública produzidos pela SMSU não são contabilizados pela Secretaria Nacional de Segurança Pública (SENASP/MJ), ou seja, não existem para as estatísticas criminais oficiais. Mesmo os convênios que foram estabelecimentos, como aqueles com a Polícia Militar e com a Polícia Civil, precisam ter suas reciprocidades revistas.

Tais observações podem ser agrupadas no **Achado nº 2: falha na integração com outros órgãos**. Isso afeta diretamente o **compartilhamento** de informações de segurança pública.

Até agora vimos problemas “da porta para fora”. Alguns entrevistados indicaram algumas questões que possuem as funções de TI como ponto em comum. A pessoa entrevistada E07 diz que “a Secretaria precisa investir mais em equipamentos (servidores, câmeras, nuvens etc.) cursos, e pessoal especializados em TI”.

Complementando, a pessoa entrevistada E02 comentou que:

A nossa Secretaria poderia investir mais em softwares (SIC) mais atualizados, para um trabalho perfeito, necessitamos de mais capacitação, cursos de aperfeiçoamento e não apenas o básico, pois o básico nós já temos, necessitamos nos aperfeiçoar com as novas tecnologias existentes no mercado.

Além desses testemunhos, o levantamento indicou, como foi comentado na visão política sistemática³⁰, que o setores de TI na SMSU e na GCM possuem indícios de tecnocracia. É emblemática a fala de uma pessoa, que preferiu manter o anonimato

²⁹ Sem deixar de lembrar a discussão sobre isso no item 3.3.

³⁰ Como foi visto no item 3.4.4.

completo, que tais setores de TI não mantêm contato suficiente com os demais setores e usuário, não compartilham algumas questões tecnológicas e, por vezes, tomam medidas sem consultar ninguém. Por outro lado, a pessoa entrevistada E09 defendeu que “a área de TI necessita de uma atenção especial, capacitação dos colaboradores e melhores equipamentos, hoje em dia é um setor primordial nas estruturas e não é muito reconhecido”.

A intenção do trabalho é que a SMSU esteja sempre preparada para alcançar suas metas e da melhor forma possível organizacional e tecnologicamente. Os problemas com TI anotados, somando a necessidade de capacitação dos servidores nisso, podem ser resumidos nas palavras da Comandante em entrevista aberta; “precisamos melhorar o relacionamento entre servidores e a tecnologia.”, o que nos leva ao **Achado nº 3: falha na administração dos serviços de TI**. Isso afeta diretamente o **tratamento** das informações de segurança pública.

Embora tenha relação com o TI, notamos um problema que merece uma atenção à parte: os formulários rotineiros dos guardas. São informações de segurança pública, desempenho, avaliação e gestão que alimentam o Sistema de Gerenciamento da GCM (SIG-GCM) e o Sistema de Gerenciamento de Pessoal e Competências (SIGPEC), cuja coleta se realiza por preenchimento manual de formulários físicos, controle por livros físicos e, por fim, inseridos no sistema por um outro guarda. Isso resulta em falhas como erro de preenchimento por letra ilegível e campos não-preenchidos; falta de transparência, dificuldade de auditoria dos dados, retrabalho e desperdício de tempo de todos servidores envolvidos no fluxo de informações. Se um superior precisar saber o que um guarda de plantão no dia anterior realizou, em termos de segurança pública, precisará consultar os formulários físicos ou aguardar a inserção no sistema, por exemplo.

Um guarda que assuma o plantão e precise de viatura automóvel (não esteja designado para o patrulhamento a pé, bicicleta...), receberá o Formulário de Inspeção de Viaturas³¹ e a Ordem de Serviço Externo³². Com ou sem viatura, se o guarda não exercer funções administrativas, precisará preencher o formulário duplo Roteiro Diário de Policiamento e Relatório de Atividades e Serviços. Esse formulário é conhecido como RAS³³.

³¹ Disponível no Anexo IV.

³² Disponível no Anexo III.

³³ Disponível no Anexo II.

Ouvimos relatos de que o SIG-GCM será integrado ao “compstat”³⁴ da SMSU. O “compstat” já é a base da iniciativas SP+Segura e City Câmeras. Não nos parece apropriado haver a integração do SIG-GCM enquanto não houver uma reengenharia dos processos que o compõe.

Como esse quadro possui diagnóstico próprio, distinto daqueles para o Achado n. 3, resolvemos isolar este como **Achado n. 4: falha nos processos rotineiros da GCM**. Isso afeta a **coleta** e o **tratamento** das informações de segurança pública.

O City Câmeras é hoje o principal projeto de segurança da SMSU, ou seja, o que tem maior repercussão. Embora use recursos tecnológicos de terceiros, a segurança de TI sobre o sistema precisa ser redobrada.

Por isto o nosso trabalho é fortalecer a SMSU com ações referente à LGPD que entrará em vigor a partir de agosto de 2020, pois as informações sensíveis precisarão estar bem protegidas e respaldadas, ou seja, precisam ter arquitetura de TI e processos bem definidos.

A adaptação de todo o fluxo de informações de segurança pública às normas gerais da LGPD é um problema que tem relação em maior grau com o City Câmeras, o que será objeto de maior aprofundamento como o **Achado n.5: adaptação da SMSU à LGPD**. Isso afeta o **tratamento** e o **uso** de informações de segurança pública.

³⁴ “compstat”, como vimos no item 4, é uma metodologia, não um software. O software é uma versão do Microsoft Dynamics, como o Detecta da SSP. Mas é chamado de “compstat”.

6 FORMULAÇÃO DE PROPOSTAS

Após uma análise fundamentada em conceitos estudados e pesquisa de campo, passamos a fase seguinte do ciclo de políticas públicas: formulação de alternativas.

Dentro do modelo proposto por Spink (2017, p. 263), diante da impossibilidade de maior aprofundamento, consideramos mais pertinentes responder nesse fase:

- quais os objetivos e metas mais importantes;
- quais atividades para atingir esses objetivos e metas;

Sobre a formulação de alternativas, considerando a classificação elaborada por Secci (2017, p. 49) para induzir determinados comportamentos, as soluções para o tema requerem, de maneira mista, soluções técnicas e conscientização, não parecendo ser o caso de premiação ou coerção, talvez após uma avaliação de impacto.

No geral, estamos tratando de mudança de conscientização para aperfeiçoar o uso de informações de segurança pública no órgão, acompanhada por algumas mudanças tecnológicas, em maior ou menor grau dependendo do problema encontrado, como veremos no capítulo sobre propostas de soluções.

Em relação ao modelo de decisão, conforme definições de Wu et al (2014), seguimos o modelo de decisão “incremental”: todos os envolvidos (autores e atores) tem restrições de tempo, informações e recursos que impedem a procura pela decisão “racional” e não temos intenção de alterar o sistema de forma brusca.

Resumindo, estamos buscando a melhor forma de realizar os processos, o que é definido por Martins e Marini (2010), dentro do modelo proposto por eles chamado “Gestão Matricial para Resultados”, como excelência, um dos componentes da dimensão de esforço.

6.1 Propostas para o Achado n.1

Não há necessidade de maiores estudos e constatações para afirmar que uma política pública que requer a adesão do público interno e/ou externo não está atingindo seus objetivos se não está ocorrendo essa adesão.

No caso do City Câmeras, por exemplo, a prioridade é adesão do público externo da SMSU: quanto mais as pessoas compartilharem suas câmeras com o sistema, maior será a cobertura. Já para uso interno da SP+Segura e SIG-GCM, o alvo seria o público interno.

A adesão do público precisa de um planejamento estratégico de comunicação, com base no conhecimento específico em publicidade. Por mais que existam Secretarias, departamentos e assessorias de imprensa no Poder Público, não é sobre essa atividade a falha. Quando recomendamos publicidade das iniciativas, estamos falando de metodologia, métricas e outras ferramentas que garantam que a mensagem está chegando de forma adequada e eficiente ao destinatário. Isso não se confunde a atividade de relações públicas ou assessoria de imprensa³⁵.

Esse quadro nos leva a duas possibilidades: contratação de empresa de publicidade de imprensa, através de licitação ou doação, ou estabelecimento de um planejamento com recursos próprios.

6.1.1 Contratação de terceirizada

A Lei federal n. 12.232/2010 (BRASIL, 2010) fornece todo o arcabouço jurídico para a licitação e contratação de empresa de publicidade. Destacamos o art. 2º, onde está o objetivo desta proposta:

Art. 2º. Art. 2º Para fins desta Lei, considera-se serviços de publicidade o conjunto de atividades realizadas integradamente que tenham por objetivo o estudo, o planejamento, a conceituação, a concepção, a criação, a execução interna, a intermediação e a supervisão da execução externa e a distribuição

³⁵ No Brasil, a atividade de jornalismo e assessoria de imprensa são ensinadas no Bacharelado em Comunicação Social com ênfase em Jornalismo, enquanto a atividade de publicidade e propaganda é no Bacharelado em Comunicação Social com ênfase em Publicidade e Propaganda.

de publicidade aos veículos e demais meios de divulgação, com o objetivo de promover a venda de bens ou serviços de qualquer natureza, **difundir ideias ou informar o público em geral. (grifo nosso)**

Do ponto de vista da gestão pública, a lei, em seu art.3o, expressamente determina que deverá existir uma métrica para avaliar o impacto da execução do contrato, algo que não é frequente em leis licitatórias e conexas.

Também percebemos itens de gestão pública quando, no seu art. 7o, ela exige que a proposta técnica das empresas concorrentes tenha: diagnóstico das necessidade, estratégia de comunicação publicitária, ideia criativa e estratégia de mídia e não-mídia.

Temos um exemplo de edital de concorrência de 2017 do Ministério do Desenvolvimento Social³⁶ onde podemos verificar, entre outros detalhes:

- declaração expressa de que segue a Lei. 12.232/2010³⁷;
- reproduz o conteúdo dos citados arts. 3o e 7o. dessa lei ao descrever o objeto da licitação;

A única limitação que vislumbramos nessa proposta é a questão financeira-orçamentária, caso não seja possível uma doação do serviço através de chamamento público.

6.1.2 Solução orgânica

Depender dos servidores disponíveis para substituir a função de uma empresa de publicidade não é algo que possamos recomendar, por questões jurídicas.

Como não é função da SMSU executar ações de publicidade, é vedada a contratação de servidores com essa função. Mesmo que haja em seus quadros funcionários com conhecimento técnico para publicidade, não seria a função para o

³⁶ É um edital com mais de 80 páginas, sendo inviável sua reprodução na íntegra neste trabalho. Está disponível para leitura em <http://mds.gov.br/acesso-a-informacao/licitacoes-e-contratos/edital-no01-2017-contratacao-de-servicos-de-publicidade>

³⁷ A lei é citada diversas vezes no edital, tornando obrigatória sua aplicação aos contratos de publicidade.

qual foram contratados, caracterizando o desvio de função. Caberia indenização ao servidor obrigado a ter essa função e caberia improbidade administrativa ao gestor por enriquecimento ilícito do Estado (exige função à mais, mas não remunera por isso).

Isso não significa que a SMSU não possa adotar outras medidas para a publicidade de suas iniciativas, sem que caracterizem a citada improbidade.

Partindo de um planejamento estratégico, à semelhança do que valeria para uma empresa contratada, a SMSU pode analisar as possibilidades não-onerosas de publicidade (como o uso comum de redes sociais). Redes sociais como o Facebook fornecem, gratuitamente, algumas métricas para as publicações de páginas institucionais. Nada próximo ao gerenciamento do algoritmos que uma empresa profissional faria, mas ainda melhor que a inércia. Essa opção poderia ser executada tanto pela burocracia de médio escalão da SMSU quanto da GCM.

Uma segunda possibilidade envolveria os servidores da GCM: palestras sobre as iniciativas em prédios, associações e grupos afins em suas regiões de atuação. Não foge às atribuições de qualquer servidor público esclarecer as ações de seu órgão. Ressaltando, novamente, que dentro um planejamento estratégico, seria necessário elaborar os insumos, produtos e ter uma métrica para os resultados esperados. Essa abordagem exigiria a Administração da SMSU e da GCM rever alguns conceitos que já foram vistos neste trabalho, especificamente o reconhecimento dos guardas civis como burocracia de nível de rua, fundamental para a implementação desta estratégia.

Como foi visto, é necessário o engajamento dos guardas à iniciativa, através de ferramentas de conscientização. Isso caberia para todo o efetivo: qualquer guarda precisa ser capaz de oferecer um mínimo de informações sobre as iniciativas da SMSU para qualquer cidadão. Porém, não caberia uma exigência nesse nível de burocracia.

Já para a burocracia de médio escalão, em especial aqueles com função de chefia nas inspetorias regionais, além da capacitação, seria possível estabelecer metas de palestras em agrupamentos urbanos em sua região de trabalho: escolas, associações, condomínios, podendo ainda aproveitar as reuniões do Conselho Comunitário de Segurança (CONSEG) ou mesmo as reuniões do Conselho Participativo Municipal. Como a adesão dos munícipes depende de fatores alheios ao

controle dessa chefia, seria adequado apenas avaliar o desempenho pelo esforço dos chefes, não pelo resultado, seguindo o modelo de Martins e Morini (2010).

Não menos importante, é necessário ressaltar que, mesmo havendo a opção pela terceirizada, as soluções orgânicas não são excludentes desta, principalmente para o público interno. Por exemplo, as palestras pelas chefias regionais da GCM podem fazer parte da estratégia da empresa contratada, de forma complementar. Por outro lado, o treinamento e capacitação do público interno pode ser gerado pelo centro de formação da GCM ou a empresa pode treinar apenas os agentes multiplicadores, sendo atribuição destes repassar o conhecimento.

6.2 Propostas para achado nº 2

Temos três frentes para lidar com esse achado: federal, estadual e municipal.

No âmbito federal, há necessidade de estabelecer contato pelas vias oficiais com a Secretaria Nacional de Segurança Pública (SENASP) e verificar quais são os quesitos para:

- compatibilizar as estatísticas criminais da SMSU com aquelas da SENASP;
- a SENASP disponibilizar acesso, ainda que restrito aos burocratas de médio escalão, dos sistemas federais, como o INFOSEG e, para todos servidores da SMSU, os cursos EAD³⁸;

A formalização de tais acertos seria através de assinatura de convênio, do ponto de vista estritamente jurídico. Não podemos menosprezar que cabe um empenho político da SMSU ou mesmo da Prefeitura para concretizar tal intento, talvez com apoio dos parlamentares dos partidos envolvidos.

Se há um convênio em andamento com o governo estadual, ele certamente não parece satisfatório para ambas as partes.

³⁸ Temos conhecimento que os guardas civis podiam realizar os curso do EAD-SENASP. A dúvida permanece em relação aos servidores não-guardas da SMSU.

Assim como visto em relação ao governo federal, precisa haver uma compatibilização das estatísticas estaduais e municipais e acesso recíproco entre os sistemas da SSP (e suas forças policiais) e da SMSU (em especial a GCM).

Devemos lembrar que, como todas políticas públicas, não é apenas a cessão de “login” entre as Pastas. Cabe estabelecer ferramentas de monitoramento e avaliação.

As ferramentas de monitoramento auferem, ininterruptamente, se o uso dos sistemas está adequado pelo partícipes do convênio. Já as avaliações, numa frequência mensal, por exemplo, poderiam analisar o impacto dos acessos aos sistemas: houve melhoria de atividade de fiscalização de zeladoria urbana da SMSU resultante do acesso às pesquisas criminais e civis da Polícia Civil? Houve melhoria no policiamento preventivo ostensivo da Polícia Militar ao SP+Segura? E daí por diante.

Também temos o interesse da SMSU na parceria com o Metrô. Trata-se de uma empresa pública subordinada à STM (Secretaria de Estado dos Transportes Metropolitanos). Para haver uma parceria, assim como com a SSP, requer um termo de convênio ou cessão, cabendo as observações feitas anteriormente.

O maior interesse nas parcerias dentro do município está no acesso às câmeras, em especial aquelas que pertencem à SPTRANS (Secretaria Municipal de Mobilidade e Transporte). Como são Pastas que pertencem ao mesmo governo subnacional, a Prefeitura da cidade de São Paulo, qualquer formulação de convênio ou mera cessão de acesso dependeria de critérios técnicos (qual tecnologia empregada na câmeras das SPTRANS, qual a compatibilidade com os sistema da SMSU e fatores afins) e de vontade política dos atores envolvidos, principalmente do prefeito.

6.3 Propostas para o Achado n. 3

Este achado é um resumo do problemas da Administração com seus setores de TI. Embora estejamos falando do setor de tecnologia, as propostas não passam por análise de equipamentos, neste momento. Passam por algumas mudanças organizacionais.

6.3.1 Setor de TI da SMSU

Para o setor de TI da SMSU, fisicamente e organizacionalmente mais próximo ao gestor político da Pasta, recomendamos a formulação de seu planejamento em sintonia com o planejamento da Pasta.

Inicialmente, notamos que existe uma demanda para melhor entendimento dos sistemas, não só como funcional como para que servem. Assim, especificamos a identificação, valorização e capacitação como problemas.

Para resolver esses problemas, precisamos estimular a participação dos servidores e oferecer treinamentos constantes, para termos servidores mais dedicados e capacitados, tornando o setor de TI mais integrado ao planejamento da Pasta.

O devido funcionamento do setor de TI da SMSU decorrerá de aquisição de equipamentos adequados ao planejamento; reuniões de preleção, oportunidade em que o servidor pode sugerir alguma melhoria aos processos e o coordenador atualizá-los dos andamentos e próximos passos das iniciativas do setor; capacitação, no mínimo mensal, via EAD ou presencial, para manusear os processos atuais ou atualização em algum aspecto importante do trabalho.

Após um prazo médio, os servidores poderiam ser submetidos novamente a um formulário como aquele a que foram submetidos para este trabalho. Seria a melhor maneira de avaliar se as mudanças causaram o impacto desejado.

6.3.2 Setor de TI da GCM

Separamos o setor de TI da GCM porque ele possui uma particularidade distinta do setor de TI da SMSU: ele é formado integralmente por guardas civis, logo, são burocratas de nível de rua³⁹ que, porventura de um avanço profissional ou especialização ou cargo de confiança, estão em funções administrativas relacionadas à TI.

³⁹ Como vimos no item 3.5.3.

Vimos que a falha são de mão dupla: os servidores sentem-se isolados da Administração e, ao na outra mão, sofrem alegações de tecnocracia.

O modelo lógico elaborado para o setor de TI da SMSU é válido para o da GCM, porém, caberia uma alteração organizacional: protocolos eletrônicos.

Não basta o setor de TI seguir o planejamento da GCM, ter reuniões de preleção com o comando da GCM. Para recuperar o pertencimento e diminuir o sectarismo, os servidores deste setor precisam ter contato com quem continua na linha de frente, na rua. Como é inviável a realização de reuniões, dada a quantidade de servidores na rua, recomendamos a elaboração de um protocolo eletrônico de comunicação.

O desenho aproximado seria:

- todas solicitações ou sugestões dos servidores da rua para o setor de TI seriam através de meios eletrônicos, preferencialmente um “login” na intranet, com acesso individualizado;
- para evitar um volume exacerbado de mensagens, novamente lembrando o contingente da GCM, o servidor é cientificado que a mensagem segue em cópia para o seu superior imediato, para que não haja “bypass” da hierarquia;
- a solicitação é registrada e o servidor recebe um número para acompanhamento da solução. O superior dos serviços de TI recebe e repassa para o seu servidor com atribuição para resolver a solicitação;
- o solicitante será cientificado quando o problema for resolvido ou receberá a justificativa da impossibilidade de resolvê-lo.

Nesse desenho, o setor de TI terá subsídios para entender quais são as demandas mais frequentes de quem está na rua, o que, sem dúvida alguma, justificará alterações em seu planejamento e demandas para a sua Administração superior, seja o comando da GCM ou a própria SMSU.

Assim como na proposta para o setor de TI da SMSU, submeter os servidores ao mesmo questionário que foram submetidos neste trabalho, após um médio prazo, será uma forma de válida de analisar o impacto dessas mudanças.

