

# INTEGRAÇÃO DE TECNOLOGIAS NA SEGURANÇA PÚBLICA E DIREITOS HUMANOS

Volume I

Biometria Câmeras Doméstica  
Humanos Municipal AVA Inteligentes Violência  
Direitos TIC Guarda Gamificação TIC Segurança  
Dispositivos Sistema Rede de Digital Segurança  
Móveis Ead Pública Ead Criminal Mídias Digitais  
Penitenciário Rede de Ead Inverstigação Policial  
Crime Computadores Sociais Biometria Tecnologias da  
Virtual Rede de Móveis AVA Informação e Comunicação  
Internet Ead Redes Dispositivos

Organizadores

Angelita Darela Mendes  
Fernando José Spanhol  
Giovani Mendonça Lunardi  
Márcio Vieira de Souza  
Natana Lopes Pereira



SENASP



UFSC

LA MÍDIA  
GRUPO DE PESQUISA  
MÍDIA E CONHECIMENTO  
USC



PPGTIC



FAPEU

# **Integração de Tecnologias na Segurança Pública e Direitos Humanos**

**Angelita Darela Mendes  
Fernando José Spanhol  
Giovani Mendonça Lunardi  
Márcio Vieira de Souza  
Natana Lopes Pereira  
(Orgs.)**

**1ª Edição**



**Editora Hard Tech**

**Universidade Federal de Santa Catarina  
Araranguá  
2018**

**Coordenação do projeto e edição:** Angelita Darela Mendes, Fernando José Spanhol, Giovani Mendonça Lunardi, Márcio Vieira de Souza, Natana Lopes Pereira

**Projeto gráfico e editoração:** Angelita Darela Mendes, Natana Lopes Pereira

**Comitê editorial:** Angelita Darela Mendes, Fernando José Spanhol, Giovani Mendonça Lunardi, Márcio Vieira de Souza, Natana Lopes Pereira

Catálogo na fonte pela Biblioteca Universitária da  
Universidade Federal de Santa Catarina

I61

Integração de tecnologias na segurança pública e direitos humanos [recurso eletrônico] / organizadores, Angelita Darela Mendes...[et al.]. – Dados eletrônicos. – Araranguá : UFSC, 2018.  
196 p. : il., gráf., tab.

Esta obra foi elaborada com recursos públicos da Secretaria Nacional de Segurança Pública (SENASP) do Ministério da Justiça (MJ), vinculado à Rede Nacional de Altos Estudos em Segurança Pública (RENAESP).

Inclui bibliografia

ISBN 978-85-5881-007-4

E-book (PDF)

Disponível em: <[www.posticsenasp.ufsc.br](http://www.posticsenasp.ufsc.br)>

1. Tecnologia da informação . 2. Segurança pública. I. Mendes, Angelita Darela.

CDU: 007:351.74

# Agradecimentos

Esta obra foi elaborada com recursos públicos da **Secretaria Nacional de Segurança Pública (SENASP)** do **Ministério da Justiça (MJ)** por meio do Edital SENASP de Chamada Pública nº 01 de 21/07/2014, vinculado à **Rede Nacional de Altos Estudos em Segurança Pública (RENAESP)**. As pesquisas realizadas somente foram possíveis graças ao empenho e dedicação dos professores e alunos do curso de Especialização em Tecnologias da Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos (Turma 2015-2017) da Universidade Federal de Santa Catarina – *Campus* Araranguá e, também, dos demais pesquisadores vinculados ao Programa de Pós-Graduação do Mestrado Interdisciplinar em Tecnologias da Informação e Comunicação (PPGTIC/UFSC). A organização desta obra coube aos pesquisadores do Laboratório de Mídia e Conhecimento do *Campus* Araranguá – UFSC/SC.

# Prefácio

Recebi o honroso convite dos colegas Fernando José Spanhol e Giovani Mendonça Lunardi para prefaciar o livro *Integração de Tecnologias na Segurança Pública e Direitos Humanos*. Em um primeiro momento, aceitei de pronto, sem ainda conhecer o texto da obra. Não imaginava o grande desafio que estaria por vir. Na apresentação feita pelos organizadores estão os detalhes sobre cada capítulo, o contexto de produção e o financiamento das pesquisas que resultaram nesta coletânea. Vou aqui expressar algumas considerações sobre o impacto que a leitura me causou. É uma produção científica coletiva, que possibilita um olhar plural para três questões de grande relevância nos contextos internacional, nacional e local: as tecnologias digitais como ferramentas privilegiadas para iluminar a compreensão de difíceis temas de grande interesse social, como a segurança pública e os direitos humanos. Como todo bom texto, as informações contidas nas diversas pesquisas realizadas pelos autores me conduziram a *links* interpretativos teóricos e empíricos plurais, o que desafiou minha experiência acadêmica e minhas expectativas, como cidadã brasileira, sobre segurança pública e direitos humanos. A abrangência analítica e os diversos recortes escolhidos pelos pesquisadores, além de convergir para a relevância nacional das temáticas investigadas, aproximam o leitor de dados empíricos sobre a criminalidade letal e chamam à atenção para aspectos relevantes das políticas públicas relativas ao enfrentamento do fenômeno da violência e o papel das instituições nacionais. Na última década, cidades e regiões brasileiras foram invadidas por problemas político-sociais que afetam a liberdade e os direitos fundamentais da população.

Assim, é de fundamental importância a contribuição da Academia ao fornecer ferramentas científicas para construir dados e gerar incursões teórico conceituais que possibilitam desvelar problemas que afetam a segurança pública e a garantia dos direitos. Transformá-los em objeto de conhecimento gera possibilidades de intervenção. Ao fazer a leitura do conjunto de capítulos, fui levado a pensar em outras realidades que precisam de investigações de forma semelhante. Ver de perto

*frames* da violência com as lentes da ciência utilizada pelos autores desafia-nos a encontrar possíveis soluções. Ao longo dos textos, os autores abrem cenários para reflexões sobre a governança nas democracias em crise. Nesse sentido, a revolução tecnológica e informacional, que ocorreu a partir do fim da década de 90, tem propiciado a abertura de perspectivas para analisar as condições insuficientes e incongruentes das políticas nacionais, de segurança e de garantia de direitos, bem como os cenários de aumento da violência. Tensões e dilemas se avolumam, e a insuficiência de conhecimentos e de dados sobre essas questões desafia intelectuais, acadêmicos e analistas a buscarem estratégias para minimizar os problemas sociais deles oriundos. O livro, produzido no âmbito de grupos de pesquisa e de formação na Universidade Federal de Santa Catarina, contribui, de forma perspicaz, com elementos para corrigir uma leitura de governabilidade ainda insuficiente para fazer face aos grandes desafios.

Convido o leitor a explorar a análise dos dados contidos nos contextos trazidos para a cena científica por meio de um conjunto de temas de grande relevância nacional e que servem de modelo para replicar em outros campos de interesse, como *softwares* forenses; sistema penitenciário; sistemas eletrônicos, como instrumento de modernização da investigação criminal; uso das mídias digitais pela polícia militar; sistema integrado de declaração de óbito; tecnologias para controlar a violência doméstica; modelo de dados voltado para o treinamento e a formação policial; uso da biometria no controle do trabalho de policiais civis; aproximação da polícia militar com a comunidade escolar e ambientes virtuais de aprendizagem na formação profissional. Essas questões são trazidas à baila permeadas de matizes teórico-conceituais apreendidas para verificar indicadores do pensamento amplo que caracterizam os processos socioculturais de construção e de aquisição do conhecimento sobre governabilidade e políticas públicas. A forma como as tecnologias digitais são percebidas e utilizadas nas análises aproxima-se do pensamento do filósofo Pierre Lévy sobre a evolução das tecnologias digitais nas últimas décadas. Ele assinala que as redes de interação contemporâneas são novas ideografias dinâmicas, geradas pelo entrelaçamento de textos, de hipertextos, de discursos e de diálogos. Mesclam-se sistemas de comunicação, codificação e decodificação de mensagens e de sentidos que amplificam a inteligência e produzem extensões múltiplas na mente humana em suas faculdades cognitivas. Novas competências e novas formas de se adaptar à informação e ao conhecimento e de se relacionar com eles estão sendo construídas com impactos diversos na capacidade de aprendizagem das pessoas. Muitas são as competências necessárias para

maximizar o potencial das tecnologias que, sob a demanda “*online*, digital, móvel e inteligente”, possibilitam que milhões de pessoas se conectem com o mundo e usem aplicativos não somente para comunicar, informar, acessar serviços e realizar transações em seu cotidiano pessoal e profissional, mas também, especialmente, potencializar a aprendizagem. Transformar informação em conhecimento implica ativar atividades cognitivas de alto nível, como analisar, comparar e criar novos significados. Nesse contexto, compreender como a convergência digital tem possibilitado a evolução da ciência e a busca de solução para os problemas cotidianos de cada Nação coloca a produção do conhecimento e o papel da pesquisa e das instituições formativas no campo dos grandes debates.

A leitura do livro leva a uma interessante viagem de reflexão sobre etnografias produzidas pelos autores para trabalharem de forma criativa uma concepção de ciência engajada com respostas possíveis para as demandas da sociedade. Ao trazer à baila dados coletados em contextos de experiência, em seus diversos campos de atuação, os pesquisadores ampliam o reconhecimento da condição humana e da defesa dos direitos humanos na experimentação concreta de processos democráticos. Pensar nos direitos humanos nos leva a estabelecer seus nexos com a democracia e a liberdade. Ora, para que cada um possa viver como gostaria, dentro de princípios legais, são necessários, *a priori*, espaços democráticos para expandir suas liberdades. A evolução das discussões sobre os processos normativos que possam garantir a eficácia dos direitos implica pensar em um progresso duradouro para implementar políticas nacionais e internacionais saudáveis e eficazes de desenvolvimento econômico e social pela conciliação do particularismo cultural com o universalismo dos direitos. É certo que há limites para explicações macrosociais sobre a criminalidade violenta e a insegurança pública, razão por que é importante explorar contextos específicos em que ela pode proliferar. A sociedade brasileira, devido à sua complexidade sociopolítica, econômica e cultural, apresenta matizes da criminalidade, cujas manifestações são diversas, tendo em vista as características próprias de cada região do país. Essa diversidade torna refratárias as soluções uniformes. Nesse contexto, as tecnologias digitais podem ser grande aliadas para gerar possibilidades de articulação de dinâmicas analíticas em torno dos três eixos analisados.

O livro chega no momento em que inventários sobre os desequilíbrios sociais que geram a violência são urgentes. Os dados aqui analisados são importantes contribuições que, articuladas a outras, produzidas em diversos campos do

conhecimento, como a Sociologia, o Direito, a Filosofia e a Educação, são insumos complementares para construir estratégias de promoção da segurança pública cidadã que podem gerar políticas públicas preventivas importantes. Estudos bem fundamentados são geradores de contribuições que alavancam a prevenção da criminalidade, o cumprimento da lei e respeito aos direitos humanos.

Os diagnósticos realizados em cada contexto mostram uma pluralidade de dimensões e de circunstâncias locais que podem ajudar a desenhar investimentos multissetoriais e a criar parcerias e redes operacionais de reformas e de planos. Essa é uma leitura necessária para os que realizam pesquisas bem como para os operadores de políticas de segurança pública e de direitos humanos. Para agir contra o crime, é necessário incidir sobre suas causas, e as tecnologias digitais podem ser grandes aliadas na construção de redes e de laços orgânicos para coordenar políticas públicas pluridimensionais e intersetoriais. O livro é um conjunto de estudos de base útil em futuras intervenções. Vamos esperar que sua publicação desperte a curiosidade inovadora de pesquisadores e de estudiosos brasileiros confrontados com os dilemas e os desafios da segurança pública, e das violações aos direitos humanos. Estas breves considerações não esgotam a riqueza da contribuição do conjunto de textos da obra. É preciso explorá-los com lentes amplas e individuais de leitura.

Edna Gusmão de Góes Brennand – PPGE/PPGOA/UFPA

# Apresentação

Esta obra é resultado das pesquisas realizadas pelos professores e alunos do curso de Especialização em Tecnologias da Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos, em sua segunda edição (Turma 2015-2017), da Universidade Federal de Santa Catarina – *Campus* Araranguá, financiado pela Secretaria Nacional de Segurança Pública do Ministério da Justiça (SENASP/MJ), no âmbito da Rede Nacional de Altos Estudos em Segurança Pública (RENAESP), com colaboração dos pesquisadores vinculados ao Programa de Pós Graduação do Mestrado Interdisciplinar em Tecnologias da Informação e Comunicação (PPGTIC/UFSC-*Campus* Araranguá) e organizado pelo Grupo de Pesquisa do Laboratório de Mídia e Conhecimento (LabMídia/UFSC-*Campus* Araranguá/CNPq).

As pesquisas aqui apresentadas aprofundam a convergência, já explicitadas em investigações anteriores, sobre a discussão de três temas fundamentais para a sociedade brasileira: segurança pública, direitos humanos e o desenvolvimento das tecnologias da informação e comunicação. As convergências desses temas seguem a orientação de várias políticas públicas nacionais como ações estratégicas: a consolidação do Sistema único de Segurança Pública (SUSP), os programas da Secretaria Nacional de Segurança Pública do Ministério da Justiça (SENASP/MJ), o Programa Nacional de Segurança Pública com Cidadania (PRONASCI), a criação da Rede Nacional de Altos Estudos em Segurança Pública (RENAESP) e da Matriz Curricular Nacional para Ações Formativas dos Profissionais da Área da Segurança Pública. Da mesma forma, é relevante a implementação de critérios qualitativos para a distribuição dos recursos do Fundo Nacional de Segurança Pública. No âmbito das políticas públicas de Direitos Humanos vale ressaltar a terceira edição do Programa Nacional de Direitos Humanos (PNDH-3), o Plano Nacional de Educação em Direitos Humanos (PNEDH) e as várias ações desenvolvidas pela Secretaria de Direitos Humanos da Presidência da República (SDH/PR). Por sua vez, em sua Matriz Curricular Nacional para ações formativas a SENASP indica como uma das áreas temáticas de capacitação a Comunicação, informação e tecnologias em Segurança Pública. Essa indicação é corroborada no documento da Agência Brasileira de

Desenvolvimento Industrial (ABDI) que coloca como uma das ações mobilizadoras para o desenvolvimento tecnológico e o crescimento econômico do Brasil no horizonte temporal até 2025, os investimentos estratégicos em Tecnologias da Informação e Comunicação em Sistemas de Segurança Pública.

Com essas indicações e a convergência desses três temas – Tecnologias da Informação e Comunicação (TIC), Segurança Pública e Direitos Humanos – os capítulos a seguir descrevem desde políticas públicas para o uso das TIC, bem como a utilização de tecnologias em áreas específicas da Segurança Pública até a avaliação do próprio curso de curso de pós-graduação em nível de especialização que originou esta obra.

Esperamos que, mais uma vez, as pesquisas ora expostas possam contribuir com o desenvolvimento de Tecnologias da Informação e Comunicação para Sistemas de Segurança Pública e Direitos Humanos, mas também para que o incentivo a inovação tecnológica sirva também para à redução de violência, redução das desigualdades econômicas e aumento da inclusão social.

Boa Leitura.

Os organizadores

# Sumário

**Capítulo 1 – O SISTEMA PENITENCIÁRIO CATARINENSE: PLANEJAMENTO ESTRATÉGICO E TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO.....** 12  
*Antônio Altino de Farias, Paulo Cesar Leite Esteves*

**Capítulo 2 – A UTILIZAÇÃO DE SISTEMAS ELETRÔNICOS COMO INSTRUMENTO DE MODERNIZAÇÃO DA INVESTIGAÇÃO CRIMINAL.....** 31  
*Fernando Lúcio Mendes, Vilson Gruber*

**Capítulo 3 – O USO DAS MÍDIAS DIGITAIS PELA POLÍCIA MILITAR NA APROXIMAÇÃO COM A COMUNIDADE: UM ESTUDO DE CASO NO DESTACAMENTO DE BALNEÁRIO ARROIO DO SILVA.....** 47  
*Maicon dos Santos Borges, Solange Maria da Silva*

**Capítulo 4 – PROPOSTA DE UM SISTEMA INTEGRADO DE DECLARAÇÃO DE ÓBITO.....** 62  
*Roberto Hideo Omomo, Vilson Gruber*

**Capítulo 5 – UM MODELO DE DADOS VOLTADO AO TREINAMENTO E FORMAÇÃO POLICIAL.....** 77  
*Ronnie Carlos Tavares Nunes, Alexandre Leopoldo Gonçalves*

**Capítulo 6 – SOFTWARES FORENSES DIRECIONADOS À INVESTIGAÇÃO DE CRIMES VIRTUAIS EM REDES DE COMPUTADORES.....** 92  
*Samuel Nunes Juliani, Eliane Pozzebon, Luciana Bolan Frigo*

**Capítulo 7 – INSTRUMENTOS TECNOLÓGICOS PARA A PROTEÇÃO DE MULHERES VÍTIMAS DE VIOLÊNCIA: SOLUÇÃO PARA CONTROLE DA VIOLÊNCIA DOMÉSTICA?..... 106**

*Sônia Maria Dall’Igna, Giovani Mendonça Lunardi, Roderval Marcelino, Milena Petters Melo, Angelita Darela Mendes*

**Capítulo 8 – O USO DA BIOMETRIA NO CONTROLE DAS HORAS TRABALHADAS PELOS POLICIAIS CIVIS DE SANTA CATARINA E SEUS REFLEXOS JURÍDICOS..... 117**

*Thiago Marcos Ferreira, Juarez Bento da Silva*

**Capítulo 9 – FERRAMENTAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NA SEGURANÇA PÚBLICA: UMA ANÁLISE SOBRE O PORTAL SINESP E SUAS FERRAMENTAS..... 129**

*Vladimir Braga de Lima, Paulo Cesar Leite Esteves*

**Capítulo 10 – REDE DE SEGURANÇA ESCOLAR: UMA ANÁLISE SOBRE A POSSIBILIDADE DE APROXIMAÇÃO ENTRE POLÍCIA MILITAR E A COMUNIDADE ESCOLAR ATRAVÉS DAS REDES SOCIAIS ..... 142**

*Bruna da Silva Pires, Luciana Bolan Frigo, Eliane Pozzebon*

**Capítulo 11 – PLANEJAMENTO DE AÇÕES PARA APLICAÇÃO DA LEGISLAÇÃO ATUAL SOBRE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO CORRELACIONADA AS NORMAS EXISTENTE DENTRO DA INSTITUIÇÃO BRIGADA MILITAR ..... 159**

*Deivis Noal Ferreira, Solange Maria da Silva*

**Capítulo 12 – O AMBIENTE VIRTUAL DE APRENDIZAGEM NA ESTRUTURAÇÃO DE TRABALHOS DE CONCLUSÃO DE CURSO: ESTRATÉGIAS DE EAD NO ENSINO SUPERIOR PRESENCIAL ..... 174**

*Natana Lopes Pereira, Fernando José Spanhol, Angelita Darela Mendes, Giovani Mendonça Lunardi*

# O SISTEMA PENITENCIÁRIO CATARINENSE: PLANEJAMENTO ESTRATÉGICO E TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

*Antônio Altino de Farias  
Paulo Cesar Leite Esteves*

## **1 INTRODUÇÃO**

Nos últimos anos é notável a crise prisional brasileira cuja ponta do *iceberg* está na superlotação das unidades penitenciárias. O sistema prisional brasileiro, de acordo com Beber (2007, p. 11), tem sido palco de muitas análises, revelando que as pessoas privadas de liberdade necessitam de eficazes ações para auxiliar no processo de reeducação e reintegração social.

Com a instituição da Lei Federal de Execução Penal (Lei 7.210, de 11 de julho de 1984), e alterações que dispõem sobre a remição de parte do tempo de execução da pena por estudo ou por trabalho (Lei nº 12.433, de 29 de junho de 2011), bem como a constituição da República Federativa do Brasil de 1988, e demais regulamentações, abre-se uma janela de oportunidades para os sentenciados no Brasil, que estavam relegados ao esquecimento, em prisões consideradas depósitos de pessoas privadas de liberdade, na perspectiva dos direitos humanos.

No estado de Santa Catarina, a população carcerária informada era de 17.914 pessoas privadas de liberdade, estando trabalhando 5.401 (30%) e estudando 2.010 sentenciados (11,2%), segundo Brasil (2014a). Insta que o Departamento de Administração Prisional do Estado de Santa Catarina gerenciava 46 unidades prisionais no ano de 2014, sendo que destas, 13 estabelecimentos não possuíam sala de aula. Denota-se que existe grande dificuldade para pesquisa de informações

nacionais penitenciárias em razão de dados escassos ou desatualizadas e inconsistências nos números dos levantamentos, os quais não espelham a realidade.

Segundo o Diretor da Penitenciária da Região de Curitiba (PRC), a ferramenta do planejamento tem contribuído de forma significativa na melhora dos resultados da unidade prisional, assim como no envolvimento dos servidores nos processos de implementação. O apoio da Secretaria de Estado da Justiça e Cidadania (SJC) e do Departamento de Administração Prisional (DEAP) tem sido essencial e determinante para o sucesso do planejamento da unidade prisional, que possui 100% dos reeducandos trabalhando, cerca de 800 sentenciados remunerados com um salário mínimo e contribuindo com 25% para o Fundo Rotativo da Penitenciária da Região de Curitiba (SANTA CATARINA, 2017).

Nesse sentido, o planejamento estratégico merece destaque, uma vez que o processo integra toda a organização, influenciando e sendo influenciado, englobando fatores externos e internos. Com base nesse contexto, visando apresentar uma proposta de planejamento estratégico para o Sistema Penitenciário Catarinense, por meio de estudo teórico bibliográfico formulou-se a seguinte questão de pesquisa: Quais as estratégias, tecnologias de informação e comunicação que apoiam o Sistema Prisional Catarinense?

Para responder a tal questionamento realizou-se estudo teórico bibliográfico referente aos conceitos de planejamento estratégicos, *Balanced Scorecard* (BSC), Indicadores Estratégicos, Análise SWOT, descritos na seção dois. Na seção seguinte, apresentam-se os passos metodológicos empreendidos. No item quatro, buscou-se identificar as bases legais que nortearam a institucionalização da Secretaria de Estado da Justiça e Cidadania em Santa Catarina e também as tecnologias de informação e comunicação que apoiam as atividades do sistema prisional. Assim, com base nas referências teóricas e informações coletadas da Secretaria de Estado da Justiça e Cidadania de Santa Catarina, foi elaborada uma proposta de planejamento estratégico, contendo objetivos, metas e estratégias, que aprimoram o Sistema Prisional Catarinense, conforme evidenciado na seção cinco.

## **2 REFERENCIAL TEÓRICO**

Nesta seção, os fundamentos teóricos do planejamento estratégico e das tecnologias de informação e comunicação estão relacionados, dado que apoiam as

atividades do sistema prisional Catarinense, servindo, pois, de referência no desenvolvimento da pesquisa.

## 2.1 Planejamento Estratégico

A palavra estratégia tem origem grega, do termo *strategos*, que denominava o papel de comando de um general do exército, com habilidades gerenciais, psicológicas, e comportamentais no exercício da sua função (QUINN, 2001).

Em relação às metodologias para construção de um planejamento estratégico, existem várias formas diferentes apresentadas por diversos autores, entretanto, de acordo com Pereira (2007), a elaboração do planejamento estratégico pode ser realizada em três etapas, conforme tabela a seguir.

**Tabela 1** - Etapas do Planejamento Estratégico.

Planejamento Estratégico		
1ª Etapa	2ª Etapa	3ª Etapa
Diagnóstico Estratégico	Elaboração do Planejamento	Implantação
Fase de levantamentos de dados para analisar onde a empresa está, se o momento é oportuno para a realização do planejamento estratégico, face à estabilidade da organização. Para prosseguimento desta etapa, é necessária a conscientização permanente das lideranças e escolha da metodologia.	Fase em que os planos são formalizados através de reuniões que definem o estágio em que a empresa quer chegar, construção da missão, visão, valores, fatores críticos de sucesso, análise <i>SWOT</i> , maximizando oportunidades e minimizando riscos das ameaças. Nesta fase, são elaboradas as estratégias e ações necessárias do planejamento estratégico.	A fase de implantação requer permanente acompanhamento e avaliação dos resultados, para possíveis ajustes e alinhamentos com a missão e visão da organização.

**Fonte:** Adaptado de Pereira (2007).

Na década de 70, o planejamento estratégico teve uma rápida ascensão devido à utilização do modelo básico *SWOT* – *Strengths* (pontos fortes), *Weaknesses* (pontos fracos), *opportunities* (oportunidades), *threats* (ameaças), também chamado de análise de *SWOT*, definido posteriormente como escola do design por Mintzberg (2010). A primeira etapa da elaboração do planejamento é constituída pelos levantamentos de dados para a realização do diagnóstico. Na segunda etapa, são

formalizados os planos, avalia-se o ambiente interno e externo com a matriz *SWOT* e elaboram-se as estratégias. Por último, na etapa três, fase de implantação, é necessário acompanhamento, avaliação e correção, conforme Pereira (2007).

Na fase de elaboração das estratégias, segundo Porter (1998), é importante analisar e encontrar a fonte de cada força da organização, para entender e conhecer os esforços críticos e os pontos fracos, aproveitando as oportunidades e minimizando os riscos das ameaças.

## **2.2 Elaboração do Planejamento Estratégico**

A elaboração de um planejamento estratégico pode ser formal ou informal. Quando o processo é formal e estruturado, a empresa coloca no papel o planejamento estratégico, facilitando para o executivo a aplicação e evolução do plano, revelando aspectos comuns, mesmo com diferentes metodologias (OLIVEIRA, 2001b).

Organizações que escolhem trabalhar com assessoria interna possuem a vantagem de contar com profissionais que conhecem a empresa, tem presença diária, conhecem pessoas e grupos que favorecem o controle e avaliação dos processos, entretanto, o nível de aceitação é menor que um consultor externo. O ideal é que a organização trabalhe com consultores internos e externos (OLIVEIRA, 2001a).

## **2.3 Declaração de Valores, Missão e Visão**

A primeira ação da equipe de planejamento é a elaboração da declaração de valores, princípios e crenças da organização, que todos os funcionários devem seguir, gerando um diferencial competitivo e orientando o comportamento da organização (PEREIRA, 2007).

Propõe Certo e Peter (1993) que seja descrita a missão, que é a razão de existir da organização. Em linhas gerais, a missão determina o tipo de produto ou serviço que a organização produz para seus clientes seguindo os valores declarados. Já a visão mostra a direção e o caminho no qual a empresa deseja estar, em um período de tempo necessário, para alcançar os sonhos no horizonte estratégico (PEREIRA, 2007).

## 2.4 Fatores Críticos de Sucesso

A atividade de identificação dos Fatores Críticos de Sucesso (FCS) faz parte de uma técnica que busca aspectos importantes para a sobrevivência e mudanças impostas pelo ramo de atuação de uma organização. Os Fatores críticos de sucesso são essenciais, pois ajudam na construção de um diagnóstico e servem como base para a elaboração das estratégias do planejamento (OLIVEIRA, 2001a).

A matriz BSC apoia a identificação dos fatores críticos de sucesso, possibilitando o direcionamento dos esforços para o atingimento dos objetivos estratégicos. Após a identificação adequada dos fatores críticos de sucesso, definem-se os indicadores de desempenho, de tal modo que possam ser coletados e avaliados para a concretização do planejamento desejado (KAPLAN; NORTON, 2000).

## 2.5 Análise de Ambiente

De acordo com Pereira (2007), a Matriz FOFA em Português (ou inglês SWOT) possibilita a realização de uma análise ambiental interna dos Pontos Fortes (*Strengths*) e Pontos Fracos (*Weaknesses*), e análise externa das Oportunidades (*Opportunities*) e Ameaças (*Threats*), permitindo uma visão abrangente da organização, conforme segue.

**Tabela 2** - Matriz da Análise FOFA (SWOT).

Análise FOFA (SWOT)	Análise Externa Oportunidade - O	Análise Externa Ameaça - A
Análise Interna Pontos Fortes- F	Capitalizar (atacar) - Como os Pontos Fortes podem ser utilizados para aproveitar as Oportunidades?	Monitorar (defender) - O que precisamos fazer para que as Ameaças não atrapalhem nossas estratégias?
Análise Interna Pontos Fracos – F	Melhorar (restrições) - Como devemos agir com os Pontos Fracos para aproveitar as Oportunidades?	Eliminar a Vulnerabilidade (problemas) - Quais ações necessárias para evitar que nossos Pontos Fracos prejudiquem ainda mais o impacto das Ameaças?

**Fonte:** Adaptado de Pereira (2007).

A partir da Análise *SWOT* é possível identificar quatro grupos de estratégias a serem implementadas: S-O, W-O, S-T e W-T;

## 2.6 Balanced Scorecard – BSC

O *Balanced Scorecard* organiza uma estrutura que liga a missão e a estratégia, e utiliza indicadores para dar ciência aos colaboradores sobre os vetores de sucesso atual e futuro. Neste sentido, o BSC funciona como uma ferramenta que traduz a visão de uma organização, por meio de um conjunto harmônico de medidas de desempenho, distribuídas em quatro perspectivas: Financeira, processos internos, clientes, aprendizagem e crescimento. As perspectivas servem para equilibrar os objetivos de curto e longo prazo, guiar ações para atingimento dos resultados almejados, desde os mais simples aos mais complexos (KAPLAN e NORTON, 1997).

As organizações públicas têm utilizado o *balanced scorecard* como uma ferramenta de medição do desempenho e aumento da responsabilidade da administração pública, com ênfase na melhora de resultados para a sociedade (WUA *et al.*, 2010). O setor público foca um programa ou serviço e controla as medições de entrada e saída do *balanced scorecard*, fortalecendo a aprendizagem e crescimento dos servidores, equilibrando os recursos, monitorando o alcance dos programas de melhorias nos serviços para a sociedade (HOQUE; ADAMS, 2011).

## 2.7 Indicadores Estratégicos

Para Olve *et al.* (2001), a relação estabelecida entre as variáveis de quantidade e de qualidade possibilitam observar as mudanças no objeto do fenômeno estudado, tais como as metas e objetivos planejados, que revelam resultados atuais ou potenciais, também denominados de indicadores de gestão. Esses indicadores podem mensurar os fatores críticos de sucesso, objetivos estratégicos e metas da organização.

## 2.8 Partes Interessadas – Stakeholders

As partes interessadas, também conhecidas como *stakeholders*, são pessoas e organizações que impactam e são impactadas pela organização, têm envolvimento de forma positiva ou negativa, que podem influenciar na implementação e no resultado do projeto de planejamento estratégico (GUIA PMBOK, 2013).

## **2.9 Matriz GUT - Gravidade – Urgência – Tendência**

A Matriz GUT é utilizada por organizações com o intuito de priorizar os problemas e consequentemente tratá-los. Tem escalas de gravidade (possível dano que pode decorrer de uma situação), urgência (tempo para resolver o problema) e tendência (representa o aumento potencial e agravamento do problema com o passar do tempo). A Pontuação de cada escala começa com 1 (sem gravidade), 2 (pouco grave), 3 (grave), 4 (muito grave) até 5 (extremamente grave). A importância é percebida pelo valor mais alto dado pelo produto de gravidade x urgência x tendência. Ex.:  $5 \times 5 \times 5 = 125$  (maior valor, extremamente grave, ordem prioritária), conforme Colenghi (2007).

### **2.10 Mapa Estratégico**

A evolução do *balanced scorecard* que, inicialmente, tinha foco principal nos indicadores de desempenho, ganha uma nova forma para apresentar as quatro perspectivas (pessoas, processos, recursos e resultado para a sociedade) e seus macros objetivos a serem monitorados pela organização (KAPLAN; NORTON, 2004).

### **2.11 Sistemas de Tecnologias de Comunicação e Informação Aplicadas ao Sistema Prisional**

Os sistemas de tecnologias de informação e comunicação provocam alterações profundas nos processos de trabalho em unidades prisionais, podendo ser utilizados para interação entre vários agentes envolvidos em processos de segurança pública, conforme segue:

**Tabela 3 -Tecnologia Associada à Aplicação**

<b>Tecnologia</b>	<b>Descritivo</b>
Biometria	Diversas formas de identificação biométricas: identificação por impressão digital, íris, voz, traços da face, DNA, palmar etc.
RFID	Método de identificação automática através de sinais de rádio, recuperando e armazenando dados remotamente através de dispositivos chamados de tags RFID. Uma tag ou etiqueta RFID é um <i>transponder</i> , pequeno objeto que pode ser colocado em uma pessoa, animal, equipamento, embalagem ou produto, dentre outros.
Vídeo-monitoramento e câmeras inteligentes	Sistemas de vídeo que contam com sistema de OCR (identificação de caracteres) ou câmeras com detecção de movimentos e sensor de posição.
Software de inteligência	São <i>softwares</i> que atendem o ciclo de produção de informações estratégicas, contendo ferramentas para coleta, análise (redes de relacionamento, geoprocessamento, mineração de dados etc.) e difusão de informações.
Conexão ultra segura	Conexões que se utilizam de criptografia com alta dificuldade de quebra, mesmo com máquinas de alto desempenho.
Sistemas de monitoramento e bloqueio de sinais	Sistemas que podem monitorar e bloquear rádio frequências para o ambiente prisional.
Redes integradas de telecomunicações	Redes de comunicação de missão crítica integrada entre as instituições de segurança pública baseadas em padrões abertos.
Sistemas avançados de bancos de dados	Propostas de unificação de dados dispersos em diversas bases visando alimentar o sistema de inteligência.
Sistemas de detecção e reconhecimento de padrões de vídeo	Sistemas que trabalham em conjunto com câmeras de vídeo para detecção de objetos perigosos, reconhecimento de padrões em imagens.

**Fonte:** ABDI, 2010. Adaptado de Sistemas Aplicados à Segurança Pública.

As tecnologias de informação e comunicação (TIC's) são reconhecidas como uma das principais forças no aumento da produtividade de várias economias desenvolvidas, passando a ser o cerne do que vem sendo chamado de sociedade da informação. Neste contexto, o sistema prisional deve aproveitar e beneficiar-se das

oportunidades de aprimoramento de processos que as TIC's oferecem no desenvolvimento de suas atividades administrativas e operacionais.

### **3 PROCEDIMENTOS METODOLÓGICOS**

Para realização desta pesquisa, optou-se por uma abordagem mista. A abordagem qualitativa foi empregada para aprofundamento da compreensão da organização e a quantitativa para análise de dados numéricos (GIL, 1999). A pesquisa iniciou de uma análise geral teórica de Planejamento Estratégico, com apoio de tecnologias de comunicação e informação, avaliação de dados, com o objetivo de conhecer e entender do ambiente da Secretaria de Estado da Justiça e Cidadania e do Departamento de Administração Prisional.

Quanto à natureza, utilizou-se a pesquisa aplicada, em razão de gerar conhecimentos que poderão ser aplicados na prática (GIL, 1999). Visa gerar conhecimento a partir dos dados e das informações coletadas em fevereiro de 2017, com propósito de construir uma proposta de planejamento estratégico para o Sistema Prisional Catarinense, apoiada em tecnologias de comunicação e informação. O tipo da pesquisa quanto aos objetivos é exploratória, pois torna o problema de pesquisa mais explícito e visa maior interação com o objeto estudado (LEONEL; MOTTA; BASTOS, 2007).

Para alcançar os resultados desta pesquisa, foram utilizados procedimentos de pesquisas bibliográficas, a partir de referências teóricas já analisadas, de livros, artigos científicos, páginas de *websites*, indicadores de resultados do sistema prisional, consulta de Leis e regulamentações pertinentes, visitas a estabelecimentos prisionais, e orientação do mapa estratégico 2016 - 2018 do Departamento de Administração Prisional.

## 4 DESENVOLVIMENTO DA PESQUISA

### 4.1 A Secretaria de Estado da Justiça e Cidadania – Departamento de Administração Prisional

O Sistema Penitenciário do Estado de Santa Catarina esteve sob a responsabilidade da Secretaria Executiva de Justiça e Cidadania, pela Lei Complementar nº 381, em 07 de maio de 2007, sendo a mesma órgão executivo da Secretaria de Segurança Pública e Defesa do Cidadão.

A partir de 20 de abril de 2011, a Lei complementar nº 534 estabelece novo modelo de gestão e estrutura organizacional do Estado de Santa Catarina, criando a Secretaria de Estado da Justiça e Cidadania pelo Artigo 5º, com atribuições do Artigo 23, que permitiu a gestão técnica em todas as unidades penitenciárias por Agentes Penitenciários efetivos.

### 4.2 Informações do Sistema Penitenciário de Santa Catarina

O Estado de Santa Catarina opera com 49 unidades prisionais, nada obstante existem novas unidades a serem inauguradas, unidades em construção e outras a serem construídas, conforme levantamentos quantitativos na data de 19 de fevereiro de 2017.

Na Tabela 4, foi verificado que no ano de 2017, havia **6.312 vagas** e apenas **4.998 presos provisórios**, resultando em um **excedente de 1341 vagas de presos provisórios**, enquanto há déficit de vagas em outros regimes de execução penal. Nesta mesma tabela, verifica-se um déficit de 2.332 vagas no regime semiaberto e um déficit de 2.716 vagas no regime fechado. Também é observado que os 4.998 presos provisórios representam 27% do total de encarcerados. Segundo a Comissão Parlamentar de Inquérito (CPI) e Sistema Carcerário Brasileiro - 2017, o Brasil possui 41% de presos provisórios na população carcerária, entretanto, é uma informação do ano de 2015 publicada em 2017.

Ainda na Tabela 4, no período de 2013 a 2017 foi observado que houve crescimento na população de presos provisórios de apenas de 1% a.a. (ao ano). Ressalta-se, que tanto os presos do regime semiaberto quanto os do regime fechado tiveram sua população aumentada em 6,2% a.a.

**Tabela 4 - Relatório de Alocados por Regime.**

<b>Relatório de Alocados por Regime</b>					
<b>Indicadores</b>	<b>Ano</b>				
	<b>2013</b>	<b>2014</b>	<b>2015</b>	<b>2016</b>	<b>19/02/17</b>
<b>Vagas para provisórios</b>		5.972	-	-	<b>6.312</b>
Presos provisórios	4.812	4.456	4.544	4.826	<b>4.998</b>
Vagas excedentes provisórios	-	1.516	-	-	<b>(+)1.314</b>
<b>Vagas para regime fechado</b>	-	4.047	-	-	<b>6.163</b>
Condenados em regime fechado	6.964	7.036	7.512	8.624	<b>8.879</b>
Déficit de vagas no regime fechado	-	<b>-2.989</b>	-	-	<b>-2.716</b>
<b>Vagas em regime semiaberto</b>	-	1.597	-	-	<b>2.189</b>
Condenados em regime semiaberto	3.567	3.716	4.430	4.518	<b>4.521</b>
Déficit de vagas no regime semiaberto	-	<b>-2,119</b>	-	-	<b>-2.332</b>
<b>Vagas para o regime aberto</b>	-	-	-	-	-
Condenados em regime aberto	1.970	1.527	2.035	2.457	<b>2.434</b>
Déficit de vagas no regime aberto	-	-	-	-	-
Déficit de vagas geral calculado	-	-	-	-	<b>-3.734</b>

Fonte: DEAP, adaptado pelo Autor (2017).

### 4.3 Análise SWOT – Ambiente Interno e Externo

Na Tabela 5, estão descritos elementos de oportunidades e ameaças do ambiente externo e os Pontos Fortes e Fracos do ambiente interno da organização, conforme segue:

**Tabela 5 - Matriz SWOT.**

<b>OPORTUNIDADES (O)</b>	<b>AMEAÇAS (T)</b>
<ul style="list-style-type: none"> <li>● Governo Federal; Estadual; Municipal;</li> <li>● Legislação;</li> <li>● Sociedade;</li> <li>● Tecnologia;</li> <li>● Políticas Públicas;</li> <li>● População;</li> <li>● Empresas;</li> <li>● Universidade/Instituições de Ensino;</li> <li>● Estado da Arte;</li> <li>● Família do Sentenciado;</li> <li>● Grupos Regulamentadores;</li> <li>● Mídia.</li> </ul>	<ul style="list-style-type: none"> <li>● Economia/Política;</li> <li>● Demografia;</li> <li>● Concorrentes;</li> <li>● Fornecedores;</li> <li>● Comunidade Local;</li> <li>● Facções Criminosas.</li> </ul>
<b>PONTO FORTE (S)</b>	<b>PONTO FRACO (W)</b>
<ul style="list-style-type: none"> <li>● Modelo de Organização;</li> <li>● Modelo de Gestão;</li> <li>● Diversidade de Serviços Prestados;</li> <li>● Plano de Carreira/Salarial;</li> <li>● Capacitação dos Servidores;</li> <li>● Plano de Benefícios;</li> <li>● Perfil do Dirigente.</li> </ul>	<ul style="list-style-type: none"> <li>● Sistemas de Informação e Comunicação;</li> <li>● Sistemas de Avaliação e Controle de Indicadores;</li> <li>● Integração e Fluxo de Processos;</li> <li>● Instalações Físicas; Normas e Procedimentos;</li> <li>● Relacionamento e Trabalho em Equipe;</li> <li>● Imagem frente a sociedade;</li> <li>● Clima Organizacional e Motivacional;</li> <li>● Qualidade e Inovação dos Serviços;</li> <li>● Programas Sociais e Ambientais;</li> <li>● Projetos Tecnológicos e Programas de Qualidade; Disponibilidade de Recursos;</li> <li>● Recrutamento e Seleção;</li> <li>● Flexibilização a Mudanças.</li> <li>● Adolescentes em Conflito com a Lei;</li> <li>● Sistema de Planejamento;</li> <li>● Sentenciado;</li> <li>● Cobertura Logística.</li> </ul>

**Fonte:** Matriz SWOT, adaptado de BRADFORD, DUNCAN E TRACY, 1999.

O Cruzamento de S-O, W-O, S-T e W-T permitem identificar os grupos estratégicos que apoiam na elaboração dos objetivos, metas e estratégias.

## 5 RESULTADOS E SUGESTÕES DE PLANEJAMENTO ESTRATÉGICO

Nesta etapa, apresentam-se os resultados da pesquisa orientados pelas bases teóricas e levantamento de informações do sistema prisional de Santa Catarina.

### 5.1 Renovação dos Fundamentos Estratégicos

Após realização dos estudos, identificou-se necessidade de alterações dos fundamentos estratégicos do sistema Prisional Catarinense, sendo proposto a seguinte renovação:

- **Missão:** Administrar o Sistema Prisional Catarinense com objetivo de executar o cumprimento da pena das pessoas privadas de liberdade, garantindo condições humanizadas, promovendo a ressocialização pelas atividades laborais, educação, atenção à saúde, apoio ao egresso, reintegração social, e assegurando demais direitos não atingidos pela sentença.
- **Visão:** Ser reconhecido pela sociedade como um Sistema Prisional que ressocializa, reeduca, e reintegra a pessoa privada de liberdade.
- **Valores:** Disciplina, eficácia, ética, integridade, honestidade, humanização, lealdade e probidade.

### 5.2 Elaboração de Objetivos – Metas – Estratégias

A elaboração dos objetivos buscou referências na revisão bibliográfica, análise do ambiente interno e externo, *Balanced Scorecard* e Mapa Estratégico do Departamento de Administração Prisional 2016-2018. A pesquisa sugere 35 objetivos, entretanto, nesta oportunidade estão relacionados apenas treze (13) objetivos que obtiveram avaliação de 125 pontos na Matriz GUT (nível de gravidade), conforme segue na Tabela seis (6):

**Tabela 6** - Objetivos, Meta e Estratégias para implantação até o ano 2018

OBJETIVOS	METAS	ESTRATÉGIAS
<b>1 – Planejamento Estratégico.</b>	1.1 – Implantar em todas as unidades. No período de 01/01/2017 à 31/12/2018.	1.1.1 – Treinar servidores.  <i>Continua</i>

<p><b>2 – Divulgar a Missão, Visão, Valores, objetivos e metas do Sistema Prisional do Estado de Santa Catarina.</b></p>	<p>2.1 – Alinhar ações de todos os servidores na mesma direção desejada pela SJC até dez/2017.</p>	<p>2.1.1 – Reunir Diretores, Gerentes e demais servidores para divulgação dos fundamentos estratégicos.</p>
<p><b>3 – Adequação do Sistema Prisional frente à necessidade de aumentar o número de vagas e regularizar os regimes de sentenças.</b></p>	<p>3.1 - Zerar déficit de vagas no Sistema Penitenciário. No período de 01/01/2017 à 31/12/2018.</p>	<p>3.1.1 – Construir unidades prisionais e readequar vagas excedentes de presos provisórios para abertura de vagas do regime fechado. Aumentar vagas semiaberto.</p>
<p><b>4 – Monitorar, acompanhar e fiscalizar familiares do sentenciado.</b></p>	<p>4.1 – Obter 100% dos familiares que realizam visitas registradas e monitoradas.</p>	<p>4.1.1 – Realizar revistas minuciosas e alimentar o cadastro de todos os visitantes.</p>
<p><b>5 – Ampliações de programas de educação e de atividades laborais.</b></p>	<p>5.1 – Aumentar a atividade laboral de 38% para 55% e a taxa de alunos sentenciados de 12% para 20%. No período de 01/01/2017 à 31/12/2018.</p>	<p>5.1.1 – Buscar apoio empresarial, através da associação comercial local e incentivar o estudo.</p>
<p><b>6 – Aprimoramento do Departamento de Inteligência, para que se possa prevenir possíveis rebeliões, motins e outros.</b></p>	<p>6.1 – Evitar que o Sistema Prisional seja surpreendido por ações das facções criminosas.</p>	<p>6.1.1 – Qualificar os Agentes que compõe o Setor de Inteligência com conhecimento nacional e internacional de táticas de inteligência.</p>
<p><b>7 - Realizar Força Tarefa em revisão criminal em todas as unidades prisionais.</b></p>	<p>7.1 – Revisar as sentenças de todos os reeducandos.</p>	<p>7.1.1 - Convocar equipes de revisões criminais.</p>
<p><b>8 – Aumentar quadro de Agentes Penitenciários efetivos e de servidores conforme previsão legal.</b></p>	<p>8.1 – Equacionar a falta de efetivo e cumprir a previsão legal até dez/2018.</p>	<p>8.1.1 – Realizar concurso público e nomear todos os Agentes Penitenciários da previsão legal</p> <p style="text-align: right;"><i>Continua</i></p>

<p><b>9 – Apoiar ações para as Audiências de Custódia no sentido de apresentar em juízo o preso em até 24 horas e dispor de vagas.</b></p>	<p>9.1 evitar que presos fiquem mais que 24 horas em delegacias.</p>	<p>9.1.1 Ter vagas disponíveis para presos provisórios e demais regimes.</p>
<p><b>10 – Aumentar para 400 reeducandos monitorados com tornozeira eletrônica.</b></p>	<p>10.1 – Utilização de penas alternativas e abrir novas vagas até dez/2018.</p>	<p>10.1.1 – Ampliar para todas as unidades os serviços de colocação de tornozeleiras.</p>
<p><b>11 – Implementar Software <i>on-line</i> de gestão operacional e administrativa – Tecnologia de Informação – TI (Sistema Integrado de Gerenciamento Penitenciário).</b></p>	<p>11.1 – Obter dados e informações em tempo real.</p>	<p>11.1.1 – Estruturar todas as unidades prisionais com sistemas de comunicação e informação.</p>
<p><b>12 – Realizar estudo para localização e construções de novas unidades prisionais com base na necessidade de cada comarca e região.</b></p>	<p>12.1 – Adequar a necessidade de vagas, localizado próximo ao domicílio ou residência dos apenados.</p>	<p>12.1 Orientar as construções de novas unidades prisionais com base na demanda de vagas por Regiões ou Comarcas.</p>
<p><b>13 – Aumento da Segurança e da produtividade com uso das TIC.</b></p>	<p>13.1 – Aumentar a segurança e produtividade em 10%.</p>	<p>13.1.1 – Aumentar tecnologia nos processos administrativos, operacionais e apoiar estudos especializados de segurança pública.</p>

Fonte: Adaptado de Xavier e Amaral (1999).