6.4 Propostas para o achado n. 4

As falhas nos processos rotineiros da GCM se referem, especificamente, aos servidores que estão nas ruas, cumprindo escalas de trabalho, tendo contato direto com o cliente: o cidadão.

Sem muita reflexão, parecem ser problemas meramente administrativos, sem relação com o uso de informações de segurança pública pela SMSU.

Não é assim que entendemos.

Mesmo sem ter medido quantitativamente quanto tempo um guarda civil metropolitano dedica seu horário de trabalho para o preenchimento de todos os relatórios, a mera leitura de alguns relatórios preenchidos, durante a pesquisa de campo, foi condição suficiente para notar, entre outras coisas, que:

- o tempo gasto no preenchimento poderia ser reduzido;
- os servidores envolvidos com o registro inicial (quando o guarda escalado recebe os formulários) e com o registro final (lançar no sistema as informações de cada relatório de cada guarda) poderiam ter outras funções com a implementação de soluções tecnológicas;
- os burocratas de médio escalão poderiam ter informações mais atualizadas e planilháveis com o aperfeiçoamento dos processos;
- os tomadores de decisão teriam informações melhores para elaboração de suas estratégias e formulação de alternativas se os processos fossem mais confiáveis;

Como os relatórios podem ser agrupados em gerenciamento de frotas e relatórios de atividades, requerem algumas propostas distintas, dadas as peculiaridades.

6.4.1 Gerenciamento de frota

Pela quantidade e tipo de informações a serem fornecidos no relatório de uso de viatura⁴⁰, notamos a semelhança com os formulários de aluguel de veículos. Questionamos alguns servidores sobre a natureza patrimonial das viaturas e fomos informados que todas as viaturas da GCM são alugadas.

Em que pese a economia gerada pelo aluguel da frota, e não aquisição, uma medida de gestão moderna adotada por diversas polícias do Brasil, não justifica sobrecarregar cada guarda que for usar a viatura com um processo físico de vistoria em papel.

Como a empresa vencedora é a parte interessada na conservação das viaturas, pelo fato da manutenção ser responsabilidade dela também, o gestor do contrato pode renegociar com a empresa para que esta desenvolva e forneça um aplicativo de celular que substitua os formulários de papel.

Tal aplicativo resultaria em diversas vantagens para a empresa e para o gestor da frota da GCM:

- ambos teriam informações precisas e atualizadas sobre a conservação das viaturas;
- em caso do guarda responsável encontrar danos na funilaria ou na parte interna, o aplicativo poderia aceitar o armazenamento e envio de fotos;
- o gestor da frota teria subsídios para apresentar ao comando da GCM quais as atividades da GCM que possuem maior chance de causar danos às viaturas, quais os modelos de veículos são mais ou menos resistentes para a atividade da guarda, quais inspetorias possuem melhor índice de conservação da frota, qual a vida útil dos veículos e outras;
- as informações precisam ser protegidas e divulgadas somente as pessoas com as suas respectivas responsabilidades, pois assuntos relacionados à segurança não podem ser expostos ao mundo internet.

⁴⁰ Disponível nos Anexos III e IV.

Essas informações coletadas podem levar a GCM a alterar os próximos editais para locação de veículos, estabelecendo condições para as empresas licitantes que levem a GCM a prestar um melhor serviço para a sociedade.

Se não for possível exigir que a empresa adote essa solução, a alternativa seria a contratação, por licitação, de uma empresa desenvolvedora de sistemas e programas para que elaborasse esses sistema de gerenciamento de frota. Com base na experiência dos autores deste trabalho, o custo seria por volta de R\$50.000,00. Trata-se de uma despesa com natureza econômica de custeio, podendo ser inserida em um orçamento anual ou de ser obtido por emenda parlamentar. Para contextualizar o esse valor, o projeto de LOA 2020⁴¹ da Prefeitura de São Paulo indica uma expansão orçamentária para Segurança de 6,7% em relação ao ano anterior, totalizando R\$693 milhões em 2020.

Dentro das exigências para a empresa que desenvolvesse o sistema de gerenciamento de frota, deve-se propor que haja uma avaliação anterior de como estão processos, para, após um prazo médio da implementação, o gestor do contrato ter parâmetros para a avaliação de impacto.

Como é um processo ligado diretamente ao servidores que estão na rua, deve ser exigido o treinamento de todos os servidores, evitando assim o boicote e aumentando a adesão.

6.4.2 Relatórios de atividades

Enquanto o sistema de frotas visa apenas a conservação das viaturas e minimizar o gasto de tempo dos guardas dedicados ao preenchimento dos dados, aperfeiçoar os relatórios de atividades⁴² significa aperfeiçoar diretamente a gestão do uso de informações de segurança pública pela SMSU e GCM.

As observações sobre o tempo perdido com relatórios de papel no gerenciamento de frotas são igualmente válidas para os relatórios de papel de

⁴¹ Lei Orçamentária Anual disponível em

<http://orcamento.sf.prefeitura.sp.gov.br/orcamento/proposta.php> acessado em 30out2019

⁴² Disponível nos Anexos III e IV.

atividades: temos burocracia demasiada, temos retrabalho, temos funções sobrepostas, temos atrasos na atualização.

Inicialmente, caberia uma análise pormenorizada sobre os campos do relatório, uma que seria similar àquelas que deram origem a este trabalho:

- Todos os campos são imprescindíveis?
- Quais as informações que influenciam o planejamento do órgão?
- Quais as informações que os superiores precisariam saber de forma atualizada? Quais não teriam urgência?
- Quais informações seriam compartilhadas com outros sistemas da GCM e SMSU? Quais poderiam ser compartilhadas com outros órgãos?
- Quais são, exatamente, as informações de segurança pública? E de avaliação de desempenho funcional? Algumas tem mais de uma função?

Podemos elaborar uma proposta básica, que seria ajustada conforme as respostas obtidas.

Aproveitando a proposta do gerenciamento de frotas, aqui também teríamos o preenchimento de relatório por aplicativo de celular, ligado à intranet. Mesmo havendo uma pluralidade de informações a serem preenchidas, verificamos que quase todos os campos são de múltiplas escolhas, facilmente selecionáveis por cliques em uma tela sensível ao toque.

Os gestores, médio e alto escalão, também teriam informações atualizadas, aptas para avaliar desempenho, planejamento e impacto das políticas públicas da SMSU e da GCM, além de alimentar os demais sistemas da SMSU e GCM.

Novamente, a política precisa incluir ferramentas de capacitação e conscientização, pois o sistema novo pouco adiantará se não houver adesão dos servidores na rua.

6.5 Propostas para o Achado n. 5

A SMSU, para seguir a LGPD, precisará criar e recriar, principalmente, processos internos que façam com que ela esteja se protegendo contra o vazamento de dados pessoais, tanto de cidadãos quanto dos seus funcionários, e fazer um

desenho arquitetônico de solução de segurança de TI com que faça que os dados fiquem protegidos.

Primeiramente, precisa fazer o processo com que somente algumas pessoas da SMSU tenham acesso aos dados pessoais e consequentemente sensíveis, não são todos que poderão ter acesso ao mesmo. Um exemplo disso são os bancos: os funcionários que têm acesso à algumas informações dos clientes, não tem porta “USB” no seu micro, ou seja, para que não copiem as informações, e os seus e-mails estão sendo sempre investigados, tanto o profissional quanto o pessoal, que é aberto na rede do Banco, se o funcionário tiver acesso.

A SMSU precisará criar uma política de proteção de dados⁴³, pois lá terá a definição e responsabilidade de cada funcionário, representando todas as camadas da hierarquia do órgão, e as premissas que a SMSU espera de qualquer fornecedor que venha a trabalhar com ela, em fornecimento de equipamentos e de solução, que estarão interfaciando com os dados do órgão, independentemente do conteúdo.

O trabalho que será feito não estará pronto em dias: serão semanas, pois precisarão obter as informações e assim determinar como protegê-las e usá-las. Após a criação da política, a SMSU precisará identificar os dados pessoais existentes em toda a sua organização, verificar a identificação do ciclo de vida dos dados, desde a coleta até a eliminação; fazer o inventário, classificar os dados pessoais de acordo com a LGPD, nisto fazer a integração com a política já definida; analisar os principais modelos de contrato da organização, no âmbito de relação com parceiros, colaboradores; estabelece o programa de privacidade e proteção, elaborar o plano de ação com as medidas corretivas, processar e classificar conforme criticidade, identificar as bases de dados para tratamento; trabalhando diretamente na TI, criar o relatório “Security Checkup” da infraestrutura, avaliar os níveis de aderência à LGPD em toda a organização, definir as diretrizes de adequação junto à LGPD, definir e avaliar os riscos no âmbito da organização em relação aos requerimentos; Mapa dos principais contratos afetados pela LGPR, definição do processo de capacitação com calendário de workshops e atividades de conscientização.

No próximo item, explicaremos melhor a questão da LGPD.

⁴³ Como a que estamos sugerindo no Apêndice II.

7 ANÁLISE DA LGPD

Em 14 de Agosto de 2018 foi sancionada a Lei 13.709, conhecida como LGPD (Lei Geral de Proteção de Dados Pessoais; esta lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

As normas gerais contidas nesta lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. A disciplina de proteção de dados pessoais tem como fundamentos:

- I – O respeito à privacidade;
- II – A autodeterminação informativa;
- III – a liberdade de expressão, de informação, de comunicação e de opinião;
- IV – A inviolabilidade da intimidade, da honra e da imagem;
- V – O desenvolvimento econômico e tecnológico e a inovação;
- VI – A livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Figura 5: principais Obrigações do LGDP



Fonte: retirado do site <https://www.protiviti.com/BR-por/protecao-de-dados-pessoais>

Após a publicação da LGPD, ficou definido que 14 de agosto de 2020 é a data em que usuários e empresas deverão estar oficialmente seguindo-a: obrigará que empresas e órgãos revisem todo o tratamento de dados pessoais que esta obtém e processa; os dados pessoais quando isolados já são, por sua natureza, intrinsecamente ligados às nossas percepções de privacidade e intimidade. A associação destes entre si poder gerar efeitos surpreendentes em tempo de tecnologias que se encontram facialmente como Big Data, Deep Learning e Deep Fakes.

Estas tecnologias definem bem como interpretar as redes neurais das pessoas, obtendo assim informações comportamentais, interesses, assim podem avaliar qual será o programa de TV que desejaremos ver, que nos avise do melhor caminho no trânsito para o nosso próximo compromisso mesmo que não esteja anotado em uma agenda, mas de repente veio via e-mail ou mensagem celular.

As biometrias como face, a voz, a retina e as digitais de um indivíduo que permitem identifica-lo de forma única, serão cada vez mais utilizados em sistemas neurais, que trarão todo tipo de facilidade moderna a essa pessoa, assim como tonarão seus gostos, comportamentos, deslocamentos, relacionamentos e conta bancária cada vez mais rastreáveis, mapeáveis e previsíveis.

Vejam que os dados de uma pessoa estão sempre circulando, sendo enviadas, postadas e compartilhadas; claro que depende do motivo, de um acordo com um prestador de serviço; mas a confidencialidade dos dados pessoais, não poderão ser divulgadas sem autorização do dono, com restrições severas ao compartilhamento ou por motivo relacionado à segurança.

O principal motivo da LGPD é trazer uma obrigação severa, no mesmo nível europeu⁴⁴, de todo aquele que coleta, armazena ou trata as informações pessoais, especialmente sensíveis, deverá seguir padrões mínimos de segurança com relação a tais informações, bem como deixar extremamente claro ao usuário em suas políticas de privacidade e termos condições de uso como utilizará e com quem compartilhará tais informações.

⁴⁴ Alguns dados sobre a LGPD na Europa estão no Anexo VIII.

7.1 A Lei e o Setor Público

Além do que já explicamos⁴⁵, para compreender qual o impacto que a Lei Geral de Proteção de Dados terá em cada ente que compõe o Setor Público é mister recorrer às definições fornecidas pelo Direito Administrativo no tocante a sua constituição:

O ordenamento jurídico brasileiro submete as variadas hipóteses de atuação da administração pública, nos três poderes e em todos os níveis da Federação, ora a um regime jurídico tipicamente de direito público, ora a normas oriundas predominantemente do direito privado (ALEXANDRINO; PAULO, 2017, p. 11).

Determinar qual a natureza jurídica do ente e em qual interesse age – se no interesse público e em sua finalidade ou em regime concorrencial – no caso concreto é o primeiro passo para identificar como a LGPD a ele se aplicará.

A nova lei dedica um capítulo com nove artigos (Capítulo IV) exclusivamente para abordar o tema “Tratamento de Dados Pessoais pelo Setor Público” e indica que a integração com a LAI é necessária ao fazer referência expressa em seu artigo 23 o qual transcrevemos:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019)

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019) (...)

⁴⁵ Ver Item 3.6.1.3.

Entendemos que é nesse ponto que reside uma das grandes complexidades no tratamento dispensado aos entes públicos pela LGPD, uma vez que pode acontecer de o mesmo dado ao ser utilizado para finalidades diversas requerer o atendimento de requisitos diversos.

Necessário chamar a atenção para a equiparação realizada pelo art. 23, §4⁴⁶ que atribui aos serviços notariais e de registro exercidos por delegação o mesmo tratamento dispensado aos entes públicos quando necessitarem realizar o tratamento de dados pessoais.

Apesar de não estarem dentro do escopo da LGPD e, portanto, não sujeitos às disposições sobre proteção de dados por ela trazidas, a própria LGPD estabelece algumas limitações ao tratamento de dados para essas finalidades, todas elas contidas nos incisos do seu Artigo 4º:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

- I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- II - realizado para fins exclusivamente:
 - a) jornalístico e artísticos; ou
 - b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
- III - realizado para fins exclusivos de:
 - a) segurança pública;
 - b) defesa nacional;
 - c) segurança do Estado; ou
 - d) atividades de investigação e repressão de infrações penais; ou
- IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Esses tratamentos de dados serão regidos por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei; Só será admitido o tratamento de dados para tais finalidade por pessoa jurídica de direito privado em procedimentos sob a tutela de pessoa jurídica de direito público, sendo certo que os dados pessoais constantes de bancos de dados constituídos para tais finalidades não poderão ser

⁴⁶ “§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.”

tratados em sua totalidade por pessoas jurídicas de direito privado, exceção feita às controladas pelo Poder Público.

7.2 Porque o Setor Público

Dentre todos os concentradores de dados pessoais o Estado se sobressai, afinal de contas, é ele que controla ainda que indiretamente a vida financeira, o acesso à saúde, eventuais processos judiciais colecionados durante a vida, dados educacionais, dados trabalhistas do cidadão entre outros. Além disso, o Estado é também um empregador gigante, são milhares de pessoas que vendem sua força de trabalho para os entes municipais, estaduais e federais da Administração Direta e Indireta. Mais do que isso, o governo é também o maior acionista de grandes empresas de tecnologia que a pedido dele operam com esses dados: os coletam, armazenam, utilizam etc. Ou seja, deixar o setor público fora do alcance da LGPD seria um verdadeiro atentado aos direitos fundamentais.

A inclusão do setor público no escopo da LGPD obriga-o a adequar-se investindo em questões de segurança, que são muitas vezes negligenciadas⁴⁷, e a atuar de forma a evitar a comercialização de dados pessoais para fins diferentes daqueles aos quais foram coletados, conforme o recente caso vivenciado por uma empresa pública de tecnologia.

O governo tem se tornado cada vez mais digital: basta uma rápida pesquisa nos repositórios (APP Store) para encontrarmos os mais variados aplicativos voltados ao acesso a sistemas gerenciados pelo governo. Desde aplicativos que nos possibilitam verificar faturas de consumo de energia elétrica, ou seja, dados sobre nosso consumo, aplicativos de recuperação de créditos de notas fiscais, de acesso a bancos públicos, a agências reguladoras e outros serviços como INSS e FGTS, entre tantos outros. De acordo com pesquisa conduzida pelo Internetlab “a Administração Pública também passa a adotar gradativamente o uso de aplicações de internet como estratégia para se aproximar de cidadãos e facilitar o acesso à informação e a prestação de determinados serviços”.

⁴⁷ Vide os casos divulgados de ataques ransomware à grandes hospitais públicos e à órgãos do judiciário.

No estudo conduzido pelos pesquisadores do InternetLab, foi verificado que vários desses aplicativos pedem permissões de acesso à dados de geolocalização que quando vinculados a uma pessoa identificada ou identificável são considerados dados pessoais. Além disso, muitos deles também solicitam permissão de acesso a todas as contas do usuário – de redes sociais ou não – cadastradas no dispositivo em que são instalados. Esse tipo de acesso é considerado de alto risco e muitas vezes desnecessário para o correto funcionamento do sistema, visto que o serviço permanece funcionando ainda que desabilitando várias das permissões exigidas. Diante desses fatos os pesquisadores concluíram que o poder público não vem adotando boas práticas de segurança e proteção de dados pessoais no desenvolvimento desses aplicativos, uma vez que adotam um tipo de permissão abrangente e não esclarecem para qual finalidade específica deve ser concedida determinada permissão ou ainda qual a política pública que está vinculada à coleta daquele dado ou ainda a base legal que permite tal procedimento.

No atendimento de seus serviços essenciais de arrecadação, previdência e assistência visando facilitar todo o processo de gestão dessas áreas o Estado tem implantado sistemas como, por exemplo, o E-social que é um sistema que concentra toda a vida previdenciária e profissional do cidadão cujo principal objetivo é simplificar:

[...] a prestação das informações referentes às obrigações fiscais, previdenciárias e trabalhistas, de forma a reduzir a burocracia para as empresas [...] viabilizará garantia aos direitos previdenciários e trabalhistas, racionalizará e simplificará o cumprimento de obrigações, eliminará a redundância nas informações prestadas pelas pessoas físicas e jurídicas, e aprimorará a qualidade das informações das relações de trabalho, previdenciárias e tributárias ⁴⁸.

Outros exemplos de sistemas em que a administração pública trata dados pessoais é o sistema do IRPF que apresenta todas as informações financeiras do indivíduo, dos Sistemas de Saúde gerenciados pelo DATASUS, e por fim devemos citar o DNI – Documento Nacional de Identidade criado pela Lei federal n. 13.444/2017 (BRASIL, 2017) que reunirá em um único documento digital os dados de identificação da pessoa natural inclusive o número do CPF, sendo que o art. 11 da referida lei assim preceitua:

O poder público deverá oferecer mecanismos que possibilitem o cruzamento de informações constantes de bases de dados oficiais, a partir do número de inscrição no CPF do solicitante, de modo que a verificação do cumprimento

⁴⁸ Resultando em uma enorme concentração de dados pessoais, muitos deles dados sensíveis.

de requisitos de elegibilidade para a concessão e a manutenção de benefícios sociais possa ser feita pelo órgão concedente“ (BRASIL, 2017) ⁴⁹.

Para além dos sistemas, o país tem buscado avançar também em setores relacionados à inteligência artificial e internet das coisas (IoT) tendo inclusive lançado planos de ações, nesse sentido Magrani (20, p. 81) destaca que:

O poder público demonstra já estar atento aos benefícios da IoT, entendendo que esta surge como importante ferramenta voltada para os desafios da gestão pública, prometendo, a partir do uso de tecnologias integradas e do processamento massivo de dados, soluções mais eficazes para problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros. Já existem exemplos de aplicações de IoT pelo país, e essas experiências tendem a aumentar.

Um dos principais pontos de atenção do poder público em se tratando de IoT está na melhoria da segurança pública e algumas dessas iniciativas já começam a se concretizar, por exemplo, algumas cidades têm implantado sistemas de monitoramento por câmeras que transmitem imagens em tempo real 24 horas por dia, 7 dias por semana.

Longe ainda de equiparar o Brasil à China, onde a vigilância está integrada ao dia a dia de forma quase indissociável o uso de câmeras de vigilância pelo setor público tem se ampliado e não podemos esquecer que estes dados são pessoais e que, embora já protegidos pelo direito de imagem previsto no Código Civil, também recebem guarida na LGPD devendo o seu controlador, no caso o setor público, responsabilizar-se pelo seu uso dentro da finalidade, bem como por garantir sua segurança assegurando assim sua proteção. A evidência de que essa cultura deve ser difundida e adotada dentro do setor público são os primeiros sinais de uso indevido de imagens obtidas, como no caso em que agentes públicos se utilizando do acesso ao sistema de câmeras que tinham observavam e divulgavam imagens de banhistas do sexo feminino em uma praia brasileira⁵⁰.

Diante do cenário apresentado, impossível se pensar uma lei de proteção de dados efetiva sem que o setor público estivesse incluído. A Administração Pública direta e indireta em todas as esferas – federal, estadual e municipal – é um grande

⁴⁹ Explicitando, assim, uma hipótese de compartilhamento de dados entre os órgãos públicos.

⁵⁰ “Servidores que usaram câmeras da prefeitura para ver mulheres na praia também espiaram hóspede de biquini em hotel de Guaratuba”. Disponível em: <https://g1.globo.com/pr/parana/noticia/2018/11/28/servidores-que-usaram-cameras-da-prefeitura-para-ver-mulheres-na-praia-tambem-espiaram-hospede-de-biquini-em-hotel-de-guaratuba.ghtml>

controlador de dados pessoais e em um Estado democrático de direito deve se submeter às leis também no que tange a proteção de dados.

A crescente utilização de dados pessoais e a sua importância para os mais variados aspectos de nossas vidas refletem, hoje, em um aumento da atividade normativa destinada a especificar qual estatuto jurídico deve seguir o tratamento desses dados. Não à toa, mais de 100 (cem) países ao redor do mundo já adotaram uma lei geral para regular o tratamento de dados pessoais em diferentes setores. Uma lei geral de proteção de dados pode ser definida, em termos gerais, como um marco regulatório que estabelece direitos e garantias para o cidadão em relação aos seus dados pessoais, independente de quem ou de que forma estes sejam tratados.

A ideia de “proteção” visa a assegurar que o cidadão tenha a seu dispor meios para exercer efetivo controle sobre seus dados e, também, que todo o ecossistema em torno do tratamento de dados pessoais tenha contrapesos e incentivos para que danos aos cidadãos sejam evitados. Isto sem, contudo, impedir a inovação a partir do tratamento de tais dados, elemento fundamental da sociedade da informação.

7.3 Tratamento dos dados pelo Setor Público

O principal requisito permissivo para o tratamento de dados pessoais pela Administração Pública é o que está presente no artigo 7º, III, da LGPD.⁵¹

A execução de políticas públicas é, portanto, a principal e, indubitavelmente, a melhor justificativa para que o setor público realize qualquer tipo de tratamento de dados. Sendo este um conceito muito amplo, dando larga margem para a manipulação dos dados pessoais pelo setor público, uma vez que é inerente à própria existência do Estado a consecução de políticas públicas.

Esse requisito está intimamente ligado a outros dois previstos no artigo 23 “atendimento de sua finalidade pública, na persecução do interesse público” e “com o objetivo de executar as competências legais ou cumprir as atribuições legais do

⁵¹ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

serviço público”. Tal previsão encontra guarida no princípio da supremacia do interesse público que é princípio constitucionalmente previsto, conforme Di Pietro (2018, p.132): “Esse princípio está presente tanto no momento da elaboração da lei quanto no momento da sua execução em concreto pela Administração Pública. Ele inspira o legislador e vincula a autoridade administrativa em toda a sua atuação”.

Assim podemos compreender que “se a lei tem em vista atender ao interesse geral, que não pode ceder diante do interesse individual” é neste sentido que deve ser também realizado o tratamento de dados e nesse caso resta claro que há dispensa do atendimento de qualquer outro dos requisitos previstos no artigo 7º e nos parece ser este o fundamento do qual a administração pública deve se valer para realizar o tratamento de dados.

Assim, o Estado não se exime de informar quando está realizando tratamento dos dados por meio de informações claras e atualizadas – atendendo ao princípio da transparência: “art. 6º, VI – *garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento; sobre a previsão legal que embasa/justifica tal tratamento*”. O rol de bases legais autorizadoras do tratamento de dados pessoais pela Administração Pública encontra previsão no inciso III do artigo 7 e inclui leis, regulamentos, contratos, convênios ou instrumentos congêneres.

Alguns questionamentos surgem neste ponto em relação aos instrumentos autorizadores do tratamento: seria uma portaria, por exemplo, um instrumento apto a autorizar o tratamento de dados pessoais pelo setor público? Finalidade – atendendo assim ao princípio previsto no artigo 6º, I: “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. O inciso III do artigo 23, por sua vez, exige que seja indicado um encarregado que nos termos da própria lei deverá conhecer do tratamento de dados realizados, bem como comunicar-se com titulares de dados e com a Autoridade Nacional de Proteção de Dados entre outras atribuições.

Além de atender os requisitos supracitados, a Administração Pública não se exime do dever de garantir o cumprimento de todos os demais princípios enumerados no artigo 6º: adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Há que se ressaltar que estes princípios se aplicam independentemente

da base legal utilizada para justificar o tratamento de dados e por isso deve a Administração Pública preocupar-se em garantir que eles sejam atendidos em relação a todos os dados pessoais em seu poder.

7.4 Definições

Titular

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Titular será o contribuinte, servidor ou empregado público, gestor público, pessoa física com a qual o órgão ou entidade pública possui alguma relação contratual.

Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No setor público será o órgão público, entidade pública, empresa pública ou sociedade de economia mista que toma as decisões a respeito do tratamento de dados pessoais. Por exemplo, a Receita Federal, em relação às bases de dados que gere. O órgão público que mantém um banco de dados de seus servidores ou empregados públicos também se enquadraria nesta definição.

Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Por exemplo, o SERPRO (Serviço Federal de Processamento de Dados) ou a DATAPREV (Empresa de Tecnologia e Informações da Previdência Social) atuam como operadores quando processam dados pessoais em nome de outros órgãos ou entidades públicas.

Encarregado

Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. A Autoridade Nacional poderá estabelecer normas complementares sobre a definição

e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Uso compartilhado de dados

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Órgãos de pesquisa

Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Universidades Públicas e entidades de pesquisa pública, como a Fundação Oswaldo Cruz, se enquadram nesta definição.

7.5 Responsabilidade do Órgão Público

Este ponto demonstra-se clara a necessidade da Autoridade Nacional de Proteção de dados, visto que está entre suas funções indicar as medidas cabíveis para cessar a violação da proteção de dados causada ou facilitada por alguma entidade da Administração Pública.

Faz-se mister discutir acerca de qual a responsabilidade do ente sobre os dados que estão sob sua guarda, é preciso compreender que não é porque os dados estão publicamente disponíveis – como é caso por exemplo das remunerações dos servidores públicas que estão expostas no Portal da Transparência – que ele deixa de ser um dado pessoal, informação publicamente acessível não é necessariamente uma informação pública.

Por isso, é importante notarmos que nesse caso específico existe uma base legal – Lei de Acesso à Informação – que determina que tais dados devem ser expostos. Com respaldo na finalidade específica de tornar transparente os gastos efetuados pela Administração Pública com seu pessoal, para que qualquer cidadão possa fiscalizar eventuais abusos cometidos, como, por exemplo, o descumprimento do teto salarial constitucionalmente previsto.

Todavia, embora estejam públicos tais dados ainda devem ser protegidos, visto que não podem ser utilizados para qualquer outra finalidade que não aquela prevista na LAI, não podendo um terceiro captá-los para fazer listas de fornecimento de crédito, por exemplo, ou a Administração Pública cedê-los para que terceiros os utilizem para qualquer fim.

Em relação à responsabilidade posterior do Estado em caso de uso desses dados por terceiros que se aproveitaram de uma exposição calcada na legalidade é um ponto que deve ensejar discussões.

7.6 Sanções à Administração Pública

As sanções administrativas a que se submetem os entes públicos são de certa forma mais brandas daquelas a que se submetem os entes privados e estão estabelecidas no §3º do artigo 52, sendo elas:

I – Advertência, com indicação de prazo para adoção de medidas corretivas;

IV – Publicação da infração após devidamente apurada e confirmada a sua ocorrência;

V – Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI – Eliminação dos dados pessoais a que se refere a infração;

Embora não se tenha a punição de multa (incisos II e III) para entes públicos, sanções como o bloqueio dos dados pessoais podem causar grande impacto na atuação pública e mais uma vez é mister ressaltar que as empresas públicas e

sociedades de economia mista que atuem em regime de concorrência conforme a determinação constitucional se submetem também a sanção pecuniária.

Novamente o legislador optou por deixar explícito que além da LGPD o setor público se submete a outros ditames legais, quais sejam, a lei de Improbidade Administrativa, o Estatuto do Servidor Público Federal e a Lei de Acesso à Informação.

7.7 Status

A Administração Pública vem ao longo do tempo aderindo às inovações tecnológicas a ponto de se auto intitular como Brasil – país digital. Valendo-se de aplicativos que buscam aproximar governo e cidadão INSS, FGTS, Bolsa Família, entre outros, ou que tem como objetivo facilitar a vida da sociedade, como o e-título, a CNH Digital, o Meu Imposto de Renda, está entre os maiores controladores de dados do país.

Diante destes fatos, nos chamou atenção o pouco interesse que o setor público demonstrou ao não participar dos debates que antecederam a aprovação da Lei Geral de Proteção de Dados bem como a posterior tentativa de colocar-se fora de seu alcance demonstrado as quão despreparadas estão as entidades públicas diante da nova lei.

Deve se fazer menção ao fato de que existem muitos pontos obscuros e que deverão pautar as discussões durante e mesmo após a implementação das regras de conformidade no setor público, entretanto, parece-nos que tal como o que recentemente ocorreu nos países europeus na implantação do GDPR, a administração pública tem andado a passos lentos quando se trata de adequação à lei. Conforme apresentamos no texto, são vários os aplicativos que coletam dados desnecessários para o seu funcionamento, ou seja, não se adota a minimização da coleta, também não se verifica nos diversos sistemas existentes explicações sobre a finalidade específica para qual o dado é coletado.

Desta forma, a finalidade execução de políticas públicas, autorizadora do tratamento de dados pessoais, fornece um escopo muito amplo e que consegue justificar grande parte das operações que envolvem dados pessoais realizadas pelo

setor público e entendemos que este será o fator fundamental a ser considerado quando da realização dos mapeamentos e dos relatórios de impacto. Identificar qual finalidade pública será atendida também servirá para separar as situações em que os entes públicos que atuam em regime de concorrência no mercado deverão atender aos requisitos próprios do tratamento de dados definidos para o setor público ou quando se submeterão aos requisitos e sanções aplicados aos entes privados.

Neste momento existem muito mais questionamentos do que convicções acerca de como se dará a implementação da LGPD pela Administração Pública e aqui ressalta-se também a essencialidade da existência da Autoridade Nacional de Proteção de Dados, uma vez que cabe a ela orientar e determinar muitos requisitos acerca da aplicação da lei. Outros pontos controversos e que tem motivado discussões é se a Administração Pública poderia utilizar o legítimo interesse como requisito justificador do tratamento dos dados pessoais e a que tipo de responsabilidade se submete o ente em caso de inobservância dos ditames da lei. Além disso, faz-se necessário olhar com cautela para definir quais instrumentos podem ser utilizados como base legais justificadoras do tratamento de dados pessoais?

Outro tema que deverá ser profundamente discutido é a interseção necessária – determinada pela própria LGPD – entre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados, há pontos de aparente conflito entre os dois regramentos que devem ser interpretados de forma a harmonizar os dois regulamentos.

Os impactos da LGPD na sociedade serão gigantes, acreditamos que em um futuro próximo ela se eleve a um patamar de importância muito próximo daquele em que está o Código de Defesa do Consumidor, sendo que o setor público precisa sair da zona de conforto em que está desde quando a regulamentação ainda era um projeto de lei em discussão. Capacitar pessoas para atuarem como encarregados, realizar mapeamentos e relatórios de impactos, aplicar novas metodologias como o framework na arquitetura de privacidade no desenvolvimento de seus sistemas e serviços, investir em segurança da informação. Salientamos que se o cenário se reveste de complexidade no setor privado, no setor público há outras variantes complicadoras desde o fato de que o processo de aquisições de soluções é moroso na Administração Pública – porque ela deve seguir os ditames licitatórios – até o

fato de que é necessário treinar pessoal em uma estrutura grandiosa como é o Estado, tudo isso exige tempo e estratégia. O primeiro passa rapidamente por isso, a segunda precisa ser emergencialmente definida.

7.8 O que são os dados?

A Lei LGPD tem três categorias e diferentes níveis de proteção:

1- Dado pessoal

A LGPD classifica como dado pessoal qualquer informação relacionada a pessoa natural identificada ou identificável. Pessoa natural não é apenas o contribuinte, mas também o servidor e o empregado público, pessoas físicas com as quais a administração pública se relaciona, e até mesmo os gestores públicos e demais representantes do povo com mandato eletivo. Isso significa que um grande número de identificadores constituem o dado pessoal, como o nome, o CPF, RG, informações sobre localização e assinaturas online. Em resumo, praticamente toda informação coletada sobre uma pessoa será um dado pessoal.

2- Dado pessoal sensível

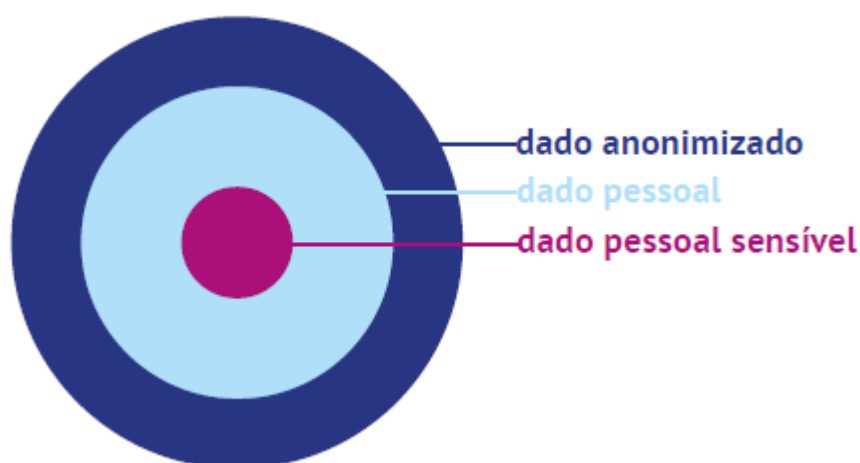
A LGPD definiu como dado pessoal sensível aquele dado pessoal “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico” de uma pessoa natural. Dados relacionados a políticas direcionadas a minorias, por exemplo a LGBTQI+, seguramente envolverão o tratamento de dados sensíveis. Na mesma linha, os sistemas de identificação biométrica, como aquele adotado pelo TSE (Tribunal Superior Eleitoral) para fins de votação eletrônica. O tratamento desses dados atrai um regime de proteção ainda mais restritivo.

3 - Dado anonimizado

Quando existe um dado que não é capaz de identificar o seu titular, utilizando os meios técnicos razoáveis e disponíveis na ocasião do seu

tratamento, ele é chamado de dado anonimizado. O dado anonimizado não será considerado dado pessoal para os fins da LGPD, salvo quando o processo de anonimização ao qual foi submetido for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Figura 6: diferentes tipos de dados



Fonte: LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E SETOR PÚBLICO. Um guia da Lei 13.709/2018, voltado para os órgãos e entidades públicas, p.13

7.9 Preparação para SMSU

A Secretaria Municipal de Segurança Urbana do Município de São Paulo tem feito realizado vários trabalhos relacionados à segurança, como vídeo monitoramento, prevenções e retenções de indivíduos de má conduta, estas informações relacionadas às pessoas precisam ser protegidas e ao mesmo tempo não divulgadas a qualquer pessoa ou por qualquer meio de transmissão.

A aplicação da LGPD gerará um aumento exponencial na quantidade de processos em todos os níveis da justiça, principalmente no Superior Tribunal de Justiça (STJ), acredita-se que poderá aumentar até em 200 mil ações, por isto a SMSU precisa fazer a parte dela e estar preparada para seguir a LGPD.

Um dos motivos para o possível aumento seria em relação aos casos de responsabilidade civil (artigo 42 e 44 da lei), objetiva e solidária do controlador e do

operador pelo tratamento irregular dos dados pessoais. Hoje no Brasil, acredita-se que apenas 23% das empresas estão em conformidade com a LGPD, outros como o setor público está com somente 8%.

A SMSU precisa se preparar em ter pessoas qualificadas para o entendimento da LGPD e claro para que os processos técnicos sigam a proteção e a divulgação das informações coletadas via videomonitoramento, call center, ações da GCM (Guarda Civil Metropolitana). As pessoas precisam ser preparadas, não necessariamente contratadas (novas contratações), por isto no mercado de tecnologia já foi feito uma pesquisa para as ver as principais habilidades de um profissional técnico tenha que ter para atuar em projetos relacionados à LGPD.

Quais HABILIDADES são mais demandadas ao contratar profissionais encarregados da adequação à LGPD?

Habilidade	% de CIOs que concorda
Conhecimento da regulação e conformidade	53%
Pensamento estratégico	46%
Visão analítica	45%
Capacidade de gerenciar projetos	42%
Boa comunicação	38%
Atenção aos detalhes	35%

Fonte: Pesquisa Robert Half

Quais profissionais PERMANENTES pretende contratar devido à nova legislação LGPD?

Cargo	% de CIOs que concorda
Analista de negócios	54%
Encarregado de proteção de dados	42%
Gestor de projetos	40%

Profissional de conformidade (compliance)	35%
--	-----

Não pretende contratar	6%
------------------------	----

Fonte: Pesquisa Robert Half

Quais especialistas para projetos pretende contratar devido à nova legislação LGPD?

Cargo	% de CIOs que concorda
Profissional de conformidade (compliance)	46%
Analista de negócios	40%
Gerente de projetos	38%
Encarregado de proteção de dados	25%
Não pretendemos contratar	9%

A LGPD foi elaborada a partir do regulamento europeu General Data Protection Regulation (GDPR)⁵² e estabelece bases legais para o tratamento de dados pessoais pelas organizações, além de garantir diversos direitos aos titulares dessas informações. A SMSU precisa ter cuidado redobrado com a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais, tanto da equipe interna e terceiros. Havendo algum incidente, deverá comunicar ao órgão regulador chamado Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

Hoje a SMSU precisará se esforçar consideravelmente para o ter o controle e qualidade quanto ao tratamento de dados pessoais e o aumento nas medidas organizacionais para gestão do risco cibernético na proteção dos dados. Tendo especialistas na área cibernética, os benefícios e os desafios que a Lei trará e os aprimoramentos técnicos que deverão ser implementados interna e externamente, como processos eficientes de atendimento aos direitos de titulares, um programa sustentável de inteligência e segurança da informação.

⁵² Como visto no item 3.6.1.3.

Lembrando que a SMSU tem todo interesse e a preocupação relacionada à privacidade, mas tem que investir principalmente no processo interno e na qualificação das pessoas, pois a privacidade e segurança das informações ganhou destaque e necessidade de um cuidado maior, surgiu o avanço tecnológico crescente. Com o aumento significativo do volume de informações digitais, a área de segurança cibernética se tornou indispensável, por isto tanto a SMSU e outros órgãos precisam estar preparadas a fim de evitar as ameaças cibernéticas que evoluem em grande velocidade, colocando em risco a reputação da SMSU.

A SMSU já tem práticas de *compliance*, mas hoje devido à LGPD deverá trabalhar fortemente num novo processo, e este processo verá não somente o trabalho da SMSU, mas também a legislação. Por isto este novo processo precisará ser desafiado e construído em quatro áreas de atuação:

- A Governança de Dados: onde dever haver a precisão e integridade das entradas, análises, relatórios, assim como implicações legais da utilização dos dados e mapeamento deles.
- A Privacidade dos Dados: que se resume na transparência do uso, no inventário, na governança regulatória e no gerenciamento de consentimento dessas informações pessoais.
- A Proteção de Dados: que abrange a confidencialidade, a proteção em todos o seu ciclo de vida e o gerenciamento de riscos de terceiros quanto aos dados pessoais.
- Relatórios e a análise de dados: que consiste no uso das informações de forma ética e com fins puramente analíticos, assim como a apuração da confiabilidade dos dados e o formato de relatórios.