## 6 CONSIDERAÇÕES FINAIS

O sistema prisional tem sido noticiado pelos meios de comunicações do mundo inteiro, como um modelo fracassado pela superlotação, motins e rebeliões,

que não cumpre a missão de executar a pena, ressocializar e integrar os indivíduos privados de liberdade no Brasil. Notadamente, as notícias e imagens que se tem acompanhado no ano de 2017 revelam o resultado de políticas repressivas de segurança do passado, que visam apenas manter o apenado afastado da sociedade, tal como um depósito de pessoas privadas de liberdade, distanciados dos direitos humanos, com a convivência de governos, universidades e sociedade.

Neste contexto, para o desenvolvimento deste trabalho, procurou-se elaborar pesquisa bibliográfica de planejamento estratégico, apresentar tecnologias de informação e comunicação em apoio à atividade de execução penal, buscar bases legais para nortear o estudo no sistema prisional, propor um planejamento estratégico, com propósito de encontrar a resposta para a pergunta da pesquisa “Quais as estratégias, tecnologias de informação e comunicação, que apoiam o Sistema Prisional Catarinense?”, e contribuir para a gestão técnica do sistema prisional Catarinense.

E assim, a relevância da proposta deste trabalho não pretende alcançar a perfeição, tendo em vista a limitação do conhecimento de informações do autor, e também porque um projeto desta magnitude necessita da participação de todas as lideranças multidisciplinares do sistema prisional.

O Sistema Prisional do Estado de Santa Catarina tem muitos desafios, principalmente no sentido de zerar o déficit de vagas e reduzir a reincidência, entretanto, nos últimos anos está sendo considerado destaque na melhora dos indicadores de políticas públicas aplicadas a pessoas privadas de liberdade. Ressalta-se ainda, a necessidade de fortes investimentos na construção de novas unidades prisionais, em áreas de tecnologias de comunicação e informação, aumento da contratação de novos servidores, implementação do planejamento estratégico institucional, para aumentar a capacidade adaptativa frente às demandas da execução penal e entrega do resultado esperado para a sociedade.

## **7 TRABALHOS FUTUROS**

Cabe ressaltar ainda, que este trabalho permitiu identificar oportunidade de desenvolvimento de pesquisa futura com gestão do conhecimento e aplicação do modelo de excelência em gestão pública, para aperfeiçoar esta proposta de planejamento estratégico para o sistema prisional do Estado de Santa Catarina.

## REFERÊNCIAS

ABDI - Agência Brasileira de Desenvolvimento Industrial. **Sistema Aplicado à Segurança Pública: Cadernos Temáticos 3 – Tecnologias de Informação e Comunicação – TIC**. Brasília, 2010.

BEBER, B. **Reeducar, reinserir e ressocializar por meio da Educação a Distância**. 2007. Tese (Doutorado em Engenharia e Gestão do Conhecimento – Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento. Universidade Federal de Santa Catarina, Florianópolis, 2007. Disponível em: <<http://repositorio.ufsc.br/xmlui/handle/123456789/90133>>. Acesso em 06 out. 2016.

BRADFORD R.W., DUNCAN P.J. e TRACY B. **Simplified strategic planning – a nonsense guide for busy people who want results fast**. Chandler House Press, 1999.

BRASIL. Congresso Nacional. Câmara dos Deputados. **Comissão Parlamentar de Inquérito Destinada a Investigar a Realidade do Sistema Carcerário Brasileiro**. CPI – sistema carcerário brasileiro [recurso eletrônico]: relatório final / Câmara dos Deputados, Comissão Parlamentar de Inquérito Destinada a Investigar a Realidade do Sistema Carcerário Brasileiro. Brasília: 2017. Disponível em: <<http://bd.camara.gov.br/bd/handle/bdcamara/31899>>. Acesso em 28 abr. 2016.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <<http://www.planalto.gov.br/constituicao>>. Acesso em 06 out. 2016.

BRASIL. **Lei nº 7.210, de 11 de julho de 1984**. Lei de execução penal. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/Leis/L7210.htm](http://www.planalto.gov.br/ccivil_03/Leis/L7210.htm)>. Acesso em: 06 out. 2016.

BRASIL. **Lei nº 12.433, de 29 de junho de 2011**. Altera a Lei nº 7.210, de 11 de julho de 1984 - LEP, para dispor sobre a remição de parte do tempo de execução da pena por estudo ou por trabalho. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2011/Lei/L12433.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12433.htm)>. Acesso em: 06 out. 2016.

BRASIL. Ministério da Justiça e Segurança Pública. DEPEN Departamento Penitenciário Nacional. **Levantamento Nacional de Informações Penitenciárias INFOPEN – junho 2014a**. Brasília, 2014. Disponível em: <<http://www.justica.gov.br/seus-direitos/politica-penal/documentos/relatorio-depen-versao-web.pdf>>. Acesso em: 06 out. 2016.

BRASIL. Ministério da Justiça e Segurança Pública. DEPEN Departamento

Penitenciário Nacional. **Levantamento Nacional de Informações Penitenciárias INFOPEN – dezembro de 2014b** Brasília, 2014. Disponível em: <[http://www.justica.gov.br/seus-direitos/politica-penal/documentos/infopen\\_dez14.pdf](http://www.justica.gov.br/seus-direitos/politica-penal/documentos/infopen_dez14.pdf)>. Acesso em: 06 out. 2016.

CERTO, S. C.; PETER, J. P. **Administração Estratégica: planejamento e implementação da estratégia**. São Paulo: Makron Books, 1993.

COLENGHI, V. M. **O&M e Qualidade Total: uma integração perfeita**. 3ª ed. Uberaba: VMC, 2007.

GIL, A. C. **Métodos e técnicas em pesquisa social**. 5 Ed. São Paulo: Editora Atlas, 1999.

GUIA PMBOK. **Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos**. 5ª ed., *Project Management Institute*(PMI): 2013.

HOQUE, Z; ADAMS, C. The rise and use of balanced scorecard measures in Australian Government Departments. **Financial Accountability & Management**, v. 27 n. 3, p. 308-334, 2011.

KAPLAN, R. S.; NORTON, D. P. **A estratégia em ação: balanced scorecard**. 5ª ed. Rio de Janeiro: Campus, 1997.

KAPLAN, R. S.; NORTON, D.P. **Colocando em funcionamento o balanced scorecard**. Harvard Business Review: medindo o desempenho empresarial. Rio de Janeiro: Campus, 2000.

KAPLAN, R. S.; NORTON, D. P. **Mapas estratégicos: balanced scorecard**. 5. Ed. Rio de Janeiro: Campus, 2004. MINTZBERG, H. Managing. **Desvendando o Dia a Dia da Gestão**. Porto Alegre: Bookman, 2010.

LEONEL, V.; MOTTA, A. M.; BASTOS, V. **Ciência e pesquisa: livro didático**. 2ª ed. Palhoça: Unisul Virtual, 2007.

OLIVEIRA, D. P. R. **Estratégia empresarial & vantagem competitiva: como estabelecer, implementar e avaliar**. 3ª ed. São Paulo: Atlas, 2001a.

OLIVEIRA, D. P. R. **Planejamento estratégico: conceitos, metodologia, práticas**. 16ª ed. São Paulo: Ed. Atlas, 2001b.

OLVE, N. et al. **Condutores da performance: um guia prático para o uso do balancedscorecard**. Rio de Janeiro: Qualitymark, 2001.

PEREIRA, M. F. **Planejamento Estratégico: O Curso**.CAD/UFSC, 2007.

PORTER, M. E. Como as forças competitivas moldam a estratégia. In: MONTGOMERY, C. A.; PORTER, M. E. **Estratégia: a busca da vantagem competitiva**. Rio de Janeiro: Campus, p.11-27, 1998.

QUINN, J. B. Estratégias para Mudança. In: MINTZBERG, H.; QUINN, J. B. **O Processo da Estratégia**. 3ª Ed. Porto Alegre: Bookman, p. 20-26, 2001.

SANTA CATARINA. 2007. **Lei Complementar nº 381, de 2007**. Dispõe sobre o modelo de gestão e a estrutura organizacional da Administração Pública Estadual. Disponível em: <[http://leis.alesc.sc.gov.br/html/2007/381\\_2007\\_lei\\_coplementar.html](http://leis.alesc.sc.gov.br/html/2007/381_2007_lei_coplementar.html)>. Acesso em: 04 mar. 2017.

SANTA CATARINA. 2011. **Lei Complementar nº 534 de 20 de abril de 2011**. Altera dispositivos da Lei Complementar nº 381, de 2007, que dispõe sobre o modelo de gestão e a estrutura organizacional da Administração Pública Estadual e estabelece outras providências. Disponível em: <[http://legislacao.sef.sc.gov.br/legtrib\\_internet/html/leis/2011/lc\\_11\\_534.htm](http://legislacao.sef.sc.gov.br/legtrib_internet/html/leis/2011/lc_11_534.htm)>. Acesso em: 04 mar. 2017.

SANTA CATARINA. Secretaria de Estado da Justiça e Cidadania. Penitenciária da Região de Curitiba. **Relatório de Indicadores de Resultados da PRC 2017**. São Cristóvão do Sul, SC, 2017.

WUA, J. C. et al. Government performance evaluation using a balanced scorecard with a fuzzy linguistic scale. **The Service Industries Journal**, v. 30, n. 3, p. 449-462, 2010.

XAVIER, A. C. da R.; AMARAL SOBRINHO, J. **Como elaborar o Plano de Desenvolvimento da Escola, aumentando o desempenho da escola por meio do planejamento eficaz**. 2. ed. Brasília: Programa FUNDESCOLA, 1999.

## A UTILIZAÇÃO DE SISTEMAS ELETRÔNICOS COMO INSTRUMENTO DE MODERNIZAÇÃO DA INVESTIGAÇÃO CRIMINAL

*Fernando Lúcio Mendes  
Vilson Gruber*

### 1 INTRODUÇÃO

Marcada por conquistas históricas, a Constituição Federal de 1988 rompeu com o tradicional paradigma de segurança pública como instrumento de preservação da ordem pública para adotar a ideia de segurança pública destinada à tutela de direitos. Ao criar um Estado Democrático de Direito fundado nos princípios da soberania, cidadania, dignidade da pessoa humana, valores sociais do trabalho, livre iniciativa e pluralismo político, o legislador constituinte deixou claro que governantes e governados submeter-se-iam às normas previamente determinadas, de modo a fazer valer os vetores norteadores do novo Estado criado.

Conforme texto introdutório contido no manual sobre a relação polícia e os direitos humanos, editado pela comissão de direitos humanos da Câmara dos Deputados (ROLIM, 2000 *apud* ARAÚJO, 2008a, p. 5), “uma polícia para a preservação da ‘ordem’, afinal, só pode ser concebida como uma instituição a serviço da manutenção do *status quo* braço armado do Estado voltado, sempre que necessário, contra as ‘classes perigosas’”. Contrapondo-a à nova concepção trazida pela Carta Política de 1988, Araújo (2008a, p. 5) afirmou que “a ideia de segurança pública associada à ‘tutela de direitos’ remete a um conjunto de direitos básicos que devem ser garantidos. A percepção de segurança para o cidadão é a que está relacionada com o respeito a seus direitos fundamentais”. Percebe-se, assim, claramente, que as posições defendidas pelos dois modelos são completamente antagônicas. A primeira, voltada para a concepção de segurança

pública como instrumento de manutenção das instituições vigentes, ignora qualquer tipo de direitos dos cidadãos para os quais deveria existir, servindo apenas como meio para a manutenção de um sistema de continuísmo político/ideológico; a segunda, por outro lado, volta-se à nova realidade democrática vigente, de modo a conceber a segurança pública como instrumento de garantia de direitos daqueles mesmos cidadãos tidos como seus destinatários.

Tal perspectiva, como visto, adequada à nova realidade imposta, concebe a segurança pública como mais um instrumento destinado à garantia de direitos fundamentais criados pela nova ordem jurídica constitucional; deste modo, como uma de suas principais ferramentas, a investigação criminal também deve ser readequada à nova realidade, razão pela qual necessariamente obedecerá a limites rígidos e voltar-se-á à proteção de direitos.

Realizando análise histórica, Araújo faz a seguinte ponderação:

Tanto a nossa Constituição (1988), como a francesa (1791), resultam na garantia da soberania do Estado, no respeito ao exercício dos atos de cidadania e da dignidade de cada cidadão, bem como dos valores sociais das liberdades. Sendo assim, as práticas da investigação criminal devem refletir a certeza de que cada uma delas tutela a garantia do modelo político adotado pelo Estado Democrático de Direito (ARAÚJO, 2008a, p. 6).

Desse modo, percebe-se claramente que a investigação criminal, para que possa desempenhar seu papel, deverá necessariamente ser vista como instrumento de defesa da cidadania, de modo que todos os direitos a ela relacionados possam ser exercidos de maneira livre e pacífica, bem como possa ser eficazmente utilizada contra aquele que efetivamente violá-los. Assim, passou a investigação criminal a ser enxergada como instrumento legítimo para que o Estado desempenhasse seu papel acusador, submetendo o autor de determinada infração penal ao processo necessário à sua responsabilização. Para que a investigação criminal seja, entretanto, considerada legítima é preciso que seja observado o método previsto pela legislação, o que conferirá não só eficiência e regularidade ao trabalho desempenhado, mas também licitude ao produto dele resultante.

A realidade das delegacias de polícia, contudo, demonstra que os métodos de investigação tradicionalmente utilizados não conseguem mais, com a mesma efetividade, trazer resultados consideráveis à instrução do inquérito policial, instrumento destinado à documentação das diligências investigativas realizadas.

Com o passar dos anos e com o progresso tecnológico vivenciado nas últimas décadas, tanto a sociedade quanto o conhecimento científico evoluíram consideravelmente. Mudaram-se os costumes, os modos de produção, os arranjos sociais e, na mesma medida, a maneira de se praticar crimes. A mesma tecnologia antes utilizada em benefício da sociedade para a apuração de delitos passou a voltar-se contra ela mesma. Nesse contexto, os métodos tradicionalmente empregados para a investigação de delitos começaram a demonstrar sinais de obsolescência, sendo ainda, por vezes, considerados absolutamente ineficazes diante da nova realidade do fenômeno criminoso.

Assim, necessário se faz que o sistema de segurança seja conduzido aos trilhos da revolução tecnológica, permitindo que os métodos e técnicas de seu instrumento principal, a investigação criminal, sejam também influenciados pelo progresso científico, com a adoção de novas tecnologias que a tornem eficaz.

O aperfeiçoamento tecnológico das instituições responsáveis pela realização das investigações criminais no país, portanto, é medida que deve ser adotada como prioridade, dotando seus agentes de conhecimento técnico e mecanismos capazes de conferir efetividade aos trabalhos realizados, fazendo frente à nova realidade criada.

Sob esta mesma ótica, a modernização tecnológica vislumbrada pelo emprego de tecnologias da informação na atividade investigativa deve necessariamente ser acompanhada de programa de capacitação de seus quadros para operá-las, de acordo com a metodologia de emprego previamente estudada pela Instituição.

Nesse contexto, questiona-se de que forma poderia o Estado e seus agentes empregarem sistemas eletrônicos para modernização da investigação criminal realizada por seus órgãos, de modo a proporcionar maior efetividade no desempenho de suas atividades.

Assim, o presente trabalho tem por objetivo estudar a possibilidade de utilização de sistemas eletrônicos (em sua grande maioria embarcados) como fatores de eficácia à investigação criminal moderna, a partir da análise da estrutura da atividade investigativa, bem como da utilização desses equipamentos para modernização de seus elementos. A partir dessa verificação, será possível, ainda, organizar programas específicos de capacitação dos agentes públicos responsáveis pelos trabalhos, de modo que possam empregar, com eficiência, todas as técnicas e equipamentos adotados por suas organizações.

Para que se pudesse atingir o objetivo proposto, o presente artigo estruturado em seis seções. Na segunda seção, desenvolveu-se o conceito, bem como a finalidade da investigação criminal, de modo que se pudesse situar o leitor no tema chave da discussão; na terceira parte, procurou-se trabalhar as modalidades de investigação existentes; numa quarta, explicou-se o procedimento de coleta de dados e informações, isto é, o funcionamento da investigação na prática, sendo que na quinta parte foram os elementos básicos de toda investigação criminal elegidos como critérios de seleção de equipamentos eletrônicos. Ao final, em uma sexta parte, inseriu-se a conclusão, oportunidade em que se demonstrou a possibilidade de empregar tecnologias da informação e comunicação para modernização da atividade investigativa, tomando-se como parâmetro seus elementos estruturantes, de modo a possibilitar a substituição técnica de metodologias já ultrapassadas.

## **2 INVESTIGAÇÃO CRIMINAL: CONCEITO E FINALIDADE**

A atividade de investigação sempre atraiu de maneira efetiva a atenção das pessoas e povoa o imaginário de aficionados pelo tema; mesmo aqueles que de maneira não profissional passam a ter contato com o assunto, acabam sendo atraídos pela cultura popular difundida em filmes e programas televisivos em geral, que demonstram *glamour* no exercício da atividade, liberdade para agir sem qualquer restrição legal e facilidade de acesso a lugares e informações sem muito esforço.

Entretanto, longe do que retratado pela ficção, a investigação criminal é atividade que exige técnica e utilização de metodologia adequada para que seu produto seja capaz de sustentar um processo criminal. Com disciplina relativamente rígida no Brasil, a atividade de investigação possui regras e princípios que, se não observados, poderão não só levar a conclusões precipitadas (ou até mesmo equivocadas), mas também inutilizarão seu produto no processo de responsabilização do infrator.

Praticado um fato tido como criminoso, surge para o Estado o poder de sancionar o infrator de determinada norma penal, aplicando-lhe a pena previamente determinada pelo Direito. Tal poder, entretanto, é conferido ao mesmo Estado como forma de tornar pacífico o convívio social, de modo que mais adequado seria caracterizá-lo como verdadeiro poder-dever, vez que, salvo exceções, também

determinadas pela norma, certamente será exercido para a devida responsabilização do autor do fato. A este poder-dever dá-se o nome de pretensão punitiva<sup>1</sup>.

No sistema processual brasileiro, a pretensão punitiva é exercida por meio de atos estatais divididos em duas fases distintas. Numa primeira, denominada pré-processual ou investigativa, desempenhada via de regra por órgãos administrativos, serão realizados atos de investigação destinados à reunião de elementos que demonstrem não só a existência do fato criminoso, bem como de suas circunstâncias, mas também indícios que apontem sua autoria; em uma segunda fase, conhecida como processual e, portanto, desempenhada por órgãos que compõem a estrutura judiciária, haverá a produção probatória propriamente dita, de modo que os elementos de informação e demais fontes de prova reunidos na primeira fase serão submetidos à dialética necessária à formação da prova destinada ao convencimento do julgador (contraditório).

A reunião de elementos informativos quanto à autoria e materialidade de um delito (prova da existência do crime), portanto investigação criminal, é realizada, via de regra, em um procedimento administrativo específico e por órgãos especializados, a quem a Constituição entregou expressamente tais atribuições. Assim, por força dos artigos 144, §1º e 144, §4º, da Constituição da República Federativa do Brasil, a apuração de infrações penais (excetuadas tão somente as militares) é atividade destinada às Polícias Cíveis e Federal, que dirigidas por Delegados de Polícia de carreira, também, assumirão as funções de polícia judiciária dos Estados e da União, respectivamente.

Desse modo, pode-se conceituar investigação criminal como a atividade do Estado realizada por órgãos específicos e especializados com a finalidade de apurar a autoria, materialidade (prova da existência) e demais circunstâncias de determinado fato criminoso, diligências estas realizadas, via de regra, em procedimento administrativo denominado Inquérito Policial.

---

<sup>1</sup>De acordo com Badaró (*apud* LIMA, 2011, p. 238) a pretensão punitiva é “o poder do Estado de exigir de quem comete um crime a submissão à sanção penal. Através da pretensão punitiva, o Estado-Administração procura tornar efetivo o *ius puniendi*, com o exigir do autor do crime, que está obrigado a sujeitar-se à sanção penal, o cumprimento dessa obrigação, que consiste em sofrer o delinquente as consequências do crime e se concretiza no dever de abster-se ele de qualquer resistência contra os órgãos estatais a que cumpre executar a pena. Porém, tal pretensão não poderá ser voluntariamente resolvida sem um processo, não podendo nem o Estado impor a sanção penal, nem o infrator submeter-se à pena. Assim sendo, tal pretensão já nasce insatisfeita.”

Por fim, verifica-se que a investigação criminal pode ser equiparada à produção de um conhecimento científico, razão pela qual deveria ser sistematicamente realizada. Sobre o assunto, Dencker (2007, p.2) afirma que “o conhecimento científico se caracteriza pela reflexão e intenção de construção de um corpo metodicamente ordenado de conhecimentos, orientado pelo emprego científico”; na sequência, aduz que o “método científico é um conjunto de regras ou critérios que servem de referência no processo de busca da explicação ou da elaboração de previsões em relação a questões ou problemas específicos”, motivo pelo qual conclui que “o emprego do método é que faz com que o conhecimento seja considerado científico” (DENCKER, 2007 *apud* ARAÚJO, 2008b, p. 2).

### 3 MODALIDADES EXISTENTES

No que diz respeito aos tipos ou modalidades de investigação criminal desenvolvidas, é possível encontrar, num primeiro momento, classificação trazida por Araújo (2009a), que leva em consideração a natureza funcional do investigador. Conforme defende o autor, “há provas produzidas pelo investigador cujas atividades, na estrutura funcional, estão diretamente vinculadas ao controle da autoridade policial, ou seja, acontece, via de regra, no âmbito do cartório da organização policial”. Como exemplo, cita a coleta de depoimentos, reconhecimento de pessoas e coisas, dentre outras atividades realizadas sob coordenação direta do delegado de polícia (ARAÚJO, 2009a, p. 4).

Por outro lado, informa que “a prova baseada em vestígios materiais tem sua produção em laboratório e é executada por peritos sem uma subordinação funcional direta da autoridade policial” (ARAÚJO, 2009a, p. 4). Diante disso, propõe classificação do processo investigatório em cartorário e técnico científico, conforme definição abaixo transcrita:

Investigação criminal cartorária: é aquela desenvolvida sob o controle técnico-funcional direto da autoridade policial, no âmbito do cartório da organização. Exemplos: ordem de serviço expedida a uma equipe de profissionais da seção de investigação para localizar determinada testemunha ou para identificar as testemunhas de um determinado delito e o reconhecimento de um suspeito;

Investigação criminal técnico-científica: é aquela desenvolvida pelos peritos, sob a coordenação técnico-operacional indireta da autoridade policial. É feita mediante requisição da

autoridade policial que preside a investigação. Exemplos: a análise de mancha de sangue feita pelo perito no local de crime, e necropsia feita pelo legista. (ARAÚJO, 2009a, p. 4).

Em interessante estudo sobre a investigação criminal em crimes de homicídio, Mingardi<sup>2</sup>(2005, p. 11) apresentou minucioso relatório sobre as condições em que eram desenvolvidas as atividades de investigação relacionadas a crimes dolosos contra a vida no país. No trabalho apresentado, propôs classificação que, segundo Araújo (2009a, p. 4), também pode ser aplicada no contexto da investigação criminal (em sentido amplo); são elas: a investigação preliminar e a investigação de seguimento.

Sobre as classificações propostas, Mingardi (2005, p.11) explica o seguinte:

As atividades desenvolvidas durante a realização da pesquisa possibilitaram identificar a realidade da rotina investigatória. Para melhor compreensão do texto dividimos sua apresentação em 2 etapas: Investigação Preliminar e Investigação de Seguimento. A Investigação Preliminar é aquela que inicia logo após o descobrimento do crime e continua até a liberação do local pela polícia. Normalmente dura poucas horas. Já a Investigação de Seguimento ocorre após a polícia deixar o local e é feita tendo como ponto de partida os indícios ou provas obtidas na Investigação Preliminar. Pode durar dias, meses, ou mesmo não chegar a lugar algum. (MINGARDI, 2005, p. 11).

Detalhando a classificação acima proposta, Araújo (2009a, p. 4) explica que “a investigação preliminar é aquela que se inicia logo após a notícia do crime e continua até a liberação do local pela polícia”, citando como exemplo a investigação de local de crime, título sugerido inclusive como sinônimo para investigação preliminar, tal como registrado na pesquisa realizada.

Por sua vez, ao tratar da investigação de segmento, afirma ser aquela que “ocorre após a polícia deixar o local e é feita tendo como ponto de partida os indícios ou provas obtidas na investigação preliminar” (ARAÚJO, 2009a, p. 5). Em arremate, explica o autor que “as duas modalidades são gerais, abrangem a investigação cartorária e a técnico científica”, de modo que todas as classificações antes trabalhadas podem ser consideradas complementares para a explicação da estrutura da função policial investigativa (ARAÚJO, 2009a, p. 5).

---

<sup>2</sup>Autor da pesquisa Investigação de homicídios – Construção de um modelo, elaborada em 2005 e apresentada à Secretaria Nacional de Segurança Pública no ano seguinte.

Contudo, em que pese a importância doutrinária das classificações aqui trabalhadas, constata-se, salvo melhor juízo, não serem perfeitamente adequadas à realidade do instituto (investigação criminal) ou, pelo menos no primeiro caso, enfatizam de maneira demasiada os atores envolvidos e não os fatos criminosos objeto de apuração.

Considerando a natureza funcional de quem a exerce (investigação criminal cartorária ou técnico-científica), a classificação adotada privilegia a subordinação direta ou indireta à autoridade policial, sem considerar a espécie de fato criminoso investigado. Tratando-se de procedimento sistematizado, melhor seria, acredita-se, que métodos fossem desenvolvidos levando em consideração classificação que privilegiasse o tipo de fato criminoso investigado, de modo que o resultado pudesse ser alcançado com maior eficácia.

Todavia, ao reputar o momento em que é executada (investigação criminal preliminar ou de segmento), a classificação correspondente parece tratar de maneira adequada apenas os casos de crimes materiais instantâneos, cujo resultado natural (ou naturalístico) pode ser visualizado pelos investigadores em situação ideal de espaço e tempo, vez que, nesse caso, ao menos o resultado será sempre instantâneo e material, isto é, visível logo após a prática da conduta (que até poderá ser, em determinados casos, arrastada no tempo).

Em uma investigação de homicídio, por exemplo, situação específica para a qual a segunda classificação foi proposta, a conduta produtora do resultado morte é desempenhada, normalmente, em um único ato ou em atos sequenciais próximos, de modo que o normal é que o resultado (morte) ocorra de forma instantânea. Por conseguinte, é possível falar em investigação de local, já que o resultado estará posto à disposição dos responsáveis pelos atos de investigação.

Discorrendo sobre a diferenciação entre crimes instantâneos e permanentes, Nucci (2014, n.p.) afirma que “os delitos instantâneos são aqueles cuja consumação se dá com uma única conduta e não produzem resultado prolongado no tempo. Assim, ainda que a ação possa ser arrastada no tempo, o resultado é sempre instantâneo”, oportunidade em que cita como exemplos os crimes de homicídio, furto e roubo.

Por outro lado, explica que “os delitos permanentes são os que se consomem com uma única conduta, embora a situação antijurídica gerada se prolongue no tempo até quando queira o agente”. Explica, ainda, ser exemplo de tal crime o

sequestro ou cárcere privado, sendo que “com a ação de tirar a liberdade da vítima, o delito está consumado, embora, enquanto esteja em cativeiro, por vontade do agente, continue o delito em franca realização”, situação que admitiria, inclusive, a prisão em flagrante do infrator (NUCCI, 2014, n.p.). Conforme apontado pelo autor acima mencionado, são exemplos de crimes permanentes a extorsão mediante sequestro, o porte ilegal de arma e de substância entorpecente, dentre outros.

Por outro lado, tais classificações parecem não se adequarem às situações de concurso de crimes, principalmente quando praticados por organizações criminosas (e também situações de continuidade delitiva), bem como aos casos de crimes permanentes (tais como os que acima mencionados) e habituais. Com relação aos últimos, explica Nucci (2014, n.p.) serem aqueles que somente se consomem “através da prática reiterada e contínua de várias ações, traduzindo um estilo de vida indesejado pela lei penal. Logo, pune-se o conjunto de condutas habitualmente desenvolvidas e não somente uma delas, que é atípica”. Continua, ainda, afirmando tratar-se de “modalidade específica de crimes, não admitindo confusão com os instantâneos e permanentes”. Já o concurso de crimes “significa a prática de várias infrações penais por um só agente ou por um grupo de autores atuando em conjunto” (NUCCI, 2014, n.p.), situação que demandará, certamente, metodologia diferenciada de investigação.

Assim, em que pese a utilidade das classificações estudadas, acredita-se que melhor seria que fosse levada em consideração a natureza dos fatos criminosos investigados, o grau de conhecimento sobre eles, bem como a quantidade de elementos que demonstrem a própria materialidade (existência) do delito, de modo que propomos, neste trabalho, que a investigação seja classificada como prévia (ou exploratória) e posterior (ou tradicional). Tal classificação levaria em consideração, conforme acima mencionado, não só a natureza dos fatos (criminosos) investigados, mas também seu momento de consumação, o momento de sua demonstração à autoridade responsável, bem como os métodos desenvolvidos para sua realização.

Nesse contexto, a investigação prévia ou exploratória seria aquela realizada nos casos em que houvesse necessidade de demonstração da própria existência do crime (doutrinariamente conhecida por materialidade delitiva); assim, os métodos de investigação desenvolvidos poderiam ser aplicados a crimes permanentes (consumação prolongada no tempo), habituais (exigem reiteração de condutas para a própria caracterização do delito), além de situações de continuidade delitiva (prática reiterada de crimes considerados de mesma espécie e nas mesmas

condições de tempo, lugar e maneira de execução), de modo a demonstrar documentalmente sua ocorrência a partir de diligências específicas que, realizadas em conjunto, também apontariam seus autores (eventuais responsabilidades).

Tal classificação, desse modo, seria mais adequada para denominar as diligências realizadas em uma investigação de tráfico de drogas, por exemplo, quando apenas “denúncias anônimas” informassem a possibilidade de sua ocorrência. Como exemplo, pode-se citar a realização de campanhas nas proximidades de pontos indicados como locais de possível comércio de entorpecentes, interceptações telefônicas, etc., todas elas visando demonstrar a existência do delito, suas circunstâncias, bem como a preparação para a realização do flagrante, após o que técnicas de investigação de segmento seriam aplicadas.

Inadequado, portanto, classificá-las como preliminares ou mesmo de segmento, vez que não realizadas com foco em local de crime específico; igualmente, apesar de serem realizadas, via de regra, por agentes diretamente subordinados à autoridade policial, investigações técnico-científicas também poderiam ser requisitadas nessa fase dos trabalhos, de modo que a classificação voltada à natureza funcional serviria tão somente para explicar o vínculo de quem exerce a atividade.

Sob outra perspectiva, a investigação posterior ou tradicional seria aquela desenvolvida após a comunicação da ocorrência de fato criminoso perfeitamente demonstrado (prova evidente de materialidade); nesse sentido, diligências preliminares (local de crime, quando for o caso), bem como de segmento seriam realizadas para apuração de todas as suas circunstâncias e eventuais responsabilidades.

Percebe-se, via de regra, portanto, que a investigação tradicional é realizada com o objetivo de apurar crimes instantâneos (consumação imediata), sendo que também será desempenhada de maneira cartorária e técnico-científica, com a adoção dos já conhecidos métodos tradicionais.

Por outro lado, conforme anteriormente explanado, a investigação seria classificada como exploratória quando diligências específicas (cartorárias ou técnico-científicas) precisassem ser realizadas para confirmação da própria existência do delito, situação que também possibilitaria a demonstração de todas as suas circunstâncias e responsabilidades.

Vale registrar que, em nosso sistema processual, a investigação prévia ou exploratória, tal como aqui defendido, encontra previsão no artigo 5º, parágrafo 3º, do Código de Processo Penal, *in verbis*:

Art. 5º, §3º. Qualquer pessoa do povo que tiver conhecimento da existência de infração penal em que caiba ação pública poderá, verbalmente ou por escrito, comunicá-la à autoridade policial e esta, verificada a procedência das informações, mandará instaurar o inquérito. (BRASIL, 1941)

Assim, verifica-se claramente que as chamadas “VPI’s” ou procedimentos de verificação de procedência da informação, materializam verdadeira investigação prévia ou exploratória em sede de ação penal pública (aquela que independe de manifestação de vontade da vítima ou seu representante legal), vez que realizadas com o nítido propósito de reunir maiores elementos (dados e informações) acerca da própria materialidade do delito. Nucci (2013, p. 96), ao comentar os ensinamentos de Maurício Henrique Guimarães Pereira, registra o seguinte:

O nosso particular entendimento é de que, em sede de comunicação anônima ou apócrifa de crime, a própria lei concilia os interesses da administração da justiça e da honra objetiva do denunciado, que são os bens jurídicos tutelados no crime de denúncia caluniosa, com o princípio da obrigatoriedade, que é comum em ambas as fase da persecução penal, ao dispor que ‘qualquer pessoa do povo que tiver conhecimento da existência de infração penal em que caiba ação pública poderá, verbalmente ou por escrito, comunicá-la à autoridade policial’, mas, esta, somente após ‘verificar a procedência das informações’, por força da vedação constitucional, mandará instaurar inquérito.

Mais ainda, o referido autor registra que:

A investigação de uma denúncia realizada anonimamente deve ser feita em absoluto sigilo, até que se descubram elementos de veracidade, o que permitirá, então, a instauração, de ofício, do inquérito policial, como se a comunicação apócrifa não tivesse ocorrido (NUCCI, 2013, p. 96).

Assim, a classificação proposta, neste trabalho, não tem apenas objetivo acadêmico, sendo também dotada de utilidade pragmática.

#### **4 COLETA DE DADOS E INFORMAÇÕES: A INVESTIGAÇÃO NA PRÁTICA**

É possível afirmar, de maneira breve, que a atividade de investigar significa “seguir os vestígios, fazer diligências para achar, pesquisar, indagar, inquirir; investigar as causas de um fato; examinar com atenção; esquadrihar” (AURÉLIO, 1975, *apud* ARAÚJO, 2009a, p. 2). Tais verbos, contudo, serão praticados por meio de um conjunto de ações/diligências que terão por objetivo coletar os dados e informações destinados à formulação das hipóteses necessárias à explicação do fato criminoso.

Araújo (2009c, p. 2) explica que “são diversas maneiras e ferramentas para operá-la: a entrevista, a análise de vestígios, a interceptação telefônica, a interceptação ambiental, a análise de imagens e a análise de sinais”. Igualmente, ao tratar sobre a forma de seleção da ferramenta mais adequada à realização da atividade, o autor traz a seguinte lição:

A formulação da ferramenta de coleta é feita em função do fenômeno investigado e das variáveis necessárias para sua explicação. Todos os dados e informações levantados terão que ter relação com o fato em apuração para que possam ser validados como prova (ARAÚJO, 2009c, p. 2-3).

Assim, percebe-se que a investigação é materializada por procedimentos destinados à reunião de dados que, contextualizados ao fato/fenômeno investigado, gerarão informações capazes de dar significado ao conjunto de diligências realizadas, produzindo, assim, o conhecimento necessário à explicação do delito e de todas as suas circunstâncias.

Tratando-se o método científico de “um conjunto de regras ou critérios que servem de referência no processo de busca da explicação ou da elaboração de previsões em relação a questões ou problemas específicos” (DENCKER, 2007, *apud* ARAÚJO, 2008b, p. 2) e prevendo o Código de Processo Penal a sistemática base para a reunião dos dados e informações necessária à formação do conhecimento indiciário resultante da investigação criminal realizada, será possível, certamente, caracterizá-la como ciência, aplicando ao conhecimento dela produzido o adjetivo correlato (científico) (ARAÚJO, 2008b, p. 2).

## 5 ELEMENTOS BÁSICOS DE INVESTIGAÇÃO CRIMINAL COMO CRITÉRIOS DE SELEÇÃO DE EQUIPAMENTOS E SISTEMAS ELETRÔNICOS

Segundo Araújo (2009c, p. 9), “as técnicas de investigação criminal têm como elementos básicos a observação, a memorização e a descrição”. Via de regra, todas as técnicas conhecidas de investigação (campanas, coletas de dados por meio de informantes, entrevistas etc.) possuem os três elementos mencionados, sejam elas de natureza cartorária ou técnico-científica (ou exploratória ou tradicional, tal como defendido na classificação por nós proposta). Em apertada síntese, a observação pode ser considerada método de coleta de dados que utiliza, essencialmente, os sentidos (visão, audição, paladar, tato e olfato), cujo resultado será materializado em documento descritivo que exponha as impressões colhidas de forma contextualizada. Por óbvio, variarão os meios de execução da observação, a exemplo de campanas realizadas a olho nu ou por monitoramento eletrônico, bem como a maneira pela qual os dados e informações colhidos serão registrados e descritos, vez que poderão ocorrer de forma manual ou eletrônica ou por intermédio de dispositivos e *softwares* de tecnologia da informação.

Por outro lado, o segundo elemento básico de qualquer técnica de investigação conhecida é a memorização. Conquanto não sejam utilizados equipamentos eletrônicos como suporte (o que ampliará consideravelmente a capacidade de reunião de informações), a investigação contará com a capacidade de memorização do investigador, que deverá transcrever as informações relevantes para um relatório de investigação, sendo constantemente treinada e estimulada por mecanismos de melhoria de memória, situação que dependerá de capacidades cognitivas.

Por fim, é importante esclarecer que o processo de descrição corresponde ao registro dos dados e informações anteriormente memorizados, de modo que as diligências realizadas durante o processo de investigação sejam necessariamente documentadas (sendo também possível o desenvolvimento de *software* para realização de tal finalidade).

Considerando o fato de todas as técnicas tradicionais possuírem, por base, os três elementos acima mencionados, verifica-se que a utilização de equipamentos eletrônicos focada nesses elementos poderia ser capaz de atualizar e aperfeiçoar os métodos tradicionais existentes. Pensando nessa perspectiva, passamos a estudar,

ao final de 2013, dispositivos que pudessem, de alguma forma, serem empregados para modernização das técnicas tradicionais comentadas, a partir a otimização de processos vinculados a seus elementos.

O trabalho foi estruturado em quatro grupos de equipamentos (quatro eixos) que poderiam ser utilizados de maneira individual ou conjunta, em verdadeira atuação complementar: *drones*, câmeras embarcadas em viaturas para monitoramento remoto (e possível infiltração eletrônica), rastreadores veiculares e sistemas de interceptação ambiental.

Em pesquisa de campo realizada durante a participação da Polícia Civil do Estado de Santa Catarina nas eleições municipais de 2014, foi possível reunir elementos que demonstraram, de maneira pragmática, que o estudo realizado poderia tornar as investigações mais efetivas, vez que a Delegacia escolhida para o trabalho (Balneário Arroio do Silva) acabou por realizar, com a utilização dos equipamentos e sistemas escolhidos, a prisão em flagrante e indiciamento de cerca de 10 (dez) suspeitos pela prática, em tese, de crimes eleitorais em uma única tarde. Deve-se ressaltar, a respeito, que o trabalho foi realizado sob a coordenação de um Delegado de Polícia e dois agentes.

Importante esclarecer, ainda, que a pesquisa de campo mencionada foi estendida posteriormente a investigações de tráfico de drogas, armas e crimes ambientais, dentre outras atividades relevantes, sendo que foram sentidas melhorias significativas na qualidade das investigações realizadas (melhor instrução dos Inquéritos), diminuição do tempo destinado aos trabalhos, possibilidade de atuação com efetivo reduzido (já que os equipamentos auxiliaram os policiais em atividades importantes, como campanas fixas e móveis por exemplo), além de maior grau de motivação da equipe.

## 6 CONCLUSÃO

Entendendo, pois, a realidade do método investigativo atual, bem como os elementos estruturantes que compõem suas técnicas tradicionais de investigação conhecidas, percebe-se pela pesquisa realizada que existem, atualmente, sistemas eletrônicos disponíveis no mercado que podem ser utilizados para sua modernização, seja por facilitarem a observação ou memorização dos dados e informações captadas, seja por permitirem melhor descrição dos resultados da observação realizada pelos agentes responsáveis pela atividade investigativa.

Assim, *drones* e seus respectivos sistemas embarcados (câmeras, sensores, etc.), sistemas de monitoramento por vídeo embarcados em viaturas descaracterizadas, rastreadores veiculares, equipamentos para interceptação ambiental, dentre diversos outros dispositivos eletrônicos, podem contribuir para a melhoria do processo investigativo de campo se utilizados como fatores de modernização de técnicas tradicionais existentes, de modo que sejam conjugados com as já bem sucedidas técnicas de coleta de dados e informações por meio da utilização de *softwares* e sistemas de mineração de dados, análise de perfis em redes sociais e diversas outras aplicações (para coletas de evidências em meio digital).

Por outro lado, concluímos que o emprego de tais equipamentos (muitos deles projetados para finalidade múltipla, a exemplo dos *drones*) demanda criação de metodologia própria para emprego policial, vez que a utilização não especializada demonstrou, em grande parte dos casos (tanto na pesquisa realizada, quanto nas demais iniciativas isoladas conhecidas), o subemprego dos dispositivos.

Assim, propomos, para otimizar instrumentos de coletas de dados e informações e buscar efetividade dos resultados produzidos, a ampliação do estudo de equipamentos eletrônicos (a partir da seleção de sistemas profissionais), além da criação de proposta de modelo de gestão e operação integrada de Drones por órgãos de segurança pública no Estado de Santa Catarina, com sugestão de criação de curso de capacitação em gestão e operação de drones (RPA) para agentes de segurança pública, a ser implementado na Academia de Polícia Civil (trabalho atualmente desenvolvido no Mestrado do Programa de Pós-graduação em Tecnologias da Informação e Comunicação da Universidade Federal de Santa Catarina).

Na medida em que técnicas de investigação mais atuais e sofisticadas são utilizadas por pessoal capacitado para desenvolvê-las, é possível observar tendência de incremento na celeridade, bem como na eficiência e efetividade do trabalho produzido. Além disso, a correta observância do método desenvolvido poderá garantir que o resultado seja alcançado com mais qualidade, menos esforço e, principalmente, com a observância da legislação em vigor, vez que os servidores serão capazes não só de decidir pela forma correta de emprego do equipamento, mas também conhecerão seus limites técnicos e jurídicos, de modo a produzir diligências válidas, que atendam aos direitos Constitucionais dos envolvidos e confirmem legalidade e legitimidade à atuação policial.

## REFERÊNCIAS

ARAÚJO, Francisco das Chagas S. Curso investigação criminal I: módulo 1. SENASP/MJ, 2008a.

\_\_\_\_\_. Curso investigação criminal I: módulo 2. SENASP/MJ, 2009a.

\_\_\_\_\_. Curso investigação criminal I: módulo 5. SENASP/MJ, 2008b.

\_\_\_\_\_. Curso investigação criminal II: módulo 1. SENASP/MJ, 2009b.

\_\_\_\_\_. Curso investigação criminal II: módulo 2. SENASP/MJ, 2009c.

BADARÓ, Gustavo Henrique. Ônus da prova no processo penal. São Paulo: Editora Revista dos Tribunais, 2003. p. 283.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)>. Acesso em: 7 jun. 2015.

CAPEZ, Fernando. Curso de processo penal. 21. ed. São Paulo, 2014. Edição digital.

DENCKER, Ada de Freitas Maneti. Pesquisa em turismo: planejamento, métodos e técnicas, 9ª ed. São Paulo: Futura, 2007.

LIMA, Renato Brasileiro de. Manual de processo penal. vol. I. Rio de Janeiro: Impetus, 2011.

NUCCI, Guilherme de Souza. Código de processo penal comentado. 12. Ed rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2013.

MINGARDI, Guaracy. A investigação de homicídios: construção de um modelo. Secretaria Nacional de Segurança Pública: São Paulo, 2005.

ROLIM, Luiz Antônio. Instituições de Direito Romano. São Paulo: Editora Revista dos Tribunais, 2000.

---

## **O USO DAS MÍDIAS DIGITAIS PELA POLÍCIA MILITAR NA APROXIMAÇÃO COM A COMUNIDADE: UM ESTUDO DE CASO NO DESTACAMENTO DE BALNEÁRIO ARROIO DO SILVA**

*Maicon dos Santos Borges  
Solange Maria da Silva*

### **1 INTRODUÇÃO**

Quando se fala em Segurança pública, vêm à mente, alguns órgãos públicos que, por intermédio dos impostos, são designados a oferecer proteção e segurança à sociedade. Em uma visão segmentada e linear, estariam, de um lado, os órgãos públicos, que devem fazer o controle e, do outro, os cidadãos, que pagamos impostos. Contudo, nessa visão dicotômica entre sociedade e segurança pública, vê-se obstáculos à efetividade das ações de segurança pública à sociedade e ao país. Portanto, a tecnologia, que hoje está presente de forma muito habitual na sociedade, pode contribuir de forma significativa para uma aproximação e uma troca valiosa de informação entre essas instituições.

Em uma sociedade com forte influência da tecnologia, o uso das mídias digitais pode ser um aliado para difundir informações sobre a segurança pública, pois, na medida em que a população reconhece os diversos projetos desenvolvidos pela Polícia Militar, ela pode passar a confiar mais na instituição. As mídias digitais oferecem um grande suporte para qualquer instituição desenvolver um bom serviço; o uso constante de tecnologias (das mais variadas formas em mídias digitais) mudou o sentido de se obter notícia (SILVA, 2016) e informação. Ainda conforme o autor (SILVA, 2016), a notícia ampliada pelo uso constante das mídias digitais não substituiu a mídia analógica, ela apenas aliou-se e manteve um novo formato de se obter a

notícia. Sabedor dessas novidades, os mercados pelo mundo reformularam seus conceitos e investiram em tecnologias embarcadas pelas mídias digitais.