Lembrando que tudo se resume ao processo, é fundamenta que todos os níveis da SMSU e as divisões estejam empenhadas pois entendida a primeira fase, outros fatores serão importantes para o sucesso na implementação das regras da LGPD às regras. Reforçamos que deverá ser endereçado a todas as camadas do órgão, utilizando assim um *framework* de privacidade que tem como principal objetivo resolver as questões recorrentes do uso de dados com uma abordagem ampla, permitindo o foco na resolução do problema em si, utilizando a tecnologia para manter a visibilidade necessária sobre os dados e opiniões jurídicas sobre os fluxos de

tratamento de dados; complementado a linha relacionada ao novo processo, deverá ser elaborado e mantido um cronograma claro de organização do programa de privacidade (ações, esforços, e as prioridades que serão ser definidas pela SMSU para a GCM e Defesa Civil).

O esforço é e será muito grande, mas o maior desafio da SMSU é entender como conseguir se aproveitar do que já fazem para atender às demandas. O ponto principal é a confiança do Secretário e a prioridade em obter um sistema transparente. Seria interessante ver as lições aprendidas com a GDPR, já em funcionamento na Europa, o primeiro passo é garantir uma melhoria da segurança cibernética, seguida do aprimoramento das capacidades de gerenciamento de dados, disponibilização dos direitos dos titulares e remediação de processos e sistemas e direcionamento de comunicação clara aos titulares dos dados, que certamente serão responsáveis pela manutenção ou construção da confiança.

A SMSU terá maior chance de sucesso para se adequar à LGPD, se organizar a dinâmica de trabalho e priorizar os passos sugeridos acima, não deixar para depois, pois significará dominar a LGPD.

7.10 Como a Lei identifica um incidente de segurança?

A LGPD não define incidente de segurança. O CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), grupo responsável por receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet brasileira, define incidente de segurança como “qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores”.

Pelo que consta do caput do Artigo 46 da LGPD, apenas os incidentes de segurança que importarem em “acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito” deverão ser notificados.

Comunicação sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, esse é um tema de fundamental

importância para o setor público, já que diversos órgãos e entidades públicas, assim como empresas públicas e sociedades de economia mista, em todas as esferas de governo e da federação, tratam dados pessoais tanto de contribuintes como de servidores e empregados públicos, sendo que muitos desses dados se enquadram na definição de dado pessoal sensível. Portanto, o estabelecimento de uma política clara sobre o que fazer quando da ocorrência de incidentes de segurança é de vital importância. Basicamente, o incidente deve ser comunicado à Autoridade Nacional e ao titular dos dados, pelo órgão público, entidade pública, empresa pública ou sociedade de economia mista que desempenhar o papel de controlador, sempre que o incidente de segurança “possa acarretar risco ou dano relevante aos titulares”.

7.11 Ações Tecnológicas

A SMSU precisará tratar os dados de maneira diferente, ou seja, ter privacidade na arquitetura que vier a desenhar. Os regulamentos da LGPD são específicos e abrangentes, e a conformidade provavelmente significará alterações no processo atual. Acreditamos que a SMSU apesar de toda evolução na segurança junto com a tecnologia a favor, não implementou um sistema completamente novo relacionado à segurança, ou seja, não tem este recurso implementado, lembrando que os desafios não são apenas baseados em tecnologia, mas também tratar os dados de uma maneira fundamental.

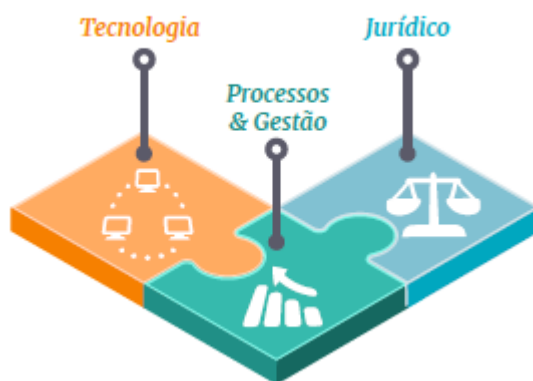
Na LGPD, precisaremos proteger os dados pessoais em todos os lugares em que o dado reside ou é trafegado no órgão, pode parecer simples, mas não é incomum para diferentes aplicativos e sistemas que acessam dados pessoais e estes dados podem ser replicados através dos sistemas de backup e em locais de recuperação de desastres. Há possibilidade de compartilhar dados em vários sistemas internos, como call center, sites de mídia social, recursos humanos e até formulários.

Obter e recuperar o consentimento:

Os cidadãos devem fornecer explicitamente com consentimento para armazenar o uso dos seus dados, o pedido de consentimento deve distinguir-se claramente de outros itens, como termos e condições; e postar formulários que são

pré-verificados, é impossível registrar tudo sem automação, e automatizar este processo exigirá ferramentas especificamente para trabalhar com seus sistemas.

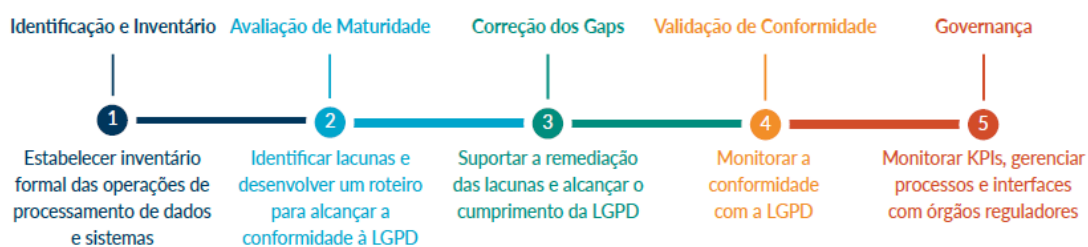
Figura 7: interconexão



Fonte: Compliance & LGPD, ICTS, pg. 6

Figura 8: etapas de Programa

Etapas de um programa



Fonte: Compliance & LGPD, ICTS, pg. 6

7.12 Softwares SMSU Informação

A SMSU via a Guarda Civil Metropolitana tem um software chamado SIG (Sistema de Informações Gerenciais) na qual possui informações referentes ao planejamento de escala, equipamentos municipais atendidos pela inspetoria, informações pessoais e funcionais dos servidores (como férias e porte de arma), relatórios de ocorrências e de atividades de serviços (RAS), entre outras questões importantes para a Guarda Civil Metropolitana.

De acordo com a entrevista que tivemos com a Comandante da GCM, Elza Paulina de Souza, o sistema é de extrema importância para a GCM e consequentemente para a SMSU, pois o SIG praticamente controla e gerencia as ações da GCM como um todo, mas há falhas principalmente nos processos internos que precisam ser revistos para melhorias internas como agilidade e melhor precisão, como também atender a LGPD.

A partir de 2019, o SIG também tem integrado o Google Earth para que os RAS⁵³ tenham georreferencia, ou seja os servidores das unidades poderão ver no mapa da cidade de São Paulo o endereço aproximado das ocorrências e das atividades desempenhadas, além da geocodificação desses importantes instrumentos da GCM, estará disponível em aplicativos, por exemplo, o perímetro de atendimento de cada unidade, a localização das câmeras da central de telecomunicações e videomonitoramento (Cetel), a delimitação das subprefeituras e dos distritos administrativos e, em um futuro próximo, o Distrito Policial responsável por cada região.

Para a Comandante Inspetora Elza Paulina de Souza, a capacitação contínua no uso do SIG-GCM e o novo aplicativo estão alinhados com a crescente importância da SMSU no cenário de gestão das informações da Prefeitura. “Muitos dados da GCM são de conhecimento público e fazem parte do processo de transparência para o cidadão. Os dados de desordens urbanas da corporação compõem o *Observatório de Indicadores da Cidade de São Paulo*, previsto na meta 118 do Programa de Metas 2013-2016, e nossas bases de dados estão listadas no *Catálogo Municipal de Base de Dados*”.

De acordo com informações coletadas a GCM depende exclusivamente de uma pessoa para que o SIG continue funcionando e interagindo com os guardas; além de ser um tema alarmante, existe a possibilidade das informações contidas no banco de dados dos sistemas estejam a mercê de ataques e acabem sendo divulgadas e compartilhadas; são informações não somente relacionadas ao indivíduo, mas também relacionadas ao guarda e as ações que estarão sendo executadas pela GCM, já pensou em ações que deveriam ser discretas forem divulgadas em mídias sociais.

Por isto que a SMSU junto com as suas respectivas divisões como a GCM e Defesa Civil precisam se adaptar e criar um processo para que o órgão esteja

⁵³ Anexo II.

seguindo a LGPD e que o processo interno seja da melhor forma para os funcionários e que siga as regras de proteção.

No processo a ser desenhado precisa ser bem definido as responsabilidades que cada usuário terá; pois dados relativos ao titular de uma ação não podem ser identificados à terceiros, considerando sempre a utilização dos meios técnicos razoáveis e disponíveis na ocasião da ação. As atividades de tratamento de dados pessoais deverão ser observadas a boa-fé com os seguintes princípios:

- Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou difusão;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- Responsabilização e Prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e inclusive das eficácias destas medidas.

De acordo com a Comandante Elza há também o Compstat Paulistano, sistema criado com origem no Compstat (do inglês “Compare Statistics”, comparar estatísticas) da Cidade de Nova York, que é utilizado desde 1994 para compilar estatísticas e dados de segurança e cruzá-los com informações geográficas, desenhando assim um mapa da criminalidade e do policiamento na cidade, e sempre tentando antecipar uma ocorrência.

Os dados que são fornecidos pelo aplicativos SP+Segura e pelo sistema INFOCRIM da Secretaria de Segurança Pública do Estado de São Paulo, são utilizados para auxiliar a Guarda Civil Metropolitana a realizar um planejamento estratégico para expandir o patrulhamento preventivo, principalmente em áreas de maior probabilidade de crimes.

De acordo com o Secretário Jose Roberto Rodrigues de Oliveira, “O principal foco é realizar atuação preventiva com crimes de oportunidade, por exemplo, furtos e roubos, já que são os crimes que mais afetam a sensação de segurança das pessoas”.

Veja a importância de proteger os dados, os criminosos, suspeitos não podem saber antes das ações que serão feitas pela GCM e ações de inteligências coordenadas pela SMSU.

As informações de delegacias de polícia e de sistema de monitoramento, o Compstat americano foi capaz de, por exemplo, mostrar o histórico de um tipo específico de crimes em uma determinada rua, bairro ou região da cidade, quem são seus autores e em qual horário do dia costumam ser perpetrados, dessa forma, mostrando padrões, o Compstat oriente as ações de segurança pública, racionalizando o processo de controle do crime e tornando-o mais eficiente; veja que estes dados coletados e as estatísticas não podem ficar à mercê de uma vazamento e/ou divulgação, pois é a inteligência da SMSU que está trabalhando para derrubar taxas de criminalidade da cidade, como foi feito em Nova York.

“É um caminho de policiamento preditivo. Você consegue antecipar a ocorrência do crime em determinadas áreas”, de acordo com o Coronel José Roberto.

Figura 9: o secretário municipal de segurança pública José Roberto Rodrigues na sala de monitoramento de câmeras da Guarda Civil Metropolitana



Fonte: Jardiel Carvalho, Folhapress.

7.13 Responsabilidade e Registros de Acesso

Podemos chamar os usuários dos sistemas de controlador e operador, ambos devem manter os registros de operações de tratamento de dados que realizarem, ou seja, o sistema precisa criar “logs” para auditorias internas e a nível de salvaguarda dos controladores e operadores. A autoridade acima do controlador poderá determinar ao controlador que elabore relatórios de impacto à proteção dos dados, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos do regulamento, observados os segredos.

O relatório deverá conter, no mínimo, uma descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

O controlador e o operador que, em razão do exercício da atividade de tratamento de dados, causem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados é obrigado a repará-lo. Os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados sendo pessoais e/ou estatísticas de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Sobre a notificação de vazamentos de dados, o controlador deverá comunicar a autoridade e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares; os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender os requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta lei e às demais normas regulamentares.

A Lei Geral de Proteção de Dados (LGPD) do Brasil exige as melhores práticas em segurança para dados pessoais e observa que os dados pessoais que tiverem sido anonimizados não serão considerados no escopo da Lei, se não puderem ser revertidos facilmente para o seu estado original por aqueles que possam obtê-los. O desafio para as empresas e órgãos públicos, é como equilibrar a necessidade de usar

estes dados para processos, análises de negócios e ultimamente o sucesso no mercado, com a proteção aos dados confidenciais contra hackers, pessoas de dentro da organização ou vazamentos acidentais.

Por exemplo, os dados têm que fluir entre várias plataformas na nuvem e nas dependências da empresa/órgão, além de serem acessados por funcionários remotos e analisados em plataformas de big data. Durante todo o processo, os dados devem estar seguros para permanecer em conformidade com a LGPD e leis semelhantes.

Diante da transformação digital, as atuais estratégias de segurança usadas por empresas se tornam insuficientes. À medida que as empresas implementam novas tecnologias como nuvem e big Data, muitas vezes escolhem soluções pontuais para proteger dados em uma plataforma ou outra. Isso leva a uma abordagem de segurança fragmentada e a falhas na proteção de dados.

As melhores práticas e soluções precisam ser requeridas à SMSU para a sua demanda, entre as melhores práticas de conformidade e segurança para um órgão com infraestrutura de TI híbrida inclua quatro aspectos que possam se tornar essenciais no processo de conformidade com a LGPD:

- Pseudonimização de dados pessoais
- Controle de Acesso a dados Sensíveis
- Monitoramento e registros de acesso aos dados
- Proteção de dados em ambientes de infraestrutura híbrida
- Autenticação segura e centralizada

7.14 Sugestão de Segurança Técnica

Para a SMSU sugerimos que usem alguns recursos para que possam proteger os dados internos, relacionados à segurança e imagens. Inicialmente é a inclusão da Criptografia que protegerá dados em repouso, controles de acesso e registro de auditoria de acesso a dados sem aplicativos de reengenharia, banco de dados e infraestrutura.

A instalação do software de criptografia transparente de arquivos é simples, escalável e rápida, com agentes instalados acima do sistema de arquivo em

servidores ou máquinas virtuais para assegurar políticas de segurança e conformidade de dados.

A solução com Mascaramento Dinâmico de dados reduz drasticamente os custos e os esforços necessários para cumprir com as políticas de segurança e normas regulatórias, como a LGPD. A solução oferece capacidades para tokenização de banco de dados e segurança de tela dinâmica. As empresas podem eficientemente realizar seus objetivos de proteger os ativos sensíveis — estejam eles em ambiente de data center, big data, em container ou na nuvem.

Os Módulos de Segurança de Hardware (HSMs) são certificados FIPS 140-2 nível 3, e INMETRO (ITI ICP-BRASIL), com uma ampla gama de usos para acelerar operações criptográficas, proteger o ciclo de vida de chave criptográfica e fornece uma base de confiança para toda a sua infraestrutura de criptografia e é uma plataforma baseada em nuvem que fornece uma ampla gama de serviços de gerenciamento de chaves.

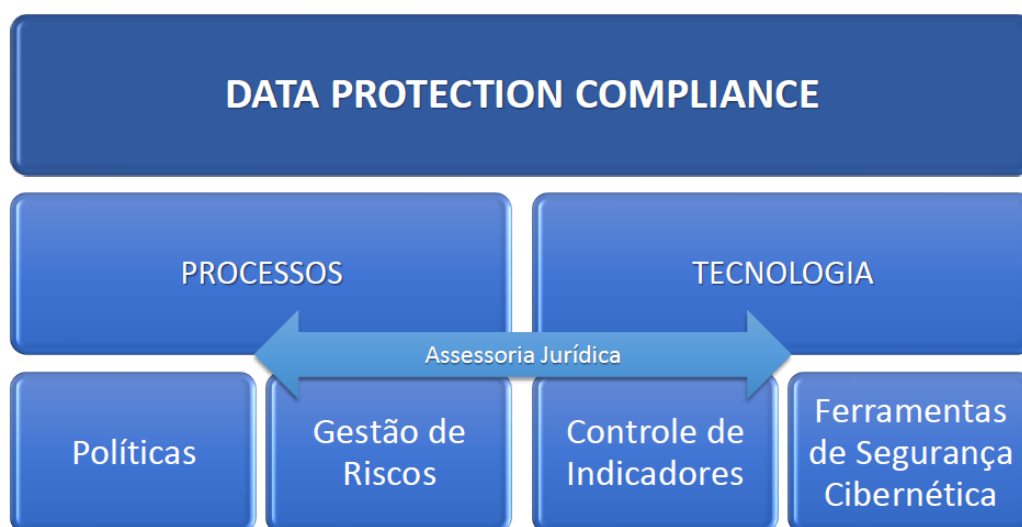
Como a SMSU trabalha fortemente com Nuvem, é possível integrá-la com criptografia, incluindo também uma camada de segurança, gerenciando centraliza mente várias nuvens, como armazenamento seguro de chaves.

Controle de acesso do usuário e autenticação, que pode ser via web ou nuvem, a SMSU poderá escalar os controles de acesso à nuvem, enquanto atende às necessidades dela, com gerenciamento de riscos e de conformidades, ao aplicar políticas flexíveis baseadas em risco e métodos de autenticação universal.

Lembrando que será necessário a implementação de um SIEM (Security Information and Event Management / Gerenciamento de eventos e informações de Segurança) que permitirá que SMSU identifique tentativas de acesso não autorizado e desenvolva parâmetros de modelos de acesso ao usuário autorizado. Elaboramos um modelo de Edital relacionado ao LGPD que a SMSU poderá usar como base⁵⁴

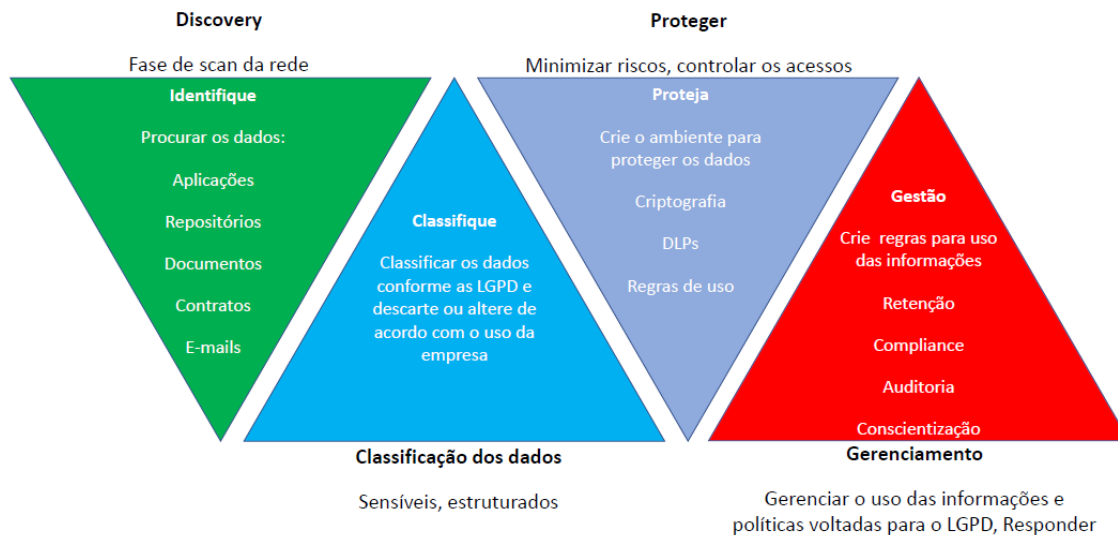
Figura 10: diagrama técnico

⁵⁴ Disponível no Apêndice II.