A Polícia Militar de Santa Catarina, vendo a necessidade de se manter sempre proativa para a população, embarcou em uma nova tecnologia digital, desenvolvida em parceria com a Secretaria de Estado da Segurança Pública (SSP) e o Centro de Informática e Automação do Estado de Santa Catarina (CIASC) e, assim, desenvolveu um sistema de gestão de atendimento, o PMSC *Mobile*. O objetivo desse sistema é diminuir o tempo de resposta e atendimento dos policiais militares nas ocorrências, demonstrando que o uso das mídias digitais já se faz presente na organização e pode fornecer agilidade aos atendimentos. Com o uso de *tablet* e *smartphone*, o sistema PMSC *Mobile* atuará nas cidades catarinenses e ampliará o uso de tecnologias pela polícia militar (SANTA CATARINA, 2016).

O dever da Polícia Militar perante a população já é conhecido desde a criação da instituição, como mantenedora dos direitos adquiridos na constituição de 1988, sempre em busca de formas de se promover e ampliar formas de prevenção. Portanto, o uso das mídias digitais em vários equipamentos tecnológicos como computadores, *tablets*, *smartphones*, entre outros, possibilita à população verificar a atuação da instituição, mediante *site* e redes sociais por essa mantidos.

A segurança pública exercida pela Polícia Militar segue premissas descritas pela constituição e deixa bem claro a preservação da ordem pública por meio de medidas preventivas que buscam dessa forma evitar problemas futuros.

A preservação da Ordem Pública dá-se em duas fases distintas: a primeira em situação de normalidade, quando esta é assegurada por ações eminentemente preventivas, por meio do exercício da Polícia Ostensiva e a segunda, em situações de anormalidade, ou seja, na quebra da ordem pública, quando ela deve ser restabelecida por meio de ações de Polícia Ostensivas repressivas, enérgicas e imediatas (SANTA CATARINA, 2016, p.1).

Como a Polícia Militar está presente em todos os estados que compõem a federação, percebe-se que a mídia digital pode ser um componente tecnológico de alta valia, uma vez que a mesma pode contribuir na construção de uma polícia moderna e tecnológica, que se aproxime da comunidade por meio de recursos disponíveis e fornecidos pelas mídias digitais, que são usadas constantemente pela população.

Segundo Martino (2014), o acesso à informação, mediante a internet com apoio das mídias digitais, nem sempre foi um fato comum no Brasil. O desenvolvimento do país contribuiu na aquisição de novas tecnologias que, por sua vez, necessitavam de mídias digitais multiplicadoras de informação.

A partir de 1995, de maneira cada vez mais rápida, as mídias digitais e a internet passam a fazer parte do cotidiano, espalhando-se não apenas no uso de computadores, mas também, em um segundo momento, em celulares, *smartphones* e outros equipamentos. O cotidiano se conecta, e com ele a necessidade de se pensar, em termos teóricos e conceituais, o que significam as mídias digitais (MARTINO, 2014, p.13).

A informação pode ser ampliada quando atrelada a uma tecnologia. O uso das mídias digitais para difundir, receber e modificar informações amplia o verdadeiro sentido da palavra informação. Amplamente necessária em nosso meio, a tecnologia, criou mecanismos para estar sempre à frente, difundindo novos meios para o ambiente da comunicação (MARTINO, 2011).

Nesse contexto, a presente pesquisa tem por objetivo demonstrar como as mídias digitais podem contribuir na construção do relacionamento entre polícia e comunidade, assim como a importância que as ferramentas de mídias digitais trazem ao serviço policial.

## **2 FUNDAMENTAÇÃO TEÓRICA**

### **2.1 Novas Mídias**

As novas mídias surgiram com o advento da computação, que por meio de dados numéricos, tornaram-se conhecidas como mídias digitais. Seu surgimento revolucionou o que se conhecia por mídia no mundo.

O termo mídias digitais é, às vezes, intercambiado com nova mídia, novas mídias, novas tecnologias e expressões derivadas. De algum modo, essas expressões procuram estabelecer uma diferença entre os chamados meio de comunicação de massa ou mídias analógicas, como a televisão, o rádio, jornais e revistas impressos, dos meios eletrônicos (MARTINO, 2014, p.10).

A mídia digital se transformou em um meio facilmente modificável. As inúmeras transformações possíveis são realizadas graças a um código básico de cada máquina que é digital, o chamado código binário. As mídias digitais modificaram as formas de comunicação existentes, ampliando e transformando os sistemas de comunicação. O relacionamento humano foi ampliado e transformado por meio dessa ferramenta, e a expansão do número de usuários não tem precedente. A barreira digital ainda continua, mas inúmeras formas estão sendo criadas para driblar as barreiras e ampliar o acesso a essa ferramenta tão importante para o desenvolvimento da sociedade (MARTINO, 2014).

Uma mídia digital é aquela que tem como suporte um objeto que permite o armazenamento e decodificação em formato digital que, via de regra, é oposto ao analógico. Um suporte analógico permite representações, como o próprio nome diz, por analogia, ou por comparações. Ele representa as grandezas de forma contínua. Como exemplos de objeto analógico pode ser citado o clássico relógio de parede, com ponteiros indicando as horas e minutos. Nesse sistema, a representação é por comparação, ou seja, é possível saber as horas e minutos comparando a posição dos ponteiros no relógio (SILVA, 2016, p.95).

Segundo Cannito (2009, p.48), “dentro do campo audiovisual, podemos denominar digital um vasto conjunto de tecnologias de captação, finalização, distribuição, recepção e reprodução de imagens e sons em diversos suportes”. Para definir de forma mais simples, os objetos de mídias digitais podem ser vistos como um conjunto de aparelhos compostos de tecnologia digital tais como: computador, telefone celular, *tablet*, revistas digitais, televisão digital, vídeo digital, foto digital, entre outros. Essas mídias digitais estão se diferenciando das mídias antigas, analógicas, não somente por sua composição de existência, a internet, mas pela velocidade, praticidade e comodidade aos usuários que essa tecnologia desenvolveu nos últimos anos (CANNITO, 2009).

Segundo Martino (2014), o computador recebe dados convertidos em uma sequência de números, esses dados são interpretados pelo computador, característica básica de uma mídia digital. A partir de conceitos-chave para as mídias digitais, Martino (2014, p.11-12) consolidou os conceitos, a partir dos autores Flew (2008), Gane e Beer (2008), Abercombrie e Longhurst (2008) e Chandler e Munday (2010), para melhor exemplificar as mídias digitais.

**Quadro 1 - Conceitos-chave de mídias digitais**

<b>CONCEITO</b>	<b>DEFINIÇÃO INICIAL</b>
Barreira Digital	Diferenças de acesso às tecnologias e mídias digitais, bem como à cultura desenvolvida nesses ambientes, vinculadas a problemas sociais e econômicos.
Ciberespaço	Espaço de interação criado no fluxo de dados digitais em redes de computadores, <i>virtual</i> por não ser localizado no espaço, mas <i>real</i> em suas ações e efeitos.
Convergência	Integração entre computadores, meios de comunicação e redes digitais, bem como de produtos, serviços e meios na internet.
Cultura participatória	Potencialidade de qualquer indivíduo se tornar um produtor de cultura, seja recriando conteúdos já existentes, seja produzindo conteúdos inéditos.
Inteligência coletiva	Possibilidade aberta pelas tecnologias de rede de aumentar o conhecimento produzido de maneira social e coletiva.
Interatividade	Interferência e interação entre usuários, ou usuários, programas e conteúdo, em diferentes níveis e formas, nos sistemas de comunicação digital em rede.
Interface	A operação das mídias digitais acontece a partir de pontos de contato “amigáveis” entre dispositivos e usuários, moldados a partir de referências culturais anteriores.
Segurança e vigilância	Possibilidade de identificação de dados gerados nas mídias digitais em rede, ultrapassando os limites público/particular e redefinindo a noção de “privacidade”.
Ubiquidade	Presença, em todos os lugares, de mídias digitais conectadas em rede, estabelecendo conexão em qualquer espaço e tempo.
Velocidade	A rapidez de conexão de dados nas mídias digitais se articula com aceleração de inúmeras atividades, processos e acontecimentos da vida cotidiana.
Virtualidade	Dados das mídias digitais existem de maneira independente de ambientes físicos, podendo se desenvolver livres, a princípio, de qualquer barreira desse tipo.

Fonte: MARTINO (2014, p.11-12).

## 2.2 Tecnologias Digitais

As inúmeras formas de tecnologias com mídias digitais, sejam elas *Hardware* ou *Software*, estão em nossa sociedade, construindo um novo modo de vida (SILVA, 2016). Para o autor, é importante ressaltar que os meios são ampliados conforme o surgimento de novas tecnologias, assim, cada objeto de mídia, usando como componente o suporte digital, forma e amplia essa vasta rede chamada tecnologia.

O computador foi o precursor da tecnologia existente, atualmente, nas suas inúmeras funções, auxiliando e transformando os mercados. A partir disso, criaram-se, outras ferramentas tecnológicas móveis com capacidade similar ao computador, que são os celulares e *tablets*, os quais inundam os mercados com tecnologia de ponta. O computador, como uma tecnologia inovadora, mostrou-se capaz de modificar e assimilar informações, antes retidas de forma manuscrita. Portanto, a forma com que essa tecnologia entrou na sociedade transformou-a em um bem de consumo necessário à vida em sociedade (SILVA, 2016).

A tecnologia, especialmente a mídia, não é apenas um instrumento para se transmitir e compartilhar informações. Mais do que um suporte para mensagens, é um elemento decisivo na formação de mente, dos modos de sentir, perceber e compreender a realidade (MARTINO, 2014, p.204).

A cultura da tecnologia está sendo enraizada, cada vez mais, no cotidiano da vida em sociedade, em que os mais variados formatos de tecnologias digitais formam uma rede de comunicação poderosa, podendo ser desde simples conversas entre amigos à resolução de negócios.

Com o avanço da tecnologia no mundo, abriram-se espaços para desenvolver mídias poderosas que nutrem as informações necessárias à sociedade, os *tablets*, hoje comuns no dia a dia, são ferramentas que mantêm e movimentam dados importantes, ferramentas que podem auxiliar na construção de dados tal como o computador. O *banner* digital, a revista digital, vídeos digitais e os *outdoors* digitais ganham, cada vez mais, espaço na mídia, favorecendo a ampliação de novos mercados (CARVALHO; SILVA, 2011).

A redemocratização do país, garantida pela constituição de 1988, deu fim a uma era marcada pelo desrespeito aos direitos humanos, praticado durante o período militar<sup>1</sup>. Por sua vez, é possível perceber que a segurança pública se tornou um dos pilares da forte constituição cidadã, assim denominada, defrontando-se, todo dia, com novos desafios para manter a ordem e o progresso da sociedade.

O conhecimento sobre as instituições públicas, muitas vezes, distantes da população, torna-se um dos degraus a ser enfrentado pela polícia Militar, ora inserida na segurança pública, com vistas a construir uma imagem de confiança para sociedade. Atualmente, a relação que se observa entre a Polícia e a sociedade é de

---

<sup>1</sup> Período Militar: Regime sob comando dos governos militares, que durou de 1º de abril de 1964 a 15 de março de 1985.

insegurança mútua, uma vez que, as funções de segurança nem sempre contemplam os estratos de baixa renda, o que os leva a serem vigiados por criminosos, que procuram um meio de subsistir e confrontar o poder do estado, abrigando-se em meio a comunidades carentes e usando o povo como “escudo” frente às forças de segurança. Da mesma forma, a confiança que a sociedade tem na Polícia Militar torna-se muito frágil em ambientes de confronto ou com elevados casos de criminalidade.

Conforme Carvalho e Silva (2011, p.62),

Mecanismos essenciais não têm sido utilizados pelos diversos governos para possibilitar o pensar, o implementar, o implantar, o efetivar, com eficácia e eficiência, uma política de segurança pública como instrumento do Estado e da sociedade.

O Estado que, apesar de enfrentar grande deficiência na área de desenvolvimento tecnológico, em muito tem se fortalecido com a ajuda de ações desenvolvidas em conjunto com a sociedade, pois esta pode, por meio diversas formas de acesso às informações privilegiadas, contribuir para o desenvolvimento de uma segurança pública de qualidade, uma vez que, conhecimentos na área de segurança têm demonstrado ser de grande auxílio na resolução de problemas com segurança no país.

Carvalho e Silva (2011, p. 63) se alinham a esse entendimento ao afirmarem que “as questões relacionadas à segurança pública não podem ser tratadas como política limitada de governo, mas como um processo amplo e complexo a ser enfrentado, tanto pelo Estado quanto pela sociedade”. E entendem que, parte das políticas públicas atuais tem se voltado para o desenvolvimento de uma política de segurança eficiente, sendo muitos investimentos aplicados em treinamento e pesquisa, para organizar um Estado seguro aos brasileiros.

A importância da segurança, no Brasil, já se tornou um compromisso de muitas classes sociais e políticas, a vivência com a criminalidade em nada tem contribuído para o desenvolvimento de uma sociedade civil organizada (CARVALHO; SILVA, 2011). Os inúmeros casos de violência na sociedade têm influência, direta ou indiretamente, na formulação de políticas de segurança pública. Assim, a contribuição da comunidade vai desde a construção de ideias para o cenário nacional, como nos pequenos conselhos comunitários, vistos pelo Brasil para auxiliar

a Polícia a cumprir sua meta constitucional, sendo que a constituição prevê a segurança como um dos valores supremos da sociedade (GUSSI, 2005).

Os fortes índices de violência que vêm acontecendo pelo Brasil influenciam os governos a investirem em inteligência e interação e, a cada dia, vê-se essa interação da comunidade, na criação, desenvolvimento e ampliação de novas políticas, em âmbitos nacional ou regional. Não se pode construir uma sociedade livre, sem uma corporação envolvida com as pessoas, então, a participação popular se torna, nesse momento, tão forte e substancial, que qualquer tentativa de progressão para redução da criminalidade deve ser, obrigatoriamente, feita com a interação da comunidade.

### **2.3 Polícia Comunitária**

A polícia militar, por meio de suas inúmeras ações, busca de forma eficaz mostrar que a relação com a comunidade não deve ser esquecida e, sim, fortalecida. Dessa forma, a polícia comunitária surge como um conceito de aproximação e construção de uma “nova polícia”.

A polícia comunitária é uma nova parceria entre a população e a polícia, buscando, acima de tudo, uma conscientização popular acerca da responsabilidade social de cada indivíduo e ainda do comprometimento de ambas as partes na solução de problemas e na busca de melhoria da qualidade de vida da comunidade. Para chegar nesse estágio, entretanto, é preciso que a polícia se aproxime do cidadão e inicie a construção de uma relação de cumplicidade, que foi negligenciada por muito tempo (MARCINEIRO, 2009, p. 126).

As inúmeras instituições que, hoje, compõem o sistema de segurança pública possuem seus serviços baseados na constituição, a premissa principal do respeito às pessoas, porém, ofertar um serviço de qualidade às pessoas em seus diversos ambientes têm se mostrado como uma barreira à polícia. Nos ambientes cercados de violência, faltam estruturas básicas de saúde e educação, aliados ao contato direto com o crime organizado, criam um empecilho à confiança que deve existir entre a sociedade e a polícia.

Segundo Marcineiro (2009), o conceito de polícia comunitária não é novidade no mundo, diversas autoridades policiais já utilizam dessa premissa e os resultados têm se mostrado surpreendentes, as ações desenvolvidas pelo modelo de polícia tradicional, restringindo-se em controlar a criminalidade e prender criminosos, tendo

com a comunidade somente uma relação distante e neutra, não modificou a segurança e, tampouco, desenvolveu uma aproximação com a sociedade. O combate ao crime não é eficaz somente na prisão em flagrante do autor, a prevenção ao crime tem resultados positivos, quando aliada às práticas da comunidade.

A vivência da polícia com a comunidade transforma simples ações em efetiva qualidade de serviço, e o conhecimento prévio da situação enfrentada pela comunidade traz ao policial uma nova forma de enfrentar os problemas. Contudo, essa aproximação deve ser baseada em mútua confiança, pois a criminalidade, cada dia mais intensa na sociedade, afasta a confiança nos órgãos de segurança pública, e traz à população o sentimento de impunidade e descrença nos serviços pelos agentes oferecidos.

A forma de se aproximar da comunidade com reuniões em que os moradores conhecem os policiais, são informados dos serviços desempenhados e das ações preventivas para evitar delitos, promove uma corrente de cooperação entre polícia e comunidade (MARCINEIRO, 2009).

Como parte fundamental na concretização da polícia comunitária, as pessoas envolvidas devem aderir ao conceito com cautela, visto que essa política de aproximação depende de vários fatores, ambientais e humanos, haja vista a diversidade de ambientes e a pluralidade de pensamentos que hoje existem na sociedade, esses fatores devem ser levados em consideração, para que esse modo de policiamento seja aderido por todos.

A confiança que a polícia procura na sociedade virá com a construção de novos pensamentos erguidos em conjunto, conforme (MARCINEIRO, 2009), deve-se fazer uso dos meios possíveis para alcançar esse objetivo, humanos e tecnológicos, haja vista que nossa sociedade já está praticamente inserida no meio global, facilitando, assim, por meio das tecnologias o conhecimento dos serviços fornecidos pela polícia militar em suas diversas esferas.

### **3 PROCEDIMENTOS METODOLÓGICOS**

Esta pesquisa utiliza a abordagem qualitativa, pois parte da percepção dos atores organizacionais para descrever a realidade investigada (VERGARA, 2000). Quanto ao seu objetivo classifica-se como exploratória-descritiva.

Inicialmente, foi realizada uma pesquisa bibliográfica sobre segurança pública, mídias digitais, mídias sociais e Polícia Militar, baseada em estudos por diversos autores da literatura especializada, dando maior confiabilidade ao trabalho sobre a importância do uso de mídias digitais pela Polícia Militar na aproximação com a comunidade.

A unidade de análise consiste no Destacamento de Balneário Arroio do Silva e, portanto, envolve o desenvolvimento de uma pesquisa de campo (LAKATOS; MARCONI, 2003), que aqui será descrito como um estudo de caso.

Nesse viés, o presente trabalho é realizado a partir de uma observação direta extensiva, por meio um questionário aplicado ao público em estudo (policiais militares do destacamento de Balneário Arroio do Silva), e cujas perguntas são fechadas, de múltipla escolha. Tal instrumento de coleta de dados foi enviado a 13 policiais militares, tendo o retorno de todos os questionários aplicados.

#### **4 MÍDIAS DIGITAIS NA POLÍCIA MILITAR**

A polícia militar faz uso das mídias digitais assim como qualquer empresa. Os objetos que possuem mídias digitais são dos mais variados, pode-se citar: Os computadores, os *notebooks*, os *smartphones*, os *tablets* entre outros. As mais variadas funções administrativas executadas por essas mídias conduzem os serviços oferecidos pela polícia militar.

A sociedade pode acompanhar integralmente as atividades desempenhadas, por meio do *site* institucional, além das redes sociais mantidas pela polícia militar de Santa Catarina, com isso, as mídias digitais trouxeram uma nova visão sobre o serviço policial. Conforme Marcineiro (2009), a imagem de confiança da instituição depende de vários fatores, com o uso das tecnologias digitais o policial terá uma relação de confiança com a comunidade, a população poderá acompanhar os diversos feitos pela instituição, dicas de segurança e prevenção, hoje disponíveis pela manutenção das mídias digitais na Polícia Militar.

A mais nova ferramenta de mídia digital presente na Polícia Militar de Santa Catarina é fornecido pelo *tablet*, conhecido como Sistema *Mobile* PMSC. Essa mídia digital foi desenvolvida com objetivo de transformar o atendimento das ocorrências, visto que a forma manuscrita de diversos procedimentos policiais atrasavam os

atendimentos, continham informações imprecisas e dificultavam na tradução dos dados para os relatórios.

Com o PMSC *Mobile*, as informações antes registradas em até onze (11) formulários de papel, agora, estão sistematizadas em um único aplicativo informatizado, tornando o processo mais ágil e menos propenso a erros.

O PMSC Gestão, outro aplicativo fornecido pelo sistema *mobile*, se destina à supervisão e controle da atividade operacional nas unidades policiais militares abrangidas pelo Sistema de Atendimento e Despacho de Emergência (SADE). O aplicativo também é permitido apenas em equipamentos de propriedade da PMSC, ou particulares de comandantes, oficiais de unidade operacional e integrantes da Agência Central de Inteligência, ou ainda policiais militares autorizados pelo EMG.

O aplicativo do SISP Móvel é usado para consultas policiais de pessoas e veículos. Ele foi desenvolvido pela Secretaria de Estado da Segurança Pública, por meio da Diretoria de Informação e Inteligência (DINI), em conjunto com o Ciasc, Polícia Civil e Polícia Militar. A ferramenta de tecnologia permite a todos os agentes de segurança pública o acesso às informações de segurança pública, justiça e fiscalização. Antes da implantação do sistema, qualquer consulta deveria ser realizada mediante um terceiro, central de atendimento (COPOM), com esse aplicativo implantado as informações de consulta poderão ser acessadas pelo próprio policial na ocorrência (SANTA CATARINA, 2016).

## 5 APRESENTAÇÃO DOS RESULTADOS

Por meio de análise dos dados coletados, constatou-se que a aproximação efetiva da polícia com a comunidade foi intensificada com auxílio das mídias digitais, corroborando os estudos de Gussi (2005), Marcineiro (2009), Marinho (2002), Martino (2014) e Marques (2016). A utilização das redes sociais, além das ferramentas de mídias digitais, tal como *tablet*, possibilita o acompanhamento das ações da polícia na comunidade de Balneário Arroio do Silva, contribuindo também à forma de atendimento e ampliação do policiamento com a ajuda da comunidade.

Com o surgimento das mídias digitais e suas inúmeras vertentes, pode-se montar um paralelo e formar um apoio na rede mundial de computadores, a fim de manter um laço entre a comunidade e a polícia. Por meio dos questionários aplicados aos policiais militares do município de Balneário Arroio do Silva, percebeu-se que a

aproximação efetiva da polícia com a comunidade foi intensificada com auxílio das mídias digitais. A tecnologia presente na instituição Polícia Militar não é recente, sendo que as ferramentas citadas, neste trabalho, já estão em uso e trazem diversos benefícios.

Segundo os participantes da pesquisa tais recursos auxiliam na redução da criminalidade, sendo de extrema importância ações que incentivem, cada vez mais, a utilização dessas tecnologias em prol da segurança.

A análise das respostas revelou ainda que as ferramentas de mídias digitais mais utilizadas no exercício diário do trabalho e no relacionamento dos policiais com a comunidade, no destacamento de Balneário Arroio do Silva, são: o computador, com 92%, seguido do *WhatsApp* (85%), *Tablet* (77%) e o celular com 69%.

As respostas do questionário demonstraram também, que algumas ferramentas apontadas pela literatura e conhecidas pelo mercado como sendo úteis no relacionamento efetivo com a comunidade, na percepção dos policiais militares do município de Balneário Arroio do Silva, têm pouca relevância naquele contexto, sendo elas: o *outdoor* digital e o *banner* digital.

Por outro lado, o *Facebook* tem sido uma ferramenta útil para o seu efetivo relacionamento com a comunidade local, sendo destacado como tal por 84% dos participantes. O *WhatsApp* é outra ferramenta muito disseminada na sociedade, sendo apontado como útil (84%).

Em relação às contribuições do uso das mídias digitais, tem-se como resultados: agilidade no atendimento (89,4%); relação de confiança com a comunidade local(93%); aproximação entre polícia militar e comunidade (92%); promoção da imagem da polícia militar perante a comunidade local (100%); redução da incidência da criminalidade na comunidade local (92%).

## 6 CONSIDERAÇÕES FINAIS

A aproximação da polícia com a comunidade deve ser construída aos poucos, visto tamanha complexidade, muitas vezes causados por anos de distanciamento. A construção de uma imagem positiva passa pela garantia em fornecer um bom serviço na comunidade e por meio de gestos de confiança a comunidade percebe o verdadeiro valor das instituições de segurança.

Com a segurança cada vez mais enxuta em recursos humanos e tecnológicos, a comunidade percebe a diminuição da chamada “sensação de segurança”, cabendo aos estados prover tal serviço, pois da segurança, dependem vários setores da sociedade.

A inserção da tecnologia para aproximar a comunidade da polícia militar, pode tornar simples atos em prevenção contínua em nosso meio, com uma polícia mais próxima do cidadão, o qual pode participar por meio denúncias, solicitações e reclamações, fatos que transformam um serviço público.

A aproximação com a comunidade, citada neste trabalho, pode ser observada com a intensificação na utilização das mídias digitais pela Polícia Militar, *sites* e redes sociais mantidas pela corporação, assim como a mais recente inovação *PMSC Mobile* tem transformado positivamente a relação da comunidade com a polícia. Por muitas vezes, os policiais são abordados e informados de situações suspeitas, nas quais o cidadão repassa, por meio do celular para os *tablets* das viaturas, imagens de pessoas e veículos que circulavam pela comunidade, permitindo aos policiais executar uma busca pelo sistema *on-line* e ainda repassar essa informação a outras viaturas com relato e imagens do fato, tornando-se assim uma informação fidedigna e segura.

A interação com a comunidade está sendo conquistada aos poucos, pois a imagem do militarismo ainda ecoa na sociedade, porém a Polícia Militar como instituição permanente de defesa da sociedade vem a cada dia aplicando ensinamentos no rumo dos direitos humanos aos policiais. A sociedade pode observar por meio das intensas campanhas de apoio à construção de laços na segurança, o programa polícia comunitária é um exemplo dessa aproximação, na qual o policial inserido e aceito pela comunidade conhece seus anseios e mantém uma confiança importante.

Assim como afirma Marcineiro (2009), as diversas ferramentas devem ser utilizadas em prol da população, citam-se nesse trabalho as ferramentas de mídias digitais, as formas preventivas e de promoção à segurança, no contexto do município de Balneário Arroio do Silva. O importante passo em direção à integração foi dado, pois no destacamento de Balneário Arroio do Silva já está em uso diversas ferramentas de mídias digitais e por meio da polícia comunitária criou-se um elo com a sociedade, no qual gerará maior confiança da população e, na corrente dessa confiança, a sociedade terá o benefício de uma segurança mais ampla.

O uso das mídias digitais pela Polícia Militar na aproximação com a comunidade: um estudo de caso no destacamento de Balneário Arroio do Silva

Os desafios ligados ao tema ainda continuarão a ser debatidos e reorganizados para sua completa solução, a aceitação do policial como parte importante na sociedade depende do policial e de cada cidadão, a utilização de maneira inteligente e constante das ferramentas de mídias digitais já tem dado frutos aos policiais na obtenção de confiança no serviço e reconhecimento da população com a construção da nova polícia cidadã.

## REFERÊNCIAS

BRASIL. Secretaria de Comunicação Social. Presidência da República. **Pesquisa brasileira de mídia 2015: Hábitos de consumo de mídia**. Disponível em <[http://www. Pesquisa Brasileira de Mídia - PBM 2015.pdf](http://www.PesquisaBrasileira.deMídia-PBM2015.pdf)>. Acesso em: 09 ago. 2016.

CANNITO, Newton Guimarães. **A televisão na era digital**. 2009. 304 f. Tese (Doutorado) - Curso de Ciências da Comunicação, Escola de Comunicação e Artes, Universidade de São Paulo, São Paulo, 2009.

CARVALHO, Vilobaldo Adelídio de; SILVA, Maria do Rosário de Fátima. **Política de segurança pública no Brasil: avanços, limites e desafios**. Pesquisa Teórica, Florianópolis, v. 14, n. 1, p.59-67, 17 jan. 2011. Disponível em: <<http://www.scielo.br/pdf/rk/v14n1/v14n1a07.pdf>>. Acesso em: 01 jul. 2016.

FERNANDES, Rubens César. **Policciamento Comunitário: como começar**. Rio de Janeiro: POLICIALERJ, 1994.

GUSSI, Evandro Herrera Bertone. **A segurança na constituição**. 2005. 171 f. Dissertação (Mestrado) - Curso de Direito, Programa de Pós-graduação em Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2005. Disponível em: <<http://hdl.handle.net/10183/8782>>. Acesso em: 18 set. 2016.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos da metodologia científica. 5. ed. São Paulo: Atlas S.a, 2003. 310 Plauria, Lélío. **A questão da Segurança Pública no Brasil**. 2011. Disponível em: <[http://acritica.uol.com.br/blogs/blog\\_do\\_lelio\\_lauria/seguranca-publica-Brasil\\_7\\_551414854.html](http://acritica.uol.com.br/blogs/blog_do_lelio_lauria/seguranca-publica-Brasil_7_551414854.html)>. Acesso em: 28 out. 2016.

MARCINEIRO, Nazareno. **Polícia comunitária: construindo segurança nas comunidades**. Florianópolis: Insular, 2009. 232 p.

MARINHO, Karina R. Leite. **Mudanças Organizacionais na implantação do Policiamento Comunitário**. 2002. Dissertação (Mestrado em Sociologia). Faculdade

O uso das mídias digitais pela Polícia Militar na aproximação com a comunidade: um estudo de caso no destacamento de Balneário Arroio do Silva

de Filosofia e Ciências Humanas da Universidade Federal de Minas Gerais, Belo Horizonte, 2002.

MARTINO, Luís Mauro Sá. **Teoria das mídias digitais: linguagens, ambientes, redes**. Petrópolis: Vozes, 2014. 273 p.

MARQUES, Archimedes Jose Melo (Ed.). **A segurança pública e a sociedade**. 2016. Disponível em: <<https://www.algosobre.com.br/interesse-publico/a-seguranca-publica-e-a-sociedade.html>>. Acesso em: 26 out. 2016.

SANTA CATARINA. Assessoria de imprensa. Quartel do Comando Geral da Pmsc. **História da PMSC**. 2016. Disponível em: <<http://www.pm.sc.gov.br/institucional/historia/>>. Acesso em: 26 jul. 2016.

SANTA CATARINA. Jorge Luis Sedrez Mendes. **Polícia Militar de Santa Catarina** (Ed.). PMSC Mobile será expandido para todos os municípios catarinenses em 2016. 2016. Disponível em: <<http://www.pm.sc.gov.br/noticias/pmsc-mobile-sera-expandido-para-todos-os-municipios-catarinenses-em-2016.html>>. Acesso em: 19 out. 2016.

SILVA, Eli Lopes Da. Labirinto rizomático de experiências com mídias digitais. 2016. 373 f. Tese (Doutorado) - Curso de Programa de Pós-graduação em Educação, Centro de Ciências de Educação, Universidade Federal de Santa Catarina, Florianópolis, 2016. Disponível em: <<https://repositorio.ufsc.br/xmlui/handle/123456789/167467>>. Acesso em: 12 dez. 2016.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 3. ed. São Paulo: Atlas, 2000.

## PROPOSTA DE UM SISTEMA INTEGRADO DE DECLARAÇÃO DE ÓBITO

*Roberto Hideo Omomo  
Wilson Gruber*

### **1 INTRODUÇÃO**

As informações vitais de nascimento e óbito são de extrema relevância para a Administração Pública, em especial, para a gestão da saúde, segurança pública, aplicação da justiça e estatística. Atestar, registrar e comunicar corretamente as causas médicas e jurídicas da morte são importantes para fins cíveis e criminais.

A Declaração de Óbito (DO) é o documento médico que atesta e informa a morte. É fundamental para proceder ao enterro da pessoa falecida e deve ser entregue no momento da liberação do corpo, seja pelos hospitais, Serviço de Verificação de Óbito (SVO) ou Instituto Médico Legal (IML).

A DO, como muitos documentos públicos, ainda se encontra no estágio de apresentação física, em papel carbono autocopiativo. A DO brasileira é composta de três (3) vias, possui 59 campos divididos em nove (9) blocos para serem preenchidas à caneta. Os trâmites de cada uma das três vias envolvem várias etapas e agentes, o que aumenta risco de perda de informações e qualidade. A complementação dos dados faltantes por outras pessoas é difícil e não tem melhorado a qualidade.

As desvantagens da Declaração de Óbito em papel são inerentes ao formulário carbonado sem integração com sistemas eletrônicos, destacando-se: risco de perda, extravios, destruição e subregistros; impossibilidade de alterações e correções; baixa qualidade da informação; excesso de etapas com dispêndio de tempo e pessoal; e atraso no processamento de dados. Mesmo que haja reconhecimento público e notório sobre as falhas e baixa qualidade inerente ao

próprio método de preenchimento manual desse modelo físico em papel da DO, existe uma tendência de responsabilizar somente o médico pelos dados e informações imprecisas, incorretas, divergentes ou faltantes na DO.

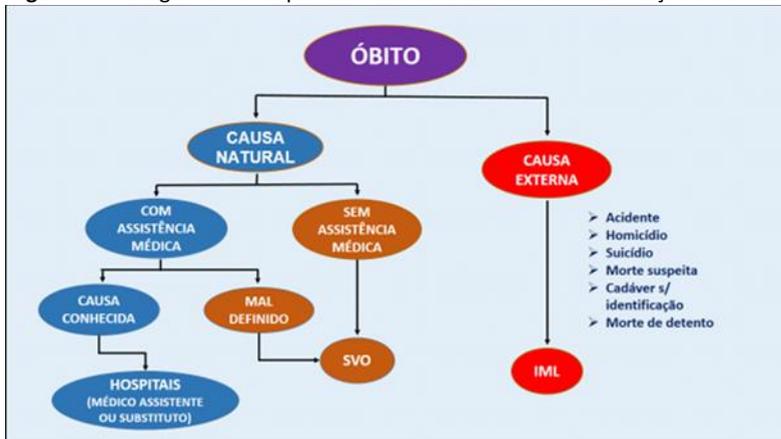
Assim, este artigo pretende descrever as possibilidades de construção de um Sistema Integrado de Declaração de Óbito (DO), utilizando Tecnologias de Comunicação e Informação (TIC). Para tanto, está organizado em 5 seções: as responsabilidades da DO em morte violenta é descrita na segunda seção; na terceira, apresentam-se alguns exemplos internacionais de DO informatizado; na quarta seção, indicam-se as bases de dados que podem ser integradas para construir um modelo nacional de DO digital; na quinta, apresenta-se uma prototipação deste sistema integrado.

## **2 DECLARAÇÃO DE ÓBITO EM MORTES VIOLENTAS**

A responsabilidade pela emissão da DO varia conforme o tipo de óbito. As informações de morte que interessam para a segurança pública são aquelas diagnosticadas como causa externa, não natural, como por exemplo, óbitos decorrentes de violência (acidente, homicídio e suicídio) ou suspeita de violência (envenenamentos, corpo não identificado ou encontrado em avançado estado de decomposição).

Para a segurança pública, o registro de evento fatal de pessoa investigada põe fim ao trabalho policial e judicial sob ponto de vista administrativo e criminal. Por outro lado, toda morte violenta ou suspeita de violência necessita de investigação policial para apurar as responsabilidades quanto às circunstâncias do óbito e responsabilização criminal do agente causador. Estudos estatísticos de mortes violentas são necessários para delinear as ações policiais. Nesse contexto, é obrigatório o encaminhamento do corpo ao Instituto Médico Legal (IML) para exame cadavérico (necrópsia) para fazer prova técnica da morte violenta e de suas circunstâncias. A responsabilidade pela emissão da Declaração de Óbito, nesses casos, é do IML conforme figura abaixo (Figura 1).

**Figura 1** - Fluxograma de responsabilidades na emissão da Declaração de Óbito.



**Fonte:** Adaptado de PRO-AIM, 2014.

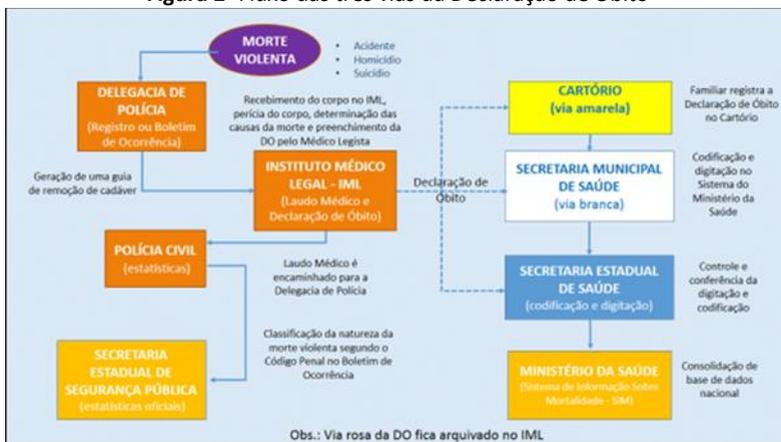
A emissão da Declaração de Óbito em mortes de causa natural, com assistência médica recente e com conhecimento da causa morte, é da responsabilidade dos hospitais, na figura de seus médicos assistentes ou dos médicos plantonistas. A emissão da Declaração de Óbito em mortes de causa natural, sem assistência médica ou com desconhecimento da causa morte, é feita pelo Serviço de Verificação de Óbito (SVO).

Das três vias da Declaração de Óbito (Figura 2), a primeira via branca é encaminhada para secretaria municipal de saúde para que o digitador insira os dados no Sistema de Informações em Mortalidade (SIM). A segunda via amarela, é entregue ao familiar do falecido que leva ao cartório para proceder ao assentamento de óbito e obter Certidão de Óbito. A terceira via, de cor rosa, fica arquivada no IML.

Tem-se observado a emissão de DO, equivocadamente, pelos hospitais, em casos de morte violenta ou suspeita de violência sem comunicação do IML, com certa frequência, como nos casos de acidentes e intoxicação exógena em que a vítima morre depois de vários dias de internação, o que dificulta, posteriormente, a instalação de inquérito policial e apuração de responsabilidades.

Faltam pesquisas nacionais a respeito do preenchimento da DO em morte violenta por médicos não legistas. Em Portugal, Silva (2015) encontrou 32 casos de morte violenta preenchidos erroneamente por médicos não legistas do total de 66 DO, ou seja, a falha nesse aspecto foi de quase 50 %.

Figura 2- Fluxo das três vias da Declaração de Óbito



Fonte: Adaptado de Borges et. al., 2013<sup>1</sup>.

Com base no preenchimento errado da DO surge a necessidade de desenvolvimento de um sistema eletrônico que possa bloquear, automaticamente, o envio de diagnósticos de morte violenta pelos médicos dos hospitais. Tal sistema permitiria, assim, realizar necrópsia correta pelos IMLs.

### 3 MODELOS INTERNACIONAIS DE DECLARAÇÃO DE ÓBITO DIGITAL

Diversos países tornaram eletrônico o atestado de óbito. Nos países mais adiantados, sistemas eletrônicos de atestado de óbito têm sido implantados desde os anos 2000. Países como Estados Unidos, França e Portugal são os pioneiros nessa área. Na América Latina, Uruguai, Colômbia e Peru usam sistemas digitais de atestado e de certificação óbito.

#### a) Estados Unidos da América

Nos Estados Unidos, o atestado de óbito é chamado de Certificado de Óbito (*Death Certificate*). A gestão dos Certificados de Óbito nos Estados Unidos é feita nos estados pelos *Centers of Disease Control and Prevention* (CDC), centralizado no *National Center for Health Statistics* (NCHS), na cidade de Atlanta, estado da Geórgia.

<sup>1</sup>Disponível em: <<http://oglobo.globo.com/arquivos/pensando-vol1.pdf>>. Acesso em: 23 maio 2016.

A versão física norte-americana é em folha única, possui 53 campos, dos quais, somente os campos 24 a 50 são preenchidas pelo médico; e vem acompanhada de mais uma folha explicativa (UNITED STATES, 2003).

Os sistemas eletrônicos de certificado de óbito variam de acordo com o estado. Mas todos os modelos eletrônicos de declaração de óbito digital permitem o preenchimento *on-line* pelos médicos, interface amigável, acesso e colaboração entre as várias instituições envolvidas como agências públicas, funerárias e administradores de cemitérios, sistema de ajuda *on-line* e sistema *web* (HEIM, 2010). Como exemplo, o estado americano do Texas possui sistema digital de certificação de óbito denominado *Texas Eletronic Death Registration* (TEDR), totalmente efetivado desde setembro de 2007 (TEXAS, 2016).

O estado da Califórnia aprovou seu programa de registro eletrônico de óbitos em 2002. A elaboração do sistema durou 13 meses e foi implementado em fevereiro de 2005. O sistema tem cerca de cem mil linhas de comando, foi construído por uma equipe de sete programadores pelo custo foi de 1,98 milhões de dólares. O estado de Minnesota possui sistema eletrônico de registros desde 1997, tornando-se totalmente eletrônico desde 2011, pois o método em papel é mais complicado, sujeito a mais erros, atrasos e dificuldades para a transmissão de dados.

#### **b) França**

Na França, as informações sobre mortalidade estão centralizadas no Centro de Epidemiologia da França Para Causa Médica da Morte (*CépiDc-Inserm* em francês). A Declaração de Óbito é denominado "*certificats de décès*" em francês. Desde 2007, a França adota sistema totalmente eletrônico de registro de óbito. O sistema eletrônico francês de declaração de óbito denomina-se CertDc. O aplicativo CertDc está disponível no site: <https://sic.certdc.inserm.fr>. O CertDc- registra e estuda cerca de 540 mil óbitos por ano.

O Código Internacional de Doenças é inserido automaticamente pelo *software* Iris. O sistema permite alterações e correções nas primeiras 48 horas. Lefeuvre *et al.*(2014) relataram que o sistema eletrônico é de fácil uso, aplicável em todas situações necessárias e que reduziu erros e inconsistências nas informações.

#### **c) Portugal**

Portugal utiliza o Sistema de Informação dos Certificados de Óbito (SICO) desde 2012; administrado pela Direção Geral da Saúde (DGS) do Serviço Nacional de Saúde (SNS), vinculado ao Ministério da Saúde (PORTUGAL, 2013). O sistema

português é acessível pela Internet, possui área específica para médicos; basta cadastrar-se e entrar com nome de usuário e senha de acesso; é disponibilizado sistema de suporte 24 horas por dia *on-line* e por *helpdesk* (PORTUGAL, 2016). No *You Tube* também existe vídeo explicativo.

Silva (2015) fez um estudo comparativo de erros de preenchimento e de lacunas em branco entre o modelo físico em papel antes da implantação do SICO e com o SICO. Encontrou 177 erros/lacunas numa amostra de 136 DO em papel contra 13 erros/lacunas em 130 exemplares no SICO. Verificou que o preenchimento correto subiu de 35,29% em papel para mais de 93% com a informatização, o que evidencia o atraso tecnológico desta atividade burocrática; um erro de processo, não erro, má vontade ou falta de treinamento de quem é obrigado a executar o processo.

#### **d) Uruguai**

Ocorrem cerca de 33 mil óbitos no Uruguai anualmente, os quais são registrados eletronicamente desde 2007. O sistema faz parte das plataformas de Governo Eletrônico (PGE), que une todo o sistema governamental (URUGUAI, 2005).

Os usuários diretos do sistema são médicos, diretores técnicos e administradores de instituições de saúde e funerárias que devem se cadastrar no sistema por telefone ou correio eletrônico, criar senha e obter uma contrassenha. O sistema possui manual explicativo no site da Internet.

O sistema uruguaio possui nove (9) funcionalidades com acesso controlado conforme o tipo de usuário. Médicos, administradores e funerárias podem iniciar o preenchimento do certificado nos campos referentes à identificação do falecido, e completar ou corrigir esses campos.

## **4 BASES DE DADOS QUE PODEM VIR A INTEGRAR O SISTEMA DE DECLARAÇÃO DE ÓBITO**

### **a) Sistema Integrado de Segurança Pública do Estado de Santa Catarina (SISP)**

O SISP possui identificação completa e endereços de todas as pessoas que fizeram carteira de identidade no estado ou que tiveram algum registro de serviço público em Santa Catarina. Esses dados, quando completos, atendem a maior parte dos campos não médicos exigidos na Declaração de Óbito (SSP-SC, 2017).

Esse sistema é gerenciado pelo Centro de Informática e Automação do Estado de Santa Catarina (CIASC); administra o registro da ocorrência policial; permite consultar pessoas e veículos por agentes de segurança pública e da justiça. Comunicada morte violenta, registra-se Boletim de Ocorrência (BO) para iniciar a investigação policial e encaminhar o corpo ao IML.

O número do BO é exigido no campo 50 do Bloco VIII da DO. A inserção desse número num sistema digital poderia ativar o preenchimento automático dos campos de identificação e endereço do falecido. Outros estados possuem sistemas próprios de identificação de seus cidadãos e de gerenciamento de ocorrências policiais que podem ser integrados da mesma forma.

**b) Código de Endereçamento Postal (CEP)**

O CEP é um conjunto de códigos numéricos de municípios e ruas criado pela Empresa Brasileira de Correios e Telégrafos (EBCT). O seu Diretório Nacional de Endereços (e-DNE) possui mais de 900 mil endereços e está disponível para uso, mediante pagamento (EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS, 2018).

O CEP serve para identificar e preencher os campos relativos ao endereço da vítima e do local do fato na DO; é exigido nos campos 16 e 23. Nos campos 17 e 24 pede-se o código do bairro. E nos campos 18 e 25, os códigos do município de residência e de ocorrência respectivamente.

**c) Código Brasileiro De Ocupações (CBO)**

O Código Brasileiro De Ocupações (CBO) é uma exigência que consta na DO no campo relativo ao código de ocupação do falecido, item quatorze (14) do Bloco I, da Identificação; e no campo 29 que trata da ocupação da mãe quando houver morte fetal ou de menor de um ano.

**d) Serviço Federal de Processamento de Dados (SERPRO)**

O Serviço Federal de Processamento de Dados (SERPRO) mantém bancos de dados das áreas tributária, financeira, contábil, orçamentária e de gestão de governo por meio de sistemas como Sistema Integrado de Administração Financeira (SIAFI), Receitanet, Siscomex, Sistema Nacional de Cadastro Rural (SNCR-Web) e Registro Nacional de Veículos Automotores (RENAVAM).

O SERPRO desenvolveu e opera o Sistema de Informações do Departamento Penitenciário Nacional (SISDEPEN) desde início de 2017; manteve convênio com a Universidade Federal de Santa Catarina para desenvolver Sistema de Certificação

Digital do SERPRO (SCDS). O SDCS é uma identidade eletrônica expedida por uma Autoridade Certificadora para assegurar confidencialidade, integridade das informações e confirmação de autoria; é particularmente útil para permitir transmissão segura da declaração de óbito digital.

**e) Sistemas do Ministério da Saúde**

O Ministério da Saúde possui vários sistemas administrativos que não são usados de forma integrada, não permitindo a exploração e utilização plena de suas funcionalidades. A integração de sistemas como o Sistema de Gerenciamento da Tabela Unificada de Procedimentos, Medicamentos, Órteses, Próteses e Materiais Especiais do SUS (SIGTAP), a Classificação Internacional de Doenças e Problemas Relacionados à Saúde (CID-10), Cadastramento Único de Saúde (CadSUS), Cartão Nacional de Saúde (CNS), Cadastro Nacional de Estabelecimentos de Saúde (CNES), Sistema de Informações de Nascido Vivo - SINASC - e o Sistema de Informações em Mortalidade (SIM) possibilitaria preenchimento rápido e correto da DO e sua comunicação instantânea.

**f) Sistema Nacional de Registro Civil (SIRC)**

Em 2014, o governo federal instituiu o Sistema Nacional de Informações de Registro Civil (SIRC) com o objetivo de estruturar e unificar o sistema brasileiro de registro civil é um sistema de cartório digital.