Fonte: <https://tecnoblog.net/245101/gdpr-privacidade-protecao-dados/>

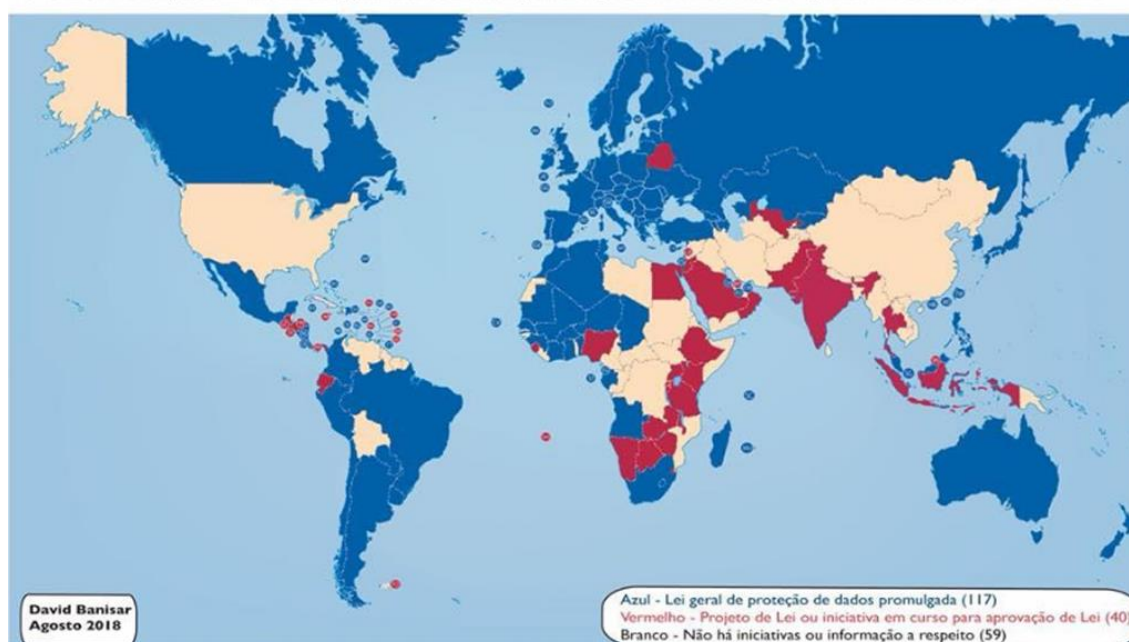
Figura 11: Discovery/Classificação dos Dados/Proteger/Gerenciamento



Fonte: <https://www.gdprtoday.org/gdpr-in-numbers-4/>

Figura 12: LGPD no mundo

Leis e Projetos de Lei gerais sobre proteção de dados e privacidade em 2018



Fonte: <https://www.gdprtoday.org/gdpr-in-numbers-4/>

7.15 Cases no Mercado Brasileiro e Europeu

1)Detran-RN

A intenção aqui neste tópico é comentar e detalhar o que for possível sobre “cases” que não podem ser referência; o Termo de Referência que estamos escrevendo à SMSU é para ajudar a prevenir casos que nem este que descreveremos abaixo.

O Detran-RN (Rio Grande do Norte) era responsável pela sua a base, ou seja, os motoristas que tiram e tiraram carteira nacional de habilitação no Estado do Rio Grande do Norte, mas como é um Detran, ele também interligação com outros Detrans via a DENATRAN (Departamento Nacional de Trânsito), com isto é possível verificar a base de outros Detrans.

Houve uma falha no sistema do Detran-RN e causou um vazamento de dados de 70 milhões de brasileiros que tem CNH; a falha foi na segurança, este vazamento aconteceu no dia 8 de outubro de 2019. Este vazamento ocorreu depois de uma

brecha na segurança ter sido descoberta, um pesquisador de segurança que anonimamente denunciou o vazamento à um site da internet, ele descobriu que era só inserir diferentes números de CPFs gerados aleatoriamente para causar um erro no site, este erro em questão dava acesso ao banco de dados de todas as unidades do Detran do Brasil, já que o órgão possui seus sistemas estaduais integrados; conforme verificado todos os brasileiros que possuem CNH tiveram os dados pessoais expostos no site do Detran-RN.

Era possível obter vários dados sensíveis, como endereço residencial, telefone, operadora e dados da CNH, como categoria, validade, emissão, restrição, registro.

Personalidades públicas também foram afetadas pela falha, como o Presidente Jair Bolsonaro, o seu filho Flávio e o jogador Neymar.

Se a LGPD já estivesse vigorando, a situação seria bem diferente. Na atual, nada aconteceu.

Lembrando que alguns Detrans se encontram debaixo da Secretaria de Segurança do Estado, vejam que o incidente poderia ser pior se houvesse vazamento de dados relacionados à Segurança Pública, na qual existem vários dados sensíveis

2) Stone

Este caso é referente à uma empresa privada, mas vale a pena comentar, pois o Ministério Público do Distrito Federal abriu investigação sobre o vazamento.

Há algumas semanas, a Stone informou ter sofrido um ciberataque com vazamento de informações e chantagem; o MPDFT está investigando as consequências do vazamento de dados.

Há algumas semanas, a Stone enviou um informe para a SEC, a Comissão de Valores Mobiliários americana, informando que havia sofrido um ciberataque com vazamento de informações e chantagem.

No documento, o promotor de Justiça Frederico Meinberg Ceroy afirmou que é responsabilidade do MPDFT incentivar a proteção de dados pessoais, bem como levar a população, empresas e órgãos públicos o conhecimento de normas e políticas a respeito do assunto.

Ainda segundo ele, o órgão deve “recomendar, diante da gravidade do incidente de segurança, ao responsável pelo tratamento dos dados a adoção de outras providências”. Ele cita como medidas a comunicação aos titulares e a ampla

divulgação do fato em meios de comunicação para reverter ou mitigar os possíveis efeitos do incidente.

Com a autuação, a empresa de pagamentos será requisitada a prestar mais informações sobre o vazamento.

A Stone informou que não foi formalmente notificada pelo Ministério Público do Distrito Federal e Territórios. “Gostaríamos de esclarecer que não há indícios de nenhum acesso, divulgação ou utilização de dados, informações pessoais de nossos clientes ou qualquer tipo de acesso à nossa infraestrutura ou efeito em nossas operações. Não temos nenhuma evidência de que foram acessados códigos-fonte materiais ou que tenha havido qualquer invasão a nossos sistemas”, informa a empresa em nota

A Stone diz ainda que fez o comunicado ao mercado e às autoridades competentes. “Tão logo a companhia seja notificada formalmente sobre a investigação do MPDFT, será do nosso melhor interesse apresentar informações sobre o incidente.

3) Polícia Militar do Estado de São Paulo

A Polícia Militar do Estado de São Paulo confirmou recentemente a informação que houve vazamento de dados relacionados aos policiais: numa abordagem rotineira de uma equipe da instituição, junto a um suspeito verificou-se que no celular do suspeito tinha dados de outros policiais militares, incluindo uma espécie de rastreador que mostra onde a viatura está no momento.

Os conteúdos encontrados no celular relacionados aos policiais militares eram dados sensíveis, como o nome completo, o número de registro, a patente, número de patrimônio da viatura, qual era a equipe na viatura.

As informações indicam que o suspeito tinha acesso direto ao Copom online, sistema interno da Polícia Militar de São Paulo; suspeitou-se que um policial militar forneceu o seu acesso ao suspeito.

A Polícia Militar do Estado de São Paulo admite o vazamento: instauraram um inquérito interno para apurar as circunstâncias dos fatos e responsabilidades pelo vazamento das informações.

O Copom online tem as seguintes funcionalidades: funções operacionais, visualizar a unidade de serviço, calcular multidão, visualizar ocorrências, mapa de dispersão, mapa de calor, localizar ocorrências, consultar pessoas, consultar veículos,

localizar ocorrências, logradouro, relatório de radares, grade operacional, painel do supervisor, membros que compõem aquela equipe e os locais onde estão.

Seguem algumas ideias de proteção neste caso: adotar políticas restritivas de segurança e informação, políticas de controle de acesso a sistemas, desenvolvimento seguro de sistemas; utilizar softwares e ferramentas que possibilitam a implementação de segurança da informação, havendo, claro, sessões de treinamentos e campanhas de conscientização para que os colaboradores sejam a primeira linha de defesa.

4) ETIAS (European Travel Information and Authorization System)

A comunidade europeia para melhorar a segurança interna, prevenir a imigração ilegal, proteger a saúde pública e reduzir os atrasos nas fronteiras, a Comissão Europeia exigirá dos brasileiros e de outros cidadãos de 14 países da América Latina uma permissão da União Europeia em suas viagens de turismo, negócios, para cuidados médicos ou se precisarem de uma conexão na Europa.

O Etias (Sistema Europeu de Informações e Autorização de Viagem) não é um visto, mas uma autorização que os viajantes devem obter ao fazer seus planos de viagem para o Espaço Schengen (incluem 26 países, mas não inclui o Reino Unido). Atualmente, os cidadãos de países da América Latina que não precisam de visto podem viajar livremente entre esses países. O Etias passa a ser um requisito obrigatório para entrar neste espaço.

Para obter o Etias, é preciso informar vários dados pessoais e outras informações, além de responder a um questionário de segurança. Para maiores de 18 anos, é cobrada uma taxa de 7 euros. O processo de solicitação e obtenção acontece em minutos, mas, caso seja necessária uma consulta adicional, o processo levará de 96 horas a duas semanas.

Em comunicado, o Conselho Europeu disse que, “antes do embarque, as companhias aéreas e marítimas terão a obrigação de verificar se os cidadãos de países sujeitos a uma autorização possuem um Etias válido.

A autorização será válida por três anos, mas será cancelada se o passaporte do candidato expirar.

Na regulamentação do ETIAS há a definição do GDPR, como qualquer forma de processamento automatizado de dados pessoais que consiste no uso de dados para avaliar certos aspectos pessoais relacionados a uma pessoa singular, em particular analisar ou prever aspectos relativos ao desempenho da pessoa singular no

trabalho, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos.

O GDPR considera problemático o perfil quando se trata do direito de proteção de dados: o artigo 22 (1) confere aos titulares de dados o direito geral de não serem submetidos com exceções listadas no artigo 22. O rastreamento do ETIAS pode, portanto, ser caracterizada como perfil na medida em que os dados pessoais dos viajantes estão sujeitos a processamento automatizado [por meio do algoritmo referido no artigo 28.º, n.º 1], a fim de avaliar se eles apresentam certas características que se supõe correlacionadas com certos "riscos" de segurança, migração ou saúde.

8 CONSIDERAÇÕES FINAIS

Um dos problemas na segurança pública no Brasil sempre foi a gestão do uso de informações.

Com o fito de diagnosticar esse problema, o Fórum Brasileiro de Segurança Pública, em parceria com o governo federal, realizou uma extensa pesquisa nos órgãos estaduais de segurança pública, onde verificou todos os fatores envolvidos nessa gestão: estatísticas, servidores, equipamentos e afins.

No entanto, com o advento da legislação sobre o Plano Nacional de Segurança Pública e do Fundo Nacional de Segurança Pública, foi explicitada a participação dos municípios, em especial de suas guardas municipais, no sistema de segurança pública. Assim, o município também passou a ser um gestor de informações de segurança pública, merecendo ser alvo da mesma pesquisa realizada nas polícias estaduais.

Diante da ausência de pesquisas no âmbito dos municípios, decidimos suprir essa lacuna escolhendo a Secretaria Municipal de Segurança Urbana e sua Guarda Civil Metropolitana como paradigma.

Aplicando ferramentas de pesquisa de campo, como entrevistas e observações diretas, procuramos aprender sobre todos os setores e servidores que lidam as informações de segurança pública no órgão, em todas as fases do fluxo de informações, quando também conhecemos as iniciativas em andamento.

Consideramos diversas teorias para fazer a melhor análise das informações coletadas e orientar as propostas, não sem deixar de adotar, como benchmarking, o choque de gestão da Polícia de New York nos anos 90, visto que é uma polícia municipalizada, modelo mais próximo das nossas guardas que as polícias estaduais, por também terem a atribuição de zeladoria urbana também.

Todo esse arcabouço teórico e prático permitiu isolarmos e identificarmos os maiores problemas no fluxo de informação de segurança pública, mesmo que alguns problemas sejam apenas incidentais ao tema.

Em relação às propostas, procuramos nos ater ao que realmente pode funcionar, considerando as teorias, práticas e experiências profissionais dos autores e que estivesse afetando o fluxo de informações de segurança pública em alguma fase: coleta, tratamento, encaminhamento, compartilhamento ou uso.

Como a Lei Geral de Proteção de Dados é um tema atual, com previsão de entrada em vigor poucos meses após a realização desta dissertação, resolvemos concentrar o debate em um capítulo específico, fazendo menções em outros apenas para demonstrar a ligação com o desenvolvimento.

O novo Regulamento Brasileiro de Proteção de Dados, que terá a sua aplicabilidade a partir de 20 de Agosto de 2020, centra-se nas pessoas físicas e na proteção de seus dados pessoais, na medida em que a proteção dos dados hoje é entendida como direito fundamental do homem, por força de evolução do conceito de privacidade, que há tempos, já era reconhecida com direito fundamental.

Para se ter a proteção dos dados pessoais, a lei assegura direitos aos titulares dos dados, com uma vasta gama de regras protetivas atreladas aos princípios da transparência e da informação; os titulares dos dados possuem a prerrogativa de invocar esses direitos sob as condições postas no regulamento, nem todos os requerimentos serão acolhidos, haja vista em que muitas situações, os responsáveis pelos tratamentos (controle) poderão sustentar razões diversas e relevantes e que normalmente dizem respeito à base legal do tratamento, a justificar a possibilidade de sua perfeita e regular continuidade.

Toda e qualquer solicitação deverá ser processada pelo responsável pelo tratamento, a quem observará o prazo de lei e manter clara a comunicação com o titular dos dados, ou seja, trata-se de um tema sensível e crucial para a completa aplicação da lei, na qual centra-se na figura do titular dos dados e prioriza os direitos a ele assegurados.

Dado pessoal é o insumo da nova economia e de políticas públicas modernas pautadas em estratégias de transformação e inovação digital. Off-Line ou on-line, pessoas, conscientemente ou não, direta ou indiretamente, fornecem inúmeros dados pessoais para as mais diversas atividades, que também são coletados e tratados para interesses públicos. Na era digital, invariavelmente negócios são baseados em dados e isso não mudará, pelo contrário, na era do Big Data, a internet das coisas e da inteligência artificial, é impossível pensar no oposto.

A discussão da proteção de dados pessoais é baseada exatamente nos atuais e futuros modelos de negócio, e não há qualquer hipótese que se sustente juridicamente de impedir uma economia baseada em dados, que são coletados, tratados e utilizados como contrapartida para excelentes serviços, públicos ou

privados, é preciso haver freios e contrapesos para que tal exploração seja realizada de forma justa, transparente e proporcional.

Temos a expectativa de que as soluções propostas sejam adotadas, visto que a natureza restritiva dos aspectos orçamentários, algo natural na administração pública, não é um fator decisivo para que parte das propostas seja colocada em prática.

Por fim, podemos afirmar que a motivação deste trabalho ultrapassa o tema escolhido. Quando estamos analisando políticas públicas, não estamos sendo apenas acadêmicos ou profissionais. Em última instância, somos todos parte da sociedade que é a cliente das políticas públicas, logo, sempre desejamos ver a melhor aplicação dos recursos públicos, mediante as melhores práticas de gestão, trazendo os melhores impactos para a nossa geração e para as gerações futuras.

REFERÊNCIAS

1988, C. d. (03 de Novembro de 2019). ***Constituição da República Federativa do Brasil de 1988***. Fonte: Planalto.gov.br:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

ARRETCHE, M. T. (1998). ***Tendências no Estudo sobre Avaliação***. In: RICO, Elizabeth Melo (org.). *Avaliação de Políticas Sociais: Uma Questão em Debate*. . São Paulo: Editora Cortez.

Bank Info Security. (12 de Outubro de 2019). Fonte:

<https://www.bankinfosecurity.com/gdpr-europe-counts-65000-data-breach-notifications-so-far-a-12489>

Blum, V. N. (2018). ***Comentários ao GDPR Regulamento Geral de Proteção de Dados da União Europeia***. São Paulo: Thomson Reuters .

____ (s.d.). ***GDPR Regulamento Geral de Proteção de Dados da União Europeia***, Coordenação: V.

BOBBIO, N. (1995). ***O Positivismo Jurídico: Lições de filosofia do direito***. São Paulo: Ícone.

Brasileiro, G. (04 de Novembro de 2019). ***Decreto n. 9630, de 26 de dezembro de 2018***. *Institui o Plano Nacional de Segurança Pública e Defesa Social e dá outras providências*. Fonte: Planalto.gov.br: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9630.htm

_____. (03 de Novembro de 2019). ***Lei n. 13.675, de 11 de junho de 2018***. *Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS)*. Fonte: Planalto.gov.br: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm

_____. (2019 de Novembro de 2019). ***Lei n. 13.709, de 14 de agosto de 2018***. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Fonte: Planalto.gov.br: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

_____. (03 de Novembro de 2019). *Planalto.gov.br*. Fonte: BRASIL. Lei n. 12.232, de 29 de abril de 2010. : http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12232.htm

_____. (03 de Novembro de 2019). *Planalto.gov.br*3444.htm Acessado em 3 de novembro de 2017. Brasília, 2017. Fonte: Lei n. 13.444, de 11 de maio de 2017. Dispõe sobre a Identificação Civil Nacional (ICN). : http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm

Daryus, **Lei GDPR e LGPD: qual a relação e os impactos no Brasil?** (20 de Outubro de 2019). Fonte: Daryus: <https://blog.daryus.com.br/lei-gdpr-e-lgpd-qual-a-relacao-e-os-impactos-no-brasil/>

DI PIETRO, M. S. (2014). **Direito Administrativo**. 27 Edição. São Paulo: Atlas.

FARAH, M. (2001). **Parcerias, novos arranjos institucionais e políticas públicas no nível local de governo**. . Rio de Janeiro : Revista de Administração Pública-RAP.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA - FBSP. **Gestão e disseminação de dados na Polícia Nacional de Segurança Pública - diagnóstico dos sistemas estaduais de segurança pública**. . (2010).

_____. e Instituto DataFolha. **Rio sob intervenção** (relatório). Rio de Janeiro. 2018.

GDPR in Numbers. (12 de Outubro de 2019). Fonte: GDPR: <https://www.gdprtoday.org/gdpr-in-numbers-4/>

Gonçalves, F., & CAPELLA, A. C. (2015). **O Processo de Agenda-Setting para os Estudos das Políticas Públicas**. . RP3 - Revista de Pesquisa em Políticas Públicas.

Helpnetsecurity. (12 de Outubro de 2019). Fonte: Helpnetsecurity: <https://www.helpnetsecurity.com/2019/02/07/gdpr-numbers-janua>

Intersoft Consulting. (s.d.). Fonte: Intersoft Consulting: <https://gdpr-info.eu/>

LIMA, R. S. (2013). **(Re)Estruturação da Segurança Pública no Brasil**. In: MINGARDI, G. (ORG). *Política de segurança: os desafios de uma reforma*. [s.l.]. Fundação Perseu Abramo.

LIPSKY, M. (2019). **Burocracia de nível de rua: dilemas do indivíduo nos serviços públicos**. . Brasília: Enap .

LOTTA, G. S. (2015). **Burocratas de médio escalão: novos olhares sobre velho atores da produção de políticas públicas**. in: LOTTA, Gabriela e CAVALCANTE, Pedro (orgs.). *Burocracia de médio escalão: perfil, trajetória e atuação*. Brasília: Enap.

MARTINS, H. F., & MARINI, C. (2010). **Um guia de governança para resultados na administração pública**. . Publix.

MEZZAROBBA, O., & MONTEIRO, C. S. (2004). **Manual de metodologia da pesquisa no direito: atualizado de acordo com as últimas normas da ABNT**. . Saraiva.

MINAYO, M. C. (1993). **Quantitativo-Qualitativo: Oposição ou Complementaridade?** . Rio de Janeiro.

MORGAN, G. (2002). **Imagens da organização**. Edição Executiva. São Paulo: Atlas.