As atividades da SIRC são captar, processar, arquivar e disponibilizar dados relativos a registros de nascimento, casamento, óbito e natimorto, produzidos pelas serventias de registro civil das pessoas naturais (BRASIL, 2014).

As plataforma e módulos do SIRC utilizam a Internet para a inserção e transmissão de dados relativos aos registros de nascimento, casamento, óbito e natimorto. A integração do SIRC ao sistema de DO permitiria envio instantâneo de informações do falecido ao cartório de registro civil.

## **5 PROTOTIPAÇÃO DE SISTEMA INTEGRADO DE DECLARAÇÃO DE ÓBITO BRASILEIRA (SisDIDO)**

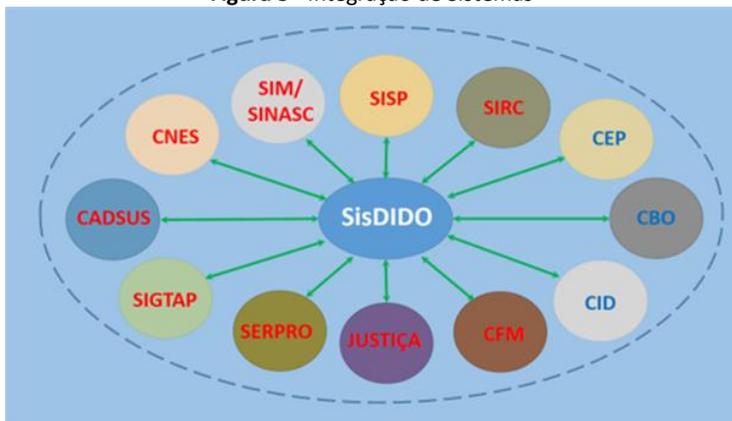
A maneira mais fácil, econômica e rápida de se criar um Sistema Integrado de Declaração de Óbito, aqui denominado SisDIDO, é integrar as diferentes plataformas de codificações e de banco de dados vistos acima.

O gerenciamento desse sistema poderia ser feito pela Fundação Nacional de Saúde (FUNASA) do Ministério da Saúde, como já ocorre com o SIM, podendo estar integrado ao próprio SIM. Mas nada impede que se faça por outro órgão federal ou mesmo estar pulverizado por órgãos estaduais assim como acontece atualmente com o sistema Registro Nacional de Veículos Automotores (RENAVAM).

Por meio da tecnologia de banco de dados relacionais é possível integrar estas plataformas. Esse tipo de banco de dados faz uso de um conjunto de tabelas para representar os dados e as relações entre os mesmos. O modelo relacional utiliza linguagem de definição de dados (*Data Definition Language* - DDL) que é um conjunto de definições expresso por uma linguagem especial para definir e armazenar dados (SILBERSCHATZ, KORTH e SUDARSHAN ,2006, p.7).

Algumas informações adicionais como os dados do médico poderiam ser importadas de plataforma como CNES ou pelo site do Conselho Federal de Medicina (CFM) conforme figura abaixo (Figura 3).

**Figura 3 - Integração de Sistemas**



**Fonte:** Elaborado pelo autor.

O SisDiDo deve contemplar requisitos funcionais como a possibilidade de solicitar, importar e incorporar dados do SISP, CEP, CID, CADSUS, CNES, CBO e SIGTAP; capacidade de transmitir automaticamente os dados e cópia eletrônica para o SISP, SIM, DATAPREV e SIRC; possibilidade de inserir alterações e correções; ser capaz de identificar inconsistências e erros críticos, principalmente na sequência da causa da morte; e ser capaz de gerar estatísticas e relatórios.

Os requisitos não funcionais que o SisDIDO deve possuir são: ser um sistema *web* ajustável a qualquer plataforma, com possibilidade de acesso pela Internet; em locais de difícil acesso ou com limitação grave de telecomunicação, são desejáveis terminais fixos ou portáteis que funcionem *off-line*; conter restrições de acesso a somente pessoas autorizadas para garantir a privacidade e segurança das informações; o cadastro médico no sistema deve ser facilitado; abranger as necessidades de dados e informações solicitadas no SIM; serem sistemas gráficos amigáveis, de fácil manuseio; com explicações e páginas de ajuda, telefones e *e-mails* de contato disponíveis 24 horas por dia; ser confiável e seguro com transmissão criptografada ponto a ponto.

Um gráfico demonstrativo de fatores críticos como questões políticas, econômicas e tecnológicas a serem superadas para viabilizar o SisDIDO é apresentado abaixo (Figura 4). É necessário reunir com os órgãos detentores destas codificações e, mediante negociação, cooperação, convênios ou compras destas plataformas, obter seus códigos de acesso e autorização para inseri-los na DO.

**Figura 4** - Fatores críticos para a implementação do SisDIDO



**Fonte:** Adaptado de *ElectronicDeathReporting System Online Reference Manual*<sup>2</sup>.

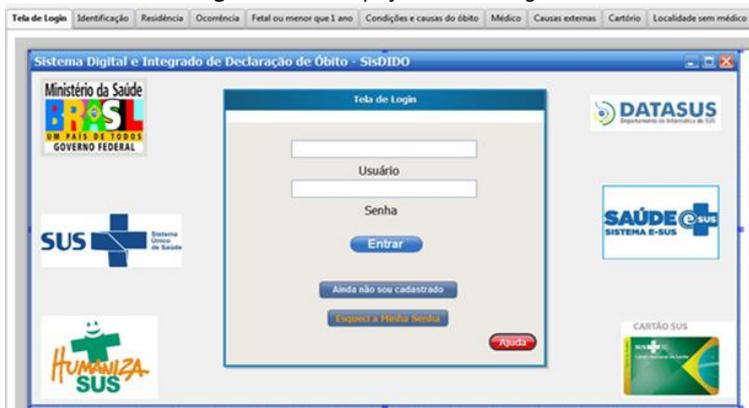
Nas figuras abaixo foram sugeridas prototipação de algumas telas do SisDIDO, mantendo-se a ordem dos blocos e campos da Declaração de Óbito em papel.

Na prototipação da Tela de Login (Figura 5), um novo usuário poderá cadastrar-se no sistema e ter acesso. O sistema localiza e confere se o usuário está

<sup>2</sup> Disponível em: <<https://www.cdc.gov/nchs/data/dvs/edrs-online-reference-manual.pdf>>. Acesso em 03 abr. 2017.

Proposta de um sistema integrado de declaração de óbito com cadastro regular no Conselho Federal de Medicina, verifica e registra o endereço IP de acesso em subnível invisível ao usuário.

**Figura 5 - Prototipação Tela do Login.**



A screenshot of a web application titled "Sistema Digital e Integrado de Declaração de Óbito - SisDIDO". The interface features a central "Tela de Login" with input fields for "Usuário" and "Senha", and buttons for "Entrar", "Ainda não sou cadastrado", and "Esqueci a Minha Senha". The page is decorated with logos for the "Ministério da Saúde", "BRASIL GOVERNO FEDERAL", "DATASUS", "SUS", "SAÚDE SISTEMA S-SUS", and "Humaniza SUS". A navigation bar at the top includes links for "Tela de Login", "Identificação", "Residência", "Ocorrência", "Fetal ou menor que 1 ano", "Condições e causas do óbito", "Médico", "Causas externas", "Cartório", and "Localidade sem médico".

**Fonte:** Elaborado pelo autor na plataforma Pencil.

Na prototipação da Tela de Identificação (Figura 6), digitando-se o nome do falecido, o sistema localiza e insere os demais dados, facilitando a atividade do médico que apenas fica obrigado a conferir e ratificá-los ou colocar algum outro. O médico precisa apenas digitar a data e hora do óbito e o tipo de óbito.

**Figura 6 - Prototipação da Tela de Identificação**



A screenshot of the "I - Identificação" screen in the SisDIDO system. The main heading is "Declaração de Óbito". It includes a "Número da Declaração" field. The form contains several input fields and dropdown menus: "Tipo de Óbito" (radio buttons for "Morte Fetal" and "Nascido Vivo"), "Data do Óbito", "Hora do Óbito", "Naturalidade", "Cartão SUS", "Nome do Falecido (a)", "Pai", "Mãe", "Data de Nascimento", "Idade", "Sexo", "Raça/Cor", "Estado Civil", "Escolaridade", and "Ocupação Habitual - CBO". At the bottom, there are buttons for "Salvar", "Voltar", "Sair", and "Ajuda".

**Fonte:** Elaborado pelo autor na plataforma Pencil.

A Figura sete (7) mostra a prototipação do bloco V: Condições e causas do óbito. As codificações do CID podem ser inseridas diretamente no campo correspondente ou por meio de consulta ao sistema como inserção de causas nos campos “a”, “b”, “c” e “d”.

**Figura 7 - Prototipação Condições e causas do óbito**

V - Condições e causas do óbito

Morte ocorreu:  Assistência médica:  Necrópsia?

CAUSAS DA MORTE  
Doença ou estado mórbido que causou diretamente a morte.

a)  Tempo  CID

CAUSAS ANTECEDENTES  
Devido ou como consequência de:

b)  Tempo  CID

Devido ou como consequência de:

c)  Tempo  CID

Devido ou como consequência de:

d)  Tempo  CID

Outras condições significativas

Tempo  CID

Outras condições significativas

Tempo  CID

Salvar Voltar Sair Ajuda

**Fonte:** Elaborado pelo autor na plataforma Pencil.

## 6 ANÁLISE CRÍTICA

Depreende-se, deste estudo, embasado nas fontes bibliográficas referenciadas, algumas críticas sobre a Declaração de Óbito conforme elencado abaixo:

- a) A causa da morte descrita na DO é um importante material para estudos epidemiológicos e estatísticos, mas carece de confiabilidade devido às inconsistências, falhas e erros de preenchimento.
- b) Este estudo demonstrou que há atraso tecnológico na DO em papel e que esse atraso é o principal fator responsável pelas dificuldades e inconsistências de dados nela contidos.
- c) Verifica-se que os dados exigidos nos diversos campos da DO encontram-se nas plataformas eletrônicas dos vários órgãos, mas que não se comunicam, que não são integrados nem são disponibilizados ao médico para uso no preenchimento da mesma.
- d) Análise de resultados de antes e após a implantação de sistemas digitais em outros países comprovaram melhora na qualidade, rapidez e

- confiabilidade das informações coletadas e que estes sistemas são fáceis e seguros de serem utilizados.
- e) Os diversos modelos internacionais de atestado de óbito digital em funcionamento citados neste trabalho comprovam que é possível criar um Sistema Integrado de Declaração de Óbito nacional.
  - f) Sistema de declaração de óbito integrado permitirá a desmaterialização da DO, agilizando, melhorando e diminuindo os processos com economia de estrutura física, diminuição de inconsistências, erros, etapas e custos, facilitando vida dos médicos, familiares e gestores.
  - g) A integração da base de dados não somente é viável, mas necessária para melhorar a gestão pública, a qualidade e segurança das informações em casos de morte violenta.

Por fim, verifica-se que é possível criar um sistema de DO nacional confiável, prático e seguro de forma mais rápida e barata convergindo e integrando várias bases de dados brasileiros já existentes.

## **7 CONSIDERAÇÕES FINAIS**

Este artigo científico fez uma descrição da Declaração de Óbito brasileira, a sua importância na Administração em especial para a segurança pública, a forma como é feita atualmente com suas dificuldades, vantagens e desvantagens.

O presente trabalho citou exemplos de sistemas eletrônicos de declaração de óbito em uso em diversos países com integração com demais sistemas governamentais e suas vantagens.

O artigo descreveu a possibilidade de construção de um sistema nacional de declaração de óbito digital por meio da integração de sistemas já existentes. Verifica-se que há necessidade de trabalhos de conscientização e de diálogos e negociações com os diferentes personagens envolvidos.

Conclui-se que um sistema digital de declaração de óbito brasileiro é possível e necessário como instrumento de melhora e agilização de processos administrativos.

## REFERÊNCIAS

BRASIL Decreto nº 8.270/14 de 27 de junho de 2014. Institui o sistema nacional de informações de registro civil - Sirc e seu comitê gestor, e dá outras providências. 2014a. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2014/Decreto/D8270.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Decreto/D8270.htm)>. Acesso em: 03 mar. 2017.

SÃO PAULO. Secretaria Municipal de Saúde. Programa de Aprimoramento das Informações de Mortalidade – PRO-AIM. Orientações para o preenchimento da declaração de óbito para causas naturais. Abr. 2014. Disponível em: <<http://www.prefeitura.sp.gov.br/cidade/secretarias/upload/saude/arquivos/proaim/Aula-Preenchimento-v2.pdf>>. Acesso em: 24 maio 2016.

BORGES, Dorian et al. 2013. “Mortes Violentas no Brasil: Uma Análise do Fluxo de Informações”, In: FIGUEIREDO, Isabel Seixas de & NEME, Cristina; LIRA, Cristiane do Socorro Loureiro. Homicídios no Brasil: Registro e Fluxo de Informações. Brasília: Ministério da Justiça, Secretaria Nacional de Segurança Pública (SENASP), (Coleção Pensando a Segurança Pública, vol. 01). Disponível em: <<http://oglobo.globo.com/arquivos/pensando-vol1.pdf>>. Acesso em: 23 maio 2016.

SILVA, José Eduardo Ferreira da. Certificação do óbito – avaliação dos procedimentos legais. Universidade de Coimbra. Portugal. 2015. Disponível em: <<https://estudogeral.sib.uc.pt/jspui/bitstream/10316/30806/1/CERTIFICA%C3%87%C3%83O-DO-%C3%93BITO-AVALIA%C3%87%C3%83O-DOS-PROCEDIMENTOS-LEGAIS-FMUC-2015-JOS%C3%89-EDUARDO-FERREIRA-DA-SILVA.pdf>>. Acesso em: 13 dez. 2016.

UNITED STATES. Department of Health and Human Services. Public Health Services. National Center for Health Statistics. Revised 11/2003. U.S. standard certificate of death. Disponível em: <<http://www.cdc.gov/nchs/data/dvs/DEATH11-03final-ACC.pdf>>. Acesso em: 21 nov. 2016.

HEIM, Rose Trasatti. Electronic death registration. Project manager. National association for public health statistics and information systems. National conference on health statistics. Ago. 2010. Disponível em: <[https://www.cdc.gov/nchs/ppt/nchs2010/26\\_trasatti.pdf](https://www.cdc.gov/nchs/ppt/nchs2010/26_trasatti.pdf)>. Acesso em: 06 maio 2016.

TEXAS. Texas Electronic Registrar - Deathregistration. Disponível em: <<https://dshs.texas.gov/vs/edeath/>>. Acesso em: 14 dez. 2016.

LEFEUVRE, Delphine et al. Quality comparison of electronic versus paper death certificates in France, 2010. Population Health Metrics. v. 12, n. 3, 2014. Disponível

em: <<http://pophealthmetrics.biomedcentral.com/articles/10.1186/1478-7954-12-3>>. Acesso em: 01 jul. 2016.

PORTUGAL. Ministério da Saúde. Serviço Nacional de Saúde. SICO - Sistema de informação dos certificados de óbito. 12 de outubro de 2013. Disponível em: <<http://spms.min-saude.pt/2013/10/sico-sistema-de-informacao-dos-certificados-de-obito/>>. Acesso em: 13 dez. 2016.

\_\_\_\_\_. Ministério da Saúde. Direção Geral da Saúde. SICO - Sistema de informação dos certificados de óbito. Disponível em: <<https://www.dgs.pt/paginas-de-sistema/saude-de-a-a-z/sico-sistema-de-informacao-dos-certificados-de-obito/perguntas-frequentes.aspx#a2>>. Acesso em: 13 dez. 2016.

URUGUAI. Agência para o desenvolvimento do governo de gestão electrónica e sociedade de informação e conhecimento – AGESIC. Artículo 72 de la Ley N° 17.930, de 19 de diciembre de 2005. Disponível em: <<http://www.agesic.gub.uy/innovaportal/v/286/1/agesic/articulo-72-de-la-ley-n%C2%B0-17930-de-19-de-diciembre-de-2005.html>>. Acesso em: 15 dez. 2016.

SECRETARIA DA SEGURANÇA PÚBLICA DO ESTADO DE SANTA CATARINA – SSP-SC. SSP e MPSC firmam convênio para ter acesso às informações do SISP e do SIG. Disponível em: <[http://www.ssp.sc.gov.br/index.php?option=com\\_content&view=article&id=1111:ssp-e-mpsc-firmam-convenio-para-ter-acesso-as-informacoes-do-sisp-e-do-sig&catid=94:novas-noticias-1&Itemid=154](http://www.ssp.sc.gov.br/index.php?option=com_content&view=article&id=1111:ssp-e-mpsc-firmam-convenio-para-ter-acesso-as-informacoes-do-sisp-e-do-sig&catid=94:novas-noticias-1&Itemid=154)>. Acesso em: 04 mar. 2017.

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS – Correios. CEP - Código de endereçamento postal. Disponível em: <<https://www.correios.com.br/para-voce/correios-de-a-a-z/cep-codigo-de-enderecamento-postal>>. Acesso em: 16 jun. 2016.

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - Correios. e-DNE. Disponível em: <<https://www.correios.com.br/Para-governo/demais-orgaos-publicos/solucoes-em-marketing/e-dne>>. Acesso em: 16 fev. 2018.

SILBERSCHATZ, Abraham; KORTH, Henry F.; SUDARSHAN, S. Sistema de banco de dados. Tradução de Daniel Vieira. Revisão técnica de Luiz Fernando Pereira de Souza. 6. ed. Rio de Janeiro: Editora campus, 2006. 781 p.

NATIONAL CENTER FOR HEALTH STATISTICS. Centers for Disease Control and Prevention. Electronic Death Reporting System Online Reference Manual. Disponível em: <<https://www.cdc.gov/nchs/data/dvs/edrs-online-reference-manual.pdf>>. Acesso em 03 abr. 2017.

## UM MODELO DE DADOS VOLTADO AO TREINAMENTO E À FORMAÇÃO POLICIAL

*Ronnie Carlos Tavares Nunes  
Alexandre Leopoldo Gonçalves*

### 1 INTRODUÇÃO

Segundo Rolim (2009), houve um aumento das pesquisas na área de segurança pública voltadas à prevenção do crime nos últimos 30 anos, sobretudo nos países de língua inglesa, realizadas por órgão governamentais, universidades e instituições mantidas com recursos privados. Entretanto, as pesquisas na área de formação e treinamento dos policiais não tiveram o mesmo incremento.

De modo geral, as academias de polícias procuram promover a identidade profissional do futuro policial por meio do compartilhamento de habilidades e atitudes que são pedagogicamente elencadas para compor o treinamento, de acordo com os valores da instituição e normas legais aplicáveis, promovendo a seleção de matérias e conteúdos específicos para o desempenho da atividade policial. Esse modelo reflete a junção do tradicional modelo de burocratização com a militarização, no qual o comportamento profissional deve ser respaldado pela aplicação da lei, tornando os policiais aplicadores imparciais da lei, promovendo a disciplina do efetivo e da menor discricionariedade durante a atuação (PONCIONI, 2007).

O modelo pedagógico adotado nas instituições é alvo frequente de análises que aconselham a adoção de um novo modelo de construção do perfil profissional, que seja capaz de superar o padrão militarizado, hierárquico e reativo de combate ao crime, focando na formação de uma polícia comunitária, que observa os princípios da dignidade da pessoa humana e aos direitos humanos (CERQUEIRA, 2006; SANTOS, 2012). A valorização da formação acadêmica e da capacitação continuada ainda é apontada como uma necessidade premente (LUIZ, 2008; CERQUEIRA, 2011).

As academias de polícia, atuando como órgão de formação e capacitação, devem estar preparadas para transmitir normas procedimentais e comportamentais de acordo com esses novos valores e saberes, por meio dos programas pedagógicos voltados à formação dos policiais e do uso adequado de ferramentas tecnológicas para apoiar tal finalidade.

Alguns trabalhos acadêmicos buscaram realizar uma análise crítica do conteúdo programático dos cursos de formação dos profissionais de segurança pública. Baraldi (2012) analisou criticamente o conteúdo programático do curso de formação para Delegado de Polícia Civil do Estado de São Paulo e ressaltou a ausência de conteúdo ligado a Direitos Humanos. Além disso, também foi notada a ausência de um curso com disciplinas básicas policiais para todos e, a partir daí, cursos especializados para cada uma das áreas.

A instituição analisada para a proposição do modelo, a Polícia Rodoviária Federal (PRF), foi criada pelo presidente Washington Luiz no dia 24 de julho de 1928 (dia da Polícia Rodoviária Federal), com a denominação inicial de “Polícia de Estradas” (POLÍCIA RODOVIÁRIA FEDERAL, 2017). Em 1935, Antônio Félix Filho, o “Turquinho”, considerado o 1º Patrulheiro Rodoviário Federal, foi chamado para organizar a vigilância das rodovias Rio-Petrópolis, Rio-São Paulo e União Indústria. Sua missão era percorrer e fiscalizar as três rodovias utilizando duas motocicletas Harley Davidson® e nessa empreitada contava com a ajuda de cerca de 450 vigias da então Comissão de Estradas de Rodagem (CER). Em 23 de julho de 1935 (dia do Policial Rodoviário Federal), foi criado o primeiro quadro de policiais da hoje Polícia Rodoviária Federal, denominados, à época, “Inspetores de Tráfego”.

No ano de 1945, já com a denominação de Polícia Rodoviária Federal, a corporação foi vinculada ao extinto Departamento Nacional de Estradas de Rodagem (DNER). Finalmente, em 1988, com o advento da Constituinte, a Polícia Rodoviária Federal foi integrada ao Sistema Nacional de Segurança Pública, recebendo como missão exercer o patrulhamento ostensivo das rodovias federais. Desde 1991, a Polícia Rodoviária Federal integra a estrutura organizacional do Ministério da Justiça e Segurança Pública, como Departamento de Polícia Rodoviária Federal (POLÍCIA RODOVIÁRIA FEDERAL, 2017).

Apesar de existirem procedimentos formais em relação à formação e treinamento policial, observa-se que não existem sistemas de informação que possibilitem subsidiar a administração com dados reais e precisos das atividades executadas. Apesar dos documentos serem produzidos e armazenados no sistema de protocolo eletrônico, esse sistema revela-se um meio inadequado para produzir

relatórios suficientemente claros e voltados ao processo de melhoramento contínuo das atividades desenvolvidas.

Além disso, importantes informações acerca da atividade ficam descentralizados por diversos departamentos, resultando numa gama de informações desorganizadas e não otimizadas para pesquisa. A falta de um banco de dados estruturado e desenvolvido especificamente para as atividades de formação e treinamento na PRF dificulta a obtenção de qualquer informação gerencial referente às atividades já realizadas. Nesse sentido, este trabalho tem como objetivo propor e desenvolver um modelo de dados que ofereça suporte à gestão das informações sobre a realização e acompanhamento de atividades de formação e treinamento desenvolvidas na PRF.

## **2 FUNDAMENTAÇÃO TEÓRICA**

Os bancos de dados podem ser classificados de acordo com o modelo em que se baseiam. Nesse sentido, pode-se classificá-los em bancos de dados hierárquicos, em rede, relacionais ou orientados a objetos (ELMASRI; NAVATHE, 2005). Os bancos de dados hierárquicos foram os primeiros a serem desenvolvidos, logo após a consolidação dos discos endereçáveis. Usavam esse endereço em sua estrutura e se caracterizam por utilizar o conceito de registro e de relacionamento pai-filho.

Com a evolução, surgem os bancos de dados relacionais, caracterizados pela organização dos dados em tabelas com linhas e colunas, sendo que cada tabela representa um mesmo tema. Baseiam-se em conceitos oriundos da teoria dos conjuntos e da álgebra relacional (SILBERSCHATZ; KORTH; SUDARSHAN, 2006), sendo largamente empregados nos mais variados cenários de aplicação.

### **2.1 Conceito de Banco de Dados Relacional**

O conceito fundamental do modelo relacional é que os dados são separados em partes menores ou subtipos de dados, em uma estrutura tabular, ou seja, em tabelas. Cada grupo de dados é mantido em sua própria tabela (SILBERSCHATZ; KORTH; SUDARSHAN, 2006). Desta forma, conjuntos de dados são organizados em linhas (comumente chamadas de tuplas) e colunas, de forma que cada tabela se refira a um determinado tema (Tabela 1).

**Tabela 1** – Exemplo de uma estrutura tabular.

Id_Aluno	Nome	Id_Disciplina
A1	João	D1
A2	Maria	D2
A3	José	D3
A4	Pedro	D4

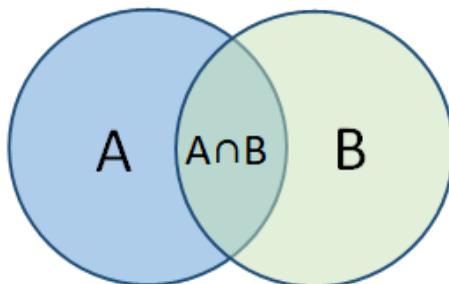
**Fonte:** Elaborado pelos Autores.

Nessa representação, uma única tabela se refere a menor parte lógica de um conjunto de dados. Cada coluna da tabela deve representar uma única categoria de informação e cada linha (ou tupla), por sua vez, deve representar uma única instância daquela informação. A ordem das colunas ou linhas não deve ser importante. Isso permite que o gerenciador de banco de dados traga as informações da forma mais rápida possível.

Um benefício dessa abordagem e forma de organização dos dados é permitir a utilização da teoria dos conjuntos e da álgebra relacional como métodos para se extrair informações. O estudo da teoria dos conjuntos foi iniciado por Georg Cantor e Richard Dedekind em 1870. Os sistemas de axiomas foram propostos no início do século XX, sendo um dos mais conhecidos o axioma de Zermelo-Fraenkel (JECH, 2003).

Assim como a aritmética caracteriza operações binárias sobre números, a teoria dos conjuntos caracteriza operações binárias sobre conjuntos, dentre elas, a união, a interseção, a diferença de conjuntos, a diferença simétrica, o produto cartesiano e o conjunto das partes (Figura 1).

**Figura 1** – Diagrama de Venn.



**Fonte:** Elaborado pelos Autores.

O modelo relacional, utilizando a álgebra relacional, é capaz de unir subconjuntos de dados, constantes em diversas tabelas, de forma extremamente rápida, apresentando-os ao usuário de forma matematicamente otimizada. Por isso, os bancos de dados relacionais são considerados um dos mais rápidos para se manipular e recombinar dados armazenados de forma tabular.

Segundo Darwen (2012), as complexas estruturas que são utilizadas para guardar dados que são visíveis em sistemas não relacionais não são visualizadas nos bancos de dados relacionais. Segundo Teorey *et al.* (2014), um Sistema Gerenciador de Banco de Dados (SGBD) é um sistema de *software* genérico para manipular bancos de dados, admitindo uma visão lógica (esquema, subesquema); visão física (métodos de acesso, agrupamento de dados); linguagem de definição de dados; linguagem de manipulação de dados; e utilitários importantes, como gerenciamento de transação, controle de concorrência, integridade de dados, recuperação de falhas e controle de segurança.

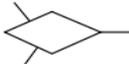
## 2.2 Banco de Dados Relacional – Representação Gráfica

Existem diversos tipos de representações utilizadas na literatura relacional, sendo algumas abordadas em livros e outras utilizadas em ferramentas CASE (*Computer Aided Software Engineering*). Todas elas realizam a modelagem de dados para descrever e definir um processo de negócio, convertendo-os em entidades, atributos e os relacionamentos entre eles.

Os dez métodos de representação comumente encontrados na literatura são: Chen; Teorey; Elmasri&Navathe; Korth&Silberschatz; McFadden &Hoffer; Batini, Ceri&Navathe; *Oracle® CASE Methods; InformationEngineering*; IDEF1X utilizado no ERWin®; e Bachman.

Segundo Song, Evans e Park (1995), muitas variações de notações de Diagramas de Entidade Relacionamentos foram desenvolvidas. Algumas notações permitem relacionamentos *n*-ários enquanto outras não. Algumas notações permitem que os atributos sejam modelados já no relacionamento. Outras representam as constantes de cardinalidade e a participação separadamente. Uma das mais comumente referenciadas na literatura é a representação de Peter Chen (Figura 2).

Figura 2 – Notação de Peter Chen.

Conceito	Símbolo
Entidade	
Relacionamento	
Atributo	
Atributo identificador	 
Relacionamento identificador	
Generalização/especialização	
Entidade associativa	

Fonte: Heuser (2009).

## 2.3 A Linguagem SQL

O desenvolvimento da linguagem SQL, que é composta por comandos de definição, manipulação e controle de dados, utilizada pelos SGBDs remonta aos estudos de Boyce e Chamberlin (2012) no laboratório de pesquisas da IBM® em San José, realizada em 1973, quando se juntaram ao projeto *System R*. O resultado foi chamado de *Sequel (StructuredEnglishLanguage)* (WADE, 2012). Desde o início, a intenção era que a linguagem *Sequel* fosse utilizada para manipulação e para definição de dados. Na prática, a linguagem foi dividida em três grupos principais. A primeira é a linguagem de manipulação de dados – DML (*Data ManipulationLanguage*), utilizada para operações de pesquisa, inserção, deleção e atualização, enquanto a linguagem de definição de dados – DDL (*Data DefinitionLanguage*), é utilizada para a criação de tabelas, visões e declarações. Já a linguagem de controle de dados – DCL (*Data ControlLanguage*) controla privilégios de acesso aos objetos do banco de dados e privilégios administrativos de sistema. Na SQL, quem define qual caminho percorrer durante o acesso é o SGBD e não o desenvolvedor (HEUSER, 2009).

### **3 MODELO PROPOSTO**

Para a análise e proposição do modelo foi considerado o evento realizado pela PRF no ano de 2016. Nesse evento foram matriculados 799 alunos, sendo distribuídos em 24 turmas, divididas em três núcleos: Alpha, Bravo e Charlie, cada qual com 08 (oito) turmas. O curso teve a duração de 96 dias, sendo 75 dias letivos, com uma carga horária de 740 h/a, distribuídas em 32 disciplinas nas seguintes áreas: Prática de Atividade Policial, Conhecimentos Gerais do Policial, Ciências Humanas da Atividade Policial, Conhecimentos Específicos do Policial e palestras com ênfase na atividade policial. As atividades ocorreram entre os dias 16 de fevereiro de 2016 e 18 de maio de 2016. No dia 20 de maio de 2016 ocorreu a formatura, com a presença do então Ministro de Estado da Justiça e Cidadania, Alexandre de Moraes.

#### **3.1 Modelagem**

A modelagem é um processo estruturado que envolve o entendimento da definição de modelo. Um modelo, segundo Cougo (1997) é a representação abstrata e simplificada de sistemas do mundo real. Esta abordagem está desacoplada das especificações tecnológicas da futura solução, já que trabalha em um nível de abstração. É o que chamamos de Diagrama de Entidade e Relacionamento (DER).

A fim de se balizar o processo de modelagem, foram utilizadas perguntas de competência (Tabela 2). Segundo Uschold (1996), a utilização de cenários como base para se definir perguntas de competência é uma estratégia mais elaborada e minuciosa. Nesse sentido, se um modelo ou uma ontologia (representação de determinado domínio de problema) conseguir responder a todas as perguntas, seu objetivo final é atingido. As ontologias consistem em um vocabulário com especificações do significado ou semântica da terminologia (FOX; GRUNINGER, 1998).

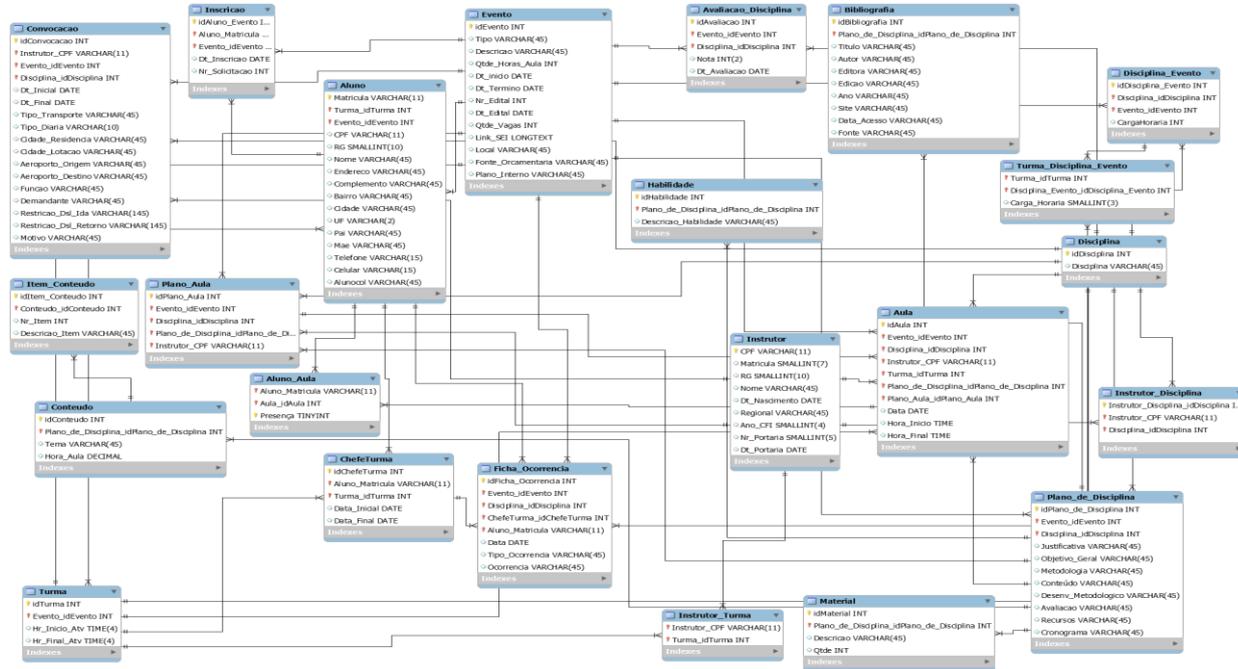
**Tabela 2** – Perguntas de competência utilizadas para nortear o modelo.

<u>Pergunta</u>	<u>Sigla</u>	<u>EntidadeEstabelecida</u>
Quais e quantos alunos estão participando do evento?	P1	Aluno, Evento
Quais os tipos de ocorrências mais frequentes registradas pelos chefes de turma?	P2	Ficha_Ocorrencia
Quais alunos não compareceram às aulas das disciplinas?	P3	Aluno_Aula
Qual o horário das aulas da turma?	P4	Aula, Turma
Quem são os instrutores da turma?	P5	Instrutor
Em qual turma o aluno está matriculado?	P6	Aluno, Turma
Quais os eventos em que o instrutor atuou?	P7	Convocação, Evento, Aula
Qual o total de horas-aula ministrada pelo instrutor?	P8	Aula
Quem são os instrutores de determinada disciplina?	P9	Instrutor_Disciplina
Quais instrutores estão aptos a ministrar disciplinas sem a necessidade de atualização pedagógica?	P10	Aula, Instrutor
Quais instrutores foram convocados para determinado evento de formação ou capacitação e quais os períodos?	P11	Convocação
Qual plano de aula determinado instrutor utilizou para ministrar sua aula?	P12	Plano_Aula
Quais são os horários de aula de cada instrutor em determinada turma?	P13	Aula
Quais as disciplinas de determinado evento?	P14	Evento_Disciplina
Qual a quantidade de horas-aulas de cada disciplina no evento?	P15	Disciplina_Evento
Quais são os materiais necessários para que cada instrutor possa ministrar a aula da disciplina?	P16	Material
Qual o Plano de Disciplina para cada evento?	P17	Plano_Disciplina

**Fonte:** Elaborado pelos Autores.

No intuito de se responder às perguntas de forma que a informação possa ser recuperada com confiabilidade, integridade, disponibilidade e segurança, o modelo apresentado na Figura 3 foi proposto.

Figura 3 – Modelo de Entidade e Relacionamento proposto.



Fonte: Elaborado pelos Autores

As chaves primárias das entidades estão precedidas do símbolo amarelo e as chaves estrangeiras são precedidas do símbolo na cor laranja. Cada tabela serve à finalidade de responder uma pergunta de competência. As principais tabelas são discutidas, a seguir, assim como, algumas das questões de competência.

A tabela “Aluno” é uma das principais do modelo e serve à finalidade de responder às seguintes perguntas de competência: P1 “Quais e quantos alunos estão participando do evento?” e P6 “Em qual turma o aluno está matriculado?”. Para consolidar as informações referentes à pergunta de competência P2 “Quais os tipos de ocorrências mais frequentes registradas pelos chefes de turma?”, utiliza-se a tabela “Ficha Ocorrência”.

Para se responder à pergunta P4 “Qual o horário das aulas da turma?” é utilizada a entidade “Aula”, na qual todos os dados podem ser obtidos. Para a resolução da pergunta P7 “Quais os eventos em que o instrutor atuou?”, utiliza-se a tabela “Evento” relacionada com a entidade “Convocação”.

A pergunta P11 questiona “Quais instrutores foram convocados para determinado evento de formação ou capacitação e quais os períodos?” A tabela “Convocação” deve ser analisada para a extração dessa informação. Por fim, a informação para consolidação da pergunta P13 “Quais são os horários de aula de cada instrutor em determinada turma?” pode ser extraída a partir da tabela “Aula”, pois ela contém os dados da disciplina, do instrutor e da turma na qual a aula foi ministrada.

### **3.2 Discussão e Exemplos de Consultas**

Utilizando o modelo proposto em função das perguntas de competência, o banco de dados foi povoado visando permitir a extração de algumas consultas que objetivam apresentar as informações julgadas pertinentes. Para essa tarefa, vários caminhos podem ser seguidos, desde a utilização de ferramentas existentes, como o desenvolvimento de novas aplicações para apresentação dos relatórios. Aqui, optou-se por utilizar o banco de dados *Microsoft Access*® para geração das consultas e confecção de relatórios. Esse banco de dados é de fácil manuseio e apresenta diversos “*wizards*” simplificando a criação de consultas e a confecção de relatórios.

Optou-se, neste trabalho, pela criação de consultas que retornem todos os dados que devem estar presentes no relatório. Assim, a consulta que apresenta os dados necessários para exibição do relatório referente à pergunta P2 consta na Tabela 3, juntamente com o relatório presente na Figura 4.

**Tabela 3** – Consulta para geração do relatório referente à P2.

```
SELECT [evento].[Descrição], [disciplina].[Disciplina], [ficha_ocorrencia].[Tipo_Ocorrencia],  
[evento].[idEvento] FROM evento INNER JOIN (disciplina INNER JOIN ficha_ocorrencia ON  
[disciplina].[idDisciplina] =[ficha_ocorrencia].[Disciplina_idDisciplina]) ON [evento].[idEvento]  
=[ficha_ocorrencia].[Evento_idEvento];
```

**Fonte:** Elaborado pelos Autores.

**Figura 4** – Ocorrências frequentes – pergunta P2.

Ocorrências mais comuns	
Descricao	Tipo_Ocorrencia
CURSO DE FORMAÇÃO PROFISSIONAL	
Disciplina	Tipo_Ocorrencia
ASPECTOS DA ADMINISTRAÇÃO PÚBLICA	
	Atraso
	Atraso
	Atraso
	Atraso
	Disciplinar
	Incidente
TIRO POLICIAL	
	Disciplinar
	Falta
USO PROGRESSIVO DA FORÇA	
	Atraso

quinta-feira, 4 de maio de 2017

Página 1 de 1

**Fonte:** Elaborado pelos Autores.

Dessa forma, verifica-se a potencialidade do modelo, como repositório de dados e informações para subsídio à tomada de decisão pela área de gestão do ensino.

## 4 CONSIDERAÇÕES FINAIS

O objetivo deste trabalho consistiu na proposição e desenvolvimento de um modelo de dados aplicável à área de treinamento e formação policial da Polícia Rodoviária Federal (PRF). Verificou-se o mapeamento de processos resultante da análise dos macroprocessos e microprocessos necessários para a concepção,

formulação e execução de um evento educacional, obtendo-se quais informações são relevantes para o evento. Essas informações evoluíram para a formulação das principais perguntas de competência, utilizadas para nortear o modelo. Optou-se por restringir o modelo às perguntas de competência elencadas, apesar da possibilidade de inclusão de outras perguntas que ficaram latentes.

Por meio da análise da literatura, foram elencados os principais elementos que pudessem subsidiar as etapas de modelagem e implementação de um banco de dados voltado à área de treinamento e formação policial. A análise documental, focada no último curso de formação profissional realizado e a elicitação dos requisitos, avançando para as perguntas de competência, serviu para definição das principais entidades, seus relacionamentos e atributos necessários para suportar o armazenamento de informações relevantes para a gestão de um evento educacional.

Alguns processos de um evento não foram abordados. Dentre eles, a investigação social dos candidatos que irão participar do Curso de Formação Profissional. De modo geral, outras possíveis entidades que não foram inseridas nesse modelo, também merecem registro:

- “Ouvidoria”: destinada a captar as observações do aluno referentes ao evento que está sendo realizado; O registro dessas informações e o seu devido trâmite também merecem a inclusão de novas entidades no modelo.
- “Investigação Social”: destinada a armazenar as informações sigilosas apuradas por meio da análise de vida pregressa de candidatos (evento Curso de Formação);
- “Conselho de Ensino”, destinado a apurar ilícitos administrativos cometidos pelos alunos, por meio de um processo disciplinar, proporcionando ampla defesa. Seu resultado pode ser ou não favorável ao aluno. Sendo desfavorável, é assinado um Termo de Ajustamento de Conduta, no qual o aluno se compromete em adequar a sua conduta, nos casos possíveis. Nos demais, a punição é estabelecida de acordo com a portaria que estabelece o grau, de acordo com o evento, podendo resultar em expulsão do candidato, no caso do Curso de Formação Profissional. Aqui mais algumas entidades seriam necessárias para registrar esse fato. O processo de desligamento que se segue também necessitaria de novas entidades cuja função seria armazenar dados

oriundos do processo de apuração de responsabilidade de infrações administrativas referentes ao evento;

- “Avaliação do Instrutor”: destina-se a registrar o resultado da avaliação dos instrutores, pelos alunos. Essa informação é obtida por meio de um questionário confeccionado pela área pedagógica e aplicado logo após o término da instrução. Suas informações são analisadas posteriormente a fim de propiciar sugestões ou correções na metodologia utilizada pelo instrutor. O conhecimento registrado nesse questionário se torna ainda mais relevante quando a instrução foi conduzida por um monitor. Um monitor é um candidato a instrutor que, apesar de ter sido aprovado no curso de formação de instrutores, ainda não ministrou a quantidade requisitada de horas-aula. Após o término do período definido, o candidato a instrutor é avaliado em aspectos comportamentais e metodológicos, resultando no conceito apto ou inapto.

Para se demonstrar a viabilidade do modelo proposto, o banco de dados foi populado com informações sobre um cenário fictício e várias consultas foram produzidas a fim de se extrair relatórios que proporcionem as informações requeridas pelas perguntas de competência. A partir dos resultados obtidos, pode-se afirmar que o modelo satisfaz ao objetivo proposto.

## REFERÊNCIAS

BARALDI, Tereza Cristina Albieri. **A formação técnico-profissional do delegado de polícia de São Paulo**. 2012. 193 f. Tese (Doutorado em Educação) Universidade Est. Paulista Júlio de Mesquita Filho. Marília, 2012.

CERQUEIRA, Homero de Gorge et al. **A disciplina militar em sala de aula: a relação pedagógica em uma instituição formadora de oficiais da Polícia Militar do Estado de São Paulo**. 2006. Dissertação de Mestrado (Educação), Pontifícia Universidade Católica de São Paulo, São Paulo.

CERQUEIRA, Homero de Gorge. **Os paradoxos do currículo da Academia de Polícia Militar do Barro Branco: a cidadania como fundamento das forças de segurança pública**. 2011. 246 f. Tese (Doutorado em Educação). Pontifícia Universidade Católica de São Paulo. São Paulo, 2011.

CHAMBERLIN, Donald D. **Early history of SQL**. IEEE Annals of the History of Computing, v. 34, n. 4, p. 78-82, 2012.

COUGO, Paulo Sérgio. **Modelagem conceitual e projeto de bancos de dados**. Rio de Janeiro. Editora Campus, 1997.

DARWEN, Hugh. **The relational model: Beginning of an era**. IEEE Annals of the History of Computing, v. 34, n. 4, p. 30-37, 2012.

ELMASRI, Ramez E.; NAVATHE, Shamkant. **Sistemas de banco de dados**. Addison-Wesley, ISBN 8588639173, 2005.

FOX, Mark S.; GRUNINGER, Michael. **Enterprise Modeling**. AI magazine, v. 19, n. 3, p. 109, 1998.

HEUSER, Carlos Alberto. **Projeto de Banco de Dados**. 6ª ed. Porto Alegre: Bookman, 2009.

JECH, Thomas. **Set Theory: The Third Millennium Edition, Revised and Expanded**. Springer. ISBN 3-540-44085-2, 2003.

LUIZ, Ronilson de Souza. **Ensino Policial Militar**. n. 139 f. 2008. Tese: (Doutorado em Educação: Currículo) Pontifícia Universidade Católica de São Paulo, São Paulo, 2008.

POLÍCIA RODOVIÁRIA FEDERAL. **História da PRF**. Disponível em: <<https://www.prf.gov.br/portal/aceso-a-informacao/institucional/historia>>. Acesso em: 20 jan. 2017.

PONCIONI, Paula. **Tendências e desafios na formação profissional do policial no Brasil**. SEGURANÇA PÚBLICA, 2007.

ROLIM, Marcos. **A síndrome da rainha vermelha: policiamento e segurança pública no Século XXI**. 2ª Rio de Janeiro: Jorge Zahar Ed. Oxford, Inglaterra: University of Oxford, Centre For Brazilian Studies, 2009.

SANTOS, Izequias Estevam dos. **Manual de métodos e técnicas de pesquisa científica**. 9ª ed. rev., atual. e ampl. Niterói: Impetus, 2012.

SILBERSCHATZ, A.; KORTH, H.F.; SUDARSHAN, S. **Sistema de Banco de Dados – Tradução da 5ª edição**. Rio de Janeiro: Campus, 2006.

SONG, Il-Yeol; EVANS, Mary; PARK, Eun K. **A comparative analysis of entity-relationship diagrams**. Journal of Computer and Software Engineering, v. 3, n. 4, p. 427-459, 1995.

TEOREY, Toby; LIGHTSTONE, Sam; NADEAU, Tom. **Projeto e modelagem de banco de dados**. Campus, 2ª ed., 2014.

USCHOLD, Michael. **Building ontologies: Towards a unified methodology**. Technical report-university of Edinburgh artificial intelligence applications institute AIAI TR, 1996.

WADE, Bradford W. **Compiling SQL into System/370 Machine Language**. IEEE Annals of the History of Computing, v. 34, n. 4, p. 49-50, 2012.

## **SOFTWARES FORENSES DIRECIONADOS À INVESTIGAÇÃO DE CRIMES VIRTUAIS EM REDES DE COMPUTADORES**

*Samuel Nunes Juliani  
Eliane Pozzebon  
Luciana Bolan Frigo*

### **1 INTRODUÇÃO**

Entre os muitos reflexos da globalização no mundo que aproximam, positiva ou negativamente, pessoas e instituições por meio das tecnologias de informação e comunicação, pode-se perceber o surgimento e, posteriormente, o crescimento exponencial de crimes ligados ao mundo digital. Em especial a internet, que faz esse papel de aproximação, tornou-se o principal campo de atuação de comunicação entre todo o mundo, fazendo com que pessoas mal-intencionadas, usando da sensação de anonimato e baixa exposição na rede, desenvolvessem técnicas para a prática de crimes nesse meio (FERREIRA, [2009]).

Por terem características de execução diferentes do crime comum, esse tipo de crime denominado Crime Virtual tem a necessidade de um tratamento diferenciado em relação à obtenção de provas para seu esclarecimento. Essa diferenciação ocorre devido ao cenário do crime ser, em parte ou no todo, em cenário abstrato. Nesse ponto, há a imprescindibilidade da realização de uma perícia específica, que analise as provas no ambiente computacional, a fim de direcionar decisões importantes para a aplicação das sanções devidas (GONÇALVES *et al.*, 2012).

Formas de proteção pessoal e, principalmente, da informação têm de estar inseridas no cotidiano dos usuários de qualquer sistema informático de comunicação e processamento de dados, pois esses podem estar expostos aos muitos tipos de ameaças, que sem uma proteção devida, podem acarretar danos, muitas vezes

irreparáveis, seja à idoneidade das pessoas ou das informações (SOARES; LEMOS; COLCHER, 1995). Muitos tipos de vírus e ataques estão por toda internet a fim de prejudicar pessoas, sistemas ou organizações e beneficiar criminosos. Recursos fundamentais que garantam a confidencialidade, integridade e disponibilidade da informação são itens de extrema importância à sustentação da segurança de dados e informações, e quem preza pela sua integridade e pela fidedignidade de seus dados e informações, tem que estar alerta a esses fundamentos (BEAL, 2005).

Diante da perspectiva explanada, tem-se, então, como objetivo deste estudo discorrer sobre as áreas que se ligam diretamente ao crime ocorrido dentro de ambientes telemáticos, perpassando por conceitos ligados a redes de computadores e segurança da informação e avançando sobre a definição e caracterização do crime virtual e a perícia forense computacional, apresentando ferramentas apoiadoras à investigação forense. Para tal, na seção a seguir, apresentam-se os procedimentos metodológicos realizados para elaboração deste estudo, sendo posteriormente abordado estudo sobre rede de computadores e a proteção da informação, e crime virtual e a perícia forense computacional (seções 3 e 4, respectivamente). Na seção 5, descrevem-se os *softwares* forenses em redes de computadores, e encerra-se o artigo com as considerações finais.

## **2 PROCEDIMENTOS METODOLÓGICOS**

A metodologia utilizada tem por base uma pesquisa teórica de cunho qualitativo, tendo por finalidade, de início, identificar o conceito de redes de computadores, expondo o funcionamento do grupo de protocolos de comunicação TCP/IP (*TransportControlProtocol/Internet Protocol*), que é o responsável por unir redes distintas, evidenciando a internet como o principal meio virtual. Nessa temática, ainda se agregam formas de assegurar à rede de computadores e aos envolvidos no processo de comunicação conceitos sobre a segurança da informação, trazendo métodos essenciais para a proteção da informação dentro da rede de computadores.

Posteriormente, é tratado do crime virtual conceituando-o e caracterizando os tipos desse crime de acordo com o seu *modus operandi*. A seguir, torna-se necessário evidenciar as fases da perícia forense computacional, explicitando as técnicas envolvidas nessa ciência forense específica para obtenção e tratamento de evidências e os modos de investigação dos crimes virtuais na grande rede de

*Softwares* forenses direcionados à investigação de crimes virtuais em redes de computadores computadores. E, por fim, serão apresentados *softwares* que contribuem para a elucidação dos crimes virtuais ocorridos em redes de computadores.

### **3 REDES DE COMPUTADORES E A PROTEÇÃO DA INFORMAÇÃO**

A comunicação sempre foi uma das maiores necessidades da humanidade. No decorrer do tempo, com essa necessidade aumentando devido ao grande crescimento da sociedade e de sua dispersão geográfica, tornaram-se imprescindíveis maneiras de efetuar algum tipo de comunicação com comunidades distantes. Pombos-correios e sinais de fumaça foram usados pelos ancestrais do homem para a comunicação e, posteriormente, a invenção do telégrafo, em 1838, deu entrada a uma nova época nas comunicações (SOARES; LEMOS; COLCHER, 1995).

A evolução na área da comunicação, processamento e armazenamento das informações possibilitou uma revolução de novas formas de comunicação, permitindo maior eficácia dos sistemas computacionais. Em seguida, com a evolução dos sistemas de computação e das arquiteturas, surgem as redes de computadores como uma forma mais eficaz de comunicação (SOARES; LEMOS; COLCHER, 1995).

Tanenbaum (1997) define redes de computadores como computadores autônomos interconectados, os quais realizam a troca de informações utilizando-se de um sistema de comunicação organizado por protocolos dentro de um arranjo topológico. No entanto, com a proliferação de todo o tipo de redes de computadores no decorrer dos anos, começou a surgir problemas com a conexão dessas redes, uma a outra que, até então, não possuíam um padrão que as compatibilizasse. Diante desse aspecto, surgiu a necessidade da criação de um modelo de referência que mais tarde se chamaria TCP/IP. Esse modelo tornou possível a conexão de redes distintas, tornando possível a troca de informações e dando início ao surgimento da internet (SOARES; LEMOS; COLCHER, 1995).

A arquitetura internet TCP/IP é organizada em quatro camadas conceituais, conforme Soares, Lemos e Colcher (1995):

- Camada de Aplicação;
- Camada de Transporte;
- Camada de Inter-rede;
- Camada de Interface de rede.

No nível de aplicação, os usuários usam aplicações para ter acesso aos serviços da camada de inter-rede. Essas aplicações interagem com a camada de

transporte no envio e no recebimento de dados utilizando-se dos protocolos TCP e UDP (*User Datagram Protocol*), presentes na camada de transporte (SOARES; LEMOS; COLCHER, 1995). A camada de transporte é responsável por permitir a conversação da origem ao destino entre as aplicações. É nessa camada que se encontra o protocolo TCP que realiza serviços orientados à conexão e o UDP que realiza serviços sem orientação a conexão (SOARES; LEMOS; COLCHER, 1995). A camada inter-redes, conforme Tanenbaum (2003, p. 45), tem a função de “[...] permitir que os *hosts* injetem pacotes em qualquer rede e garantir que eles trafegarão independentemente até o destino (talvez em uma rede diferente) “. Por fim, a camada de interface de rede é responsável pela compatibilização das redes que se ligam à inter-rede. Ela permite que qualquer tipo de rede possa se conectar desde que a rede possua uma interface que compatibilize a sua tecnologia específica com o protocolo IP (SOARES; LEMOS; COLCHER, 1995).

Destarte, é essencial que elementos que proporcionem segurança à informação sejam levados em consideração para que os dados e informações que trafegam pela rede de computadores obtenham maior nível de segurança garantindo os três objetivos principais na preservação da informação: confidencialidade, integridade e disponibilidade (BEAL, 2005), definidos conforme esse autor, como:

- **Confidencialidade:** processo de garantir que o acesso às informações seja restrito a usuários legítimos;
- **Integridade:** garante que as informações não sejam alteradas ou excluídas sem autorização. Consiste em prevenir contra a criação, alteração ou destruição não autorizada, garantindo que as informações permaneçam completas e precisas;
- **Disponibilidade:** garante que a informação seja disponibilizada apenas para os usuários legítimos.

Um sistema pode estar exposto a muitos tipos de ameaças, as quais podem comprometer os três itens citados anteriormente. Tais ameaças podem causar todo tipo de violação em um sistema, ocasionando, principalmente, grandes danos às informações. Em vista disso, torna-se muito importante a necessidade de proteção contra a manipulação, intencional ou não, das informações confidenciais e dos dispositivos periféricos do computador por elementos não autorizados. As ameaças podem ocorrer a qualquer momento e surgem das falhas de segurança das pessoas e das organizações, causando danos, perdas e prejuízos muitas vezes irreparáveis (SOARES; LEMOS; COLCHER, 1995).

A seguir, estão dispostas algumas ameaças mais comuns dentro do ambiente digital:

- **Vírus:** programa com fins maliciosos que tem a capacidade de apagar ou alterar arquivos de usuários, prejudicar o funcionamento do sistema operacional, causar excesso de tráfego na rede, entre outros males (ALECRIM, 2011).
- **Spam:** é um *e-mail (electronic mail)* indesejado, não solicitado pelo usuário e que, geralmente, é despachado para muitas pessoas. Pode conter vírus agressivos que capturam informações pessoais, mas na maioria das vezes os *e-mails* aparecem como propagandas. Também são chamados de UCE (*UnsolicitedCommercial E-mail*) (GUERRA, 2012).
- **Phishing:** é a fraude que ocorre por meio do envio de mensagens não solicitadas. Essas mensagens levam o usuário a acessar páginas falsas pensando ser de uma empresa, banco ou organizações conhecidas. Ao acessar a página, o usuário tem seus dados pessoais e/ou financeiros capturados (KOLLING, [2010]a).
- **Engenharia social:** é a habilidade de conseguir acesso a informações confidenciais, utilizando habilidades de persuasão. Nesse modelo de ameaça, o fator humano é o alvo devido à falta de percepção das pessoas em relação à importância das informações que elas detêm (CIPOLI, 2012).

Em contrapartida, existem mecanismos de proteção às ameaças digitais como forma de prevenir ou mesmo mitigar a ação de pessoas mal-intencionadas. Dentre esses mecanismos, pode-se citar:

**Firewall:** “[...] barreira de proteção que controla o tráfego de dados do computador e da internet. O objetivo desse dispositivo é permitir somente a transmissão e recepção de dados autorizados e confiáveis” (KOLLING, [2010]b).

**Criptografia:** Uma das ferramentas automatizadas mais importante para a segurança de rede e das comunicações por conseguir converter dados legíveis em algo sem sentido, possuindo a capacidade de recuperar os dados originais a partir desses dados sem sentido (STALLINGS, 2008, p. 15).

**Virtual Private Network:** esta técnica tem a capacidade de conectar dois computadores utilizando uma rede pública, como a *internet*. Para haver total

*Softwares* forenses direcionados à investigação de crimes virtuais em redes de computadores segurança, esta tecnologia faz o uso do protocolo de tunelamento, que consiste, basicamente, em um canal principal onde há uma entrada e uma saída de informação, sem que o usuário externo a esse canal possa ter acesso às informações transmitidas (MARTINS, 2009).

**Antivírus:** são programas com a finalidade de detectar, prevenir e eliminar vírus de um computador.

Após visto os conceitos pertinentes à rede de computadores e à segurança da informação, é essencial o estudo relacionado com a ocorrência do crime virtual e do seu modo de investigação por meio da ciência forense específica.

## 4 CRIME VIRTUAL E A PERÍCIA FORENSE COMPUTACIONAL

Com o grande aumento da utilização de sistemas computadorizados e a expansão da internet, tornou-se frequente o uso desse meio de comunicação para a realização de crimes. Não possuindo fronteiras para a prática desse tipo de conduta, os malfeitores podem realizar tais crimes a partir da comodidade de seu lar, bastando apenas que tenham conhecimento e os equipamentos necessários. Essa conduta torna-se atrativa devido ao baixo risco de exposição dos criminosos, pois o crime virtual frequentemente desafia a detecção, haja vista que o crime é “limpo” e sem violência (STAIR; REYNOLDS, 2006).

Costa (1995p.2) define como crime virtual “[...] toda a ação típica, antijurídica e culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão”. Segundo o autor, a ação típica corresponde ao comportamento humano previsto em lei como crime, sendo que nos crimes relacionados à informática esta ação se concretiza no momento em que a utilização de um sistema de informática afeta um bem ou interesse juridicamente protegido (COSTA, 1995).

Silva (2003) classifica os crimes virtuais em puros, impuros e comuns. Os crimes puros são aqueles que se referem aos tipos novos, surgidos com o uso da informática, em que o sistema informático serve como meios e fim almejado pelo agente. Por outro lado, os crimes impuros são os tipos nos quais o sistema de comunicação serve somente como meio para a prática de um delito, claramente já definido na legislação penal. E, por último encontram-se os crimes comuns situados na esfera das ações, cujo sistema informático é mera ferramenta para a prática de

*Softwares* forenses direcionados à investigação de crimes virtuais em redes de computadores crimes comuns, valendo ressaltar, ações já previstas como típicas em nossa legislação penal (SILVA, 2003).

Como processo principal de investigação desse tipo de crime, existe a Perícia Forense Computacional, que é a ciência forense específica para a consubstanciação do cenário do crime e criação de laudos e provas substanciais ao desvendamento do ilícito ocorrido. Gonçalves *et al.*, (2012, p. 2, 3) afirmam que “a computação forense é a ciência que, por meio de técnicas e habilidades especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio de praticá-lo”. Basicamente o processo da realização da perícia forense computacional envolve quatro processos distintos: **Identificação, Preservação, Análise e Apresentação** (ROSA, 2011).

A fase que compreende o processo de identificação das evidências incumbe ao perito buscar e relacionar todas as evidências possíveis, levando em consideração o tipo do crime ocorrido, pois cada tipo de crime apresenta evidências particulares (ROSA, 2011). Freitas (2006) reforça que em cada tipo de crime investigado as evidências podem variar; o autor cita, como exemplo, casos de crimes de pedofilia ou pornografia, em que certamente o perito buscará por vestígios do tipo imagem ou vídeo, prioritariamente. O perito no processo de identificação das evidências deve procurar basicamente por informações próximas ao acontecimento, ligar nomes a pessoas, datas e, claro, obter informações sobre o sistema que fora afetado; buscando sempre na coleta das informações respeitar a ordem de volatilidade dos dados capturados, seguindo do mais volátil ao menos volátil (ROSA, 2011).

Após a realização da identificação das evidências, é realizada a preservação das mesmas de forma que não haja dúvidas sobre a veracidade das evidências (ROSA, 2011). De acordo com Cagnani e Santos ([2007?]), a perícia não deve ser realizada nos dados originais apreendidos, ou seja, o primeiro passo a ser seguido na realização de uma perícia computacional é o de gerar uma imagem exata da mídia original e fundamentar todos os trabalhos sobre essa imagem. Os dados originais devem ser preservados até o dia do julgamento do processo a que estão vinculados. Os autores enfatizam sobre a obrigatoriedade e responsabilidade do perito em registrar os materiais recebidos, os acessos a esses materiais, as pessoas que tiveram contato com as evidências, devendo sintetizar qual o motivo para realização desse contato.

Na fase posterior, é realizada a análise das evidências, sendo esta a de maior duração no processo geral da perícia forense computacional. O perito torna-se a peça chave dessa fase, cabem a ele as tarefas de reconstrução do cenário do crime,

caso seja possível, elaboração de relações entre as evidências e eventos coletados no decorrer da investigação e responder questões que estão diretamente relacionadas à perícia forense. É importante manter documentadas todas as atividades que foram realizadas nessa fase (ROSA, 2011). Ao final dessa fase, conforme Freitas (2006) é possível responder questões do tipo: qual a versão do SO (Sistema Operacional) investigado; quem se conectou a máquina no momento do crime; que arquivos foram usados e/ou excluídos; quais portas estavam abertas no SO; e quem fez *login* no computador recentemente.

Por último, encontra-se a fase de apresentação da análise. Para que sejam apresentados os resultados obtidos na investigação, faz-se necessária a criação do laudo pericial, que basicamente é a descrição que o perito realiza após ter as correlações das evidências e análises. Esse laudo tem a obrigatoriedade de ser redigido de forma clara, organizada, concisa, imparcial e conclusiva, servindo como prova cabal para a elucidação do crime virtual investigado (ROSA, 2011).

## 5 SOFTWARES FORENSES EM REDES DE COMPUTADORES

Este capítulo tem por objetivo apresentar alguns *softwares* que podem ser utilizados para investigações nos casos de crime virtual contribuindo, dessa forma, para a forense computacional. As ferramentas utilizadas são destinadas à captura de dados na rede de computadores a fim de direcionar a investigação.

### 5.1 CallerIp

O *software* CallerIP tem a função de auxiliar na indicação de entradas, saídas e invasões de IP na máquina em que estiver instalado. Esse programa tem a finalidade de informar qual o IP que está conectado ou tentando se conectar, mostrando em um mapa *mundi* qual a sua localização juntamente com endereço, telefone e o responsável por aquele IP (VARGAS, 2007). Essa ferramenta permite a possibilidade de monitoramento de atividades das portas que estão abertas no sistema que geralmente não estão protegidas por *firewalls*. Dessa forma, essa ferramenta pode identificar a invasão antes que o sistema ou as informações sejam prejudicados (VISUALWARE, 2014). Esse *software* pode ser utilizado também para a investigação de funcionários que estão utilizando aplicações que facilitam o acesso à rede interna de computadores, tornando-a vulnerável. Dessa forma, essa ferramenta é utilizada para monitorar as entradas e saídas dos IPs do sistema operacional, de forma a

Softwares forenses direcionados à investigação de crimes virtuais em redes de computadores identificar qual a aplicação está sendo utilizada para esse tipo de prática (VARGAS, 2007). A Figura 1 evidencia a tela principal do CallerIP:

Figura 1- tela CallerIP



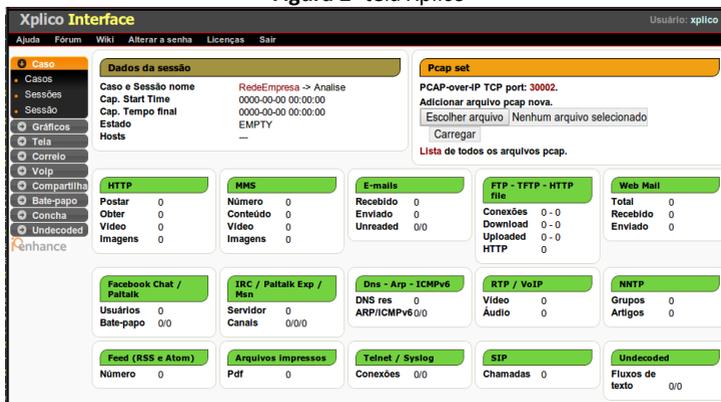
Fonte: VISUALWARE (2014)

## 5.2 Xplico

Xplico é uma Ferramenta de Análise Forense de Rede (*NFAT - Network Forensic Analysis Tool*) cujo objetivo é extrair de um tráfego de internet capturado ou rede local e seus protocolos como: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPV4, IPV6 e outros, arquivos pcap (*Packet Capture Data Format*) obtidos por ferramentas de captura de tráfego dedados ou aquisição em tempo real para análise (VIEIRA, 2011). A ferramenta realiza o processamento, extração, classificação e disponibilização de informações de protocolos de arquivos de tráfego de redes, sendo que não possui a função de analisador de protocolos de rede como o *Wireshark* (GALVÃO, 2011, p. 3).

Tendo como principal característica a capacidade de extração do conteúdo a partir de um arquivo pcap, essa ferramenta pode, por exemplo, extrair todos os *e-mails* transportados pelos protocolos POP, IMAP e SMTP, todo o conteúdo transportado pelo protocolo HTTP, todas ligações de VoIP, e ainda o conteúdo dos protocolos FTP, TFTP (*Trivial File Transfer Protocol*), entre outros (LIMA, 2010).

Figura 2- tela Xplico



Fonte: Galvão (2011)

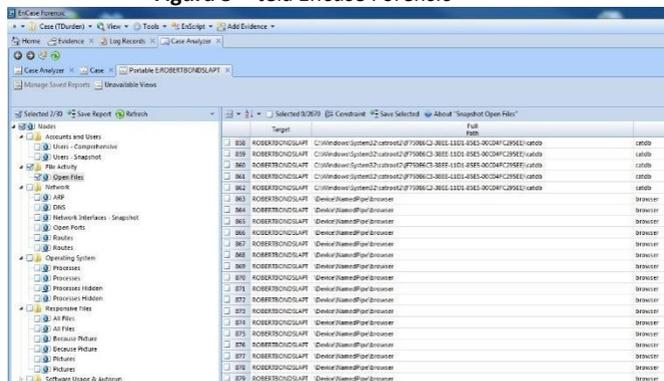
### 5.3 Encase Forensic

Devido a sua característica não tão invasiva o EnCase Forensic é uma das ferramentas mais utilizadas pelos peritos forenses na busca por evidências em um ato criminoso. Comumente adotada pelas instituições governamentais e aplicada também em investigações militares, a ferramenta mostra-se vantajosa quando o assunto se trata de segurança e integridade das evidências. A ferramenta tem a capacidade de realizar análise simultânea de múltiplas máquinas em uma rede LAN/WAN em nível de disco e memória, analisar múltiplas plataformas, identificar dlls (*Dynamic-Link Library*) injetadas no sistema, identificar processos ocultos entre outros. Outra vantagem notória desta ferramenta é a de proporcionar ao usuário relatórios minuciosos do conteúdo abordado em um nível de aceitação legal para serem utilizados em processos judiciais (GOLDMAN, [S.d.], p. 16).

Vargas (2007) salienta que a ferramenta EnCase é uma das mais completas quando o assunto trata de perícia forense computacional por conseguir realizar:

- Padronização de laudos periciais;
- Organização do banco de dados ligado às evidências;
- Fornecer senhas ou as quebrá-las;
- Recuperar arquivos excluídos.

Figura 3 - tela Encase Forensic



Fonte: GOLDMAN [S.d.]

## 6 CONSIDERAÇÕES FINAIS

O aumento exponencial de crimes virtuais estimulados pelo grande avanço das tecnologias de comunicações e a consolidação da internet como o meio de comunicação amplamente difundido entre as massas, contribuiu para a constituição de uma ciência forense capaz de investigar e proporcionar provas fiéis para a análise e juízo de crimes em que os sistemas informáticos são utilizados como meio ou fim para a prática do delito.

Nesse contexto, observou-se a necessidade de conceituar redes de computadores e descrever o principal modelo de referência que conecta o mundo todo em uma só rede de comunicação. São nessas redes que dados e informações trafegam de um lado ao outro, porém, acabam muitas vezes sofrendo interferências criminosas e gerando inconveniências a quem navega. Diante disso, foi tratado da do tema que envolve a segurança da informação, descrevendo elementos mitigadores desses inconvenientes. Simultaneamente, a perícia forense computacional mostrou-se fundamental para o processo de investigação e construção da prova, observando que a utilização de ferramentas forenses contribui seriamente para o resultado final.

Diante disso, é notável que todo o processo de investigação, que envolve a busca pela prova capaz de culminar na punição do infrator virtual, não é um processo pautado em métodos formais de investigação pelo contrário, muitas vezes tem que se recorrer a procedimentos empíricos e de certa forma pontuais e peculiares ao

*Softwares* forenses direcionados à investigação de crimes virtuais em redes de computadores investigador, observando a relevância de sempre preservar a prova. No entanto, isso não necessariamente é uma deficiência, mas sim uma característica a ser absorvida.

## REFERÊNCIAS

ALECRIM, Emerson. Vírus de computador e outros malwares: o que são e como agir. Infowester. 2011. Disponível em: <<http://www.infowester.com/malwares.php>>. Acesso em: 20 nov. 2016.

BEAL, Adriana. Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

CAGNANI, Caio; SANTOS, Valdecir de Deus dos. Computação forense: fundamentos. [2007?]. Disponível em: <<http://pt.scribd.com/doc/47774532/computacao-forense-fundamentos>>. Acesso em: 09 fev. 2017.

CIPOLI, Pedro. O que é engenharia social. Canaltech. 2012. Disponível em: <<http://corporate.canaltech.com.br/o-que-e/seguranca/O-que-e-Engenharia-Social/>>. Acesso em: 20 nov. 2016.

COSTA, Marco Aurélio Rodrigues da. Crimes de informática. Jus Navigandi. 1995. Disponível em: <<http://jus.com.br/artigos/1826/crimes-de-informatica/2>>. Acesso em: 6 maio 2016.

FERREIRA, Lóren Pinto. Os “crimes de informática” no direito penal brasileiro. [2009]. Disponível em: <[http://www.oab.org.br/editora/revista/revista\\_08/anexos/crimes\\_de\\_informatica.pdf](http://www.oab.org.br/editora/revista/revista_08/anexos/crimes_de_informatica.pdf)>. Acesso em: 20 mar. 2016.

FREITAS, Andrey Rodrigues. Perícia forense aplicada à informática: ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

GALVÃO, Ricardo Kléber Martins. Análise de tráfego de redes com Xplico. 2011. Disponível em: <[http://www.ricardokleber.com/palestras/2011\\_12\\_02\\_-\\_HacknRio2011\\_-\\_Analise\\_De\\_Trafego\\_de\\_Redes\\_com\\_Xplico.pdf](http://www.ricardokleber.com/palestras/2011_12_02_-_HacknRio2011_-_Analise_De_Trafego_de_Redes_com_Xplico.pdf)>. Acesso em: 15 mar. 2017.

GONÇALVES, Márcio. et al. Perícia forense computacional: metodologias, técnicas e ferramentas. Revista Científica Eletrônica de Ciências Sociais Aplicadas da Eduvale. Jaciara, MT. a. V, n. 07, nov. /2012, p. 1-17. Disponível em: <[http://edualesl.revista.inf.br/imagens\\_arquivos/arquivos\\_destaque/LXkEA5FVHGZF1FB\\_2015-12-19-2-33-33.pdf](http://edualesl.revista.inf.br/imagens_arquivos/arquivos_destaque/LXkEA5FVHGZF1FB_2015-12-19-2-33-33.pdf)>. Acesso em 21 mar. 2016.

GOLDMAN, Alfredo. Artigo sobre computação forense. [S.d.]. Disponível em: <<http://grenoble.ime.usp.br/~gold/cursos/2008/movel/gradSemCorrecao/FelipeBulleC.pdf>>. Acesso em: 18 mar. 2017.

GUERRA, Ráisa. O que é spam. Tecmundo. 2012. Disponível em: <<http://www.tecmundo.com.br/spam/223-o-que-e-spam-.htm>>. Acesso em: 220 nov. 2016.

KOLLING, Gabriella S. Ameaças à segurança do computador. [2010]a. Disponível em: <[http://seguranca-da-informacao.info/mos/view/Amea%C3%A7as\\_%C3%A0\\_Seguran%C3%A7a\\_do\\_Computador/>](http://seguranca-da-informacao.info/mos/view/Amea%C3%A7as_%C3%A0_Seguran%C3%A7a_do_Computador/>). Acesso em: 20 nov 2016.

\_\_\_\_\_. [2010]b. Disponível em: <<http://seguranca-da-informacao.info/mos/view/Solu%C3%A7%C3%B5es/>>. Acesso em: 20 nov. 2016.

LIMA, Gustavo. Xplico 0.6.0: Uma ferramenta que dá um plus ao que foi capturado pelo Wireshark. 2010. Disponível em: <<http://blog.corujadeti.com.br/xplico-0-6-0-uma-ferramenta-que-da-um-plus-ao-que-foi-capturado-pelo-wireshark/>>. Acesso em: 15 mar. 2017.

MARTINS, Elaine. O que é VPN? Tecmundo. 2009. Disponível em: <<http://www.tecmundo.com.br/1427-o-que-e-vpn-.htm>>. Acesso em: 21 nov. 2016.

NASCIMENTO, Nelson José do. Ameaças e vulnerabilidades da informação: como precaver. Portal Educação. 2013. Disponível em: <<http://www.portaleducacao.com.br/educacao/artigos/48819/ameacas-e-vulnerabilidades-da-informacao-como-precaver>>. Acesso em: 09 nov. 2016.

ROSA, Ana Paula Teixeira. Forense de memória: extração e análise de dados armazenados em memória volátil. 2011. Disponível em: <[http://www.peotta.com/arquivos/forense/Monografia\\_AnaPaula\\_UnB\\_vFinal.pdf](http://www.peotta.com/arquivos/forense/Monografia_AnaPaula_UnB_vFinal.pdf)>. Acesso em: 09 fev. 2017.

SILVA, Rita de Cássia Lopes da. Direito penal e sistema informático. São Paulo: Revista dos tribunais, 2003.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. Redes de computadores: das LANs, MANs e WANs às redes ATM. 2. ed. Rio de Janeiro: Campus, 1995.

STAIR, Ralph; REYNOLDS, George W. Princípios de sistemas de informação: uma abordagem gerencial. São Paulo: Pioneira Thomson Learning, 2006.

STALLINGS, William. Criptografia e segurança de redes.4. ed. São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, Andrew S. Redes de computadores. Rio de Janeiro: Campus, 1997.

\_\_\_\_\_. Redes de computadores. Rio de Janeiro: Elsevier, 2003.

VARGAS, Raffael. Perícia forense computacional: ferramentas periciais. Gerência de TI. 2007. Disponível em: <<http://imasters.com.br/artigo/6485/gerencia-de-ti/pericia-forense-computacional-ferramentas-periciais/>>. Acesso em: 14 mar. 2017.

VIEIRA, Vinícius. Xplico: uma ferramenta de análise forense de redes. 2011. Disponível em: <<http://sejalivre.org/xplico-uma-ferramenta-de-analise-forense-de-redes/>>. Acesso em: 15 mar. 2017.

VISUALWARE. CallerIP IP andportmonitoring. 2014. Disponível em: <<http://www.calleripro.com/detail.html>>. Acesso em: 11 mar. 2017.

## **INSTRUMENTOS TECNOLÓGICOS PARA A PROTEÇÃO DE MULHERES VÍTIMAS DE VIOLÊNCIA: SOLUÇÃO PARA CONTROLE DA VIOLÊNCIA DOMÉSTICA?**

*Sônia Maria Dall'Igna  
Giovani Mendonça Lunardi  
Roderval Marcelino  
Milena Petters Melo  
Angelita Darela Mendes*

### **1 INTRODUÇÃO**

A violência doméstica é uma realidade que permeia os tempos! A mulher, em razão de circunstâncias imemoriais, sofre como vítima atávica de agressões no ambiente de convivência. Nesse viés, Porto (2014) enfatiza que a violência é uma constante na natureza do ser humano, uma vez que desde os primórdios este triste fato acompanha o cotidiano da humanidade, comparado pelo autor a uma condição selvagem da natureza humana.

Passaram-se séculos sem que houvesse mudanças significativas. O homem ocupou o papel principal, submetendo as mulheres ao longo dos tempos. Numa sociedade ainda desigual como vive-se, atualmente, a ideia de justiça deve proporcionar políticas de prevenção, com a finalidade de proteger grupos vulneráveis, integrando essa categoria, mulheres em diferentes situações de violência.

Assim, paralelamente aos mecanismos já existentes de defesa, surgiram possibilidades tecnológicas a partir da evolução de dispositivos móveis, cujos recursos podem ser colocados ao lado das políticas públicas que o Estado desenvolve.

Vários Estados brasileiros abriram os olhos para as vantagens de por em prática mecanismos preventivos em favor de mulheres vítimas de violência e estão apostando no aperfeiçoamento do sistema de socorro imediato, expandindo seus projetos e aumentando o número de mulheres protegidas.

Seriam esses recursos a solução para a diminuição dos índices de violência contra mulheres?

## **2 BREVE HISTÓRICO DA VIOLÊNCIA CONTRA MULHER**

As denúncias de violência doméstica, no Brasil, surgiram somente a partir de 1978, após a promulgação da Lei do Divórcio (Brasil, 1977). A lei possibilitou visibilidade às agressões domésticas e as denúncias, finalmente, foram contabilizadas, pois veio à tona a motivação para as separações, muitas vezes oriundas de agressões no ambiente familiar.

Somente em 1985 foi criada a primeira Delegacia da Mulher, em São Paulo, para realizar o atendimento diferenciado às vítimas dos crimes de violência doméstica. Não havia ainda legislação específica que se ocupasse do tema. A Constituição Federal de 1988, § 8º, artigo 226, entretanto, faz menção à violência doméstica, propondo mecanismos para erradicá-la (BRASIL, 1988).

Após longo e doloroso caminho jurídico, originado de penalização internacional em favor de Maria da Penha Maia Fernandes, uma farmacêutica aposentada do estado do Ceará, que, após sofrer diversas agressões do marido, inclusive duas tentativas de homicídio, as quais a condenou à paraplegia, surge a Lei nº 11.340, de 07 de agosto de 2006, denominada Lei Maria da Penha (BRASIL, 2006). Todavia, vale ressaltar que Maria da Penha obteve a condenação do seu agressor apenas quando os crimes estavam quase prescritos. Somente em 2015, com o advento da Lei nº 13.104/2015 tipificou-se o crime de Femicídio (BRASIL, 2015). Tal informação torna-se relevante e alarmante para este estudo uma vez que a taxa de feminicídios no Brasil é a quinta maior do mundo, segundo artigo da ONU, publicado em 09 de abril de 2016 (ONU, 2016).

Diante desse quadro, as políticas públicas de prevenção à violência doméstica investem na criação de mecanismos de defesa e de proteção.

### 3 DISPOSITIVOS MÓVEIS

Com o avanço exponencial ocorrido na última década no que se refere às Tecnologias da Informação e Comunicação (TIC), desde o uso simples dos dispositivos móveis, evolução das redes de distribuição de sinal, até o desenvolvimento das tecnologias via satélite, surgiram várias possibilidades de aplicação dos mesmos.

Tal desenvolvimento modificou comportamentos sociais em todas as esferas, começando pela educação, relações empresariais e segurança. Como se constata, cotidianamente, com os recursos tecnológicos atuais, as informações podem ser acessadas e utilizadas em qualquer lugar e em qualquer momento.

Diante desse fenômeno, o extremo crescimento dos chamados computadores pessoais impulsionou milhões de pessoas a adquirirem *laptops*, *palmtops* ou algum tipo de *personal digital assistant* (PDA), os conhecidos *smartphones* (SACCOL, 2007). A usabilidade de tais dispositivos móveis encontrou espaço em segurança pública, especialmente porque a expansão das redes de sinal associada à oferta de *smartphones* a preços acessíveis, tornou-se mais popular e mais confiável para o seu uso com fins protetivos.

Observa-se, então, que os *smartphones* estão sendo utilizados, também, como ferramenta para pedidos de socorro. Dessa forma, o popular “Botão do Pânico” adquiriu muitas roupagens, desde aplicativos que criam um grupo de pessoas às quais o usuário poderá pedir ajuda, em caso de perigo, como o *Circleof 6*, até dispositivos conjugados a serviços públicos protetivos.

### 4 APLICATIVOS DE PROTEÇÃO À MULHER

No Brasil os dispositivos de auxílio emergencial às mulheres vítimas de violência surgiram com variadas formas de funcionamento e apresentam diferentes composições. Nos vários Estados que já se utilizam de ferramentas tecnológicas, as formas de aplicação diferem entre si, com semelhança, entretanto, no atendimento à mulher vítima de violência.

#### a) Londrina (PR)

Foi a primeira cidade do Paraná que implantou um “Botão do Pânico”. Trata-se de um *pager* que, quando acionado, emite um alerta à polícia, com dados e a localização geográfica da vítima e do agressor. Além disso, um microfone é acionado e o som do local em que a mulher está é transmitido ao vivo aos policiais. O juiz poderá, assim, ter provas gravadas da agressão. Entretanto, apenas em agosto de 2016 o Projeto de Lei abordando o tema foi submetido à Assembleia Legislativa para a sanção do Governador (G1 –GLOBO, 2013).

#### **b) Vitória (ES)**

Cidade que lidera os índices de violência contra a mulher no Brasil, Vitória faz parte de um projeto piloto, lançado pelo Tribunal de Justiça do Estado do Espírito Santo (TJ-ES), em parceria com a Prefeitura, implantando o dispositivo com a ajuda dos agentes municipais. Os agentes recebem o sinal por meio de um *smartphone* e o tempo de resposta seria de três minutos. O Botão do Pânico dispara informações para a Central Integrada de Operações e Monitoramento (CIOM), com a localização exata da vítima, para que um carro da Patrulha Maria da Penha seja enviado ao local. Em 2016 foi veiculada notícia de expansão do projeto, que está se desenvolvendo em etapas, aumentando gradativamente o número de mulheres protegidas (Botão do Pânico).

#### **c) Piauí**

Apresenta-se também como o primeiro Estado a adotar o botão do pânico para as mulheres vítimas de violência doméstica e familiar. A assinatura do termo de aquisição do dispositivo de segurança preventiva foi realizada em 2013. A implantação da medida protetiva de urgência será feita primeiramente em Teresina, Parnaíba e Picos. Sobre os dados que levaram o Piauí a implantar o sistema, um levantamento realizado naquele ano mostrou que 92% das violências contra mulheres foram nos lares. Em Parnaíba esse número chegou a 43%. Outra informação importante é que existem mais de seis mil processos com relação a esse assunto (G1, 2017).

#### **d) Porto Alegre/RS**

No Rio Grande do Sul, mais precisamente na Capital Porto Alegre, foi lançado oficialmente, em 17 de dezembro de 2015, o aplicativo para celulares PLP 2.0, concedido às mulheres vítimas de violência doméstica e familiar com Medida Protetiva de Urgência deferida pelo Poder Judiciário. O projeto é coordenado pela

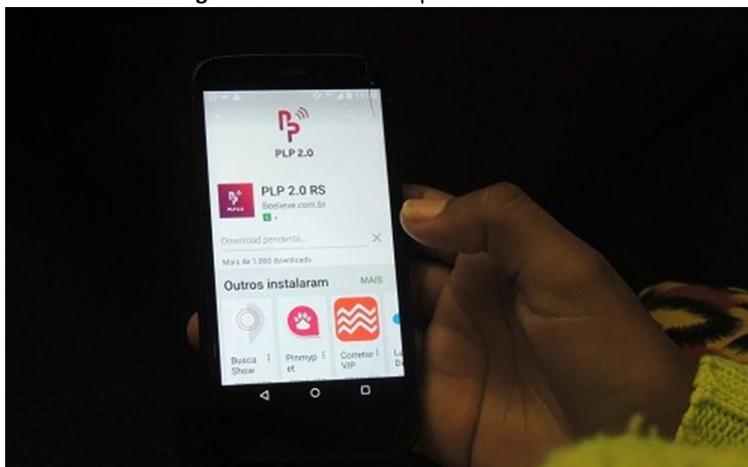
Instrumentos tecnológicos para a proteção de mulheres vítimas de violência: solução para controle da violência doméstica?

Secretaria de Segurança Pública – SSP, com o fim de tornar mais célere o atendimento nos casos de urgência.

Vale ressaltar o diferencial do Aplicativo do Rio Grande do Sul, que possui parceria com o Programa “Promotoras Legais Populares” (PLP’s). O programa de formação das PLPs é um efetivo instrumento de afirmação e disseminação dos direitos humanos das mulheres, particularmente em relação à violência doméstica e aos direitos sexuais e direitos reprodutivos. Começou na capital gaúcha, Porto Alegre, em 1993, e, 20 anos depois, está funcionando em catorze (14) municípios do Estado e em onze (11) Estados brasileiros, com a finalidade básica de conceder apoio jurídico e assistencial às mulheres vítimas de violência doméstica (SSP RS, 2017).

Com o objetivo do socorro imediato, o aplicativo PLP 2.0 utiliza a estrutura da Delegacia de Atendimento à Mulher - DEAM, Patrulhas Maria da Penha e demais volantes da Brigada Militar, para o trabalho operacional, juntando esforços para a utilização desse aplicativo como ferramenta de defesa, o que possibilita resposta imediata às cadastradas que solicitarem auxílio emergencial acionando os seus *smartphones*.

**Figura 1** – Interface do Aplicativo PLP 2.0



**Fonte:** SSP RS, 2016.

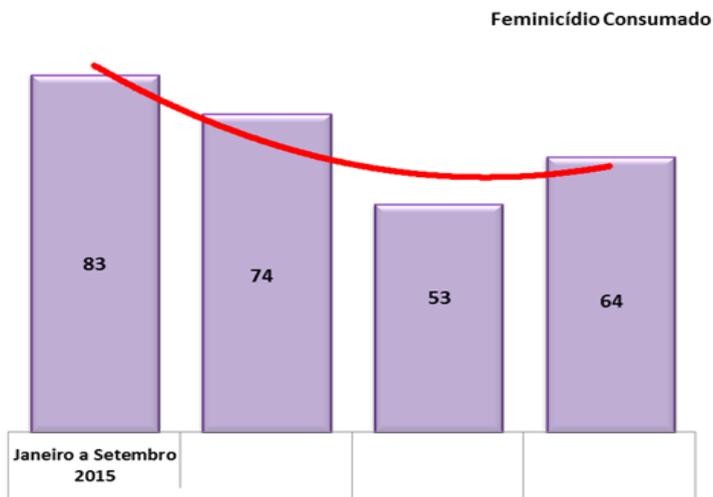
## 5 ÍNDICES DE VIOLÊNCIA ANTES DO APLICATIVO PLP

A Secretaria da Segurança Pública do Rio Grande do Sul possui uma importante ferramenta para medir os índices de violência com base nas ocorrências policiais lavradas em todo o Estado.

Trata-se do Observatório de Violência contra a Mulher, organismo que armazena, com base em ocorrências policiais, as informações que alimentam o banco de dados da Polícia Civil, processa os números ali encontrados para comparar anos, meses, dias, bem como propiciar diferentes formas de avaliação, separando os eventos por local, faixa etária, entre outros diferenciais. Assim, foram coletados dados do Observatório para elaborar o comparativo entre os períodos de janeiro a setembro de 2012 e o mesmo em 2015, na cidade de Porto Alegre, transparecendo a seguinte situação:

Registrou-se aumento nos feminicídios, os quais pularam de 53 para 64 casos (20,8%). Foram onze (11) vítimas a mais nesse período em comparação ao mesmo período do ano anterior.

**Figura 2** – Gráfico de Feminicídios antes do Aplicativo PLP 2.0



**Fonte:** Observatório de Violência contra a Mulher – Secretaria da Segurança Pública<sup>2</sup>

## **6 ÍNDICE DE VIOLÊNCIA APÓS A IMPLANTAÇÃO DO APLICATIVO PLP 2.0**

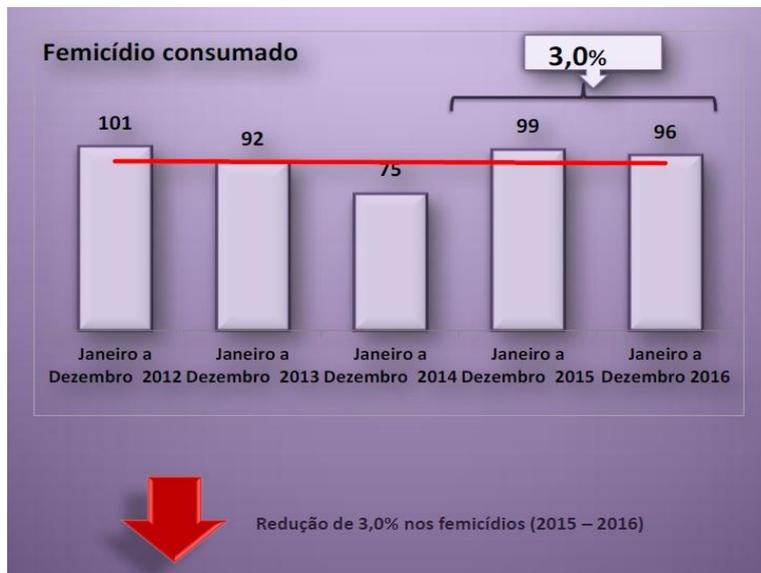
Após a implantação do aplicativo, ao final de 2015, foram inseridas mulheres vítimas de violência possuidoras das Medidas Protetivas, eis que corriam risco de vida, deferidas pela Juíza Titular da Vara de Violência Doméstica e Familiar.

Demonstrando que o recurso concedido às mulheres vítimas já inicia concretamente um serviço de proteção diferenciado, foi realizado levantamento das ocorrências policiais de Femicídios e os números apresentaram modificação.

Como pode ser observado na figura três (3), houve queda no índice de mortes, traduzido na diminuição dos Femicídios consumados, que sofreram uma redução de 99 para 96 casos (3,0%). Foram três (3)vítimas a menos em comparação ao mesmo período do ano anterior. Mesmo que pequena, esta redução traduz o sucesso da nova ferramenta tecnológica.

O esforço dos diversos parceiros, a saber, Secretaria da Segurança Pública, Central de Observação do Departamento de Comando e Controle Integrado – DCCI, Delegacia de Proteção à Mulher, Patrulhas Maria da Penha, Equipes Volantes do esforço dos diversos parceiros, a saber, Secretaria da Segurança Pública, Central de Observação do Departamento de Comando e Controle Integrado – DCCI, Delegacia de Proteção à Mulher, Equipes Volantes de Atendimento e Promotoras Legais Populares, produziu resultados positivos como aponta a estatística.

Figura 3 – Gráfico de Femicídio após o Aplicativo PLP 2.0



Fonte: Observatório de Violência contra a Mulher – Secretaria da Segurança Pública

## 7 CONCLUSÃO

O objetivo do presente artigo foi pesquisar sobre o histórico de violência sofrido por mulheres ao longo dos tempos, verificar as ferramentas tecnológicas existentes com o fim de proteção às mulheres vítimas e avaliar, por meio de estudo de caso, a utilização do aplicativo denominado PLP 2.0, criado para a proteção de mulheres agredidas, já portadoras de medidas protetivas concedidas pela Vara de Violência Doméstica e Familiar do Poder Judiciário do Estado do Rio Grande do Sul.

Assim, foram enumerados alguns dispositivos protetivos existentes no país, com características específicas em cada Estado, focando ao final no dispositivo implantado em Porto Alegre.

São visíveis as diferenças existentes entre os aplicativos implantados em outras unidades da Federação, já que utilizam *paggers* e *smartphones*, entretanto com

estrutura mais enxuta, envolvendo contato entre as Guardas Municipais e as vítimas, deslocando-se para o atendimento, de forma linear, quando acionados.

Já em Porto Alegre ocorre a reunião de vários órgãos, a Segurança Pública, por meio do DCCI, que monitora e dispara a chamada com prioridade para o atendimento às mulheres pelas Patrulhas Maria da Penha, projeto da Brigada Militar, ou por meio das viaturas volantes de atendimento emergencial que estiverem mais próximas.

Ainda, o acionamento do socorro inclui chamada para as Promotoras Legais Populares que atenderão o caso concedendo auxílio assistencial, social e psicológico às vítimas.

Assim sendo, com o Aplicativo PLP 2.0 formou-se uma rede de atendimento que inclui a DEAM, as Patrulhas Maria da Penha, as Promotoras Legais Populares (que vão acompanhar as vítimas durante os episódios de socorro) e a Secretaria da Segurança Pública que coordenará e monitorará o andamento dos atendimentos, por meio do DCCI.

Com base nas estatísticas elaboradas pelo Observatório da Violência contra a Mulher da Secretaria da Segurança Pública do Estado do Rio Grande do Sul, foi possível observar que, comparando os índices de Femicídio, antes e depois da implantação do Aplicativo PLP 2.0 houve uma concreta diminuição. E assim, três (3) vidas femininas foram poupadas. Trata-se de projeto sólido, mesmo que mais lento, que redundará em resultados concretos na diminuição dos índices da violência doméstica.