OLIVEIRA, A. (2013). **Burocratas da linha de frente: executores e fazedores das políticas públicas**. Revista de Administração Pública.

PATTON, M. Q. (2002). **Qualitative Research and Evaluation Methods**. . Sage Publications.

PAULO, P. d. (s.d.). **Decreto n. 50.388, de 17 de janeiro de 2009**. Reorganiza a secretaria municipal de segurança urbana-smsu, em cumprimento ao disposto no art. 28 da l.14879, de 07/01/09, bem como dispõe sobre o seu quadro de cargos de provimento em c. São Paulo (Prefeitura). Decreto n. 50.388, de 17 de janeiro de 2009. Reorganiza a secretaria municipal de segurança urbana-smsu, em cumprimento ao disposto no art. .

PINHEIRO, P. P. (2019). **Proteção de Dados Pessoais, Comentários à Lei Número 13.709/2018(LGPD)**. São Paulo: Saraiva.

SECCHI, L. (2017). **Políticas públicas: conceitos, esquemas de análise, casos práticos**. 2a. ed. São Paulo: Cengage Learning.

SPINK, P. K. (2017). **Avaliação Democrática: Propostas e Práticas**. in: ALVES, Mário Aquino. BRIGAGÃO, Jacqueline, BURGOS, Fernando. *Por uma gestão pública democrática: 25 anos de Centro de Estudos em Administração Pública e Governo. Programa Gestão Pública e Governo. Programa Gestão Pública e Cidadania*.

WILLIS, J. J. (2007). “**Making Sense of COMPSTAT: A Theory-Based Analysis of Organizational Change in Three Police Departments.**” . Law and Society Review Mar.

_____, MASTROFSKI, S. D., & WEISBURD, D. (2004). **Compstat and bureaucracy: A case study of challenges and opportunities for change**. *Justice Quarterly*, v. 21, n. 3, p. 463-496.

WU, X., RAMESH, M., HOWLETT, M., & FRITZEN, S. (2014). **Guia de políticas públicas: gerenciando processos**. . Brasília: Enap.

APÊNDICE I – entrevista

Uso de informação de segurança pública na Secretaria Municipal de Segurança Urbana

Prezado(a) participante: este formulário contém perguntas sobre seu histórico profissional, detalhes da sua função e iniciativa em que trabalha. A finalidade é subsidiar nosso trabalho de conclusão de curso no Mestrado Profissional em Gestão e Políticas Públicas na FGV. Embora pegamos o nome e outros dados pessoais no começo, somente os dados **desidentificados** serão utilizados. Isso significa que não divulgaremos seu nome e dados pessoais nem no nosso trabalho e nem para o seu empregador. Os dados são somente para entendermos o perfil do servidor e como isso se relaciona com as atribuições. Agradecemos sua colaboração! Atenciosamente, Leonardo e **Livia** (alunos FGV)

Endereço de e-mail *

Endereço de e-mail válido

Este formulário coleta endereços de e-mail. [Alterar configurações](#)

Nome *

Texto de resposta curta

Data de nascimento *

Mês, dia, ano

Raça/Cor da Pele *

☐ Branca

☐ Negra

☐ Parda

☐ Indígena

☐ Amarela

Segundo o organograma da Secretaria, quantos superiores você possui até (e inclusive) o Secretário da Pasta? (Ex.: se existir um(a) e este for subordinado diretamente ao Secretário, você possui 2 superiores) *

Texto de resposta curta

Conte-nos, de forma resumida, como você chegou na atual função: convite, progressão funcional.... *

Texto de resposta longa

Formação acadêmica *

☐ Ensino fundamental

☐ Ensino médio

☐ Ensino médio técnico

☐ Ensino superior - curta duração (até 2 anos)

☐ Ensino superior - duração comum (4 anos ou mais)

☐ Especialização/ pós graduação lato sensu

☐ Mestrado (strictu sensu)

☐ Doutorado (strictu sensu)

Tempo de serviço público (em anos) *

Texto de resposta curta

Tempo na atual função (em anos) *

Texto de resposta curta

Contratação para a função atual *

☐ Servidor de carreira designado

☐ Servidor de carreira aposentado, porém comissionado

☐ Servidor comissionado, oriundo de carreiras de fora da Secretaria

☐ Servidor comissionado, oriundo da iniciativa privada

☐ Outros...

Qual o nome exato do setor em que trabalha (setor, divisão, departamento....) *

Texto de resposta curta

Possui subordinados/auxiliares? *

☐ Sim

☐ Não

Qual a relação entre sua formação acadêmica e a função que exerce? *

☐ Minha formação acadêmica é mais que suficiente para exercer a função.

☐ Minha formação acadêmica é suficiente para exercer a função.

☐ Minha formação acadêmica é menos que suficiente para exercer a função.

☐ Minha formação acadêmica é insuficiente para exercer a função.

☐ Minha formação acadêmica é não possui nenhuma relação com a função que exerce.

Você recebeu algum treinamento ou capacitação pela Secretaria ou outro órgão da própria Prefeitura para exercer a sua função? *

☐ Sim

☐ Não

Existe alguma documentação para consulta, física ou eletrônica, onde tenha informações sobre suas atribuições e do seu setor? *

☐ Sim

☐ Não

☐ Não sei.

Qual é a sua função? Quais as suas atribuições? *

Texto de resposta longa

Quando iniciou o exercício da sua função, você sentiu a necessidade de algum conhecimento específico (ex.: maior conhecimento de Windows, Linux, Pacote Office, programa específico da função, normas, procedimentos burocráticos....) *

- ☐ Sim
- ☐ Não

Após o seu início da função, houve alguma capacitação ou treinamento para você trabalhar melhor? *

- ☐ Não houve.
- ☐ Sim, mas apenas uma vez desde que iniciou.
- ☐ Sim, ocorre esporadicamente.
- ☐ Sim, ocorre com frequência anual.
- ☐ Sim, ocorre com frequência mensal.
- ☐ Sim, ocorre com frequência semanal.

Existe algum estímulo, por parte do seu setor ou da Secretaria, para que você faça cursos de qualificação para a sua função? *

- ☐ Sim
- ☐ Não

Em caso de dúvidas no exercício da função, como você resolve? *

- ☐ Tenho liberdade para pesquisar uma solução. Se resolver, não preciso reportar ao meu superior.
- ☐ Tenho liberdade para pesquisar uma solução. Se resolver ou não, preciso reportar ao meu superior.
- ☐ Existe um outro servidor ou setor com a função de dirimir dúvidas.
- ☐ Necessariamente preciso relatar para o meu superior imediato e ele decidirá/orientará.
- ☐ Outros...

Existem formas de você propor alterações na sua função ou no seu setor?

- ☐ Não existem formas para propor.
- ☐ Posso propor a qualquer momento para o meu superior imediato.
- ☐ Existem reuniões apropriadas para esse fim diariamente (ex.: preleção)
- ☐ Existem reuniões apropriadas para esse fim semanalmente.
- ☐ Existem reuniões apropriadas para esse fim mensalmente.
- ☐ Existem reuniões apropriadas para esse fim esporadicamente.
- ☐ Outros...

Quais equipamentos você tem acesso para a sua função, desde mobiliários, materiais de escritório e materiais de informática? *

Texto de resposta longa

Existe uma remuneração adicional para quem trabalha com o uso de informações de segurança pública na Secretaria? *

- ☐ Sim
- ☐ Não

No exercício da sua função, qual o seu poder de decisão? *

- ☐ Não possuo poder de decisão.
- ☐ Posso pouco poder de decisão, posso escolher entre 2 ou 3 opções de atuação.
- ☐ Posso médio poder de decisão, tenho mais de 3 opções de atuação.
- ☐ Posso alto poder de decisão, posso decidir livremente como vou atuar.

Como o seu superior imediato analisa seu poder de decisão? *

- ☐ Não possuo poder de decisão, cumpro exatamente o que o meu superior determina.
- ☐ Meu superior analisa cada decisão minha no exercício da função.
- ☐ Meu superior analisa minhas decisões no exercício da função diariamente.
- ☐ Meu superior analisa minhas decisões no exercício da função semanalmente.
- ☐ Meu superior analisa minhas decisões no exercício da função mensalmente.
- ☐ Meu superior analisa minhas decisões no exercício da função esporadicamente.
- ☐ Meu superior analisa minhas decisões no exercício da função raramente ou somente quando minha decis ...
- ☐ Minhas decisões não são analisadas pelo meu superior imediato.

Relação entre a sua função e os materiais disponíveis no seu setor. *

- ☐ Os materiais disponíveis são mais que suficientes para cumprir minhas atribuições.
- ☐ Os materiais disponíveis são suficientes para cumprir minhas atribuições.
- ☐ Os materiais disponíveis são insuficientes para cumprir minhas atribuições.

Relação entre a sua função e técnicas e materiais complexos. *

- ☐ Não necessito de nenhuma técnica ou material complexo no exercício da minha função.
- ☐ Tenho conhecimento suficiente para usar a técnica ou material complexo necessários no exercício da min ...
- ☐ Não tenho e/ou não recebi conhecimento suficiente para usar a técnica ou material complexo necessário ...
- ☐ Precisei de capacitação ou treinamento a técnica ou material complexo necessários no exercício da minh ...

Você tem conhecimento ou recebeu capacitação/treinamento sobre a Lei Geral de Proteção de Dados Pessoais (LGPD)? *

- ☐ Tenho ou recebi totalmente
- ☐ Tenho ou recebi parcialmente
- ☐ Tenho ou recebi insuficientemente
- ☐ Não tenho ou não recebi totalmente

Você tem conhecimento ou recebeu capacitação/treinamento sobre como as informações que você lida na sua função ou no seu setor são protegidas (art. 37 da LGPD)? Relate como você e seu setor lidam com esse tema, inclusive parcialmente. *

Texto de resposta longa

No art.38, parágrafo único, da LGPD, diz que a autoridade nacional (governo) pode determinar a elaboração de relatório que "...deverá conter, no mínimo, uma descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados". Você ou seu setor possuem recursos para elaborar esse tipo de relatório? Relate como você e seu setor lidam com esse tema, inclusive parcialmente.

Texto de resposta longa

O art. 35 da LGPD diz que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Você possui conhecimento para cumprir isso? Seu setor possui protocolos para cumprir isso? E parcialmente? Relate como você e seu setor lidam com esse tema, inclusive parcialmente.

Texto de resposta longa

O art. 49 da LGPD diz que "os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares." O sistema (ou sistemas) que você usa cumpre isso? Seu setor possui protocolos para cumprir isso? E parcialmente? Relate de forma resumida.

Texto de resposta longa

Comentários, críticas e/ou sugestões sobre o questionário.

Texto de resposta longa

Comentários, críticas e/ou sugestões sobre a sua função.

Texto de resposta longa

Comentários, críticas e/ou sugestões sobre a Secretaria.

Texto de resposta longa

Comentários, críticas e/ou sugestões sobre o uso de informações de segurança pública

Texto de resposta longa

Comentários, críticas e/ou sugestões sobre qualquer outro tema

Texto de resposta longa

APÊNDICE II

A SMSU vem solicitar que a requisitante forneça uma solução que tenha uma política de proteção de dados conforme descrito abaixo, pois a SMSU tem uma política de segurança de informação que determinará sempre a proteção dos dados que estão na SMSU.

1) Objetivo:

O controle da sua privacidade é muito importante para SMSU. Por este motivo, solicitamos que a solução siga esta Política, que abrange a forma como coletamos, usamos, divulgamos, transferimos e armazenamos suas informações.

Através da prática desta Política, A SMSU buscará ter transparência em relação à sua forma de atuar. É importante que os todos dediquem um tempo para conhecer nossas práticas de privacidade.

2) Aplicação da Política

Esta Política é endereçada a proteger todos os usuários e ações de segurança da SMSU. Para buscar a garantia de que suas Informações Pessoais estão seguras, comunicamos ativamente nossas diretrizes de privacidade e segurança a:

- (i) os Colaboradores e Administradores da SMSU,
- (ii) os Colaboradores e Administradores das empresas contratadas pela SMSU,
- (iii) os Representantes Legais da SMSU em São Paulo.

Além disso, A SMSU exige que os listados acima atuem ativamente na aplicação desta

Política, impondo-se lhes estritamente as salvaguardas de privacidade.

A SMSU considerará, dentre outros motivos, que o descumprimento desta Política significa uma grave insubordinação por parte do Administrador e Colaborador. Muitas das diretrizes desta Política são igualmente aplicáveis aos Terceiros. Todos os Colaboradores e Administradores da SMSU, especialmente aqueles do Comitê de Conduta, são responsáveis por garantir que esta Política seja compreendida e implementada pelos Terceiros, especialmente (i) pelas empresas contratadas da SMSU, (ii) pelos Representantes Legais da SMSU, (iii) pelos parceiros da SMSU, e (iv) pelos fornecedores da SMSU.

Todos os Colaboradores e Administradores da SMSU deverão seguir os princípios e diretrizes desta Política. Para tanto, eles devem buscar e disseminar

ativamente informações necessárias, participando, inclusive, de todos os treinamentos promovidos pela SMSU.

Em hipótese alguma, nenhum dos abrangidos por esta Política tem ou terá autorização para descumpri-la, direta ou indiretamente, mediante o uso de quaisquer terceiros.

Esta Política será aplicável e deverá ser cumprida ainda que, em determinados aspectos, a legislação aplicável seja menos rigorosa.

3) Definições

Termo Descrição

3a) Administrador (es)

Significa, quando referidos no singular ou plural, os Secretários, os membros do Conselho de Administração? E dos Comitês de Assessoramento a este último.

3b) Anonimização

Processo pelo qual as Informações se tornam não identificáveis, considerando-se a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu processamento.

3c) Cidadãos

São os cidadãos que precisaram dos serviços prestados pela SMSU.

3d) Colaborador (es)

Inclui: (i) os empregados contratados mediante contrato de trabalho e sob o regime da Consolidação das Leis do Trabalho, (ii) os estagiários, (iii) os menores aprendizes e (iv) os empregados temporários.

3e) Confidencialidade

Propriedade da informação, em que a mesma não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

3f) SMSU

São todas as diretorias que compõem a SMSU, ou seja, Secretaria Municipal de Segurança Urbana (com todas as suas diretorias e processos).

3g) Informações Pessoais

Qualquer informação relacionada direta ou indiretamente ao Cidadão ou a uma pessoa qualquer e que possa ser usada para identificar ou contatar uma pessoa ou Cidadão. Consistirá, especialmente, informação de caráter físico, psicológico, mental, econômico, cultural ou social do Cidadão ou pessoa.

3h) Informações Não Pessoais

Dados que, analisados de forma independente, não permitem a associação direta a um Cidadão específico.

3i) Política

Significa esta Política de Proteção à Privacidade.

3j) Pseudonomização

Processo pelo qual as Informações Pessoais relativas a um Cidadão deixam de poder ser atribuídas a este Cidadão sem recorrer a informações suplementares. Observe-se que estas

Informações suplementares devem ser mantidas separadamente e sujeitas a medidas técnicas e organizacionais para garantir que as Informações Pessoais não possam ser atribuídos ao Cidadão individualmente considerado.

3k) Representante (s) Legal (ais)

Significa toda a pessoa física ou jurídica que tenha recebido um mandato, judicial ou não, para representar jurídica e/ou negocialmente a SMSU.

3l) Terceiro (s)

Significa os contratados que não sejam Colaboradores e/ou Administradores, mas se apresentam ou atuam em nome da SMSU, inclusive, prestadores de serviços, consultores e quaisquer outras pessoas físicas ou jurídicas.

3m) Termo de Consentimento de Uso de Dados Pessoais

Autorização dada pelo Cidadãos para uso das informações pessoais, nos termos desta Política.

Ao consentir com o uso, os Cidadãos que já possuem informações pessoais na base de dados da SMSU consentem com o uso destas informações pretéritas.

3n) Tratamento da informação

Uso adequado da informação de acordo com as diretrizes estabelecidas nos diversos cenários que ocorrem no dia a dia (armazenamento, transmissão, descarte, impressão, etc.).

4) Introdução

A Política de Proteção à Privacidade trata do uso e tratamento de dados pessoais, trazendo diretrizes, procedimentos e regulamentação ao tema.

5) Diretrizes

Coleta e uso de Informações Pessoais

Pode ser solicitado que você forneça suas Informações Pessoais a qualquer momento que esteja em contato com a SMSU. Somente compartilharemos e

utilizaremos essas Informações Pessoais de maneira consistente com o indicado nesta Política. As informações coletadas também podem ser analisadas conjuntamente com outras informações a que a SMSU tiver acesso, de forma a garantir o fornecimento e melhoria da segurança pública, sempre respeitando o disposto nesta Política.

Exemplos de Informações Pessoais que podem ser coletadas e armazenadas ao utilizar nossos serviços (SMSU), interage com as ferramentas e interfaces disponibilizadas no site ou contato telefônica, podemos coletar várias informações suas, as quais incluem, mas não se limitam, ao seu nome, endereço de correspondência, CPF,

Número da carteira de identidade, telefone, e-mail e preferências de contato. Estas informações podem incluir dados gerais de caráter demográfico (por exemplo, gênero, data de nascimento, estado civil, portador de deficiências ou não).

Ao navegar no nosso website, poderemos coletar informações que permitem identificar seu equipamento (endereço de IP/MAC estático, cookies persistentes) e outras informações que vierem a ser clicadas pelo Cidadão (histórico de atividades, perguntas e respostas relacionadas à segurança etc.).

As Informações Pessoais coletadas pelos nossos canais de comunicação, nos permitem manter o Cidadão atualizado sobre os mais recentes projetos e ações relacionadas à segurança. Se não quiser participar de nossa lista de distribuição, o Cidadão poderá optar por não a receber a qualquer momento, atualizando suas preferências. As Informações Pessoais também são utilizadas para criar, desenvolver, operar, fornece e atender melhor todas as regiões da Cidade de São Paulo.

De tempos em tempos, poderemos usar suas Informações Pessoais para enviar avisos importantes, como comunicações sobre os serviços e alterações em nossos termos, condições e procedimentos. Como essas informações são importantes para sua interação com a SMSU.

Podemos também usar Informações Pessoais para propósitos internos, como auditoria, análise de dados e pesquisas visando a melhoria dos serviços prestados pela SMSU.

A SMSU pode coletar, usar, transferir e revelar Informações não Pessoais para qualquer órgão de segurança. Nestas hipóteses, serão tomadas as medidas necessárias para agregação, anonimização e, se for o caso, pseudonomização das informações, utilizando-se das melhores práticas existentes no país.

Se as Informações Não Pessoais forem agregadas com Informações Pessoais, as informações combinadas serão tratadas como Informações Pessoais enquanto permanecerem combinadas.

Exemplos de usos de Informações Pessoas coletadas

A SMSU poderá utilizar os dados e informações coletados para as seguintes finalidades:

- Responder a eventuais dúvidas e solicitações do Cidadão.
- Cumprimento de ordem judicial.
- Cumprimento de legislações
- Constituir, defender ou exercer regularmente direitos em âmbito judicial ou administrativo.
- Garantir a segurança dos Cidadãos.
- Manter atualizados os cadastros dos Cidadãos para fins de contato por telefone fixo, celular, correio eletrônico, SMS, mala direta, redes sociais ou por outros meios de comunicação.
- Gerar análises e estudos, sejam estatísticos ou identificáveis, com base no comportamento de uso das ferramentas, site, serviços da SMSU.
- Gerar informações que auxiliem no estudo de implantação de novas metodologias da SMSU.
- Aperfeiçoar o uso e a experiência interativa durante a navegação do Cidadão no site e serviços, bem como das demais ferramentas e plataformas lançadas pela SMSU.
- Aprimorar o funcionamento do site, produtos e serviços bem como das demais ferramentas e plataformas lançadas pela SMSU.

Os dados obtidos somente poderão ser acessados por profissionais devidamente autorizados pela SMSU, respeitando a necessidade a que serão submetidos.

Cookies e outras tecnologias

O site, os serviços on-line, os aplicativos interativos, as mensagens de e-mail relacionadas a SMSU podem usar “cookies” e outras tecnologias, como pixel tags e web beacons.