Pode-se concluir, portanto, que são positivos os resultados colhidos dos números coletados no Observatório de Violência, sendo um forte indicativo de que a tecnologia do aplicativo PLP 2.0 implantada está atingindo seus objetivos.

## REFERÊNCIAS

BRASIL. Constituição (1988). Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)>. Acesso em: 13 out. 2016.

BRASIL. Lei nº 11.340, de 7 de agosto de 2006. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_Ato2004-2006/2006/Lei/L11340.htm](https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11340.htm)>. Acesso em: 13 out. 2016.

BRASIL. Lei 13.104 de 09 de março de 2015. Disponível em: <[http://www.planalto.gov.br/CCIVIL\\_03/\\_Ato2015-2018/2015/Lei/L13104.htm](http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2015/Lei/L13104.htm)>. Acesso em: 30 mar. 2017.

G1. Londrina aprova utilização do 'Botão do Pânico' para proteger mulheres. Disponível em: <<http://g1.globo.com/pr/norte-noroeste/noticia/2013/12/londrina-aprova-utilizacao-do-botao-do-panico-para-protoger-mulheres.html>>. Acesso em 02 mar. 2017.

G1. Piauí adota botão do pânico para vítimas de violência. Disponível em: <<http://g1.globo.com/pi/piaui/noticia/2013/09/piaui-adota-botao-do-panico-para-vitimas-de-violencia-domestica.html>>. Acesso em 02 mar. 2017.

ONU. Taxa de feminicídios no Brasil é quintamais do mundo; diretrizes nacionais buscam solução. Disponível em: <<https://nacoesunidas.org/onu-femicidio-brasil-quinto-maior-mundo-diretrizes-nacionais-buscam-solucao/>>. Acesso em: 02 mar. 2017.

PORTO, Pedro Rui da Fontoura. Violência doméstica e familiar contra a mulher: Lei 11.340/06: análise crítica e sistêmica. Porto Alegre: Livraria do Advogado, 2014.

Radio Guaíba. Lançado no RS aplicativo pioneiro no combate à violência doméstica. Disponível em: <<http://www.radioguaiba.com.br/noticia/lancado-no-rs-aplicativo-pioneiro-no-combate-a-violencia-domestica/>>. Acesso em 02 mar. 2017.

SACCOL, Amarolinda Zanela. Tecnologias de informação móveis, sem fio e ubíquas: definições, estado-da-arte e oportunidades de pesquisa. Rev. adm. contemp. Vol.11, n. 4, Curitiba, oct./Dec. 2007.

SSP RS. INDICADORES DA VIOLÊNCIA CONTRA A MULHER, Relatório com dados Estatísticos entre 2012 a 2015. Resumo Indicadores de Violência contra as Mulheres e Meninas 2012 a 2015. Disponível em: <<http://www.ssp.rs.gov.br/indicadores-da-violencia-contra-a-mulher>>. Acesso em: 20 nov. 2016.

THEMIS. Promotoras Legais Populares. Disponível em: <<http://themis.org.br/fazemos/promotoras-legais-populares/>>. Acesso em 02 mar. 2017.

Instrumentos tecnológicos para a proteção de mulheres vítimas de violência: solução para controle da violência doméstica?

Vitória. Botão do Pânico busca proteger mulheres da violência doméstica. Disponível em: <<http://www.vitoria.es.gov.br/cidadao/botao-do-panico-busca-protger-mulheres-da-violencia-domestica>>. Acesso em 02 mar. 2017.

## O USO DA BIOMETRIA NO CONTROLE DAS HORAS TRABALHADAS PELOS POLICIAIS CIVIS DE SANTA CATARINA E SEUS REFLEXOS JURÍDICOS

*Thiago Marcos Ferreira  
Juarez Bento da Silva*

### 1 INTRODUÇÃO

A Polícia Civil de Santa Catarina tem como missão agir na defesa da sociedade e preservação da ordem pública, promovendo e participando de medidas de proteção à sociedade e ao indivíduo, exercendo com excelência suas atribuições, por meio da apuração de crimes e contravenções por meio da investigação criminal. A Instituição atua na segurança pública do cidadão, tendo como objetivos a garantia da segurança e bem-estar da população, imprescindíveis à efetivação do direito à segurança.

Em virtude da importância da Polícia Civil para o Estado e para a sociedade, torna-se fundamental a modernização dos sistemas que envolvam tecnologias de informação e comunicação, afinal, para evoluir, é essencial acompanhar, no que for possível, o progresso tecnológico. Conforme ensinam Oliveira *et al.* (2016, p. 43 e 44):

A segurança pública vem enfrentando uma série de problemas na atualidade. Os gestores e as autoridades constituídas não têm medido esforços no sentido de dar mais atenção a esta área, principalmente na busca por um atendimento melhor aos cidadãos e que estão sofrendo na pele a falta da prestação de um serviço qualificado. A inovação associada à Tecnologia da Informação e Comunicação (TIC) é de suma importância para o desenvolvimento de várias atividades, como as ocorridas nas

áreas industriais, de saúde, de ensino, etc., e não seria diferente na segurança pública.

A respeito das tecnologias, este trabalho traz à tona uma questão muito relevante para todos os servidores da Polícia Civil de Santa Catarina. A inovação aqui proposta passa pela implantação de um moderno sistema biométrico de controle da jornada de trabalho dos servidores.

Este estudo pretende demonstrar que o atual sistema de controle da jornada de trabalho dos servidores da Polícia Civil de Santa Catarina, que é feito por meio de relatórios em planilhas em Excel, está ultrapassado e obsoleto. Além disso, demonstrar que o uso da tecnologia dos sistemas biométricos é muito mais eficiente. A falha no controle preciso das horas trabalhadas causa prejuízos tanto para a Administração quanto para os funcionários da Instituição. Percebe-se que as planilhas nem sempre condizem com a realidade, pois podem ser facilmente adulteradas, manipuladas ou até mesmo corrompidas.

Atualmente, o método de controle é muito vulnerável e suscetível a diversas falhas, afinal, há margem para alterações ou preenchimento não tão precisos. Um funcionário poderá, por exemplo, preencher sua planilha em desacordo com a realidade para obter um saldo positivo no banco de horas e, com isso, passar a ter direito a folgas, quando na verdade não tem. As normas de controle de frequência dos servidores devem ser suficientes para que não haja atuação do servidor aquém ou além da sua jornada de trabalho estipulada por lei, sem que ocorra a devida compensação das horas faltantes ou concessão de folga para as horas trabalhadas em excesso, isto é, além das normais.

Para resolver isso, necessário se faz implantar um novo sistema de controle de horas trabalhadas que seja imune às falhas humanas, captando com absoluta precisão as horas trabalhadas pelos servidores. O controle ponto nada mais é do que uma forma utilizada para registrar as horas trabalhadas por um funcionário, bem como a quantidade de horas extras e quantas horas o funcionário tem direito a receber ao final do período de um mês. Obviamente, o sistema pode ser programado para realizar as mais diversificadas funções. Com a implantação de sistemas eletrônicos de controle de horas trabalhadas, torna-se possível gerenciar com precisão a rotina dos funcionários. Todos os registros permanecem armazenados no servidor de controle de acessos. Nesse servidor é realizado também todo o cálculo de horas trabalhadas, horas excedentes e horas faltantes de cada um dos servidores, bem como a emissão de relatórios para consultas futuras e compensação de horas.

Um dos melhores sistemas existentes é o biométrico, que utiliza uma tecnologia de ponta, praticamente imune às falhas, capaz de emitir relatórios precisos ao final de cada mês. Primeiramente, é feito o cadastro biométrico para cada um dos funcionários, que passarão a ter contabilizados com exatidão aqueles minutos de chegada com antecedência ou atraso, que geralmente passam despercebidos em outros sistemas de controle. É extremamente benéfico para todos, tanto os funcionários quanto os diretores, pois é possível auferir produtividade, qualidade, assiduidade, pontualidade, inclusive para seleção de candidatos a processo promocional por merecimento.

Outro benefício em curto prazo que já se pode observar com a implantação desse novo método de controle de jornada de trabalho é o desafogamento da Gerência responsável pela Gestão de Pessoas, que é o setor responsável pela conferência, envio e todo manejo das planilhas de horas dos servidores. As secretarias das delegacias regionais de polícia, onde são centralizadas as planilhas antes do envio para o setor de Gestão de Pessoas, também terão seus processos potencializados, uma vez que não precisarão mais fazer o controle regionalizado das planilhas. Mais um aspecto favorável abordado no trabalho é o jurídico, uma vez sendo notáveis os avanços a partir da mudança na forma de realizar o controle da jornada de trabalho. Hoje em dia, muitas ações tramitam no judiciário catarinense pleiteando direitos conhecidos como trabalhistas, sendo a cobrança de pagamento de horas extras a ação mais comum. Caso haja um sistema biométrico de controle de ponto, a produção de provas por parte da administração será facilitada, pois será necessário apenas imprimir as informações constantes nos relatórios eletrônicos de horas trabalhadas.

Por esses motivos, e também pela facilitação, agilidade no controle, praticidade, custo-benefício, é que se torna imprescindível a substituição do atual precário, impreciso e falho sistema de controle de horas trabalhadas por meio de planilhas, por um sistema mais moderno, eficaz, que garanta a todos o respeito aos deveres e direitos trabalhistas. Para tal, é descrito na seção 2 os procedimentos metodológicos utilizados para realização do presente estudo. Nas seções 3, 4 e 5 relatam-se, respectivamente, sobre o uso da biometria, jornada de trabalho e controle de horas trabalhadas pelos policiais civis de Santa Catarina, e sistema biométrico de controle de horas trabalhadas. Os aspectos jurídicos relevantes são identificados na seção 6, sendo posteriormente apresentadas as considerações finais na seção 7.

## 2 PROCEDIMENTOS METODOLÓGICOS

A forma de pesquisa apresentada como base deste trabalho é a exploratória-descritiva, pois é feito um grande diagnóstico, análise e descrição do atual sistema de controle de horas trabalhadas. A pesquisa exploratória estabelece critérios, métodos e técnicas para a elaboração de uma pesquisa e visa oferecer informações sobre o objeto desta e orientar a formulação de hipóteses (CERVO; BERVIAN; SILVA, 2007). Os estudos exploratórios buscam descobrir ideias e intuições na tentativa de obter maior conhecimento com o fenômeno pesquisado.

No estudo aqui proposto, a pesquisa exploratória está presente por haver uma necessidade de ampliar a familiarização do tema abordado pelo pesquisador, já que imprescindível se faz o aprimoramento de ideias em busca de novas respostas, visando identificar também as causas dos problemas pesquisados.

A finalidade da pesquisa descritiva é observar, registrar e analisar os fenômenos ou sistemas técnicos, sem, contudo, entrar no mérito dos conteúdos. Na pesquisa descritiva realiza-se o estudo, a análise, o registro e a interpretação dos fatos do mundo físico sem a interferência do pesquisador (BARROS; LEHFELD, 2007).

Trazendo à realidade do trabalho aqui desenvolvido, a pesquisa descritiva é utilizada para demonstrar as variáveis do objeto de estudo, que é o controle da jornada de trabalho. Utilizando esse método, é possível descrever as mudanças vislumbradas com as implantações a serem feitas, além de possibilitar uma vasta visão acerca das mudanças nos processos.

Pode-se afirmar também que foi utilizada a pesquisa bibliográfica, já que foram pesquisados materiais já publicados, principalmente livros, artigos científicos e outros materiais disponibilizados na internet. Nesse processo permanente de pesquisa, julgou-se fundamental aplicar o procedimento bibliográfico de pesquisa, uma vez que para delimitar os critérios e assuntos a serem abordados, foi de extrema importância estudar artigos, livros e trabalhos já publicados sobre o tema aqui abordado.

Ainda quanto aos objetivos, a pesquisa é também explicativa. A pesquisa explicativa registra e analisa fatos, realiza a interpretação e estuda suas causas. Esse método visa ampliar conceitos, estruturar e contextualizar modelos teóricos, relacionando hipóteses em uma visão mais sistêmica do objeto de estudo em geral, formulando hipóteses e ideias. Conforme ensina Gil (1999), a pesquisa explicativa tem como objetivo básico a identificação dos fatores que determinam ou que

contribuem para a ocorrência de um fenômeno. É o tipo de pesquisa que mais aprofunda o conhecimento da realidade, pois tenta explicar a razão e as relações de causa e efeito dos fenômenos. Esse tipo de pesquisa visa estabelecer relações de causa-efeito por meio da manipulação direta das variáveis relativas ao objeto de estudo, buscando identificar as causas do fenômeno. Normalmente, é mais realizada em laboratório do que em campo (MARCONI; LAKATOS, 2003).

Por ser uma pesquisa estritamente teórica, que visa aprofundar o conhecimento na área de estudo, entende-se que é a partir do momento em que se conhece a razão da utilização do atual sistema de controle de jornada que podem ser identificadas as variáveis do processo e também a relação entre essas variáveis, estabelecendo uma relação de causa e efeito.

Quanto à abordagem, a pesquisa qualitativa se mostra presente na comparação da eficácia dos métodos de controle atuais e o sugerido neste trabalho. Segundo Trivinos (1996), a abordagem qualitativa trabalha os dados buscando seu significado, tendo como base a percepção do fenômeno dentro do seu contexto. O uso da descrição qualitativa procura captar tanto a aparência do fenômeno como também suas essências, procurando explicar a origem, as relações e as mudanças, tentando prever as consequências. Quem utiliza esse método busca explicar o porquê das coisas, exprimindo o que convém ser feito, valendo-se de diversas abordagens, uma vez que com os dados analisados procura produzir novas informações.

Por fim, é preciso observar que a pesquisa também é participante, afinal, caracteriza-se pelo envolvimento e identificação do pesquisador. A pesquisa participante foi criada por Bronislaw Malinowski: para conhecer os nativos das ilhas Trobriand, ele foi se tornar um deles. Rompendo com a sociedade ocidental, montava sua tenda nas aldeias que desejava estudar, aprendia suas línguas e observava sua vida cotidiana (FONSECA, 2002).

### **3 O USO DA BIOMETRIA**

A biometria, antes de tudo, refere-se a uma ciência responsável por analisar características biológicas. É responsável por estudar as medidas e estatísticas quantitativas dos seres humanos. Características biométricas são encontradas em várias partes do corpo humano e também no comportamento humano, como exemplo: face, voz, palma da mão e dedos, olhos, retina e íris, geometria das mãos,

dentre outras. Até mesmo gêmeos univitelinos possuem tais características distintas um do outro (HISTÓRIA... 2018). Aliada às tecnologias existentes na atualidade, a biometria ainda tem seus limites de aplicação desconhecidos, uma vez que é vasto o campo de atuação disponível para investimentos nessa área.

Cada vez mais a biometria vem se popularizando e sendo muito utilizada em negócios e no cotidiano, principalmente na área de segurança. Esse crescente campo tecnológico está se tornando parte integrante do dia-a-dia das pessoas, pois cada ser humano é único e possui características distintas, o que assegura a legitimidade de identificação. Nessa lógica de sistemas modernos, a biometria substitui as já ultrapassadas senhas numéricas ou criptografas. O próprio corpo se torna a senha para ingressar em determinada sala, acessar determinada informação ou até mesmo registrar o horário de chegada e saída insuscetível de fraudes ou erros.

No exterior, há alguns anos os Estados Unidos da América implantou sistemas de biometria no combate ao terrorismo. As autoridades coletaram dados biométricos de todos os presos e também de cidadãos comuns em países como Afeganistão e Iraque, além de outros envolvidos com o terror (EUA... 2010). No Brasil, o governo federal, por meio do Tribunal Superior Eleitoral já realizou o cadastro de grande parte dos eleitores para que utilizem o sistema biométrico de impressão digital nas votações. No país, também podem ser facilmente encontrados em caixas eletrônicos de instituições bancárias, aeroportos, empresas e até mesmo clubes sociais.

Em Santa Catarina, o governo já implantou o sistema biométrico em diversos órgãos, tais como o Instituto Geral de Perícias, que desde o ano de 2014, confecciona a Carteira de identidade com a nova tecnologia biométrica de impressão digital

Os sistemas biométricos capturam características do indivíduo em sinais analógicos ou digitais por meio de interfaces homem-máquina, codificam as informações e armazenam para análise computacional (ABDI, 2010). A finalidade da utilização dos sistemas com tecnologia biométrica é assegurar a inviolabilidade e prevenir possíveis fraudes na autenticação de usuários, seja restringindo acessos ou controlando horários e pessoas.

#### **4 JORNADA DE TRABALHO E CONTROLE DE HORAS TRABALHADAS PELOS POLICIAIS CIVIS DE SANTA CATARINA**

O método utilizado atualmente para controlar as horas trabalhadas pelos servidores da Polícia Civil catarinense é o de relatórios em planilhas em um *software* chamado *Excel*, da fabricante *Microsoft*. Os modelos padrões das planilhas são encaminhados pelo setor de Gestão de Pessoas às secretarias das Delegacias Regionais de Polícia, as quais têm a incumbência de distribuir a todas as delegacias de sua região, bem como cobrar o preenchimento e envio até o último dia do mês de trabalho.

Os relatórios são preenchidos diariamente pelos servidores e, até o segundo dia útil do mês subsequente, devem ser encaminhados ao chefe imediato para análise e posteriormente, enviados por *e-mail* para a secretaria da Delegacia Regional, onde é feita uma conferência para minimizar equívocos de preenchimento e, por fim, devolvidos ao setor de Gestão de Pessoas. No destino final, as planilhas passam por uma nova revisão e então são inseridas as horas extras em outra planilha, chamada de banco de horas, que é encaminhada mensalmente às Delegacias Regionais, a fim de tornar possível um planejamento da folga daqueles policiais que tenham direito de usufruí-la, já que trabalharam horas a mais no mês anterior.

Apenas com essa descrição do processo de recebimento, preenchimento, envio, conferência, retorno e fruição, é possível concluir que as chances de algo dar errado são enormes, além do tempo que leva para resolver todas as burocracias, bem como a exorbitante quantidade de servidores que gastam horas realizando a mesma tarefa.

Estima-se que atualmente o quadro de servidores efetivos ativos da Polícia Civil catarinense seja de quatro mil pessoas, distribuídas em trinta regionais. Para cada servidor, uma planilha por mês (POLÍCIA... 2017). O número de folhas gastas com as planilhas, somadas ao tempo que cada um leva para preenchê-las e ainda a necessidade de retorno para cada regional para conferência e depois uma nova conferência pelo setor de Gestão de Pessoas, torna esse método um tanto burocrático, além de estar ultrapassado tecnologicamente. É preciso insistir também no fato de que o livre preenchimento das planilhas por parte dos servidores não impede que haja manipulação das informações ali constantes, o que pode gerar

prejuízos tanto para os cofres públicos, quanto para os servidores, dependendo, é óbvio, do tipo de adulteração.

Quando se trata de interesse público, pode-se afirmar que ele é indisponível, ou seja, não se pode correr o risco de quem quer que seja se beneficiar ilegalmente em detrimento do interesse coletivo. A indisponibilidade do interesse público é um princípio jurídico basilar da administração pública, previsto na Constituição Federal, que preceitua que uma vez caracterizado o interesse público, não pode a administração dispor dele.

## **5 SISTEMA BIOMÉTRICO DE CONTROLE DE HORAS TRABALHADAS**

Inicialmente, pode-se afirmar que há sistemas biométricos de controle de ponto para cada tipo de biometria existente. O mais usual e comum é o de impressão digital, tanto pelo custo-benefício quanto pela confiança dos dados obtidos. Para decidir por um ou outro sistema deve-se fazer uma análise da instituição em diversos aspectos, levando em conta o número de funcionários, o fluxo de entrada e saída, além de possível movimentação de funcionários em diferentes locais ou cidades durante a jornada de trabalho.

Por isso, para a Polícia Civil catarinense, por ser uma Instituição com uma grande quantidade de pessoas em seu quadro de servidores, além de ter grande movimentação de servidores em diferentes cidades ao longo de um dia de trabalho, o sistema biométrico mais adequado para dar total suporte e garantir segurança é o de impressão digital. Os sistemas biométricos de impressão digital são os mais antigos e estão em constantes mudanças e inovações. Além de serem simples, são também sistemas que possuem tradição de uso, principalmente pelas polícias.

Esse sistema de controle de ponto biométrico é um dos mais modernos existentes na atualidade, impossibilitando qualquer tipo de fraude ou alteração de dados. O gerenciamento do sistema é previamente programado pelo fabricante do *software*, de acordo com a necessidade da Instituição, ou seja, é possível emitir relatórios completos com dados sobre o total de horas trabalhadas, horas-extras, feriados, faltas, adicional noturno, compensação de horas, banco de horas etc. O principal requisito do sistema é a realização de um pré-cadastro de todos os usuários, afinal, para reconhecer a impressão digital, é imprescindível haver um banco de dados contendo todas as informações dos usuários no sistema.

## 6 ASPECTOS JURÍDICOS RELEVANTES

A Polícia Civil do Estado de Santa Catarina possui atribuições previstas na Constituição Federal e na Constituição Estadual. Suas principais funções são exercer as funções de polícia judiciária, apurar as infrações penais no âmbito do território estadual, manter serviços diurnos de atendimento aos cidadãos, fiscalizar jogos e diversões públicas, proteger pessoas e bens e os direitos e garantias individuais. É comandada pelo Delegado Geral de Polícia, e desenvolve os serviços de sua competência no âmbito das quatrocentas e cinquenta nove delegacias de polícia distribuídas em praticamente todas as cidades do Estado, divididas em trinta regionais (POLÍCIA ...2017). A Polícia Civil de Santa Catarina é composta por Delegados, Agentes, Escrivães e Psicólogos policiais. Cada servidor ativo no quadro institucional deve obrigatoriamente cumprir uma carga horária semanal de quarenta horas, estipulada pela Lei Complementar n.º 453, de 05 de agosto de 2009.

Com relação à jornada de trabalho, convém notar que a Lei Complementar n.º 609, de 20 de dezembro de 2013, instituiu providências acerca da regulamentação do banco de horas dos servidores da Polícia Civil. Em 31 de julho de 2015, o Governador do Estado adotou a Medida Provisória n.º 203, que dispõe sobre as formas de cumprimento da jornada de trabalho e o banco de horas no âmbito da Polícia Civil do Estado de Santa Catarina. Por jornada de trabalho, entende-se o espaço de tempo durante o qual o servidor deve prestar serviço ou ficar à disposição do empregador.

A forma de cumprimento da jornada de trabalho e do banco de horas foi definida finalmente pela Lei Estadual n.º 16.774, de 30 de novembro de 2015. O texto legal define os critérios para controle da jornada de trabalho dos Policiais Civis. O artigo 6º, §4º, assim dispõe: “Deverá ser encaminhado à Delegacia-Geral da Polícia Civil relatório mensal discriminado da jornada de trabalho individual a ser cumprida pelos policiais civis de cada unidade na forma estabelecida neste artigo”. Cumpre examinar os benefícios jurídicos que a implantação do sistema de controle biométrico da jornada de trabalho trará para o Estado e para os servidores.

No âmbito do Direito Trabalhista, inúmeras ações deixarão de ser ajuizadas em face do Estado cobrando por horas trabalhadas e não pagas ou não usufruídas em forma de folga (banco de horas). Atualmente, muitas ações tramitam no Judiciário catarinense cobrando horas extras não pagas pelo Estado. Do mesmo modo, adicionais noturnos também são cobrados. Com o sistema biométrico implantado, ocorrerá uma redução nas demandas instauradas, tendo em vista que o

sistema captura com precisão as horas trabalhadas pelo respectivo servidor, já que as horas são aferidas eletronicamente. Ademais, o Estado também não sofrerá prejuízos relacionados àqueles servidores que possivelmente preenchem a planilha com horas a mais do que as efetivamente trabalhadas.

Sob outro enfoque, o aumento na assiduidade dos funcionários será enorme, pois será mais fácil detectar possíveis tentativas de fraudes por parte de servidores e punir aqueles que cometerem faltas injustificadas, responsabilizando administrativa, civil e criminalmente aqueles que não cumprirem a legislação. O sistema a ser implantado só trará benefícios para instituição, uma vez que se trata de um método de segurança para o servidor e para própria instituição que fiscalizará com mais rigor a jornada de trabalho de seus funcionários, sendo que eles terão ciência das horas efetivamente trabalhadas.

## **7 CONSIDERAÇÕES FINAIS**

A cada dia a biometria está se tornando um recurso valioso para identificação e reconhecimento de pessoas, pois se trata de uma técnica acessível, segura e confiável. Várias entidades de segurança, por todo o mundo, públicas e privadas, estão empenhadas na utilização da biometria na área de segurança, tanto no controle de acesso, quanto na identificação de usuários do sistema.

O trabalho analisou o atual método de controle da jornada de trabalho dos servidores da Polícia Civil de Santa Catarina, procurou avaliar sua eficácia e características e também demonstrou as suas principais falhas. Além disso, sugeriu-se a substituição do atual método de controle por um sistema moderno, já utilizado na maioria das empresas do setor privado, que é o biométrico, cujas horas trabalhadas são registradas eletronicamente.

Demonstrou-se a necessidade de modernização do sistema de controle de jornada de trabalho dos policiais civis de Santa Catarina, apontando que as planilhas em *Excel* estão ultrapassadas e já não são suficientemente seguras a ponto de garantir total eficácia da apuração e veracidade dos dados obtidos. Comprovou, com base nas tendências e recentes aquisições do Governo do Estado de Santa Catarina, que sistemas biométricos já estão sendo utilizados em diversos setores da área de Segurança Pública, sendo possível almejar sua implantação no controle da jornada de trabalho dos servidores da Polícia Civil catarinense.

Com a implantação de sistemas biométricos de controle de horas trabalhadas, por impressão digital, torna-se possível gerenciar com precisão a rotina dos funcionários. Todos os registros permanecem armazenados no servidor de controle de acesso. Nesse servidor é realizado também todo o cálculo de horas trabalhadas, horas excedentes e horas faltantes de cada um dos servidores, bem como a emissão de relatórios para consultas futuras e compensação de horas. É extremamente benéfico para todos, tanto para os funcionários quanto para a administração pública, pois é possível auferir produtividade, qualidade, assiduidade, pontualidade, inclusive para seleção de candidatos a processo promocional por merecimento.

Por esses motivos, e também pela facilitação, agilidade no controle, praticidade, custo-benefício é que se torna imprescindível substituir o atual precário, impreciso e falho sistema de controle de horas trabalhadas por meio de planilhas, por um sistema mais moderno, eficaz, que garanta a todos o respeito aos deveres e direitos trabalhistas.

## REFERÊNCIAS

ABDI – Agência Brasileira de Desenvolvimento Industrial. **Sistemas Aplicados à Segurança Pública. Cadernos Temáticos – Tecnologias de Informação e Comunicação (TIC)**. Brasília: ABDI, 2010. Disponível em: <[http://www.abdi.com.br/Estudo/Caderno %20Tem%C3%A1tico%20TIC%20-%203%20\(Vers%C3%A3o%20Final\)-%20Sistemas%20Aplicados%20a%20Seguran%C3%A7a%20Publica.pdf](http://www.abdi.com.br/Estudo/Caderno%20Tem%C3%A1tico%20TIC%20-%203%20(Vers%C3%A3o%20Final)-%20Sistemas%20Aplicados%20a%20Seguran%C3%A7a%20Publica.pdf)>. Acesso em 24 de abr. 2017.

BARROS, Aidil Jesus Paes; LEHFELD, Neide Aparecida de Souza. **Fundamentos da Metodologia Científica**. 3. ed. São Paulo: Makron, 2007.

CERVO, Amado Luís; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

**EUA avançam nas técnicas de biometria para combater terrorismo**. 2010. Disponível em: <<http://idgnow.com.br/seguranca/2010/09/24/eua-avancam-nas-tecnicasde-biometria-para-combater-terrorismo/>>. Acesso em: 02 fev. 2017.

FONSECA, João José Saraiva. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas, 1999.

**HISTÓRIA Geral da Biometria.** Disponível em: <<http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=25030>>. Acesso em: 14 fev. 2018.

MARCONI, Maria de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

OLIVEIRA, Joel Souza de ; GRUBER, Vilson; MARCELINO, Roderval; LUNARDI, Giovani Mendonça; "As Tecnologias da Informação e Comunicação na Gestão Administrativa e Operacional da Segurança Pública", p. 43-54 . In: **SPANHOL, Fernando José; LUNARDI, Giovani Mendonça; SOUZA, Márcio Vieira de. (orgs.) Tecnologias da Informação e Comunicação na Segurança Pública e Direitos Humanos**. São Paulo: Blucher, 2016.

POLÍCIA Civil do Estado de Santa Catarina. 2017. Disponível em: <<http://www.pc.sc.gov.br/institucional/policia-civil>>. Acesso em: 14 fev. 2018.

SANTA CATARINA, **Lei Complementar n.º 453, de 05 de agosto de 2009**. Institui Plano de Carreira do Grupo Segurança Pública - Polícia Civil, e adota outras providências.

SANTA CATARINA, **Lei n.º 16.774, de 30 de novembro de 2015**. Dispõe sobre as formas de cumprimento da jornada de trabalho e o banco de horas no âmbito da polícia civil do Estado de Santa Catarina e estabelece outras providências.

TRIVIÑOS, Augusto Nivaldo Silva. Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação. O positivismo. A fenomenologia. O marxismo. São Paulo: Atlas, 1996.

---

## FERRAMENTAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NA SEGURANÇA PÚBLICA: UMA ANÁLISE SOBRE O PORTAL SINESP E SUAS FERRAMENTAS

*Vladmir Braga de Lima  
Paulo Cesar Leite Esteves*

### 1 INTRODUÇÃO

Conforme descreve Vitor Marques em seu artigo “A Importância da Tecnologia da Informação” (MARQUES, 2014), atualmente as Tecnologias da Informação e Comunicação (TIC) participam ativamente do cotidiano dos mais variados tipos de organizações, às vezes como eficientes armas de gestão da informação e apoio às decisões, às vezes como ferramentas que facilitam a otimização de serviços, o que anteriormente centralizava-se apenas em mão de obra humana. Partindo dessa premissa, observa-se que com as instituições de Segurança Pública, esse panorama não é diferente, visto que, cada vez mais as TIC têm se mostrado como fortes aliadas na realização de serviços e procedimentos nessa área de extrema importância para a população.

É importante destacar, também, que a utilização das TIC contribui de forma significativa para uma gestão eficaz dos órgãos e instituições de Segurança Pública, tornando-os cada vez mais eficientes. Nesse viés, Peter Drucker em seu livro “*Managing for Results: Economic Tasks and Risk-taking Decisions*” (DRUCKER, 1964), informa que a eficiência consiste em fazer certo as coisas e geralmente estará ligada ao nível operacional, como a realização de operações com menos recursos, menos tempo, menor orçamento, menos pessoas, menos matéria-prima etc. Já a eficácia consiste em fazer as coisas certas, frequentemente relacionada ao nível gerencial (DRUCKER, 1964).

Descreve ainda em seu artigo, o autor Vitor Marques (MARQUES, 2014), que a velocidade com que a informação e o conhecimento circulam sem fronteiras, potencializam a importância do capital intelectual. Dentro dessa ótica, constata-se que as instituições que investem em Tecnologia da Informação e Comunicação, especificamente, no caso da Segurança Pública, certamente estarão à frente quanto a futuras ações a serem desempenhadas, bem como a prevenção e a antecipação ao cometimento de delitos, ressaltando ainda mais a importância da inserção das TIC nesse cenário.

Nesse viés, o presente trabalho visa, a partir do entendimento sobre a importância da inserção das TIC no cenário das instituições de Segurança Pública, analisar a utilização dessas ferramentas na Segurança Pública. Como fonte desta pesquisa descritiva foram explicitadas na seção 2 deste artigo algumas ferramentas de TIC utilizadas na segurança pública, como o Sistema Nacional de Informações de Segurança Pública, Prisional e sobre Drogas (SINESP ou Portal Sinesp), da Secretaria Nacional de Segurança Pública do Ministério da Justiça (SENASP/MJ), destacando entre elas o Sinesp Cidadão, Sinesp Seguro, Sistema Nacional de Estatística de Segurança Pública e Justiça Criminal (SINESPJC), e o Sistema de Informações sobre Gabinetes de Gestão Integrada (INFOGGI). Após descrição de tais sistemas, encerra o presente estudo com as considerações finais na seção 3.

## **2 FERRAMENTAS DE TIC NA SEGURANÇA PÚBLICA**

### **2.1 Portal Sinesp**

Instituído pelo Governo Federal por meio da Lei 12.681 (BRASIL, 2012), e regulamentado pelo Decreto 8.075 (BRASIL, 2013), o Sistema Nacional de Informações de Segurança Pública é um portal de informações integradas que possibilita consultas operacionais, investigativas e estratégicas, com informações sobre drogas, segurança pública, justiça, sistema prisional, entre outras. Esse portal foi implementado em parceria com os entes federados com o objetivo de subsidiar a realização de diagnósticos sobre criminalidade, formular e avaliar políticas públicas, promover uma comunicação segura e padronizada, integrando nacionalmente as informações, trazendo com isso maior confiabilidade ao processo de coleta, tratamento, análise e divulgação dessas informações.

A base de dados estatísticos do Portal Sinesp é alimentada por meio do sistema SINESPJC, o qual foi implantado no ano de 2004 pela SENASP com o objetivo de efetivar a coleta de dados criminais, atividades policiais e de bombeiros, registradas pelas polícias militares e civis dos entes federados. Com isso, conforme explica o vídeo disponibilizado pelo “Canal Sinesp Seguro” por meio do *website* “YouTube” (SINESP SEGURO, 2014), foi possível obter como solução de procedimentos policiais, uma tecnologia que faz a integração nacional, de sistemas já informatizados ou não, entre as instituições. Por intermédio dessa tecnologia, os dados e informações são compartilhados nacionalmente, facilitando consultas integradas no Portal Sinesp e otimizando recursos no combate sistemático da criminalidade.

É importante enfatizar que ainda hoje são utilizados procedimentos manuais para o envio de dados, porém, assim que todos os entes federados tiverem suas bases de dados diretamente integradas ao Sinesp, o processo de coleta por meio do SINESPJC deixará de ser utilizado.

De acordo com o *website* de acesso público do Portal Sinesp (PORTAL SINESP, 2012), os dados estatísticos coletados pelos estados devem ser enviados e corrigidos no período máximo de 90 dias, sendo 60 dias para envio e 30 dias para as correções. Exemplificando: os dados coletados de janeiro de 2017 devem ser enviados até o dia 31 de março do mesmo ano, tendo ainda até o dia 30 de abril para que sejam feitas as devidas correções. Após se passarem os 90 dias, os entes federados ainda poderão enviar os dados coletados, porém, com pena de responderem como “inadimplentes” no que se refere à cláusula 4ª do “Termo de Adesão ao Sinesp” (ALERGS, 2013, p. 2). Caso os entes federados não consigam enviar os dados coletados no período de 90 dias, ainda assim terão a possibilidade de efetuar o envio tardio, porém, esse fato prejudicará a distribuição de recursos do Governo Federal referentes à área da segurança pública, aos entes federados. Isso deve-se ao fato de que os recursos que serão disponibilizados para a celebração de convênios entre União, Estados e Distrito Federal, baseiam-se em índices e cálculos obtidos mediante os dados enviados.

Como forma de melhorar a gestão dos serviços e obter maior consistência nos relatórios gerados a partir dos dados coletados pelos entes federados, foram designados alguns servidores, indicados e nomeados pelos Secretários Estaduais de Segurança Pública e Defesa Social, como “Gestores do Sinesp”, sendo que cada Unidade da Federação, possui três gestores com seus respectivos suplentes, os quais

atuam nas áreas de Estatística e Análise Criminal, Inteligência e Tecnologia da Informação.

Atualmente, a base de dados estatísticos do Sinesp é alimentada apenas pelo envio de dados das polícias civil e militar. Contudo, como Sinesp é um sistema modular, espera-se que com o passar do tempo, novas instituições integrem o sistema e com isso iniciem o processo de envio dos seus dados.

Quanto à validação dos dados enviados pelos entes federados, esse processo é feito através da SENASP, a qual extrai esses dados periodicamente, para validação e geração de relatórios e estatísticas. Cabe ao gestor estadual do Sinesp, ao observar qualquer inconsistência nas informações enviadas, realizar uma análise mais detalhada, e caso for necessário, aplicar as devidas medidas corretivas.

Cabe ainda destacar, que os relatórios do Sinesp não trazem as informações do ano atual, devido ao fato de que o processo de alimentação da base de dados é feito pelas Unidades Federativas e órgãos parceiros. Sendo assim, se faz necessário considerar o período de envio, tratamento e análise desses dados, antes de qualquer divulgação, evitando com isso a publicação de dados inconsistentes. Atualmente, esses relatórios só disponibilizam dados e informações de municípios, independente da sua população, e do Brasil como um todo, não sendo possível gerar relatórios por bairros, quadras ou outras regiões, pois a atual base de dados utilizada pelo Sinesp, impossibilita a geração de relatórios mais detalhados. Essa mudança na geração de relatórios, alcançando todos os municípios, bairros e suas regiões, deverá ocorrer assim que os sistemas dos entes federados estejam totalmente integrados ao Sinesp. Cabe destacar também, que os dados criminais disponibilizados pelo Sinesp são os mesmos divulgados no Anuário Brasileiro de Segurança Pública (ABSP).

O Portal Sinesp conta ainda com os seguintes módulos: “Sinesp Segurança”, sistema responsável pela gestão, autenticação e controle de acesso de usuários, “Sinesp Auditoria”, para gestão e auditoria de transações, nesse caso consulta e atualização de dados dos sistemas Sinesp, o “Sinesp CAD”, sistema de apoio às centrais de atendimento e despacho das forças policiais e o “SinespPPE”, sistema de informações de apoio às delegacias, na gestão dos procedimentos policiais de maneira eletrônica.

Deve-se salientar que, devido à sua importância e complexidade, foram expostas neste trabalho apenas as ferramentas: Sinesp Cidadão, como forma de integração da Segurança Pública com a comunidade, Sinesp Seguro, como

ferramenta de inteligência policial, SINESPJC como sistema de coleta e tratamento de dados estatísticos, e o INFOGGI, como sistema de gestão e auxílio aos Gabinetes de Gestão Integrada, além do Portal Sinesp já detalhado.

## 2.2 Sinesp Cidadão

Como iniciativa do Governo Federal, e com o objetivo de aproximar o cidadão da Segurança Pública do país de maneira direta e objetiva, foi criado o Sinesp Cidadão. O Sinesp Cidadão é uma das principais ferramentas de TIC do Portal Sinesp, pois permite o acesso aos serviços disponibilizados pela SENASP à toda população, possibilitando que o usuário efetue consultas tanto por meio do acesso *web* através do Portal Sinesp (SINESP CIDADÃO, 2016). Nesse caso, somente consultas de situação de legalidade das placas de veículos, conforme pode ser observado, a seguir, na Figura 1 (um), bem como por meio de um aplicativo para dispositivos móveis, o qual é mais usual e possui mais funcionalidades, ilustrado na Figura 2 (dois).

Figura 1 - Tela de acesso *Web* ao Sinesp Cidadão.

O aplicativo Sinesp Cidadão é um módulo do Sistema Nacional de Informações de Segurança Pública - Probanis e sobre Dragan, o Sinesp (Lei 12.881/2012), o qual permite acessar direto pelo cidadão aos serviços do Secretariado Nacional de Segurança Pública do Ministério da Justiça.

O Sinesp Cidadão é composto por dois módulos:

**01 - Consulta Veículos** permite ao cidadão consultar a situação de registro ou furto de qualquer veículo do Brasil. As informações são consultadas diretamente no banco de dados do Departamento Nacional de Trânsito (DENATRAN), conforme parâmetros estabelecidos no site e o Ministério da Justiça.

Após instalar o aplicativo, basta clicar no ícone "Veículos" e digitar a placa para saber a situação do veículo. Caso a resposta seja positiva para furto ou roubo, a informação "VEÍCULO HURTADO/ROUBADO" aparecerá destacada em vermelho na tela de seu smartphone. É possível verificar também se o veículo é clonado, caso as características do mesmo não correspondam ao registrado pelo aplicativo.

**02 - Consulta Mandado de Prisão:** assegura o direito ao cidadão de consultar os mandados de prisão aguardando cumprimento e vigentes, com a finalidade de acionar a polícia. As informações são consultadas no Banco Nacional de Mandados de Prisão (BNMP) do CNJ, graças a parceria entre este órgão e o Ministério da Justiça.

Para consulta via web, maiores detalhes da consulta e acesso à emissão da certidão, será necessário acessar o Portal do CNJ: <http://www.cnj.gov.br/portal>. Se será possível gerar uma certidão dos mandados que estejam aguardando cumprimento e vigentes. A certidão na conter data e hora em que foi gerada.

Em caso de dúvida, ou mais informações, encaminhar e-mail para [sistemas@cnj.gov.br](mailto:sistemas@cnj.gov.br)

**03 - Consulta de Mandado de Prisão:** O Sinesp Cidadão e o CNJ não se responsabilizam pelas informações contidas nos mandados de prisão encaminhados, a base de dados do CNJ é somente um repositório dessas informações, que são geradas pelos Tribunais. Em caso de dúvidas referentes a um mandado, procurar o órgão expedidor.

**Vale destacar que para os casos de retorno por meio para o registro de veículo ou para a renovação de prazo, o cidadão deverá informar imediatamente a polícia através do telefone 190 e não tentar qualquer tipo de autuação como a aproximação ou a abordagem por conta própria.**

**04 - Consulta de Mandado de Prisão:** O aplicativo é voltado para o uso do cidadão, desde modo, os profissionais de segurança pública não podem restringir suas pesquisas somente ao aplicativo. Sugere-se continuar as informações em outras fontes, como Diários, Integros, Tribunais de Justiça e etc...

O Sinesp Cidadão foi desenvolvido em parceria com o Serviço Federal de Processamento de Dados (SERPRO).

Secretaria Nacional de Segurança Pública | Ministério da Justiça | Subdivisão SERPRO

Fonte: [www.sinesp.gov.br/sinesp-cidadao](http://www.sinesp.gov.br/sinesp-cidadao) (2016)

Figura 2- Telas dos Módulos de Consultas do Sinesp Cidadão.



Fonte: Aplicativo Sinesp Cidadão (2016).

O Sinesp Cidadão é composto atualmente por três módulos de consultas, sendo eles, módulo de consultas de veículos, mandado de prisão e desaparecidos. Esses módulos são disponibilizados à população por intermédio de um aplicativo para dispositivos móveis, o qual pode ser adquirido gratuitamente nas principais lojas de aplicativos para *smartphones*, como “Google Play”, “AppStore” e “Windows Store”, após instalado no dispositivo, e estando conectado à internet, já se faz apto para a realização de consultas. Segue abaixo, a explicação dos respectivos módulos:

**Módulo 1 - Veículos:** permite que o cidadão efetue consultas sobre as situações de furto ou roubo de qualquer veículo do Brasil. Essas consultas trazem informações como marca, modelo, cor, ano e parte do chassi do veículo, possibilitando, ainda, saber se o veículo consultado é clonado. As informações são consultadas diretamente na base de dados do Departamento Nacional de Trânsito (DENATRAN), atualizada pelos Departamentos Estaduais de Trânsito (DETRAN), com base nos boletins de ocorrência (BO), registrados nas delegacias de Polícia Civil.

**Módulo 2 - Mandado de Prisão:** assegura ao cidadão o direito de consultar os mandados de prisão vigentes e aguardando cumprimento, tendo como finalidade o auxílio às forças policiais. As consultas podem ser realizadas pelo nome da pessoa que se queira pesquisar, podendo ser incluído o nome da genitora com vistas a evitar homônimos, e também mediante dos números de documentos como Registro Geral (RG), Cadastro de Pessoa Física (CPF), Carteira Nacional de Habilitação (CNH), título eleitoral, certidão de nascimento e certidão de casamento. As informações são

consultadas no Banco Nacional de Mandados de Prisão (BNMP) do Conselho Nacional de Justiça (CNJ), o qual é atualizado diretamente pelos juízes que decretam os mandados.

**Módulo 3 - Desaparecidos:** permite ao cidadão o direito de consultar pessoas desaparecidas, bem como auxiliar os órgãos de Segurança Pública. Segundo o artigo “Aplicativo Sinesp Cidadão ganha módulo para localizar pessoas desaparecidas”, publicado pelo Portal Brasil (PORTAL BRASIL, 2014), as informações são consultadas em um banco de desaparecidos com mais de 4000 cadastros de pessoas desaparecidas, sendo estas repassadas pelas delegacias especializadas dos estados. Ainda conforme descrito no artigo citado anteriormente (PORTAL BRASIL, 2014), atualmente, somente os estados do Espírito Santo, Santa Catarina e Sergipe, assinaram o termo de cooperação com o Governo Federal e compartilharam as informações sobre pessoas desaparecidas, porém, a SENASP tem uma boa expectativa para que as demais Unidades Federativas também associem seus bancos de dados ao aplicativo, melhorando assim, a utilização do serviço no país.

De acordo com o artigo “Aplicativo ajuda a recuperar mais de 323 mil veículos roubados” publicado pelo Portal Brasil (PORTAL BRASIL, 2016), até o final de setembro de 2016, o aplicativo já havia sido baixado mais de 8,8 milhões de vezes, o qual teria recebido mais de 523 milhões de consultas. Pelo módulo de consultas “Veículos”, o aplicativo ajudou a recuperar mais de 323 mil veículos furtados ou roubados e, pelo módulo de consultas “Mandado de Prisão”, ajudou na prisão de 69 mil foragidos.

## 2.3 Sinesp seguro

De acordo com os dados obtidos no *website* de acesso público do Portal Sinesp (PORTAL SINESP, 2012) e também pelo vídeo disponibilizado pelo “Canal Sinesp Seguro” no *website* “YouTube” (SINESP SEGURO, 2014), o sistema Sinesp Seguro é uma plataforma de comunicação segura e criptografada para criação, edição e compartilhamento de documentos, envio de mensagens e *chats* entre os usuários da rede privada do MJ. Esse sistema possui duplo fator de autenticação, sendo eles, lógico e físico, garantindo maior segurança na proteção das informações, dentro e fora da organização. O Sinesp Seguro foi desenvolvido e institucionalizado pela SENASP/MJ e é composto por tecnologia 100% nacional, utiliza a infraestrutura do Centro de Processamento de Dados (CPD) e rede do Serviço Federal de

Processamento de Dados (SERPRO) para o tráfego de informações entre os órgãos da administração pública federal, estadual e municipal.

Em conformidade com o “Canal Sinesp Seguro” (SINESP SEGURO, 2014), as informações trocadas dentro desse sistema acabam tendo toda estrutura de textos legíveis modificada para textos indecifráveis devido a utilização de técnicas de criptografia, ou seja, o Sinesp Seguro cria um ambiente digital totalmente blindado para a comunicação, colaboração e interligação entre as equipes de profissionais da área de segurança do país. Esse sistema pode ser facilmente acessado por meio de dispositivos como computador, *notebook*, *tablet* ou *smartphone*, e somente quem adquire e ativa a licença do Sinesp Seguro poderá acessar a plataforma, obtendo com isso, um sistema seguro e protegido. Outro fator importante é que, somente após autorização prévia emitida pelos Chefes de Inteligências das instituições, a plataforma poderá ser utilizada pelas equipes e profissionais das áreas de segurança pública federal, estadual e municipal.

## 2.4 SINESPJC

O SINESPJC ou Sistema Nacional de Estatística de Segurança Pública e Justiça Criminal, desenvolvido entre os anos de 2004 e 2010, é um sistema informatizado de coleta de informações de segurança pública e justiça criminal produzidos pelos entes federados. De acordo com os dados obtidos no portal público do Instituto Brasileiro de Geografia e Estatísticas (CES-IBGE, 2017), esse sistema reúne informações sobre o número de ocorrências, natureza do fato registrado, perfil da vítima, perfil do autor, meios empregados, dentre outras. O envio e a validação dos dados contidos nesse sistema são de compromisso dos Gestores Estaduais, os quais contam com uma equipe tecnicamente capacitada de coordenação de pesquisas e análises de informações.

Para viabilizar a coleta em âmbito nacional e gerar comparabilidade entre os dados produzidos em cada estado, a SENASP produziu uma metodologia de padronização das categorias e critérios de classificação de ocorrências, assim como suas unidades de medida, de forma a compatibilizar as categorias classificatórias utilizadas nas diferentes Unidades da Federação. Esse trabalho resultou na produção de um manual que orienta os gestores estaduais que são responsáveis pelo envio dos dados alocados nas Secretarias de Segurança Pública, nas Polícias Cíveis e nas Polícias Militares das Unidades da Federação.

Esse sistema conta ainda com a bilateralidade dos sistemas “Sinesp Integração”, também conhecido por “Integração BO”, um serviço *online* de integração com os estados da Federação para recepção de dados das Secretarias de Segurança Pública que comporão as estatísticas da base nacional de procedimentos policiais, bem como os sistemas “DW Sinesp - Estatísticas e Análise”, os quais sintetizam as informações estatísticas da Justiça Criminal coletadas pelo SINESPJC e as informações estatísticas da Justiça Criminal coletadas pelo SINESPJC, respectivamente. Ambos os sistemas são integrantes do Departamento de Pesquisa, Análise de Informação e Desenvolvimento de Pessoal em Segurança Pública (DEPAID).

As informações sobre os procedimentos policiais coletadas pelo SINESPJC têm como fonte os boletins de ocorrências criminais, registrados pelas Polícias Cíveis e Militares das Unidades da Federação, e seu objetivo principal é a consolidação de uma base nacional de dados sobre ocorrências criminais e atividades de polícia, resultando em painéis gerenciais, gráficos analíticos, relatórios, mapas estatísticos e planos de ação, conforme demonstra a Figura3(três).

**Figura 3 – Consolidação Base de Dados Nacional.**



Fonte: SINESP SEGURO (2014).

O SINESPJC divide-se em dois módulos de ocorrências criminais e atividades de polícia. No “Módulo de Coleta” as informações são coletadas de maneira agrupada, por meio de formulários que estão disponíveis em um portal da internet para os estados. Já no “Módulo de Análises”, após efetuada a coleta de informações, vários relatórios estatísticos são gerados referentes a Segurança Pública, os quais são analisados e disponibilizados aos órgãos e às instituições da Segurança Pública dos estados brasileiros.

De acordo com as informações obtidas no Portal Sinesp (PORTAL SINESP, 2012), embora o SINESPJC seja de ampla importância, apresenta algumas limitações como a falta de periodicidade no envio das informações, falta de controle na qualidade das informações enviadas, uma vez que muitos envios são realizados de forma manual e através de metodologias diferentes, e falta de integração, não sendo possível nenhum tipo de cruzamento de dados das polícias civis e militares com os dados de outras bases federais e estaduais.

## 2.5 INFOGGI

Parte integrante do Departamento de Políticas, Programas e Projetos (DEPRO), o Sistema de Informações sobre Gabinetes de Gestão Integrada ou INFOGGI, é um sistema *online* acessado pelo Portal Sinesp, por meio de autenticação segura, que pretende ajudar no combate ao crime nos estados e municípios. Esse sistema foi idealizado, especialmente, para servir de suporte aos Gabinetes de Gestão Integrada (GGI).

Conforme descrevem os autores Zarantonello e Medeiros Filho na “Cartilha GGI” (ZARANTONELLO, MEDEIROS FILHO, 2016), o INFOGGI tem como principal objetivo auxiliar o Secretário Executivo na gestão dos gabinetes, porém, é importante mencionar que o sistema possui diversas funcionalidades, como planejar, registrar, acompanhar ações demandadas dos GGI e emitir relatórios sobre as atividades dos Gabinetes.

De acordo com Celso Perioli, na época Secretário Nacional de Segurança Pública, em seu artigo de introdução na “Cartilha GGI” (PERIOLI, 2016), após a implementação do INFOGGI, a integração entre a SENASP e os Gabinetes se tornou uma realidade visível, pois desde a sua criação, toda a produção, arquivamento e documentação dos trabalhos gerados pelos mais de 180 Gabinetes, já podem ser observados no sistema, demonstrando com isso a eficiência da ferramenta e possibilitando maior solidez e confiabilidade aos trabalhos cadastrados.

Como sistema voltado para a gestão e integração, o INFOGGI disponibiliza a rede de contatos de todos os Gabinetes do país para promover interação e troca de experiências entre os GGI, permitindo também a criação de um canal de diálogo entre os Gabinetes e a Secretaria Nacional de Segurança Pública. Como fonte de consulta, o sistema permite a criação de um banco de dados que gerencia todo o *rol* de atividades do gabinete, seus participantes, ações desenvolvidas e resultados

aplicados, propiciando a confiabilidade e a garantia de que todo o histórico do GGI ficará arquivado e sem risco de perdas ou extravio.

Por fim, é preciso ressaltar que o INFOGGI é um dos programas integrantes do Sistema Nacional de Informações de Segurança Pública, e está, portanto, inserido no Portal Sinesp disponível na internet, o qual objetiva centralizar as informações sobre Segurança Pública no Brasil e, ainda, englobar desde estatísticas criminais até o registro e promoção das ações de prevenção e enfrentamento à criminalidade. Portanto, os Gabinetes de Gestão inseridos no INFOGGI poderão tanto contribuir na alimentação da base de dados do Portal Sinesp, informando, por exemplo, ações que vêm sendo desenvolvidas no âmbito local, como também poderão absorver informações úteis ao desenvolvimento de estudos e direcionamento dos trabalhos dos GGI, mostrando-se como uma importante ferramenta de produção de conhecimento na seara da Segurança Pública.

### **3 CONSIDERAÇÕES FINAIS**

É sabido que a evolução tecnológica é constante e que as TIC estão cada vez mais presentes no cotidiano das pessoas, um conceito inovador hoje pode, em um piscar de olhos, passar a ser ultrapassado. Isso tudo, é devido à grande quantidade de informações que é despejada sobre as pessoas a cada dia. Porém, é preciso considerar que quem detém o conhecimento está sempre um passo à frente, tanto no que se refere à tomada de decisões quanto no desempenho de ações futuras.

No caso da Segurança Pública, as ferramentas de TIC têm sido um fator determinante no desempenho dessas atuações, auxiliando em ações preventivas e consequentemente na antecipação ao cometimento de delitos. Ao longo deste trabalho, objetivou-se analisar a importância da utilização das ferramentas de TIC disponibilizadas pelo Portal Sinesp e, com base na análise das informações apresentadas, pode-se afirmar que as ferramentas de Tecnologia da Informação e Comunicação do Portal Sinesp realmente são importantes à Segurança Pública, pois não só ajudam no gerenciamento dos processos estratégicos e operacionais como também promovem uma comunicação mais segura, de forma padronizada e integradora de informações em âmbito nacional.

A pesquisa mostrou que o Sinesp possui um grande potencial na gestão das informações sobre a criminalidade, pois possibilita a geração de relatórios de estatísticas criminais por meio dos dados coletados pelos entes federados e é

extremamente eficiente na otimização dos procedimentos policiais, possibilitando consultas específicas nas diversas áreas da Segurança Pública, como inteligência policial, consultas investigativas, de caráter estratégico, operacional, sobre drogas, sistema prisional, justiça criminal, entre outros.

Com este projeto, espera-se que se torne cada vez mais efetiva a aplicabilidade dessas ferramentas na Segurança Pública, bem como sejam criadas novas políticas integradoras, incentivando a aproximação da sociedade para com as forças policiais, como é o caso do aplicativo Sinesp Cidadão, resultando com isso, melhoria na gestão da informação, como também na otimização de diversos procedimentos das áreas de Segurança Pública.

## REFERÊNCIAS

ALERGS. Termo de Adesão do Estado do Rio Grande do Sul ao Sinesp. BANCO DE DADOS DE PROCESSO LEGISLATIVO DA ASSEMBLEIA LEGISLATIVA RS. Brasília, 2013. Disponível em: <[http://proweb.procergs.com.br/ANEXOS/ANEXO\\_CON\\_0057\\_2014\\_9.PDF](http://proweb.procergs.com.br/ANEXOS/ANEXO_CON_0057_2014_9.PDF)>. Acesso em 27 fev. 2017.

BRASIL. Decreto Nº 8.075, de 14 de agosto de 2013. Dispõe sobre o Conselho Gestor do Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas, instituído pela LEI Nº 12.681, de 4 de julho de 2012. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2013/Decreto/D8075.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8075.htm)> Acesso em 02 set. 2016.

BRASIL. LEI Nº 12.681, de 4 de julho de 2012. Institui o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas - SINESP; altera as Leis nos 10.201, de 14 de fevereiro de 2001, e 11.530, de 24 de outubro de 2007, a Lei Complementar no 79, de 7 de janeiro de 1994, e o Decreto-Lei no 3.689, de 3 de outubro de 1941 - Código de Processo Penal; e revoga dispositivo da Lei no 10.201, de 14 de fevereiro de 2001. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12681.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12681.htm)> Acesso em 02 set. 2016.

CES-IBGE. Base de dados do Comitê de Estatísticas Sociais do IBGE sobre o Sistema Nacional de Estatística de Segurança Pública e Justiça Criminal - SINESPJC. 2017. Disponível em: <<http://ces.ibge.gov.br/base-de-dados/metadados/ministerio-da-justica-mj/sistema-nacional-de-estatistica-de-seguranca-publica-e-justica-criminal-Sinespjc.html>>. Acesso em 27 fev. 2017.

DRUCKER, P. F. Managing for Results: Economic Tasks and Risk-taking Decisions. Nova Iorque, Ed. Harper & Row, 1964. ISBN 0887306144.

MARQUES, V. Artigo: A importância da Tecnologia da Informação. PORTAL TI ESPECIALISTAS, 22 de agosto de 2014. Disponível em: <<https://www.tiespecialistas.com.br/2014/08/importancia-da-tecnologia-da-informacao/>> Acesso em 12 dez. 2016.

PERIOLI, C. Cartilha GGI - Introdução. MJ, Brasília, 2016. 10 p. Disponível em: <[http://www.justica.gov.br/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/outras\\_publicacoes/pagina-3/19cartilha\\_ggi-corrigida.pdf](http://www.justica.gov.br/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/outras_publicacoes/pagina-3/19cartilha_ggi-corrigida.pdf)>. Acesso em 8 fev. 2017.

PORTAL BRASIL. Aplicativo Sinesp Cidadão ganha módulo para localizar pessoas desaparecidas. 20 de outubro de 2014. Disponível em: <<http://www.brasil.gov.br/cidadania-e-justica/2014/10/aplicativo-sinesp-cidadao-ganha-modulo-para-localizar-pessoas-desaparecidas>>. Acesso em 14 dez. 2016.

PORTAL BRASIL. Aplicativo ajuda a recuperar mais de 323 mil veículos roubados. 26 de setembro de 2016. Disponível em: <<http://www.brasil.gov.br/cidadania-e-justica/2016/09/aplicativo-ajuda-a-recuperar-mais-de-323-mil-veiculos-roubados>>. Acesso em 15 dez. 2016.

PORTAL SINESP. Portal Sinesp - Sistema Nacional de Informações de Segurança Pública, prisional e sobre Drogas - Acesso Público. 2012. Disponível em: <<https://www.sinesp.gov.br>>. Acesso em 12 dez. 2016.

SINESP CIDADÃO. Sinesp Cidadão. 2012. Disponível em: <<https://www.sinesp.gov.br/sinesp-cidadao>>. Acesso em 12 dez. 2016.

SINESP SEGURO. Canal Sinesp Seguro. YOUTUBE. 2014. Duração em minutos: 4:14. Disponível em: <<https://www.youtube.com/watch?v=YU6M5zodgEE>>. Acesso em 15 fev. 2017.

ZARANTONELLO, F. C. MEDEIROS FILHO, G. G. Cartilha GGI. MJ, Brasília, 2016. 43 p. Disponível em: <[http://www.justica.gov.br/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/outras\\_publicacoes/pagina-3/19cartilha\\_ggi-corrigida.pdf](http://www.justica.gov.br/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/outras_publicacoes/pagina-3/19cartilha_ggi-corrigida.pdf)>. Acesso em 8 fev. 2017.

## **REDE DE SEGURANÇA ESCOLAR: UMA ANÁLISE SOBRE A POSSIBILIDADE DE APROXIMAÇÃO ENTRE POLÍCIA MILITAR E A COMUNIDADE ESCOLAR POR MEIO DAS REDES SOCIAIS<sup>1</sup>**

*Bruna da Silva Pires*

*Luciana Bolan Frigo*

*Eliane Pozzebon*

### **1 INTRODUÇÃO**

O primeiro artigo da Constituição Brasileira de 1988 retrata a condição de um país democrático de direito, onde o povo tem o poder exercido por meio de representação ou de forma direta (BRASIL, 1988).

As eleições no Brasil, seja ela federal, estadual ou municipal, consolidam esse poder de representação que reafirma a soberania da vontade do povo. No entanto, a restrição imposta à participação democrática repousa sobre a atuação direta nas questões do Estado. Com relação à segurança pública, a participação é fator essencial para a obtenção de resultados eficazes, pois sem articulação entre polícias, prisões e judiciário, inclusive sem o envolvimento da sociedade organizada, não existe eficácia e eficiência nas ações de controle da criminalidade e da violência e nas de promoção da pacificação social (CARVALHO; SILVA, 2011).

Desde o ano 2000, quando o Plano Nacional de Segurança Pública (PNSP), que é considerado a primeira política nacional e democrática de segurança do Brasil, seguido pela instituição do Programa Nacional de Segurança Pública com Cidadania

---

<sup>1</sup>Este estudo é baseado no trabalho de conclusão de curso especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos da Universidade Federal de Santa Catarina, de autoria de Bruna da Silva Pires e orientada pela Prof. Dr<sup>a</sup>. Luciana Bolan Frigo.

(Pronasci) em 2007, tornou-se imprescindível a participação da sociedade na elaboração das políticas públicas voltadas à segurança, por entenderem que a cooperação da sociedade por meio de suas instituições representativas torna-se crucial para o delineamento de qualquer política pública. A complexidade da questão implica a necessidade de uma efetiva interação social, como forma de democratizar o aparelho estatal para garantir uma segurança cidadã (CARVALHO; SILVA, 2011).

Diante da necessidade de aproximar a população dos problemas de segurança pública, a Secretária Nacional de Segurança Pública - SENASP, incentivou a implementação da Filosofia de Polícia Comunitária, a qual possui como pilares centrais a solução dos problemas sociais com a participação da comunidade e também a prevenção criminal (FERNANDES, 2011).

Assim, o policiamento comunitário é pautado em ações de prevenção e contribuição da sociedade na resolução dos conflitos sociais, principalmente os que envolvem criminalidade e violência. Em Santa Catarina, os CONSEGs (Conselhos Comunitários de Segurança), Rede de Vizinhos Solidários, PROERD (Programa Educacional de Resistência às Drogas), Rondas Comerciais e a Rede de Segurança Escolar, objeto de estudo do presente trabalho, são programas que incentivam a participação efetiva da população, conforme preconizam os fundamentos da polícia comunitária.

Na área de abrangência da 1ª Cia do 19º Batalhão da Polícia Militar de Santa Catarina/Araranguá (19º BPM), os princípios da polícia comunitária escolar, a qual envolve a polícia militar, os pais, os alunos, os professores e demais funcionários das instituições de ensino público e privado, são difundidos através da Rede de Segurança Escolar (Ronda Escolar). Contudo, a presença policial nas escolas ainda é considerada estranha à rotina escolar, mesmo que se tenham palestras e visitas nas salas de aula para difundir a atuação da ronda escolar e, conseqüentemente, aproximar a comunidade escolar da polícia militar.

Pensando numa forma de inovar ou aprimorar a comunicação com a comunidade escolar, buscou-se analisar de que forma as redes sociais virtuais podem auxiliar na aproximação entre polícia militar e a comunidade escolar, pois com o advento de novas tecnologias fica-se conectado, praticamente, 24 horas por dia, mesmo enquanto desempenham-se outras tarefas. Sendo que a participação da sociedade é indispensável à resolução dos problemas relacionados à criminalidade, e as TIC (redes sociais digitais) são as ferramentas úteis para construir uma arena moderna, adequada, eficiente e eficaz para o debate e deliberação desses temas,

bem como compartilhar informações de como a polícia e outras instituições de segurança pública atuam, desmistificando alguns entendimentos errôneos sobre o assunto.

Nesse sentido, Marcineiro (2001) entende que o conhecimento é fundamental para a evolução de metodologias de trabalho melhores e a transmissão de conhecimento pelos meios digitais é muito mais rápida, de baixo custo e com um alcance infinitamente maior. Se boa parte das pessoas dominasse um mínimo de conhecimento da área, possibilitaria que a sociedade participasse de forma efetiva das políticas públicas e as ferramentas de TIC (Tecnologia da Informação e Comunicação) são perfeitas para a transmissão do conhecimento.

Sendo assim, buscou-se no presente estudo, analisar de que forma as redes sociais virtuais - ferramenta muito utilizada pelos estudantes – podem contribuir na política de aproximação.

## **2 POLÍCIA COMUNITÁRIA ESCOLAR E AS REDES SOCIAIS VIRTUAIS**

### **2.1 Fundamentos**

O policiamento comunitário escolar tem como objetivo trabalhar em parceria com a comunidade escolar para identificar, priorizar e resolver os problemas existentes. A necessidade desse tipo de policiamento surgiu devido ao aumento significativo do número de crianças e adolescentes na escola, em especial na escola pública, que resultou no surgimento de violências, como agressões físicas e verbais contra professores e alunos, brigas, depredações, *bullying*, furtos, roubos, ameaças, porte de armas etc. Ante a complexidade dos problemas, que fogem à competência escolar, a presença de policiais militares é requisitada de maneira frequente para manter a segurança dentro e no entorno da escola (SABÓIA OBRZUT, 2011).

Dessa maneira, a atuação da polícia militar com ênfase na comunidade escolar tornou-se imperiosa, pois, o policiamento comunitário escolar é considerado “a basilar atividade de “policiamento ostensivo” em “ação de presença” que deve atuar precipuamente preventivamente (ações proativas), e atuar supletivamente na repressão a crimes e a atos infracionais” (BARANKIEVICZ, 2012, p.133).

No estado de Santa Catarina, a Polícia Militar regulamentou o policiamento comunitário escolar através do POP 115/2017 (Procedimento Operacional Padrão), o

qual criou o programa Rede de Segurança Escolar. De acordo com as informações veiculadas no site oficial da PMSC, a finalidade desse programa consiste em proteger e orientar os alunos quanto a medidas comportamentais preventivas, bem como fortalecer e ampliar vínculos com a comunidade escolar; assessorar a comunidade escolar na construção de soluções pacíficas dos problemas de segurança; proporcionar uma consultoria de segurança às Unidades de Ensino, pautada em preceitos de prevenção ambiental e situacional; estabelecer em parceria com a comunidade escolar, grupos de discussão para atuação na prevenção situacional do crime de acordo com a polícia de proximidade. E ainda propõe a utilização de um grupo do *WhatsApp* ou telegram (aplicativos móveis) como ferramenta de comunicação entre um representante da polícia militar e os diretores das unidades escolares.

Na 1ª Cia do 19º Batalhão da Polícia Militar de Santa Catarina, situada em Araranguá-SC, o policiamento comunitário escolar é realizado através das Rondas Escolares desde o ano de 2009. Com o passar dos anos, essa prática foi se aperfeiçoando e atualmente abrange os municípios de Balneário Arroio do Silva, Maracajá e Araranguá, contemplando 47 instituições de ensino, nas quais palestras são ministradas, bem como visitas e conversas nas salas de aula são práticas rotineiras.

Com o objetivo de aperfeiçoar o policiamento comunitário escolar, buscou-se com o presente trabalho analisar a possibilidade de utilizar as redes sociais virtuais como ferramentas da política de aproximação, pois, com a predominância da filosofia de polícia comunitária nas ações da Polícia Militar no Brasil, a participação social na resolução de problemas de segurança pública tornou-se imprescindível para o alcance de resultados positivos. E por essa razão, os órgãos de segurança pública tiveram que acompanhar a evolução dos meios de comunicação, principalmente das redes sociais virtuais. Nesse ínterim,

No âmbito mundial, podemos citar os países anglo-saxões Estados Unidos e Austrália. O primeiro, desde que implantou o policiamento comunitário, os departamentos de polícia tentam aumentar o seu envolvimento com os moradores da comunidade local e a aplicação da lei, sendo que o *Facebook* apresentou-se como um forte aliado (DYE, 2009, p.36).

Seguindo a tendência mundial e nacional, a PMSC também criou perfis nas mídias sociais. O diálogo entre instituição policial e cidadão, por meio da rede social *Facebook*, demonstra a interação e a aproximação que já vem ocorrendo na cidade

de Jaraguá do Sul/SC, uma das *fanpages* mais atuantes da PMSC, por exemplo, corroborando os princípios de Polícia Comunitária; o cidadão que recebe um atendimento via rede social cria uma impressão positiva da instituição pública, sentindo-se acolhido pelo órgão policial, o que se reverte na tão almejada sensação de segurança para a coletividade e, em última análise, na própria resolução dos problemas da segurança pública (BACCIN; CRUZ, 2015, p.28).

Em Araranguá, município onde está instalada a sede do 19º BPM, o aplicativo *Whatsapp* é ferramenta primordial no Projeto Vizinho Solidário, lançado em 2015. Segundo a página oficial no *Facebook* do 19º BPM, esse projeto consiste na parceria firmada entre a comunidade e a Polícia Militar, em que pequenos núcleos de moradores de determinado bairro ou, mais especificamente, determinada rua reúnem-se com o propósito de conscientizar os demais moradores a participarem ativamente da segurança de todos. Esse grupo de vizinhos participa de um treinamento e recebem orientações sobre estrutura de redes, segurança na transmissão de informações, dicas de segurança pessoal e residencial, bem como informações a respeito de arquitetura para o crime, algumas mudanças são indicadas e realizadas. A melhoria da iluminação pública, seguida da colocação de câmeras de segurança instaladas ao longo de toda a rua, adquiridas com recursos dos próprios moradores, são alguns exemplos de mudanças. As imagens capturadas por essas câmeras ficam à disposição dos moradores e de um representante da Polícia Militar. Por conseguinte, um grupo de *whatsApp* é criado, no qual participam os moradores da rua em que o projeto foi implantado e um representante da Polícia Militar, o que facilita a troca de informações e promove a agilidade nesse processo<sup>2</sup>.

Diante desses exemplos, denota-se que a utilização das redes sociais para auxiliar na prática das ações de polícia comunitária é considerada eficaz.

## 2.2 Metodologia, Resultados e Discussão

Analisando que a rede de segurança escolar que atua na 1ª Cia do 19º BPM não trabalha atualmente com uma página no *Facebook* ou outra ferramenta virtual, foi realizada uma pesquisa para identificar de que maneira os integrantes da comunidade escolar (alunos, professores, funcionários, pais) fazem uso das redes sociais virtuais e se os mesmos consideram essa prática benéfica para aproximá-los

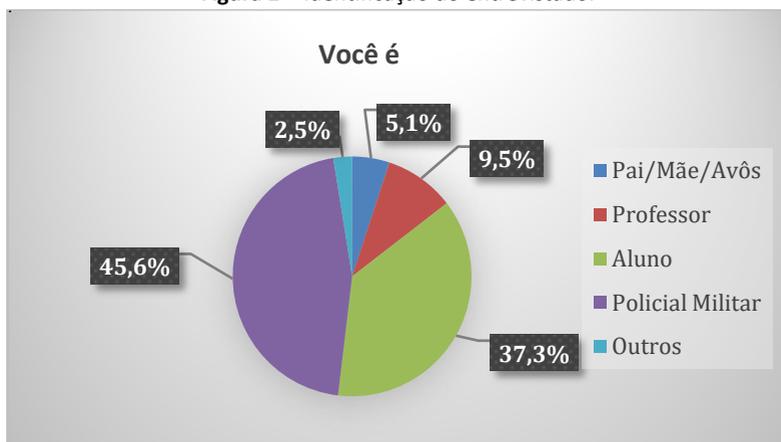
---

<sup>2</sup> Informações obtidas na página oficial PMSC, disponível em: [http://www.pm.sc.gov.br/noticias/em-ararangua-pm-lanca-oficialmente-projeto vizinho-solidarioquote.html](http://www.pm.sc.gov.br/noticias/em-ararangua-pm-lanca-oficialmente-projeto-vizinho-solidarioquote.html) - Acesso em 26/01/2017.

da polícia militar. Nessa pesquisa, foram entrevistadas 158 pessoas, e a mesma foi aplicada para policiais militares, pais/responsáveis, estudantes, professores e funcionários das instituições de ensino públicas e privadas.

Após a coleta dos dados, foi possível constatar que a maioria dos entrevistados eram policiais militares e alunos, conforme podemos verificar no gráfico abaixo.

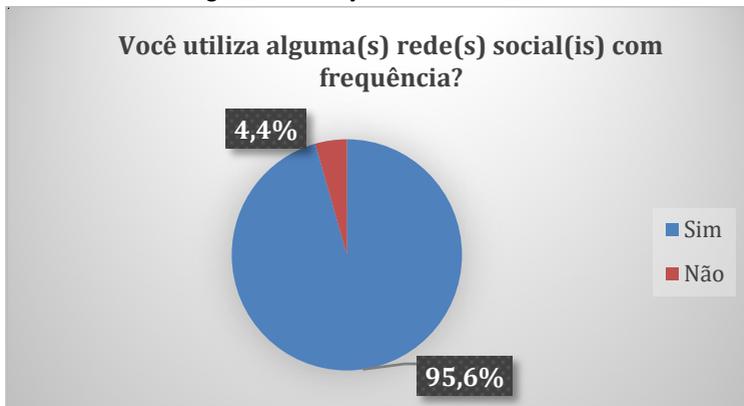
**Figura 1 - Identificação do entrevistado.**



**Fonte:** Elaborado pelo autor.

Sobre a utilização das redes sociais virtuais, 95,6% acessam as redes sociais com frequência. Sendo que a maioria dos entrevistados tem acesso às redes sociais durante cinco ou mais dias por semana. E o tempo utilizado por dia pelos entrevistados acessando as redes sociais é de até 1 hora para 31%; até 2 horas para 25,3%; e, até 5 horas para 11,4%.

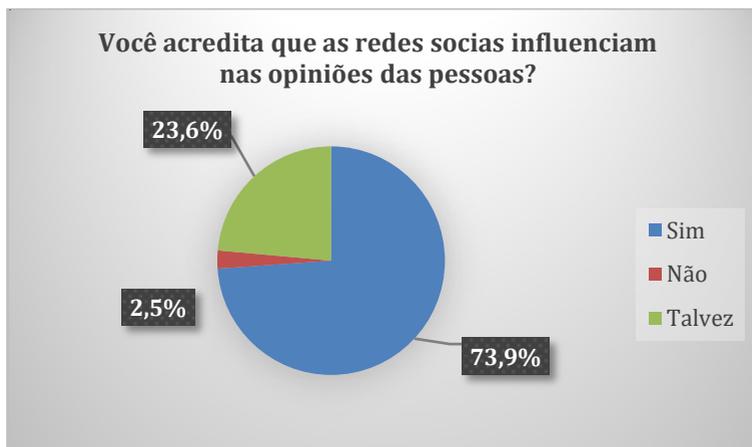
**Figura 2 - Utilização das Redes Sociais Virtuais.**



Fonte: Elaborado pelo autor.

Em relação ao poder de influência das informações veiculadas nas redes sociais, 73,9% dos entrevistados acreditam que pode influenciar; e 23,6% responderam que talvez possa haver influência na formação de sua opinião.

**Figura 3 - Poder de influência das redes sociais na formação de opinião dos entrevistados.**



Fonte: Elaborado pelo autor.

Rede de segurança escolar: uma análise sobre a possibilidade de aproximação entre polícia militar e a comunidade escolar através das redes sociais

No que tange à aproximação da comunidade com os serviços realizados pelas instituições de segurança pública, a maioria dos entrevistados acredita que as redes sociais podem auxiliar na relação de aproximação.

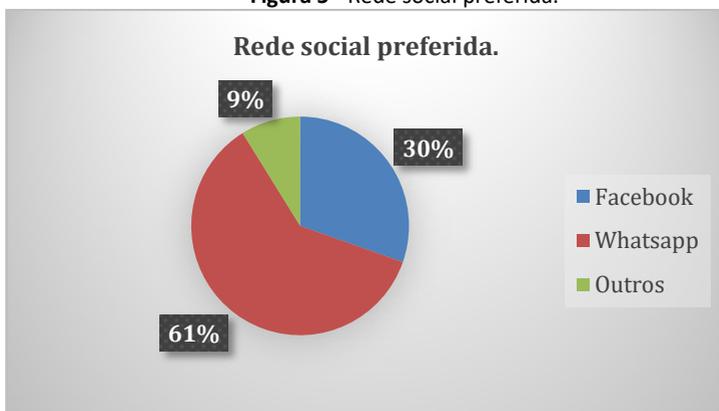
**Figura 4** - Sobre aproximação da comunidade com os serviços de segurança pública.



Fonte: Elaborado pelo autor.

Quanto à preferência dos tipos de redes sociais virtuais, o *WhatsApp* e o *Facebook* são as opções que predominam no interesse dos entrevistados. Ressaltando que 81,5% dos entrevistados possuem conta no *Facebook*.

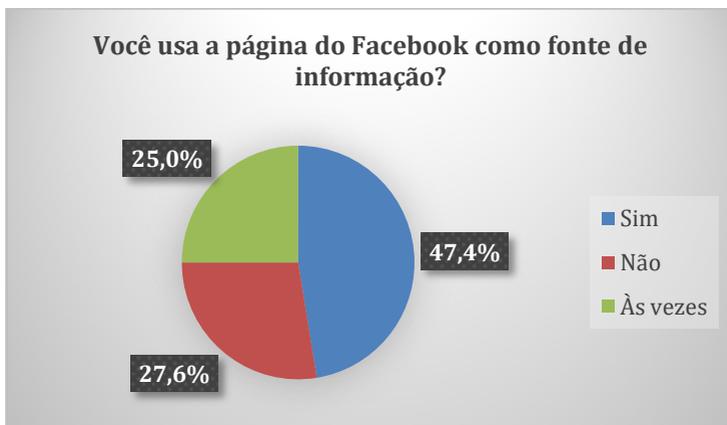
**Figura 5** - Rede social preferida.



Fonte: Elaborado pelo autor.

Iniciando uma abordagem sobre o uso do *Facebook* como fonte de informação e considerando que a maioria predominante dos entrevistados acessa com frequência essa rede social, questionou-se acerca do poder de influência das publicações postadas nas *fanpages* do PROERD e do 19º BPM quanto à imagem da polícia militar, e obtiveram-se os seguintes resultados:

**Figura 6** - Utilização do *Facebook* como fonte de informação.



Fonte: Elaborado pelo autor.

**Figura 7** - Influência no pensamento acerca da Polícia Militar.



Fonte: Elaborado pelo autor.

Rede de segurança escolar: uma análise sobre a possibilidade de aproximação entre polícia militar e a comunidade escolar através das redes sociais

Finalmente, no sentido de que a aproximação entre a comunidade escolar e a polícia militar pode ser aperfeiçoada através de uma rede social, objetivo principal desta pesquisa, a maioria dos entrevistados acredita nessa possibilidade.

**Figura 8** - Rede social virtual como ferramenta de aproximação entre a comunidade escolar e a polícia militar.



**Fonte:** Elaborada pelo autor.

Essas respostas explicitadas por meio dos gráficos mostram que as redes sociais virtuais fazem parte da nossa rotina, influenciando no pensamento das pessoas e ferramenta de comunicação indispensável.

### 3 CONSIDERAÇÕES FINAIS

A necessidade de sentir-se seguro foi a principal razão para os homens viverem agrupados. O fato de viver em sociedade, mesmo que em pequenos grupos, gerava sensação de proteção contra inimigos externos. Mas, para uma boa convivência em sociedade certas regras precisavam ser cumpridas para a sobrevivência do grupo. Por este motivo, alguns componentes do grupo receberam a competência de policiar o cumprimento das regras sociais, e assim, nascia o embrião do que hoje chamamos de Polícia.

No decorrer do tempo, a polícia desempenhou seu papel das mais variadas formas. Na Grécia, a polícia foi pouco utilizada (necessária); em contrapartida, na república romana, se fez grande uso das forças policiais para manter a ordem na

megalópole Roma. Já no período absolutista da Idade Média, a polícia – forças militares do monarca – se distanciou significativamente do povo e da sua função original. Nessa época, sob a vontade do poder da igreja ou do monarca, as ações da polícia visavam única e exclusivamente à manutenção do poder, a defesa territorial e a intimidação do povo para que não se insurgissem contra os monarcas, nem contra os dogmas da Santa Igreja. Somente no ano de 1829, em Londres, a polícia reaparece como organização desvinculada das forças armadas e com a função de manter a ordem pública e a segurança das pessoas.

O ato de policiar evoluiu e foi influenciado por diversas ideologias de polícia, dentre as quais se destacam: Ideologia Militarista, Ideologia de Controle Social, Ideologia Reativa e Ideologia Preventiva. Com base nessas ideologias de polícia, nas condições de seus Estados e em suas peculiaridades culturais, os países desenvolveram diversos modelos de polícia, sendo que no Brasil, os mais influentes foram o modelo anglo-saxão de polícia (descentralizado) e o modelo oriental (proativo). Este último é o único baseado na Ideologia Preventiva, ou seja, na escola oriental o trabalho das agências de preservação da ordem pública é centrado no tratamento proativo do crime, agindo sobre os elementos que possibilitam a prática do crime, quais sejam: um ambiente apropriado para a prática do crime, um agente disposto a praticar tal crime e uma vítima em potencial.

Todavia, esses modelos não se mostraram eficientes para resolver o crescente problema do crime e da violência que apresenta índices cada vez mais elevados. A criminalidade está presente em todos os locais e a população não consegue mais ter ao menos sensação de segurança, pois é sabido que o policiamento reativo não é eficaz na erradicação da violência e da criminalidade. Os problemas de segurança pública devem ser observados com uma visão mais ampla, na qual todos são corresponsáveis.

Com o advento das mudanças democráticas estabelecidas na Constituição Federal de 1988, exigiram-se das polícias uma nova postura e uma ruptura com os antigos paradigmas da segurança pública. A procura incessante por respostas ao problema do crime e da violência, bem como a busca por adequar as polícias a um modelo democrático, levaram as polícias do Brasil ao encontro da Filosofia de Polícia Comunitária. Desse modo, o Brasil segue o mesmo caminho que trilharam os Estados Unidos da América, Japão, Canadá, Espanha e outros países que encontraram na democratização das polícias a solução para inúmeros problemas de segurança pública através do policiamento comunitário.

Na Filosofia de Polícia Comunitária, a função da polícia não é apenas defender os interesses do Estado através do controle social como o modelo latino-francês apregoa, ou de patrulhar as ruas e controlar o crime atendendo as chamadas de emergência e prendendo criminosos, tal qual o modelo anglo-saxão. E sim, buscar a prevenção do crime, estabelecendo parcerias com a comunidade, identificando problemas e agregando recursos da polícia, Estado e comunidade na resolução dos conflitos existentes.

Em 2000, o Plano Nacional de Segurança Pública (PNSP) que é considerado a primeira política nacional e democrática de segurança do Brasil, seguido no ano de 2007, do Programa Nacional de Segurança Pública com Cidadania (PRONASCI), permitiram a participação da sociedade na elaboração das políticas públicas voltadas à segurança. Em Santa Catarina, bem como, em diversos outros Estados do Brasil, no encalço da participação da sociedade nos problemas de segurança e motivados por incentivos da Secretaria Nacional de Segurança Pública (SENASP), vem sendo paulatinamente implementada a Filosofia de Polícia Comunitária.

Na 1ª Cia do 19º Batalhão da Polícia Militar de Santa Catarina, como em outros batalhões de polícia do estado, a Rede de Segurança Escolar é ferramenta essencial para a prática do policiamento comunitário através das rondas escolares. Esse tipo de atuação objetiva prevenir que os crimes ocorram no ambiente escolar ou nas proximidades das instituições de ensino; e, além disso, atua junto à comunidade escolar na resolução dos problemas sociais.

Além da Rede de Segurança Escolar, existem outras iniciativas que aproximam a comunidade da polícia militar que também são praticadas na área do 19º BPM, como a Rede de Vizinho Solidário, PROERD e CONSEGS. Mas, o fato do sucesso da Rede de Vizinho Solidário por causa da interação dos integrantes por meio de um grupo do *WhatsApp*, e das *fanpages* do PROERD e do 19º BPM no *Facebook* com números bastante interessantes de seguidores, direciona a atenção para o uso das redes sociais virtuais como aliada das ações de policiamento comunitário. Destaca-se que as redes sociais são um dos principais meios que a sociedade dispõe para o compartilhamento da informação e do conhecimento e consequente solução de problemas, valendo-se das relações existentes entre seus integrantes.

Nessa conjuntura, denotou-se no presente trabalho que a sociedade convive em rede, mas atualmente prevalecem as redes sociais virtuais. E considerando que o *Facebook* é preferência mundial, o qual no mês de abril do ano de 2016 atingiu a marca de 1(um) bilhão de usuários acessando a página diariamente, analisou-se a

possibilidade de utilizar as redes sociais virtuais para auxiliar o trabalho da Rede de Segurança Escolar, principalmente através do *Facebook*.

Assim, um questionário foi aplicado para os integrantes da comunidade escolar da área de competência da 1ª Cia do 19º BPM, o qual levou a verificação de que a maioria dos entrevistados possui uma conta em alguma rede social virtual, bem como conhecem a *fanpage* do 19º BPM no *Facebook*. Além disso, as informações compartilhadas nas redes sociais virtuais apresentam-se como um campo fértil para difundir a filosofia e divulgar as ações da polícia militar, pois a maioria dos entrevistados utiliza essas ferramentas virtuais como fonte de informação. E o mais importante, quando questionados sobre a possibilidade de aproximação entre a polícia militar e os pais, alunos e professores das escolas através de uma *fanpage* como do *Facebook*, as respostas foram positivas.

Portanto, ao final deste estudo pode-se concluir que os métodos ortodoxos de participação social, na era do conhecimento e da vida digital, não são ferramentas adequadas à transmissão de conhecimento e participação social democrática que a demanda da criminalidade exige para soluções adequadas, preventivas e duradouras. A utilização das TIC no policiamento comunitário escolar é alternativa com enorme potencial de sucesso, tendo em vista a abordagem dos assuntos referentes aos problemas de segurança pública através destas ferramentas tornar-se mais atrativa para a comunidade escolar.

## REFERÊNCIAS

ABRAMOVAY, Mirian et al. **Escola e violência**. Brasília: Unesco, 2003.

ALEXANDER, Dan. Using **Technology to Take Community Policing to the Next Level**. 2011. Acesso em: 25 set. 2014.

ARAUJO, Conceição. Artigo **O que são os blogs**. Disponível em: <http://www.infoescola.com/informatica/o-que-sao-blogs/> - Acesso 17/04/2017.

BACCIN, Leonardo RinconStankiewicz; CRUZ, Tércia Maria Ferreira da. **Uma reflexão sobre a utilização das redes sociais como forma de auxílio à atuação da polícia comunitária**. Revista Ordem Pública. ISSN 1984-1809 v. 8, n. 2, jul. /dez., 2015 e 2237-6380 ACORS. <http://www.acors.org.br> [rop.emnuvens.com.br/Rop](http://rop.emnuvens.com.br/Rop) – Disponível em: <file:///C:/Users/Max/Downloads/131-252-1-SM.pdf> – Acesso em 16/04/2017.

BARANKIEVICZ, Valdemar; **Patrulha Escolar- uma filosofia de polícia comunitária em apoio às escolas. Curitiba, 2012, 28 p.**

BARROS, D., NEVES, C., SEABRA, F., MOREIRA, J. e HENRIQUES, S. **Educação e tecnologias: reflexão, inovação e práticas.** 2011. Lisboa: [s.n.], ISBN: 978-989-20-2329-8.

BORDIN, Marcelo. **POLÍCIA COMUNITÁRIA: entre a retórica do estado e a prática cotidiana.** Revista Online Vigilância, Segurança e Controle Social na América Latina, Curitiba, p. 349-368.2009. ISSN 2175-9596 – Disponível em: file:///C:/Users/Max/Downloads/ssscla-2681%20(4).pdf – Acesso em 23/11/2016.

BRASIL. **Constituições da República Federativa do Brasil, 1824 a 1969.**11ª Ed. São Paulo: Saraiva 1995.p.57.

CAPELAS, Bruno. **Brasileiro que criou o instagram; Mike Krieger fala sobre futuro do aplicativo.** Matéria publicada em 11/12/2014. Disponível em <http://link.estadao.com.br/noticias/geral,brasileiro-que-criou-o-instagram-mike-krieger-fala-sobre-futuro-do-aplicativo,10000029973> - Acesso em 22/04/2017.

COLOMBIER, Claire. **A violência na escola.** Tradução de Roseana KligermanMurrayl. São Paulo: Summus, 1989.

COMMUNITY Policing Consortium. **Understanding Community Policing: A Framework for Action.**Washington: Bureau of Justice Assistance, 1994.

CRUZ, Ruleandson do Carmo. **Redes sociais virtuais: premissas teóricas ao estudo em ciência da informação** – TransInformação, Campinas, 22(3):255-272, set./dez., 2010.

DUARTE, Luiz Ricardo. **Aspectos da implantação e da avaliação do policiamento comunitário.** 2004. 94 f. Monografia (Especialista em Segurança Pública) – Curso de Pós-Graduação em Segurança Pública. Universidade do Sul de Santa Catarina, Palhoça, 2004.

DYE, S. **Policing in local law enforcement: A commitment to getting out-of-the-car.** 2009. Acesso em: 25/09/2016.

FBI - Federal Bureau of Investigation. **Stories: The FBI on Facebook And YouTube. AndTwitterand More.** 2009. Acesso em: 20/09/2016.

FERNANDES, Luís. **Redes sociais online e educação: contributo do Facebook no contexto das comunidades virtuais de aprendentes.** Lisboa: Universidade de Nova Lisboa. Acedido em agosto, v. 29, p. 2012, 2011.

FIGUEIREDO, A. D. (1995) **What are the big challenges of Education for the XXI century: proposals for action, invited contribution for the preparation of the White Book on Education and Training**. Publicado em 22/05/2004. Disponível em: <http://eden.dei.uc.pt/~adf/whitebk.htm>.

FREITAS, J. **Internet na Educação – Contributo para a construção de redes educativas com suporte comportamental**. 2004. Tese de Doutoramento em Ciências da Educação. Faculdade de Ciências e Tecnologias – Universidade Nova de Lisboa, Lisboa.

GONÇALVES, Luciana Barreto. **Seminário Integrado: Redes Sociais Virtuais e Ferramentas Colaborativas**. 2012. 50p. Curso de Especialização em Mídias da Educação – Universidade Federal do Rio Grande do Sul. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/95663/000916560.pdf?sequence=1> - Acesso em 25/02/2017.

HENDEN, Pablo David. **Atuação preventiva ou reativa? Como policiar uma “imputável” sociedade**. Florianópolis/SC. 2010. 105fls. Disponível em: <http://biblioteca.pm.sc.gov.br/pergamum/vinculos/000000/0000004D.pdf> - Acesso em: 18/04/2017.

HOLLOWAY, Thomas. **Polícia no Rio de Janeiro: repressão e resistência no numa cidade do século XIX**. Rio de Janeiro: Fundação Getúlio Vargas, 1997.

LAKATOS, Eva Maria. **Fundamentos de metodologia científica 1**. Marina de Andrade Marconi, Eva Maria Lakatos. - 5. ed. - São Paulo: Atlas 2003.

MACHADO, J.R.& TIJIBOY, A. V. **Redes Sociais Virtuais: um espaço para efetivação da aprendizagem cooperativa**. Em: Revista Novas Tecnologias na educação. Volume 3. Número 1. CINTED – Universidade Federal do Rio Grande do Sul. 2005. Disponível em: <http://s3.amazonaws.com/academia.edu.documents/42899689/13798-48449-1> -Acesso em 27/02/2017.

MARCINEIRO, Nazareno. **Polícia Comunitária: Construindo segurança nas comunidades-Florianópolis**. Editora Insular, 2009. 232 p.

MARIA, SabóiaObrzutDulcelena. Programa de Desenvolvimento Educacional. Produção Didático-Pedagógica: **Unidades Didáticas para a composição de um caderno pedagógico**, Irati, p.06, ago.2011.

MARTELETO, Regina Maria. **Análise de redes sociais: aplicação nos estudos de transferência da informação**.*Ci.Inf*. [online].2001, vol.30, n.1, p.71-81. ISSN0100-1965.

MATOS, Márcio Giani Rosa de. **Redes Sociais e a Polícia Comunitária: estudo de caso dos CONSEGs do Vale do Araranguá** / Márcio Giani Rosa de Matos; orientador, Marcio Vieira de Souza - Araranguá, SC, 2015. 112 p. Disponível em: <http://posticsenasp.ufsc.br/files/2015/07/TCC-marcio.pdf> - Acesso em 21/09/2016.

MINISTÉRIO DA JUSTIÇA, **Redes sociais, mobilização e segurança pública: Evolução da rede de atores da segurança pública no processo preparatório da 1ª Conferência Nacional de Segurança Pública**, Coordenação Geral da 1ª Conferência Nacional de Segurança Pública, Ministério da Justiça – Ano I. Brasília, DF, 2009.

PRIOTTO, Elis Palma. Boneti, Lindomar Wessler. **VIOLÊNCIA ESCOLAR: na escola, da escola e contra a escola**. Rev. Diálogo Educ., Curitiba, v. 9, n. 26, p. 161-179, jan. /abr. 2009. Disponível em: <file:///C:/Users/Max/Downloads/dialogo-2589.pdf> - Acesso em 12/03/2017.

PRIOTTO, Elis Palma. **Características da violência escolar envolvendo adolescentes**. In: Educere. Congresso de Educação da PUCPR, 6, 2006. Curitiba. Anais... Curitiba: Champagnat, 2006. p 16-28.