Essas tecnologias nos ajudam a entender melhor o comportamento do Cidadão, informando que partes de nosso site foram visitadas e ajudando e medindo a eficácia das ações e pesquisas na web.

As informações coletadas por cookies e outras tecnologias são tratadas como Informações Não Pessoais. À medida que as Informações Não Pessoais sejam combinadas com Informações Pessoais, as informações combinadas são tratadas como Informações Pessoais para os propósitos desta Política de Privacidade.

Quando o Cidadão usa um dispositivo móvel para acessar os Serviços, é possível limitar as informações que podem ser recolhidas pela SMSU. Os sistemas operacionais dos dispositivos móveis são diferentes – o Cidadão deverá verificar o menu “Configuração” de dispositivo móvel para saber como alterar suas preferências relacionadas a “Limitar Publicidade Rastreada”. Se optar por ativar essa função. A SMSU também utiliza cookies e outras tecnologias para coletar e armazenar Informações Pessoais quando dos serviços, aplicativos e site são utilizados.

Compartilhamento de Informações Pessoais

A legislação e/ou as agentes públicos, locais ou internacionais, poderão requerer da SMSU que revele suas Informações Pessoais. Podemos também revelar Informações Pessoais se for determinado que, para propósitos de segurança nacional, cumprimento da legislação ou outras questões de ordem pública, a revelação será necessária ou apropriada.

Também podemos revelar suas Informações Pessoais se for determinado que a revelação é razoavelmente necessária para impor nossos termos e condições ou proteger nossas operações ou Cidadãos.

Compartilhamento de Informações Pessoais dentro da SMSU

Nós nos comprometemos a manter um nível consistente e adequado de proteção para as Informações Pessoais que são processadas e/ou transferidas entre as diversas pessoas jurídicas.

6) Proteção de Informações Pessoais

A SMSU leva a segurança de suas Informações Pessoais muito a sério. Os serviços on-line da SMSU protegem suas Informações Pessoais durante a transmissão usando criptografia, como Transport Layer Security (TLS). Quando suas Informações Pessoais são armazenadas pela SMSU, utilizamos sistemas de computador cujo acesso é limitado, uma vez que são mantidos em instalações que incluem medidas físicas de segurança. Os dados são armazenados de maneira criptografada, mesmo quando utilizados serviços de armazenamento de Terceiros.

Considerando que nenhum sistema de segurança é absolutamente seguro, a SMSU se exime de quaisquer responsabilidades por eventuais danos e/ou prejuízos

decorrentes de falhas, vírus ou invasões do banco de dados de seus produtos, serviços e site, salvo nos casos em que tiver agido com dolo ou culpa.

Quando algum produto, serviço, aplicativo, fórum de mensagem, sala de bate-papo ou serviços de rede social da SMSU é usado, as Informações Pessoais que o Cidadão compartilha são visíveis a outros Cidadãos e podem ser lidas, coletadas ou usadas por eles. Você é responsável pelas Informações Pessoais que escolhe enviar nesses casos.

Se você listar seu nome e endereço de e-mail em uma postagem de fórum, essas informações serão públicas. Tome cuidado quando usar esses recursos.

Integridade e retenção de Informações Pessoais

A SMSU permite que o Cidadão mantenha facilmente suas Informações Pessoais precisas, completas e atualizadas. Reteremos suas Informações Pessoais pelo período necessário para satisfazer as finalidades descritas nesta Política, a menos que um período de retenção mais longo seja exigido ou permitido pela legislação.

Acesso a Informações Pessoais

O cidadão pode ajudar a assegurar que suas informações e preferências de contato estejam corretas, completas e atualizadas. Para Informações Pessoais armazenadas, ofereceremos o acesso ao cidadão para qualquer finalidade, incluindo solicitar a atualização, correção e exclusão dos dados, contanto que a SMSU não seja obrigada pela legislação ou para fins comerciais legítimos a retê-los.

Podemos recusar o processamento de solicitações que sejam infundadas/vexatórias, prejudiquem a privacidade de outros, violem quaisquer legislações aplicáveis, sejam extremamente impraticáveis ou cujo acesso não seja de outra forma exigido pela legislação.

Solicitações de acesso, correção ou exclusão podem ser feitas por meio do Formulário de Contato de Privacidade. Boa parte das Informações Pessoais mantidas pode ser atualizadas e corrigida pelo próprio cidadão através do mesmo Termo de Consentimento para Uso de Dados Pessoais.

Caso o acesso ou a requisição de correção seja negada, o Grupo DASA comunicará o motivo da negativa por escrito ao cidadão.

Perguntas de privacidade

Se tiver qualquer (i) dúvida sobre esta Política ou sobre o processamento de dados ou (ii) se quiser fazer uma reclamação devido a uma possível violação desta

Política, entre em contato conosco. É possível nos contatar pelo Canal da Conduta. Nós nos esforçaremos para fornecer as informações sobre as opções de reclamação que podem ser aplicáveis a suas circunstâncias.

7) Penalidades

Os Colaboradores e Administradores que descumprirem a Política de Proteção à Privacidade estarão sujeitos às sanções previstas na Política de Consequências.

8) Responsabilidades

A Política de Proteção à Privacidade é de responsabilidade da Diretoria Jurídica e de Compliance.

Referências

Marco Civil da Internet (Lei 12.965/2014)

Lei Geral de Proteção de Dados (Lei 13.709/2018)

ANEXO I

PROPOSTA DE TERMO DE REFERÊNCIA MPGPP-SMSU

Orientador: Prof. Dr. Renato Sérgio de Lima
Orientandos: Leonardo Fonseca Netto e Lívio José Lima e Rocha
Cliente: Secretaria Municipal de Segurança Urbana, representada pelo Sr. Cel. José Roberto Rodrigues de Oliveira.
Proposta: Análise dos processos de produção de informações estatísticas e informações de segurança pública pela Secretaria Municipal de Segurança Urbana (SMSU)

1. Antecedentes

O conceito de governança democrática em segurança pública defende que a segurança pública não se limita às forças policiais estaduais: trata-se de responsabilidade de todos os órgãos públicos, de todos entes federativos, além da sociedade e suas organizações.

Ao analisarmos as melhores práticas em segurança pública que foram implantadas e tiveram sucesso pelo mundo, uma simples amostragem demonstra que os maiores sucessos foram obtidos em práticas municipais. É a administração municipal quem tem o maior contato com os cidadãos e com as causas que afetam, direta e indiretamente, a segurança pública.

Na cidade de São Paulo, que sempre consta como uma das maiores metrópoles do mundo em qualquer ranking, a administração municipal conta com uma Pasta especializada para a segurança pública: a Secretaria Municipal de Segurança Urbana – SMSU, assim denominada pela Lei Municipal n. 13.396, de 26 de julho de 2002.

Entre os órgãos que compõe tal Pasta, destaca-se a Guarda Civil Metropolitana, criada pela Lei Municipal n. 10.115/1986 e reconhecida como integrante da segurança pública no art.144, §8º da Constituição Federal.

Pelas atribuições da SMSU previstas na legislação, não resta a menor dúvida da importância da Pasta como integrante da segurança pública.

2. Problemas

Com a edição da Lei Federal nº 13.675/2018 e os Decretos Federais nº 9.489/2018 e 9.630/2018, tivemos a criação e regulamentação da Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e do Sistema Único de Segurança Pública (Susp). Essa legislação é expressa em determinar a ação coordenada dos órgãos de segurança pública dos entes federativos, estaduais e municipais.

A PNSPDS, entre vários princípios, cita a “promoção da produção de conhecimento sobre segurança pública”. Entre as diretrizes, ela elenca

“sistematização e compartilhamento das informações de segurança pública, prisionais e sobre drogas, em âmbito nacional”. Praticamente repete tal diretriz na lista de objetivos quando diz que “integrar e compartilhar as informações de segurança pública, prisionais e sobre drogas”.

Por fim, mas não menos importante, as guardas municipais são citadas nominalmente como integrantes operacionais do Susp.

Essa legislação citada, transpondo para o nível municipal, significa que, no caso específico da SMSU, há necessidade de diagnosticar se o processo de produção de estatísticas e informações de segurança pública da Pasta atendem, plenamente, os parâmetros de tal legislação.

Para verificar isso, são necessárias que algumas perguntas, como as listadas abaixo, sejam respondidas:

- a – como é feita a coleta de dados?
- b- como são inseridos?
- c – como são transmitidos?
- d – qual perfil de quem lida com os dados?
- e – como chegam nos tomadores de decisão?
- f – qual a pertinência dos dados coletados?
- g – como esses processos afetam a gestão pública da Pasta?

3. Objetivos

A finalidade do trabalho é analisar esse fluxo de informações, em seus aspectos organizacionais, tecnológicos e finalísticos.

Especificamente, ao final, pretendemos responder as seguintes perguntas:

- o que pode ser melhorado nos processos?
- quais são as propostas que podemos elaborar?

4. Abordagem

Análise de documentos e dados disponibilizados pelo cliente e seus funcionários. Entrevistas com diversos funcionários responsáveis pelos pontos-

chaves e suas propostas de melhoria e recomendações quanto ao formato organizacional, formas de controle e mecanismos de transparência interna ou externa. Análise tecnológica dos processos envolvidos. Levantamento de campo dos setores envolvidos.

5. Metodologia

A ser definida pela equipe.

6. Produtos

Serão produzidos os seguintes produtos:

- a-) relatório final a ser protocolado na Secretaria de Registro da EAESP-FGV até o dia 31 de agosto de 2019;
- b) Apresentação do relatório diante de banca, com participação do representante da organização envolvida;
- c) Relatório individual de cada integrante da equipe contendo uma abordagem mais específica sobre algum ponto do relatório;
- d) Apresentação dos resultados aos gestores da instituição parceira.

7. Conteúdo

Relatório elaborado pela equipe contendo:

- a) Diagnóstico da situação e análise;
- b) Proposta de medidas específicas e justificativas, além de procedimentos relacionados à implementação das medidas propostas. As medidas propostas devem ser priorizadas e diferenciadas para o curto, médio e longo prazo;
- c) Anexos: lista de participantes; este termo de referência; lista de pessoas entrevistadas; fontes de dados consultados;
- d) Referências bibliográficas.

Cliente:

Secretaria Municipal de Segurança Urbana – SMSU
Rua da Consolação, 1379
São Paulo – SP



Representante:

José Roberto Rodrigues de Oliveira (assinado no original)
Secretário

Contato:

Sandra Helena Peticarrari

ANEXO II

 CIDADE DE SÃO PAULO SEGURANÇA URBANA	 GUARDA CIVIL METROPOLITANA	Visto do CR	
		Controle da Unidade	
Unidade:		Nº	Nº Sist.

ROTEIRO DIÁRIO DE POLICIAMENTO

<input type="checkbox"/> APÉ <input type="checkbox"/> VIATURA <input type="checkbox"/> BICICLETA <input type="checkbox"/> MOTO <input type="checkbox"/> NÁUTICA <input type="checkbox"/> DRONE <input type="checkbox"/> PATINS <input type="checkbox"/> PATINETE <input type="checkbox"/> OUTROS _____								
Data	Hs. Início	Hs. Término	Placa	Prefixo Rádio	KM Inicial	KM Final	Nº Talão	ORDINÁRIO <input type="checkbox"/>
								DEAC <input type="checkbox"/>
ENC:			RF:		MOT:		RF:	
AUX:			RF:		AUX:		RF:	
AUX:			RF:		AUX:		RF:	
Hr. Cetel	Hr. no Local	Hr. Encer.	Natureza Ocorrência /	Local			Talão	

Nº	Indicador	Cod. / CEP	Endereço / Posto	Nº	Hs. Início	Hs. Término	KM/D	Observação
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
Grupos			Atividades					
AT 1-Atividades de Policiamento			AT1.1-Deslocamento AT1.2-Patrolhamento AT1.3-Policiamento Temporário AT1.4-Policiamento Fixo AT1.5-Intervenção Policial					
AT 2-Suporte Operacional			AT2.1-Vídeo Monitoramento AT2.2-Operador de Rádio AT2.3-Armaria					
AT 3-Atividade Institucional			AT3.1-Representação AT3.2-Reunião AT3.3-Cerimônia					
			AT4-Atividade Disciplinar AT5-Atividade Física					
AT 6 - Intervalo			AT6.1-Alimentação AT6.2-Abastecimento AT6.3-Preparação/Verificação AT6.4-Reparo/Manutenção AT6.5-Proteção					

[illegible]

ANEXO III

Deveres do Motorista		 Prefeitura do Município de São Paulo																	
I – Inspeccionar antes da partida <input type="checkbox"/> combustível, óleo e água <input type="checkbox"/> pneus, buzina, limpador de pára-brisa <input type="checkbox"/> faróis, molas e amortecedores <input type="checkbox"/> correia do ventilador <input type="checkbox"/> bateria e cabos elétricos <input type="checkbox"/> espelho retrovisor		Ordem de Serviço Externo <div style="display: flex; justify-content: space-between;"> nº _____ </div> <div style="display: flex; justify-content: space-between;"> VTR. Nº.: _____ data _____ </div>																	
II – Inspeccionar durante o serviço <input type="checkbox"/> direção e embreagem <input type="checkbox"/> freios de pé e mãos <input type="checkbox"/> aquecimento do motor <input type="checkbox"/> dinamo e amperímetro		<div style="display: flex; justify-content: space-between;"> motorista /operador _____ reg. Funcional _____ Distintivo _____ </div>																	
III – Inspeccionar após o serviço <input type="checkbox"/> combustível, óleo e água <input type="checkbox"/> funcionamento do motor <input type="checkbox"/> vazamentos em geral <input type="checkbox"/> bateria e cabos elétricos		<div style="display: flex; justify-content: space-between;"> apresentar-se ao funcionário sr. S.M.S.U. / G.C.M. ID 10 </div> <div style="display: flex; justify-content: space-between;"> da divisão _____ unidade _____ </div> <div style="display: flex; justify-content: space-between;"> Av. Santos Dumont, 767 – Bom Retiro </div> <div style="display: flex; justify-content: space-between;"> endereço _____ </div>																	
No Acidente: 1 - sinalize o local. 2 - não discuta e evite comentários. 3 - anote testemunhas. 4 - anote os dados necessários. 5 - avise o chefe mais próximo.		<div style="display: flex; justify-content: space-between;"> com a viatura prefixo _____ placas _____ </div> <div style="display: flex; justify-content: space-between;"> carimbo e assinatura do encarregado _____ reg. Funcional _____ </div>																	
Havendo Vítimas: 1 - preste socorro, mesmo que não seja do seu carro. 2 - prestejia as autoridades e não abandone o local. 3 - seja sereno e educado.		CONTROLE DO RELÓGIO <div style="border: 1px solid black; padding: 5px; text-align: center;"> INÍCIO <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">R</div> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">C</div> </div> TÉRMINO <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">R</div> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">C</div> </div> </div>																	
OBS: coloque na quadricula: OK – se não houver defeito. X – se houver defeito. Os motoristas devem comunicar aos encarregados os defeitos observados, avarias, ou falta de acessórios no veículo, sob pena de responsabilidade pessoal.		fornecimento de combustível <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>odômetro/horímetro</th> <th>litros</th> <th>b.nº</th> <th>assim. responsável</th> </tr> </thead> <tbody> <tr> <td>_____</td> <td>álcool</td> <td>_____</td> <td>_____</td> </tr> <tr> <td>_____</td> <td>gasolina</td> <td>_____</td> <td>_____</td> </tr> <tr> <td>_____</td> <td>diesel</td> <td>_____</td> <td>_____</td> </tr> </tbody> </table>		odômetro/horímetro	litros	b.nº	assim. responsável	_____	álcool	_____	_____	_____	gasolina	_____	_____	_____	diesel	_____	_____
odômetro/horímetro	litros	b.nº	assim. responsável																
_____	álcool	_____	_____																
_____	gasolina	_____	_____																
_____	diesel	_____	_____																
ao voltar km/hora _____		ao partir km/hora _____																	
percurso km/hora _____		Horas normais de trabalho _____																	
Horas extras _____		assinatura do motorista _____																	

ANEXO IV



**PREFEITURA DE
SÃO PAULO**

SECRETARIA MUNICIPAL DE SEGURANÇA URBANA
GUARDA CIVIL METROPOLITANA
COMANDO OPERACIONAL 1
INSPETORIA DIVISÃO 10

FORMULÁRIO DE INSPEÇÃO DE VIATURAS		OSE Nº		VTR		DATA		
CONDUTOR		RF		DIST.				
PLACA		KM INICIAL		ITÊNS INSPECIONADOS				
NÍVEL DO COMBUSTÍVEL		ITÊNS DO MOTOR		DOCUMENTAÇÃO		SITUAÇÃO		
		NÍVEL ÓLEO DO MOTOR		OK	C/N	DOCUMENTO CRLV	OK C/N	
		NÍVEL FLÚIDO DO FREIO		OK	C/N	CARTÃO DE ABASTECIMENTO	OK C/N	
		NÍVEL FLÚIDO DE DIREÇÃO		OK	C/N	TWV	OK C/N	
		NÍVEL FLÚIDO ARREF.		OK	C/N	OSE	OK C/N	
		NÍVEL ÁGUA LIMPA PARA BRISA		OK	C/N	HABILITAÇÃO/FUNCIONAL	OK C/N	
PARTE INTERNA DA VTR				PARTE EXTERNA DA VTR				
PALAS CONTRA SOL		OK	C/N	ESPELHOS RETROVISORES				
BANCOS / CAPAS		OK	C/N	INT. <input type="checkbox"/> LDO DIR. <input type="checkbox"/> LDO ESQ. <input type="checkbox"/>	ALARME		OK C/N	
TAPETES		OK	C/N	PARA-BRISA / VIDROS	OK	C/N	PALHETAS	OK C/N
BUZINA		OK	C/N	PORTAS	OK	C/N	TRAVAMENTO DO CAPO	OK C/N
FORRAÇÃO PORTAS DIANTEIRAS		OK	C/N	PNEUS	OK	C/N	ANTENA	OK C/N
FORRAÇÃO PORTAS TRASEIRAS		OK	C/N	CALOTAS	OK	C/N	ADESIVOS	OK C/N
EXTINTOR DE INCÊNDIO		OK	C/N	GIROFLEX	OK	C/N	ESTEPE	OK C/N
PEDAIS		OK	C/N	SIRENE	OK	C/N	CHAVE DE RODA	OK C/N
ALAVANCA ABRIR CAPO		OK	C/N	FAROL/LANTERNAS	OK	C/N	MACACO	OK C/N
RÁDIO COMUNICADOR		OK	C/N	LUZ DE FREIO / RÉ	OK	C/N	TRIÂNGULO	OK C/N
FREIO DE ESTACIONAMENTO		OK	C/N	SETAS / PISCA-ALERTA	OK	C/N	CHAVE VTR	OK C/N
OBSERVAÇÃO:								
ASSINATURA DO CONDUTOR				ASSINATURA DO TRÁFEGO				

ANEXO V

VOAR RPA

VOAR CONSCIENTE

VOAR PARA SERVIR

LEGISLAÇÃO

O Núcleo de Monitoramento aéreo **DronePol** atua em total conformidade com as Legislações, em Especial a ICA 100-40 do Departamento de Controle de Espaço Aéreo (DECEA) - RBAC-E 94 da Agência Nacional de Aviação Civil (ANAC) Código Brasileiro de Aeronáutica (CBA) AIC 23/17 do DECEA Homologação da Agência Nacional de Telecomunicações (ANATEL)

CONTATO

Rua da Consolação, 1379.
São Paulo/SP
(11) 3124-5143
dronepol@prefeitura.sp.gov.br

SECRETARIA MUNICIPAL DE SEGURANÇA URBANA
Guarda Civil Metropolitana




153



DRONEPOL

RPAS - Remotely Piloted Aircraft Systems

SEGURANÇA DE VOO

Cumprir normas e procedimentos diariamente são requisitos indispensáveis à composição da Equipe DRONEPOL, visando maior segurança e redução dos riscos de acidentes nas mais variadas Operações.

CURSO DE OPERAÇÃO E FISCALIZAÇÃO DE RPAS

**OPERAÇÕES**

ÁREAS DE RISCO

GRANDES EVENTOS



APOIO AMBIENTAL

CONTROLE DE PÚBLICO E TRÂNSITO

**REGIÃO DA NOVA LUZ**

APOIO ÀS OPERAÇÕES DA GCM



VOO NOTURNO

Grupo de usuários de entorpecentes, na "cracolândia"



SALVAMENTO AQUÁTICO
LANÇAMENTO DE BOIAS

ATUAÇÃO

Objeto inédito nesta composição, no Brasil, o DTG - DRONEPOL atua na realização de fotografias aéreas e vídeos de alta resolução, para subsidiar planejamentos e tomadas de decisão. Produz imagens em ortomosaico, modelo em 3D e imagens panorâmicas.



MODELO 3D

DEFESA CIVIL

**HISTÓRIA**

FORMANDOS

Primeira turma de formandos em sala de aula no GRPAe.



Logo após a realização do CURSO DE OPERAÇÃO DE RPA, no Grupamento de Radiopatrulha Aérea, da Polícia Militar do Estado de São Paulo, em maio de 2017, foram iniciadas as atividades do DRONEPOL. As Equipes são desde então, compostas por Guardas Civis Metropolitanos, que realizam em média 100 voos/mês, em apoio à diversos setores da Prefeitura de São Paulo.

CLIENTES

O DRONEPOL, além dos trabalhos de rotina da Secretaria Municipal de Segurança Urbana, opera também em apoio às outras Secretarias Municipais e outros Órgãos Públicos, quando solicitado.

DIVERSIDADE OPERACIONAL

• OSTEINSIVIDADE nas Operações.



ANEXO VI



CITY CÂMERAS



POR QUE O PROJETO?

Os desafios da gestão de uma cidade segura incluem a implementação de tecnologias que permitam que com muito menos recursos humanos e materiais seja possível agir de forma proativa no combate à criminalidade.

QUAL É O OBJETIVO?

O Projeto City Câmeras é uma iniciativa que visa instalar 10 mil câmeras em São Paulo nos próximos quatro anos, visando inibir a ocorrência de crimes e aumentar a segurança e o bem-estar da população. O programa será uma importante ferramenta do poder público para detectar, prevenir e reagir às situações de emergência, ocorrências e zeladoria do espaço público.



AÇÃO INTEGRADA E TECNOLOGIA DE PONTA POR UMA SÃO PAULO MAIS SEGURA

• QUEM PARTICIPA?

O principal diferencial do programa é a participação da população. Para formar essa ampla rede de monitoramento, além das câmeras dos órgãos públicos, serão utilizadas câmeras de segurança residenciais e de pontos comerciais distribuídas por São Paulo.

• TEMPO DE GRAVAÇÃO DAS IMAGENS

Plataforma de armazenamento em nuvem com capacidade para sete dias de gravação.

• QUEM TERÁ ACESSO ÀS IMAGENS?

As imagens integradas serão transmitidas para o comando da GCM e compartilhadas com os demais órgãos de segurança (Polícias Civil e Militar) por um canal de comunicação de dados da internet, sendo possível a realização de uma triagem de ações que acontecem em ruas e avenidas da cidade.



PASSO A PASSO

1º CÂMERA RESOLUÇÃO 720P 1 MEGA PIXEL - 12 FPS

- Uso de câmeras com tecnologia HD
- Transmissão mínima de 12 FPS (frames/fotos por segundo)
- Protocolo RTSP

2º CADASTRO DA CÂMERA NA PLATAFORMA EM NUVEM

Contrate uma plataforma de armazenamento em nuvem. Gravação mínima de 7 dias em nuvem.

3º REALIZE O CADASTRO citycameras.prefeitura.sp.gov.br

4º INSTALE A PLACA

Identifique que você faz parte do Projeto City Câmeras.



Para aderir ao projeto é preciso atender aos requisitos técnicos que garantam qualidade das imagens, capacidade de envio e compartilhamento na rede de monitoramento da Guarda Civil Metropolitana.

ANEXO VII

SOBRE O SP+SEGURA

A plataforma de tecnologia **SP+SEGURA** tem como objetivo otimizar recursos públicos e aumentar a produtividade e a eficiência das autoridades, permitindo operação e gestão com inteligência.

Através da integração em tempo real do cidadão e centro de controle, acreditamos que reduziremos em muito o tempo de resposta e aumentaremos a efetividade das ações e também a confiança da população.

PRINCIPAIS BENEFÍCIOS

- ✓ Menor tempo de Resposta
- ✓ Estratégia de Segurança assertiva
- ✓ Informações detalhadas no tempo certo
- ✓ Redução de Custos
- ✓ Eficiência do Efetivo
- ✓ Maior produtividade
- ✓ Transparência ao Cidadão
- ✓ Gestão Estratégica



VIOLÊNCIA SE COMBATE COM INFORMAÇÃO E INTELIGÊNCIA

Plataforma de Tecnologia Operacional e de Gestão para **Segurança Pública**

COMO FUNCIONA

• Do ponto de vista operacional, através de seu smartphone, o cidadão pode enviar um alerta em tempo real de uma ocorrência. A tecnologia enviará os dados referentes ao endereço da ocorrência para o Centro de Controle. Em caso de urgência o aplicativo facilitará sua ligação para os órgãos de segurança.

• O Centro de Controle acompanhará todo o atendimento no mapa através da solução de Geolocalização e GPS oriundos dos dispositivos móveis.



MÓDULOS DE TECNOLOGIA

Módulo Cidadão: Aplicativo de Celular "SP+Segura" com interface amigável e Geolocalização que permite ao usuário enviar alertas em tempo real, além de outras funcionalidades para sua segurança.

Módulo Viatura: Aplicativo com Geolocalização que permite à patrulha atender chamadas de ocorrências próximas à viatura, além de comunicação com o Centro de Controle.

Módulo CICC (Centro Integrado de Comando e Controle): Permite ao departamento acompanhar as viaturas ou patrulhas em tempo real no mapa, receber alertas do cidadão, encontrar as viaturas disponíveis mais próximas da ocorrência, conversar e despachar as viaturas e acompanhar todo o atendimento pelo Sistema de Geolocalização.

Módulo Gestor: Solução Web que permite ao gestor coletar informações estatísticas e estratégicas para tomada de decisão, com otimização de recursos, estratégias de ações em campo e definição de prioridades efetivas às regiões.

Módulo Prefeitura: Solução Web que permite ao gestor receber ocorrências ou denúncias do cidadão em tempo real.



ANEXO VIII

Números GDPR

A LGPD foi constituída com base na GDPR (General Data Protection Regulation) que é da Comunidade Europeia, a LGPD entrará em vigor oficialmente a partir de 20 de Agosto de 2020.



Os números do GDPR poderão ser referência para os futuros números do LGPD, a intenção é apresentar os impactos que estão acontecendo na Europa neste momento.

GDPR: Europa conta até agora com 65.000 notificações de violação de dados, US \$ 63 milhões em multas impostas desde que a lei de privacidade entrou em vigor.)

É o que diz um novo relatório do Conselho Europeu de Proteção de Dados que fornece a "primeira visão geral sobre a implementação do GDPR e os papéis e meios das autoridades nacionais de supervisão". O EDPB (European Data Protection Boarder), com sede em Bruxelas, é um órgão europeu independente, criado como parte do GPDR, que foi ao ar no mesmo dia do início da aplicação do regulamento: 25 de maio de 2018. O mandato do EDPB é garantir que as regras de proteção de dados sejam aplicadas de maneira consistente em toda a UE, bem como incentivar as autoridades de proteção de dados da UE a cooperar.

O relatório baseia-se em dados fornecidos por muitos países no Espaço Econômico Europeu, que inclui todos os 28 estados membros da UE, além da Islândia, Liechtenstein e Noruega, que também estão em conformidade com o GDPR.

Os dados do relatório cobrem os primeiros nove meses do GDPR que entraram em vigor. "O número total de casos [GDPR] relatados por autoridades de proteção de 31 países da UE é de 206.326", diz o relatório.

Tais casos incluem reclamações. Nos termos do artigo 77 do GDPR - "Direito de reclamar com uma autoridade supervisora" - os europeus podem registrar queixas junto aos órgãos reguladores sobre as práticas de proteção de dados das organizações, como também puderam fazer antes da promulgação do novo regulamento.

Esses casos também incluem notificações de violação de dados. Entre suas disposições, o GDPR exige que organizações que sofrem uma violação que possa ter exposto as informações pessoais dos europeus notifiquem as autoridades relevantes.

"A maioria dos casos está relacionada a reclamações, notavelmente 94.622, enquanto 64.684 foram iniciadas com base na notificação de violação de dados pelo controlador", diz o relatório da EDPB. Desses casos, 52% foram encerrados e 1% são objeto de ações judiciais nos tribunais nacionais.

O relatório da EDPB também serve como uma verificação de status de como as Autoridades de proteção estão abordando a nova lei de privacidade. O conselho conclui que o GDPR está sendo aplicado de forma consistente nos Estados membros, apoiado por uma ampla cooperação entre as autoridades de privacidade.

"De 25 de maio de 2018 a 18 de fevereiro de 2019, nenhuma resolução de disputa foi iniciada. Isso significa que, até agora, as Autoridades de proteção conseguiram chegar a um consenso em todos os casos atuais, o que é um bom sinal em termos de cooperação", segundo para o relatório.

O conselho afirma que isso se deve em grande parte a um sistema de TI preexistente - o sistema de informações do mercado interno, ou IMI - que foi reaproveitado para apoiar as autoridades de supervisão. "Este sistema fornece uma maneira estruturada e confidencial de compartilhar informações entre as Autoridades de proteção" e entrou no ar no dia em que o GDPR entrou em vigor, observa o relatório.

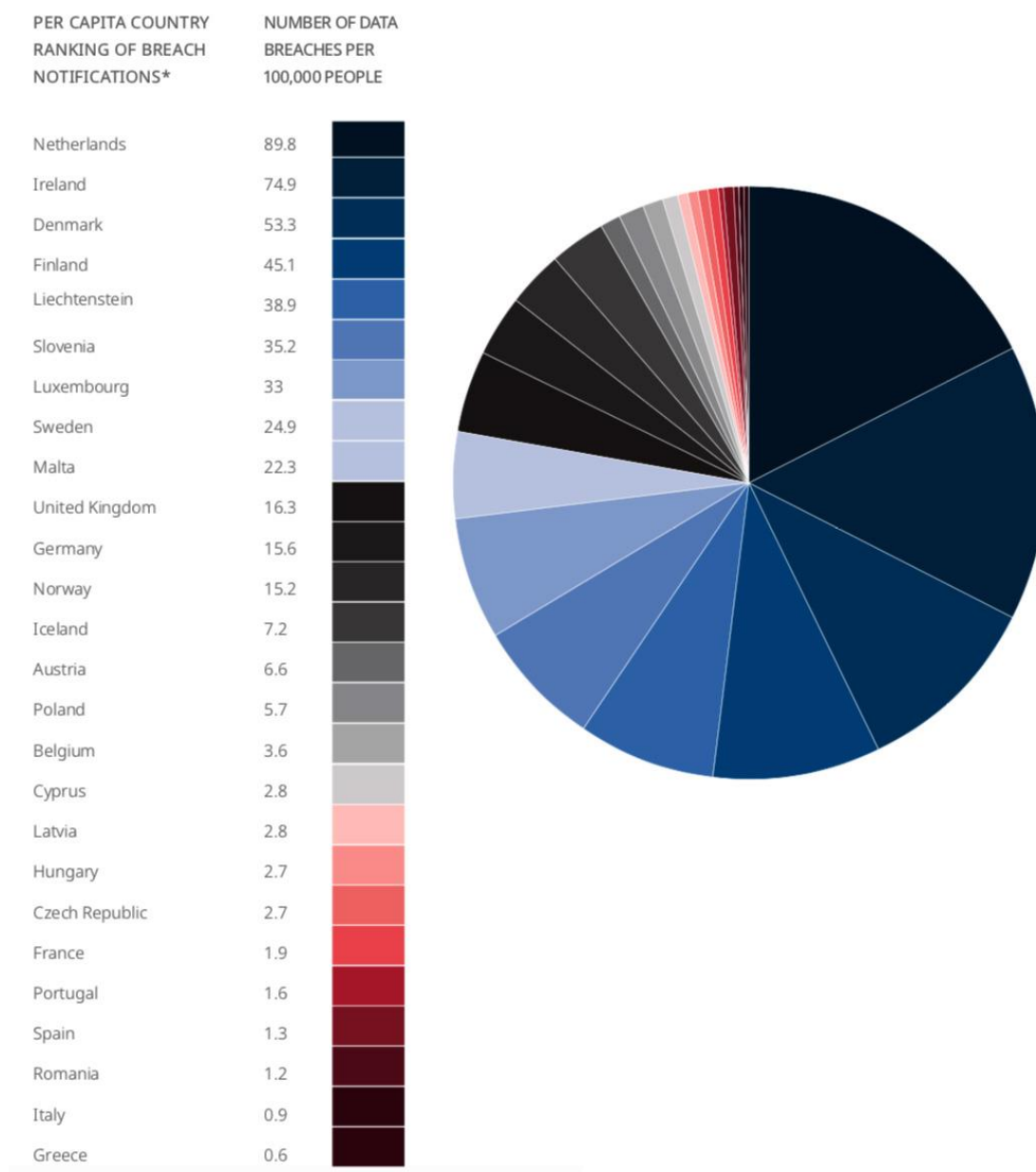
"O feedback dos reguladores nacionais sobre esse sistema é realmente positivo", diz o relatório. "Um subgrupo de especialistas dedicado foi criado para

garantir o aprimoramento contínuo do sistema com base no feedback coletado por meio de um suporte dedicado ao helpdesk de TI fornecido aos membros da EDPB pelo Secretariado da EDPB."

O sistema IMI oferece aos reguladores de privacidade europeus uma única versão da verdade. "Antes que um caso seja produzido no registro de casos do sistema, as autoridades competentes precisam ser identificadas", afirma o EDPB. "Este registro é o banco de dados central a partir do qual diferentes procedimentos podem ser iniciados, como assistência mútua, operação conjunta e mecanismo de balcão único".

Qualquer estado membro da UE pode iniciar uma investigação do GDPR sobre as práticas de segurança e privacidade de dados de uma organização. Mas qualquer organização que tenha seu "estabelecimento principal" em um país europeu - em outras palavras, uma sede europeia - pode se qualificar para um mecanismo de balcão único sob o GDPR que garante que apenas o órgão de controle de privacidade do país em que está sediada conduz qualquer investigação de privacidade.

Isso colocou a Irlanda na vanguarda de muitas investigações, porque o Facebook e muitas outras empresas autoridades de proteção têm sua sede na Europa (Irlanda, segmentadas para Facebook, Twitter, Outros). Outras autoridades de proteção de tecnologia com sede europeia na Irlanda incluem Apple, Microsoft, Twitter, Dropbox, Airbnb, LinkedIn, Oath, WhatsApp, Yelp e MTCH Technology, proprietária da Match, OkCupid, PlentyOfFish e Tinder. O Google está no processo de tornar a Irlanda seu principal estabelecimento na UE.



GDPR breach notifications per capita

"Desde 25 de maio de 2018, foram iniciados 642 procedimentos para identificar a SA principal e as Autoridades de proteção envolvidas em casos transfronteiriços", observa o relatório da EDPB. Desses, 306 dos casos foram encerrados.

"Até agora, nenhuma disputa surgiu sobre a seleção da principal SA", acrescenta, o que significa que a cooperação transfronteiriça parece estar funcionando.

O relatório da EDPB - novamente examinando os primeiros nove meses do GDPR em pleno vigor - serve como uma atualização para a pesquisa divulgada pelo

escritório de advocacia DLA Piper que examinou os primeiros oito meses do GDPR (consulte: Relatórios de violação de dados na Europa sob o GDPR superior a 59.000)

"Com base em nossa própria pesquisa, que abrange 23 dos 28 estados membros da UE, juntamente com números da Noruega, Islândia e Lichtenstein - os três estados membros adicionais do Espaço Econômico Europeu - calculamos que houve 59.430 violações de dados relatadas no mesmo período na Europa. ", Disse o DLA Piper. "Os Países Baixos, a Alemanha e o Reino Unido ficaram no topo da tabela com o maior número de violações de dados notificadas às autoridades de supervisão, com aproximadamente 15.400, 12.600 e 10.600 violações notificadas, respectivamente."

As descobertas da EDPB incluem algumas ressalvas semelhantes, pois nem todos os membros da UE ou do EEE compartilham dados. Notavelmente, os dados do Reino Unido estão ausentes em todos os gráficos contidos no relatório da EDPB. O regulador de privacidade da Grã-Bretanha, o Information Commissioner's Office, não respondeu imediatamente a um pedido de comentário.

O aumento constante das notificações de violação de dados - mais recentemente, de 59.000 em janeiro para 65.000 em fevereiro - não significa que as autoridades de proteção violações ocorram com mais ou menos frequência, diz Brian Honan, que lidera a consultoria BH Consulting de segurança da informação, com sede em Dublin. Em vez disso, mais violações estão sendo trazidas à tona graças às notificações obrigatórias de violações do GDPR.

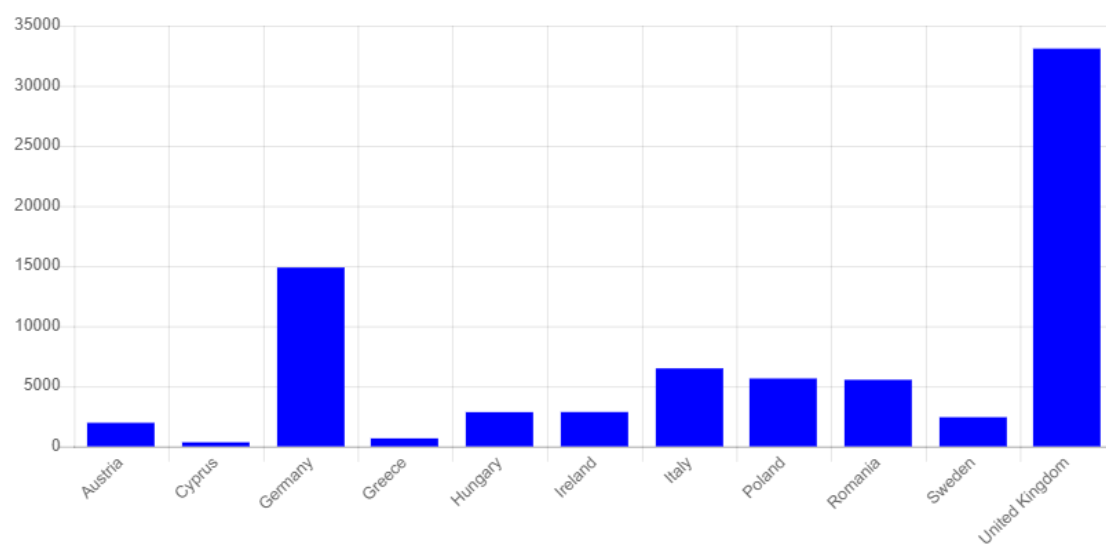
Paul Chichester, diretor de operações do Centro Nacional de Segurança Cibernética da Grã-Bretanha - o braço público da agência de inteligência GCHQ - diz que, embora o GDPR esteja trazendo à tona violações, ele não acha que sua frequência mudou muito no ano passado.

"Não acho que tenha mudado drasticamente o número ou o volume de violações que estamos vendo", disse ele ao Information Security Media Group durante uma conferência de imprensa na recente conferência CyberUK da NCSC em Glasgow, na Escócia (veja: Cybersecurity Drives Intelligence Agencies in Do frio).

"O que mudou maciçamente é a conscientização", disse ele. "As pessoas estão muito mais interessadas em se preparar para violações, e vimos pessoas se preparando para o que querem fazer depois de uma violação".

Para os europeus e para os defensores da privacidade, essa pode ser a melhor medida para determinar se o GDPR é avaliado como um sucesso.

Reclamações



Notificações de Violações