PUFF, Jefferson. **PM do Rio aposta em Whatsapp e Facebook para denúncias e lança manual para as redes**. 2015. Acesso em: 15/10/2016.

RECUERO, Raquel. **Redes sociais na internet** – Porto Alegre: Sulina, 2009. (Coleção Cibercultura) 191 p.

RIBEIRO, Dalnei; HOFFMANN, Marcos Erico. **O bullying e outras práticas de violência no ambiente escolar: a atuação da polícia militar de Santa Catarina**. CAMINHOS Revista online de divulgação científica da Unidavi, Especial Pós-Graduação: Gestão de Segurança Pública e Inteligência Criminal. Editora Unidavi, p 11. Ano 5 (n. 9) - jan. /mar. 2014.

SÁ, Elizabeth Schneider de et al. **Manual de normalização de trabalhos técnicos científicos e culturais**. 2. Ed. Petrópolis: Vozes, 1996.

SENASP; **Curso Nacional de Promotor de Polícia Comunitária** / Grupo de Trabalho, Portaria SENASP nº 002/2007 –Brasília– DF: Secretaria Nacional de Segurança Pública: 2007.

SENASP; **Curso Nacional de Polícia Comunitária Escolar**. Disponível em: <https://pt.scribd.com/doc/144285365/Modulo2-Policimento-escolar>. Acesso em: 15/07/2016.

SILVA, Paulo Henrique. **O que é um site**. Artigo publicado em 24/03/2009. Disponível em: <http://www.webartigos.com/artigos/o-que-e-um-site/15908/> - Acesso em 13/04/2017.

Rede de segurança escolar: uma análise sobre a possibilidade de aproximação entre polícia militar e a comunidade escolar através das redes sociais

SOUSA, Maíra de Cássia Evangelista de. **A dinâmica da notícia nas redes sociais na internet – Dissertação de Mestrado UFSC – Orientadora Dr<sup>a</sup>. Raquel RitterLonghi, Florianópolis, 2013.**

SOUZA, Márcio Vieira de; SIMON, Rangel Machado. **Redes Sociais e MOOCs: análise de mídias para uma educação em rede** – XI Congresso Brasileiro de Ensino a Distância 2014 Florianópolis/SC, 05 – 08 de agosto de 2014 – UNIREDE: p. 313-327.

SOUZA, Benedito Celso de. **A polícia Militar na Constituição**. Ed. Universitária de Direito, 1986, São Paulo.

TOMAEL, Maria Inês; ALCARA, Adriana Roseclerand DI CHIARA, Ivone Guerreiro. **Das redes sociais à inovação**. Ci. Inf.[online]. 2005, vol.34, n.2, pp. 93-104. ISSN 0100-1965.

TRIVIÑOS, Augusto Nivaldo Silva. **Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação**. São Paulo: Atlas, 1987. 175 p.

TROJANOWICZ, Robert; BUCQUEROUX; Bonnie. **Policamento Comunitário: como começar**. Tradução Mina Seinfeld de Carakushansky. 2 ed. São Paulo: Editora Parma, 1999.p.4|5.

VARGAS, Sérgio Rogério Silva de. **Educação não escolar e política de segurança pública: tensões emergentes**. / Sérgio Rogério Silva de Vargas. UNOESC, 2015.112f.

\_\_\_\_\_, **Manual de Policiamento Comunitário: Polícia e Comunidade na Construção da Segurança** [recurso eletrônico] / Núcleo de Estudos da violência da Universidade de São Paulo (NEV/USP). – Dados eletrônicos. - 2009.104 p. Disponível em:<http://www.nevusp.org/downloads/down247.pdf> . Acesso em 13/08/2016.

## **PLANEJAMENTO DE AÇÕES PARA APLICAÇÃO DA LEGISLAÇÃO ATUAL SOBRE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO CORRELACIONADA ÀS NORMAS EXISTENTES DENTRO DA INSTITUIÇÃO BRIGADA MILITAR**

*Deivis Noal Ferreira  
Solange Maria da Silva*

### **1 INTRODUÇÃO**

Este trabalho propõe que seja observada a legislação vigente, aplicando a realidade, viabilizando a possibilidade de desenvolver atividades possuindo um amparo legal nas mais diversas áreas de atuação. Ainda, pretende uma análise de correlação entre as leis aprovadas recentemente e o que existe na Corporação, com o objetivo de apontar as lacunas existentes. No meio Institucional é importante que exista previsão escrita regulamentando o uso dos serviços de tecnologia da informação e comunicação. Esses documentos devem possuir a definição de alguns conceitos para levar a conhecimento do usuário, principalmente, aquele que não possui formação técnica no assunto, cabe salientar que é a maioria. Será abordado o fenômeno informacional não apenas como uma construção social, mas o usuário da informação dentro da Instituição, limitado por um contexto político-histórico-cultural e que deve obedecer ao conteúdo das normas regulatórias vigentes.

Para analisar essas questões, tomou-se como referência teórico-metodológica a análise dos casos práticos observados na atividade fim, compreendendo a legislação e a análise doutrinária desses fenômenos, bem como uma breve explanação da tipificação dos delitos informáticos com o intuito de exemplificar as consequências para o uso indevido dos serviços. A pesquisa descreve alguns princípios que podem ser utilizados como referência, apontando as delimitações do objeto das Notas de Instrução da Instituição, indicando alternativas

para as situações em que ocorram cometimento de falta grave por usuários ao descumprir o previsto em norma. Também analisa princípios constitucionais que podem ser observados como referência para orientar a utilização das TIC pelos usuários. Salientando a importância da normatização interna da Instituição quanto ao auxílio aos gestores no controle do uso correto do acesso à informação.

Diante das garantias previstas na Constituição Federal, como o princípio da legalidade, quando alguém só poderá ser punido se, anteriormente ao fato praticado, existir lei que o considere como crime, ainda que o fato seja imoral, antissocial ou danoso não existirá a possibilidade de punir o autor.

Cabe ressaltar que a Constituição Federal estabelece que:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XXXIX – Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal...

A observância do princípio da legalidade leva ao questionamento da tipicidade do crime, em que um fato somente será típico se a lei descrever, previamente, todos os elementos da conduta humana tida como ilícita. Diante dos institutos da legalidade e tipicidade, buscou-se impor limites ao poder punitivo do Estado, em que um indivíduo somente pratica uma conduta prevista como crime, se a conduta assim se encontrar descrita dentro do nosso ordenamento vigente.

Segundo Pedroso (2008), penalista brasileiro:

Não basta, conseqüentemente, que o fato concreto, na sua aparência, denote estar definido na lei penal como crime. Há mister corresponda à definição legal. Nessa conjectura, imprescindível é que sejam postas em confronto e cotejo as características abstratas enunciativas do crime com as características ocorrentes no plano concreto, comparando-se uma a uma. Se o episódio a todas contiver, reproduzindo uma exatidão e fidelidade a sua imagem abstrata, alcançará a adequação típica. Isso porque ocorrerá a subsunção do fato ao tipo, ou seja, o seu encarte ou enquadramento à definição legal. Por via de consequência, realizada estará a tipicidade, primeiro elemento da composição jurídica do crime (PEDROSO, 2008, p.45).

Ante o exposto, para a caracterização do crime necessita de alguns fatores indispensáveis, como a tipificação expressa como crime por lei; uma conduta comissiva ou omissiva e sendo expressa como tal, seja também vigente para surtir efeitos perante todos. O princípio da tipicidade tem o objetivo de classificar as condutas humanas em normas penais proibitivas ou em normas negativas, incriminando todos os fatos que possam estar desviados de uma conduta aceita socialmente. Assim, e somente através dela, é que se pode verificar uma transgressão à norma penal e devido a tal agressão é que poderá cominar uma aplicação de uma pena.

Nos crimes informáticos, devido a uma falta ou ausência de normas legais que o tipifiquem, socorrem-se à analogia para tentar ajustar as condutas atípicas à norma penal e à realidade social, mesmo sendo proibitiva a aplicação desta dentro da esfera penal. Vale observar que a analogia jurídica aplicada na norma penal incriminadora não pode ser considerada válida, nos casos prejudiciais ao réu, como bem explica Capez (2010):

A aplicação da analogia em norma penal incriminadora fere o princípio da reserva legal, uma vez que um fato definido em lei como crime, estaria sendo considerado como tal. Imagine considerar típico o furto de uso (subtração de coisa alheia móvel para o uso), por força da aplicação da analogia do artigo 155 do Código Penal (subtrair coisa alheia móvel com ânimo de assenhoramento definitivo). Neste caso, um fato não considerado criminoso pela lei passaria a sê-lo, em evidente afronta ao princípio constitucional do art. 5º, XXXIX (reserva legal) (CAPEZ, 2010, p.59).

Com a evolução do tema, obrigou-se a elaboração de uma lei com alcance para regular exclusivamente crimes digitais, os casos existentes eram decididos com adaptações de artigos que já constavam no Código Penal brasileiro. Com a nova legislação, que criminaliza a invasão de dispositivos informáticos, subsidiou-se a Justiça com instrumentos próprios para esse tipo de situação, tornando-se assim mais ágil. Trazendo para o nível Institucional, para que ela possa ser utilizada para proporcionar resultados produtivos. O progresso da informática, por meio das TIC, em todas as áreas proporciona maior acessibilidade às tecnologias, acesso à rede mundial em qualquer lugar (*tablet, smartphones, notebooks*, etc.).

Diante dessas colocações iniciais, e seus desdobramento, o presente estudo irá percorrer diversos fatores relevantes no tocante à previsão legal e aos princípios norteadores correlacionados à realidade de outras Instituições. Para tal, apresentam-

Planejamento de ações para aplicação da legislação atual sobre tecnologia da informação e comunicação correlacionada às normas existentes dentro da instituição Brigada Militar

se os procedimentos metodológicos na seção 2. Após o planejamento da elaboração de tal estudo, realizam-se pesquisas sobre leis e normas reguladoras relacionadas a tecnologia da informação, a legislação aplicada a tecnologia da informação, e a definição de delitos informáticos (seções 3, 4 e 5 respectivamente). No item 6, relata-se sobre o planejamento de ações na área de TI para corporação, sendo finalizado o presente estudo com as considerações finais na seção 7.

## **2 PROCEDIMENTOS METODOLÓGICOS**

Para realização deste estudo, adotou-se estudo exploratório por meio de procedimentos bibliográficos e documentais, visando maior familiarização com as variáveis do estudo (FREIRE, 2013). Tal método servirá para ordenação e organização dos dados e saberes coletados, consiste em retirar conclusão genérica a partir de fatos particulares analisados e através de pesquisa de campo junto aos usuários.

Assim, a interpretação dos dados coletados está focada na análise dos fenômenos encontrados na atividade fim (estudo de campo), compreendendo a legislação e a análise doutrinária desses fenômenos. Ainda será observada a influência de tais fatores na instituição, sempre tendo como balizador o tema da pesquisa efetuada. Para dar prosseguimento utilizou-se método comparativo, no qual, partindo da pesquisa efetuada, serão comparados os institutos e procedimentos utilizados na aplicabilidade do tema. Então, espera-se que seja possível verificar as semelhanças e diferenças entre esses, de forma a ampliar o conhecimento na realidade atual da Instituição e seus efeitos.

## **3 LEIS E NORMAS DE REGULADORAS RELACIONADAS À TECNOLOGIA DA INFORMAÇÃO**

Diretrizes Gerais

A finalidade da estruturação em normas regulatórias deve ser estabelecer um padrão relativo ao gerenciamento do Sistema de Comunicações na Brigada Militar, desde a aquisição, o recebimento, a distribuição, o recolhimento, a desativação, a identificação, a manutenção de material e serviços na área de TIC. Segue o princípio da eficácia do Sistema de Comunicações, é garantida pela presteza, clareza, informalidade e uso correto da informação.

Planejamento de ações para aplicação da legislação atual sobre tecnologia da informação e comunicação correlacionada às normas existentes dentro da instituição Brigada Militar

### Notas de Instrução (NI)

Tem como objetivo uniformizar conceitos e fixar doutrina policial militar; padronizar a execução de atividades peculiares; unificar a interpretação da legislação em vigor, aplicada à Brigada Militar; definir processos corporativos. A elaboração das Notas de Instrução cabe aos Órgãos integrantes do Comando-Geral e aos que compõem o nível departamental de apoio (Departamentos).

### Notas de Instrução Temáticas

Ao observarmos especificamente as Notas de Instruções Temáticas vigentes, relacionadas à área de TIC, cabe destacar a nota de instrução tecnológica nº 001.1, de 25 de novembro de 2014, que prevê os procedimentos na Brigada Militar quanto à administração, às responsabilidades e à utilização do serviço de correio eletrônico adotado como canal oficial de comunicação na Corporação.

## **4 LEGISLAÇÃO APLICADA A TECNOLOGIA DA INFORMAÇÃO**

### Legislação Relacionada à Lei de Acesso à Informação

A Lei Nº 12.527, de 18 de novembro de 2011, dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações, previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

### Portaria nº. 119/2015-SSP/RS

No âmbito do Estadual, com objetivo de consolidar as normas de gestão, utilização, coordenação e supervisão dos sistemas de informação e dos bancos de dados criminais e administrativos utilizados no âmbito da Secretaria de Segurança Pública do Estado do Rio Grande do Sul e das instituições vinculadas: Brigada Militar, Instituto Geral de Perícias, Polícia Civil e Superintendência dos Serviços Penitenciários ou que sejam objeto de compartilhamento por meio de convênio ou instrumento.

## **5 DEFINIÇÃO DE DELITOS INFORMÁTICOS**

Para melhor entendimento quando se trata de delito ou crime, cabe uma breve descrição de conceitos dos elementos necessários para configuração do fato

típico, que é o primeiro substrato do crime, ou seja, o primeiro requisito ou elemento do crime. São elementos do fato típico a conduta, o resultado, o nexa causal entre a conduta e o resultado e a tipicidade. Na falta de qualquer desses elementos, o fato passa a ser atípico e, por conseguinte, não há crime.

Conduta é a ação ou omissão humana, voluntária e consciente, dolosa ou culposa, dirigida a determinada finalidade. O resultado é a transformação que a conduta criminosa provoca, é a lesão ou ameaça a um bem jurídico penalmente tutelado. Nexa Causal é o vínculo estabelecido entre a conduta do agente e o resultado. E a tipicidade é a ligação entre o fato e o tipo penal, é o enquadramento da conduta praticada à definição típica legal (CLAUDIO, 2017, p. 01).

Ainda no campo do entendimento, importante salientar a previsão de delito de acesso não autorizado a sistemas computacionais. Em rigor, para que um delito seja considerado informático é necessário que o bem jurídico por ele protegido seja a inviolabilidade de dados. A pura utilização do computador para a execução de um delito, não caracterizaria o crime informático, se o bem jurídico afetado não fosse a informação automatizada. Aos delitos em que o computador foi o instrumento para a execução do crime, mas não houve ofensa ao bem jurídico, inviolabilidade dos dados, definem-se os delitos informáticos impróprios e aqueles em que o bem jurídico afetado foi a inviolabilidade dos dados, denomina-se delitos informáticos próprios.

Segundo Viana (2001, p. 37), os crimes informáticos impróprios, nos quais o computador é mero instrumento de realização do crime, não havendo violação de dados, como nos casos de difamação, calúnia e injúria; crimes informáticos próprios, nos quais o bem jurídico violado são os dados computacionais; crimes informáticos mistos, nos quais há a violação de dados computacionais e de outros bens jurídicos distintos; crimes informáticos mediatos ou indiretos, os quais servem de instrumento para a consumação de outro delito não-informático, como no caso de furto de dinheiro de contas bancárias pelo computador.

Existem várias nomenclaturas que possam dirigir-se a esses delitos (virtuais, informáticos, cibernéticos, de informática, dentre outros), deve-se subdividir os crimes informáticos em dois grandes grupos, ficando o primeiro com os crimes violadores do computador e seus componentes; e o segundo com os crimes violadores de bens jurídicos já protegidos pelo ordenamento há tempos, sendo o computador o instrumento para sua realização.

Os delitos mais complexos em que tanto a norma que visa tutelar o bem jurídico, quanto à proteção da inviolabilidade dos dados, sejam afetados são

denominados como delitos fundamentos de direito penal informático Mistos. Nos casos em que um delito informático próprio é praticado como crime-meio para a realização de um crime-fim não informático, este acaba por receber daquele a característica de informático, será o delito informático mediante ou indireto

Os delitos informáticos Próprios são aqueles que a inviolabilidade é protegida pela norma penal no acesso a informações automatizadas. Além do delito de acesso não autorizado a sistemas computacionais, há ainda outras modalidades de crimes como a interferência em dados informatizados; é uma modalidade de crime informático próprio abrangida pelo acesso não autorizado a sistemas computacionais. A hipótese procura prevenir a alteração ou destruição de dados armazenados em sistemas computacionais e sua execução implica necessariamente em um acesso não autorizado.

Até a criação da lei 12.737 de 30 de novembro de 2012 a interferência em sistemas computacionais não estava tipificada no ordenamento jurídico brasileiro. A interceptação ilegal é um crime informático próprio no qual os dados são capturados durante sua transferência de um sistema computacional para outro. O agente não obtém acesso direto ao computador da vítima, limitando-se a interceptar os dados em trânsito entre duas máquinas. Assemelha-se a uma escuta telefônica (grampo), pois os dados são lidos durante sua transmissão.

Na legislação brasileira não havia um tipo penal específico visando à repressão dos vírus informáticos, mas era possível a punição utilizando como referência o crime de dano (art. 163 do CP) quando a conduta destruir, inutilizar ou deteriorar os dados armazenados no sistema computacional. Ademais, nota-se a impossibilidade do enquadramento da conduta do crime informático no crime de dano, tornando clara a necessidade da criação de um fato típico, para proteger o usuário da internet.

Conhecida como Lei Carolina Dieckmann, a Lei dos Crimes Cibernéticos 12.737 de 30 de novembro de 2012, alterando o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, que dispõe sobre a tipificação criminal de delitos informáticos, crimes relacionados ao meio eletrônico, como violar dados de usuários, invadir computadores ou tirar sites do "ar". O projeto que deu origem à lei foi elaborado na época em que fotos íntimas da atriz Carolina Dieckmann foram copiadas de seu computador e espalhadas pela rede mundial de computadores.

Com o objetivo de adequar o direito às mudanças tecnológicas que transformam rotineiramente a sociedade, visando suprir o vácuo legislativo que anteriormente havia sobre o tema, lembrando que no crime constitui fato típico,

devendo todas as suas nuances estarem previstas especificamente na norma, sob pena de atipicidade da conduta. Diante da falta de previsão específica da legislação, era muito difícil a identificação dos sujeitos e a obtenção de provas para a condenação criminal quanto aos crimes virtuais, que exige certeza.

A edição da Lei n. 12.737, introduzindo os arts. 154-A, 154-B, e alterando os arts. 266 e 298, do Código Penal:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Sobre o art. 154-A do Código Penal, cabe ressaltar que ele trouxe para o ordenamento jurídico o crime novo de “Invasão de Dispositivo Informático”, baseia-se na conduta de “invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou

tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”. A pena prevista para o crime simples é de detenção de 3 meses a um ano e multa, havendo, entretanto, a previsão das formas qualificada e causas de aumento de pena.

A redação do art. 154-A do CP, tende a proteger o bem jurídico tutelado representado pela liberdade individual, a privacidade e a intimidade das pessoas como de modo geral. É um crime comum e o sujeito ativo do crime cibernético pode ser qualquer pessoa (física ou jurídica, de direito público ou de direito privado) e sujeito passivo, pode ser qualquer pessoa passível de sofrer dano moral ou material decorrente da violação do seu sistema de informática. Crime de ação múltipla, apresentando os núcleos “instalar” e “invadir”, podendo o agente praticar ambas as condutas e responder por crime único no mesmo contexto.

O art. 154-A, § 1º, do CP, prevê a forma equiparada do crime cibernético, incriminando com a mesma pena do “*caput*” a conduta de quem “produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*”, sendo esse, também, um crime de ação múltipla que exige dolo específico, tal qual o *caput* do art. 154-A do CP.

O art. 154-A, § 2º, do CP presume causa de aumento de pena de um sexto a um terço, no caso da ocorrência de prejuízo de caráter econômico/financeiro para a vítima, sendo tal causa de aumento aplicável somente para a forma simples do delito, e não para a forma qualificada, prevista no parágrafo seguinte, em razão da topografia do dispositivo em comento.

O art. 154-A, § 3º, do CP cita pena e regime prisional diferenciado (seis meses a dois anos de reclusão e multa) para as seguintes hipóteses: 1) quando a invasão possibilitar a obtenção de conteúdo de comunicações eletrônicas privadas; 2) quando possibilitar a obtenção do conteúdo de segredos comerciais ou industriais; 3) quando possibilitar a obtenção do conteúdo de informações sigilosas, assim definidas em lei; e 4) quando possibilitar o controle remoto não autorizado do dispositivo invadido. Ressalte-se que as figuras qualificadas acima descritas configuram crime subsidiário, de subsidiariedade expressa, pois que em seu preceito secundário prevê a norma que ela somente será aplicada “se a conduta não constitui crime mais grave”.

Por sua vez, os parágrafos 4º e 5º, I a IV, do CP, ocorrem nas causas de aumento de pena, aplicáveis somente para a forma qualificada do delito (§ 3º, do art. 154-A, do CP).

Planejamento de ações para aplicação da legislação atual sobre tecnologia da informação e comunicação correlacionada às normas existentes dentro da instituição Brigada Militar

O artigo Art. 154-B destaca o procedimento previsto na ação penal:

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Nesse sentido, como se refere à crime condicionado à representação da vítima, muitos casos serão omitidos por falta de exercício do direito subjetivo, se o agente passivo for a União, Estados, DF ou Municípios ou contra empresas concessionárias de serviços públicos, a ação é incondicionada.

Art. 3 os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública  
Art. 266. ....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Falsificação de documento particular

Art. 298. ....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

O artigo 266 tipifica o crime de perturbação ou interrupção de serviços ligados à comunicação, estabelecendo a pena de 1 (um) a 3 (anos), e multa, para quem cometer o crime. Ao incluir os parágrafos, o ordenamento amplia o alcance da norma para os serviços telemáticos ou de utilidade pública, incluindo, assim, os ilícitos cometidos não só contra o interesse público, mas, também, contra dados informáticos, norte principal da inovação legislativa analisada.

O parágrafo incluído no artigo 298, que tipifica o crime de falsificação de documento particular, estende os efeitos da norma aos cartões de crédito e de débito, os quais receberam do legislador a qualidade de documento particular devidamente reconhecido, e protegido, pelo ordenamento.

## **6 PLANEJAMENTO DE AÇÕES NA ÁREA DE TI PARA CORPORAÇÃO**

### **6.1 A Política de Segurança da Informação e Comunicações (POSIC)**

Observando o guia de Orientações ao Gestor em Segurança da Informação e Comunicações (SIC), aprovado pelo Gabinete de Segurança Institucional, órgão essencial da Presidência da República, com o intuito de coordenar a atividade de Segurança da Informação e Comunicações, mantendo o compromisso do Estado de promover ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. Direcionada ao âmbito da Administração Pública Federal (APF), mas com conceitos perfeitamente utilizáveis no âmbito da Polícias Militares. A POSIC é um documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta ou indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SIC. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação de uma organização.

### **6.2 Orientações Derivadas do Departamento de Segurança da Informação e Comunicações (DSIC)**

O trabalho desenvolvido pelo Grupo de Trabalho (GT) – “Elaboração de Guia de Orientações ao Gestor de SIC”, instituído no âmbito do Comitê Gestor da Segurança da Informação (CGSI), por meio da Portaria Nº 26 do Conselho de Defesa Nacional (CDN), de 15 de julho de 2014, na qual reúne métodos e instrumentos, visando orientar os gestores, com importantes aspectos inerentes à relevância do tema nos dias atuais. O Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicações foi elaborado com o propósito de oferecer ao leitor orientações e dicas referentes à implementação das ações de segurança da informação nas organizações públicas federais, mas podem ser adotadas pelos demais Órgãos Públicos.

As políticas de Segurança da Informação específicas da Instituição devem ser de fácil leitura e entendimento, podem seguir a estruturação em níveis estratégico, tático e operacional conforme sugerido na Figura um (1).

Planejamento de ações para aplicação da legislação atual sobre tecnologia da informação e comunicação correlacionada às normas existentes dentro da instituição Brigada Militar

**Figura 1:** Políticas (Estratégico), Normas (Tático) e Procedimentos (Operacional).



**Fonte:** Guia básico de orientações ao gestor em segurança da informação e comunicações.

Ainda observando o Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicação publicado em 2015 pelo Governo Federal, recomenda-se a normatização dos respectivos assuntos, envolvendo as áreas de tecnologia, pessoas, ambiente e processos. Além disso, sugere-se que temas ainda não normatizados no governo federal, mas já amparados por outras normas, também sejam analisados à luz das necessidades específicas de cada órgão, vale citar alguns destes temas:

- 1) Planejamento e Gestão de SIC;
- 2) Tratamento da Informação;
- 3) Formação de Equipes de Tratamento de Incidentes de Segurança em Redes Computacionais;
- 4) Gerenciamento de Incidentes de Segurança em Redes Computacionais;

### **6.3 Fatores para Elaboração de um Plano de Gerenciamento**

Diante da resistência natural das mudanças, principalmente as culturais, muito presente dentro de uma Instituição Militar, da elevação do foco na tecnologia para o foco no usuário e da avaliação da TIC sob a perspectiva da prestação dos serviços, as atividades a serem realizadas devem buscar reduzir os impactos resultantes de um uso indevido dos meios disponíveis. Tais ações evitam a interrupção de serviços que possam afetar o desempenho da atividade fim, ou seja, interfira no policiamento ostensivo vindo a prejudicar, por exemplo a suspensão do

Planejamento de ações para aplicação da legislação atual sobre tecnologia da informação e comunicação correlacionada às normas existentes dentro da instituição Brigada Militar

uso de um serviço que traria mobilidade para o policial que está na rua atendendo ao público.

Assim, o plano de ação deve ser claramente definido e documentado, para ser usado quando ocorrer um incidente que atinja pessoas, recursos, serviços e outras ações ligadas à execução do serviço de ponta.

Alguns passos para desenvolver a estrutura das normas a serem aplicadas:

(A) Revisar conceitos e definições.

(B) Definir forma de coleta de informações.

(C) Relacionar áreas inseridas na abrangência do trabalho.

(D) Reunir com patrocinador do projeto.

(E) Reunir individualmente com as áreas para analisar as informações coletadas.

O treinamento minimiza as dificuldades para o desenvolvimento da estrutura por parte de quem gerencia. A fase de percepção de foco em serviços e processos, da expansão dos limites funcionais.

## **7 CONSIDERAÇÕES FINAIS**

O desenvolvimento do presente estudo possibilitou uma análise de como a previsão legal das TIC é de grande importância no ambiente dos Órgãos de TIC da Polícia Militar. Além disso, também permitiu uma pesquisa para obter dados mais consistentes sobre as etapas do processo, identificou que o grau de conhecimento em informática dos profissionais possui importantes implicações práticas, visto que, além de identificar a falta de previsão de obrigações do usuário, através de normas, para utilização da rede de dados, utilização da rede *e-mail*, até mesmo a utilização indevida de equipamentos de informática da Instituição e principalmente a utilização de dados/informações de uso exclusivo na atividade policial. Vale ressaltar que os resultados foram obtidos com base na análise dos processos disponíveis pela Instituição ao usuário final das TIC na PMERS, podendo este ser divergente no momento da implantação do plano de ação que por ventura venha ser executado. Estudos futuros podem analisar os efeitos dos resultados obtidos após implantação de um plano de ação nortear o uso das informações disponíveis.

Por isso, existe a necessidade de se elaborar uma política na qual determine previsão legal de procedimentos para as condutas praticadas nos crimes informáticos, inibindo a ocorrência desses delitos, tal ausência de regimento encoraja o surgimento de novos delitos nesse meio tecnológico. Seus agentes sempre serão agraciados com o benefício da impunidade, pois no direito penal não se pode atribuir uma pena ou impor uma sanção a uma conduta que o ordenamento penal não considere expressamente como criminosa, mesmo que tal conduta produza prejuízos financeiros ou atente contra a integridade humana, bens resguardados pelo direito penal. Embora atualmente estejamos presenciando o surgimento de novos tipos legais, que dado a suas singularidades, subsidiam os operadores do direito em geral, em todos os ramos legais e não só em relação à matéria penal.

A solução, então, passa necessariamente pela criação de normas específicas que venham trazer tipicidade a essas condutas perpetradas pelo uso das novas tecnologias acompanhadas de sanções penais específicas que coíbam a prática dos crimes informáticos que como dito, anteriormente, podem causar graves danos aos bens resguardados pelo direito penal.

Por fim, vale ressaltar que a existência desse tipo de delito não faz mais parte de nossa imaginação ou de um suposto futuro e sim da realidade atual que assola a todos, portanto, deve ser levada a sério pelas autoridades competentes no sentido de realizar de forma efetiva as mudanças necessárias para tentar acabar como o território sem lei instalado no universo virtual.

## REFERÊNCIAS

BARBOSA JUNIOR, Sergio Jose. Crimes informáticos: delitos virtuais no direito brasileiro. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 19, n. 4008, 22 jun. 2014. Disponível em: <<https://jus.com.br/artigos/29634>>. Acesso em: 23 março 2017

BARUFFI, Helder; CIMADON, Aristides. A metodologia científica e a ciência do Direito. 2. Ed. Dourados: Evangraf, 1997.

\_\_\_\_\_. A sociedade brasileira. São Paulo: Timétis, 1997.

BECCARIA. Dos Delitos e Das Penas, São Paulo: José Bushatsky, 1978

Planejamento de ações para aplicação da legislação atual sobre tecnologia da informação e comunicação correlacionada às normas existentes dentro da instituição Brigada Militar

BRASIL. Lei nº 9.394, de 20 de dezembro de 1996. Estabelece as Diretrizes da Educação Nacional. Diário Oficial [da República Federativa do Brasil], Brasília, v. 134, nº 248, 23 dez. 1996.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Diário Oficial [da República Federativa do Brasil], Brasília, seção 1, nº 01, 18 nov. 2011.

BRASIL. Presidência da República. Casa Militar. Departamento de Segurança da Informação e Comunicações. Guia básico de orientações ao gestor em segurança da informação e comunicações: versão 2.0 /Casa Militar, Departamento de Segurança da Informação e Comunicações; organizadores Danielle Rocha da Costa, José Ney de Oliveira Lima. – Brasília: Presidência da República, 2016.

CAPEZ, Fernando. Curso de Direito Penal, volume 1, parte geral. São Paulo; Saraiva, 2010.

CLAUDIO, Olívia. Crimes Cibernéticos: teoria do crime. Jusbrasil. <https://oliviaclaudio7.jusbrasil.com.br/artigos/446342507/delitos-informaticos>. Acesso em maio 2017.

MEDEIROS, João Bosco. Redação Científica: a prática de fichamentos, resumos, resenhas. 10ª ed. São Paulo: Atlas 2008.

MIRABETTI, JulioFabrinni, manual do direito penal, volume 2, parte especial, São Paulo. Atlas 27 de 2010.

PEDROSO, Fernando de Almeida. Direito Penal, Parte Geral: Estrutura do Crime. LEVD: São Paulo. 1993.

VIANA, Túlio Lima. Do acesso não autorizado a sistemas computacionais: fundamentos do direito penal informático. Belo Horizonte: UFMG, 2001. Disponível em: <<http://www.bibliotecadigital.ufmg.br>>. Acesso em: 24 mar. 2017

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. Manual de direito penal brasileiro: parte geral. 11.ed. São Paulo: Revista dos Tribunais, 2015.

## **O AMBIENTE VIRTUAL DE APRENDIZAGEM NA ESTRUTURAÇÃO DE TRABALHOS DE CONCLUSÃO DE CURSO: ESTRATÉGIAS DE EAD NO ENSINO SUPERIOR PRESENCIAL**

*Natana Lopes Pereira,  
Fernando José Spanhol  
Angelita Darela Mendes  
Giovani Mendonça Lunardi*

### **1 INTRODUÇÃO**

O uso constante das Tecnologias da Informação e Comunicação – TIC - vem gradativamente modificando a forma de absorção de conhecimento, desencadeando em uma nova construção cultural na sociedade denominada “*cultura digital*”. Essa contínua transformação ocasiona a necessidade de aperfeiçoar por meio das TIC o processo de ensino-aprendizagem, uma vez que a forma tradicional utilizada em sala de aula não é mais eficaz na nova geração de estudantes. Sousa *et al.* (2011) enfatizam que devido a essa evolução os cursos superiores estão aderindo ao uso de Ambientes Virtuais de Aprendizagem - AVA, como ferramenta auxiliar no ensino-aprendizagem.

O AVA, inicialmente destinado somente à Educação a Distância, era uma tecnologia educacional restrita e com recursos limitados. Com a evolução das TIC surgem inúmeros recursos tecnológicos que possibilitam maior interação entre os atores envolvidos minimizando diversas dificuldades encontradas pelos alunos na Ead, como por exemplo, o processo de comunicação entre orientando e orientador para elaboração de Trabalhos de Conclusão de Curso – TCC. Segundo Machado *et al.* (2014a) o aperfeiçoamento e constata atualização dessa tecnologia educacional

proporciona maior efetividade à elaboração de TCC por meio de técnicas (roteiro, atividades, suporte virtual e (ou) presencial).

Nesse contexto e diante da aderência das TIC no ensino superior presencial e a distância (Ead), o trabalho proposto tem como objetivo mediar o processo de estruturação de trabalhos de conclusão de cursos presenciais por meio do AVA, utilizando como estratégia Técnicas de Ead. Para atender tal objetivo, além do estudo de caso realizado, foram aplicados dois (2) instrumentos de coleta de dados às duas (2) turmas do curso de pós-graduação (lato sensu) em Tecnologias da Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos – Pós TIC SENASP. Destaca-se que o estudo de caso somente ocorreu na segunda turma do curso, para posteriormente realizar uma análise comparativa da mediação do AVA no processo interação e estruturação de TCC.

Oferecido na Universidade Federal de Santa Catarina – UFSC campus Araranguá, o curso Pós TIC SENASP utiliza a plataforma Moodle como suporte ao ensino presencial. Essa plataforma de acordo com Silva (2011) possui diversas ferramentas de TIC que contribuem no processo de ensino-aprendizagem. O curso é de modalidade presencial e de periodicidade quinzenal. É realizado no âmbito da Rede Nacional de Altos Estudos em Segurança Pública (RENAESP), através do termo de cooperação com a Secretaria Nacional de Segurança Pública (SENASP) do Ministério da Justiça (MJ).

O artigo está organizado nas seguintes seções: Primeira seção são apresentados os aspectos introdutórios da pesquisa. Na segunda seção expõe-se o embasamento teórico. Na seção três estão os métodos da pesquisa. Na quarta seção apresenta-se o roteiro de atividades elaborado para estruturação de trabalhos de conclusão de cursos presenciais, aplicado no AVA. Na seção cinco discutem-se os resultados da pesquisa. Na sexta seção finaliza-se com as considerações finais.

## **2 A UTILIZAÇÃO DO AMBIENTE VIRTUAL DE APRENDIZAGEM NA EDUCAÇÃO A DISTÂNCIA PARA ELABORAÇÃO DE TRABALHOS DE CONCLUSÃO DE CURSO**

A Educação a Distância - Ead - é conceituada por Moore e Kearsley (2010) como processo de comunicação que ocorre por meio de diversas tecnologias sendo caracterizada pelos atores envolvidos não estarem compartilhando ao mesmo

tempo o mesmo espaço físico. Segundo Caetano, Moraes e Zanin (2014) ela surgiu da necessidade de qualificação profissional e cultural por pessoas que não poderiam frequentar uma instituição de ensino de forma presencial.

A evolução dessas tecnologias e de novos recursos de mídias proporcionam mesmo à distância, de acordo com Simão Neto (2010), ensinar a saber, a saber fazer, a saber conhecer, a saber conviver e a saber ser, sendo esses processos fruto do diálogo, da colaboração, da troca de experiências por meio de recursos tecnológicos do Ambiente Virtual de Aprendizagem .

Poppe (2015) elenca a importância de desenvolver um ambiente com recursos que promovam a interação e acesso dos alunos, por meio de uma sala de aula virtual de estudos. Nesse ambiente o autor lista os recursos ou ferramentas que podem auxiliar o aluno no processo de ensino-aprendizagem como o e-mail, fórum, chat, tira dúvidas, espaço de postagem, material de apoio entre outros.

O aprimoramento das ferramentas de Tecnologias da Informação e Comunicação – TIC disponíveis no AVA proporcionam uma nova dimensão no processo de orientação de TCC em Ead, uma vez que os diversos recursos de comunicação disponíveis no AVA possibilitam maior interação entre orientado, orientador e tutor (SILVA; SIHRLEI; SILVA, 2012). No processo de orientação em Ead Machado *et al.* (2014a) relata que alguns estudantes perdem o contato com o orientador, sendo um agravante na orientação em Ead. O autor relata a importância da comunicação assíncrona entre os atores envolvidos no processo de orientação por meio de fóruns realizados a cada etapa do trabalho de monografia.

Poppe (2015) enfatiza que o processo de elaboração de TCC em Ead deve possuir um planejamento claro e objetivo e com etapas para o desenvolvimento do trabalho. Por meio do AVA deve-se promover espaços de interação utilizando chat a cada item definido, além de fóruns para dúvidas do TCC. Esses ambientes proporcionam maior proximidade e interação entre os discentes, orientadores e tutores auxiliando na orientação para definição de critérios primordiais para pesquisa.

### **3 PROCEDIMENTOS METODOLÓGICOS**

A pesquisa apresenta um estudo de caso realizado no curso Pós TIC SENASP turma 2015-2017 da Universidade Federal de Santa Catarina – UFSC Câmpus

Araranguá, sobre a utilização do AVA na elaboração de Trabalho de Conclusão de Curso – TCC. Freire (2013) caracteriza o estudo de caso, como um estudo aprofundado e exaustivo para identificar a aplicabilidade de uma teoria, suas limitações e diferenças.

Para melhor compreensão do estudo realizado utilizou-se a abordagem qualitativa ou mista. Essa abordagem de acordo Freire (2013, p.53) “pode ser entendida como uma pesquisa qualitativa que busca entender o contexto pela percepção de seus participantes, mas não abre mão da segurança oferecida pela pesquisa quantitativa”.

Segundo seus objetivos a pesquisa é caracterizada como pesquisa exploratória. Gil (2010, p.27) enfatiza que a pesquisa exploratória “tem como propósito proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses”.

Nos procedimentos para realização do estudo utilizou-se a pesquisa bibliográfica e documental. Marconi e Lakatos (2010, p.157) definem pesquisa documental como uma fonte de coleta de dados constituída de fontes primárias. A pesquisa bibliográfica, realizada por meio de leitura e análise de periódicos e livros, segundo Gil (2010) é desenvolvida mediante material já elaborado, principalmente livros, artigos científicos revistas, teses, entre outros.

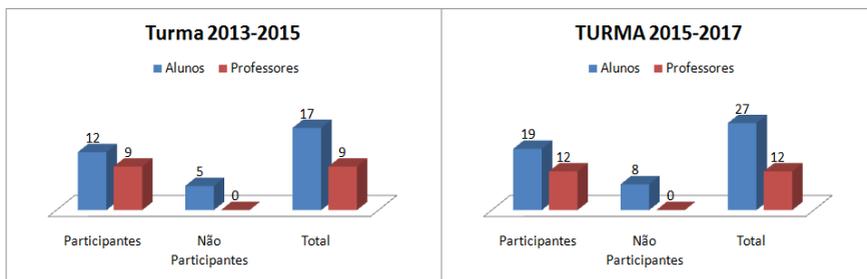
Para elaboração da pesquisa foi necessária a realização das seguintes fases: Estudo sobre a utilização de AVAs no processo de orientação na Ead; Coleta de dados turma 2013-2015; Elaboração e Aplicação do Roteiro de atividades turma 2015-2017; Coleta de dados turma 2015-2017; Análise e apresentação dos resultados.

Para especificação da concordância das afirmações dos formulários elaborados, utilizou-se a escala *Likert*, composta por cinco (5) níveis. De acordo com Rocha (2011), ela foi proposta por **Rensis Likert** em 1932, combina um conjunto de respostas em relação ao objeto pesquisado, em que os respondentes são solicitados a informarem o grau de concordância ou discordância das afirmações.

A pesquisa destinou-se aos profissionais de Segurança Pública e Direitos Humanos participantes do processo de orientação de Trabalho de Conclusão de Curso – TCC do curso Pós TIC SENASP e seus respectivos orientadores – professores da Universidade Federal de Santa Catarina – UFSC, que compõem o corpo docente do curso.

Na primeira turma (2013-2015), a pesquisa direcionou-se aos dezessete (17) alunos concluintes do curso e seus respectivos orientadores (nove (9) professores) obtendo retorno de nove (9) docentes e doze (12) discentes. Na turma 2015-2017 fizeram parte da pesquisa os alunos regulares (27 acadêmicos) e seus orientadores (doze (12) professores). Participaram da coleta de dados dezenove (19) discentes e doze (12) docentes.

**Figura 1** - Quantitativo participantes da pesquisa



**Fonte:** Desenvolvido pelos(as) autores(as).

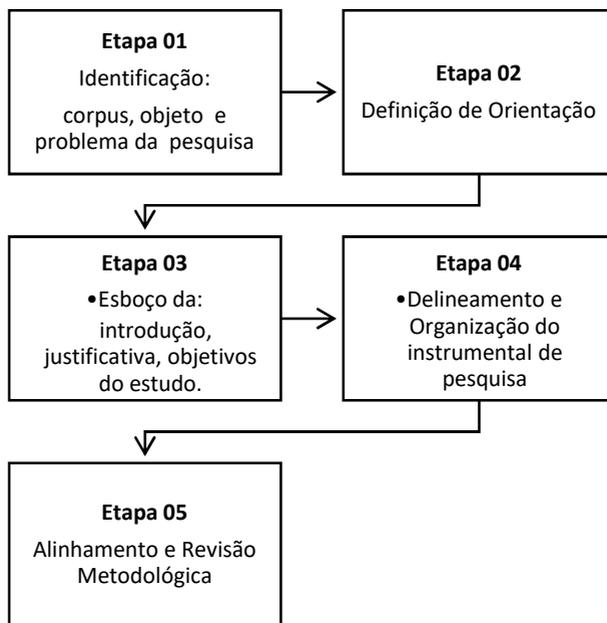
## 4 ESTRUTURA DO ROTEIRO PROPOSTO

O roteiro de atividades proposto aos alunos da segunda turma do curso (2015-2017) teve como principal ferramenta o recurso Fórum do AVA. Essa ferramenta segundo Silva (2011) é caracterizada pela possibilidade de envio de anexos, pela interação de forma assíncrona e pela troca de conhecimento. Saldanha (2011 *apud* MOORE; KEARSLEY, 2008) afirma que ele permite por meio de discussão de temas, o intercâmbio de sentidos, possibilitando o aprimoramento de competências e contribuindo para a construção colaborativa do conhecimento.

A forma de interação por meio do fórum foi dividida em três (3) modos, tendo como base a classificação de Machado *et al.* (2014b *apud* LÉVY, 1999): Muitos para muitos: Atividades em fóruns abertas sem restrições de grupos possibilitando interação entre os mesmos. Um para muitos: Fóruns com acesso restrito ao orientador e seus respectivos orientandos. Um para um: Fóruns com acesso restrito do orientador e o orientando individualmente.

As atividades propostas seguiram as seguintes etapas:

**Figura 2** - Etapas roteiro de atividades



**Fonte:** Desenvolvido(a) pelos(as) autores(as).

## 5 APRESENTAÇÃO E DISCUSSÃO DOS DADOS

Após análise dos dados coletados em pesquisa aplicada aos orientadores e orientandos das duas turmas do curso (2013 - 2015 e 2015 - 2017), pode-se realizar um estudo comparativo referente à utilização do Ambiente Virtual de Aprendizagem - AVA no processo de interação e estruturação das monografias.

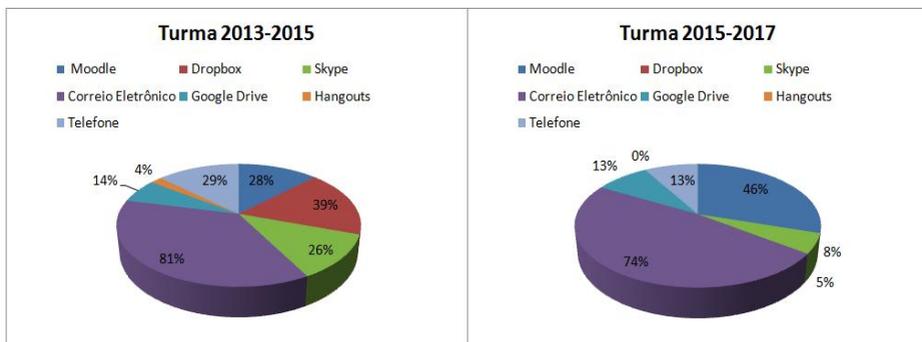
Na coleta de dados a pesquisa inicialmente demonstrou crescimento no número de elaboração de pré projetos de 42,2%, em comparação com a turma 2013-2015. Em relação ao processo de comunicação, os dados demonstraram que 60% dos orientadores da turma 2015-2017 interagiram de forma presencial com os orientandos. Em um comparativo com a turma 2013-2015 houve um aumento significativo na comunicação presencial de 40% dos envolvidos. A frequência de comunicação não sofreu alterações consideráveis, ocorrendo mensalmente por 60% (turma 2015-2017) e 55,60% (turma 2013-2015).

A pesquisa também analisou a utilização das TIC no processo de comunicação entre os atores envolvidos. Os resultados demonstraram que ocorreu uma redução de aproximadamente 40% na utilização das TIC como ferramenta de comunicação entre orientando e orientador em comparação à turma 2013-2015, sendo que 30% não obtiveram opinião e 10% discordaram totalmente.

Entre as tecnologias informadas pelos professores e alunos, destacou-se como a mais utilizada no processo de orientação em ambas as turmas o correio eletrônico. Na análise comparativa, pode-se identificar o aumento de 20% na utilização do Moodle, sendo identificado como a segunda tecnologia mais utilizada na turma 2015 - 2017.

Além do Correio Eletrônico e o Moodle em ambas as turmas, identificou-se também a utilização do *Google Drive*, *Telefone*, *Dropbox*, *Hangouts* e do *Skype* na turma 2013-2015, já na turma 2015-2017 os índices dessas tecnologias decaíram ou foram nulos.

**Figura 3** - Tecnologias utilizadas na interação



**Fonte:** Desenvolvido pelos(as) autores(as).

A pesquisa também indicou qual a tecnologia mais utilizada pelos alunos no decorrer do curso, sendo elencado o notebook em primeiro lugar. O telefone celular obteve o segundo maior índice com crescimento de 41,4% (primeira turma) para 78, 9% (segunda turma). Também analisou-se a utilização de tecnologias analógicas como o caderno sendo utilizado por 25% (primeira turma) 21,1% (segunda turma).

De acordo com a análise e comparação dos dados informados pelos professores/orientadores e alunos/orientandos de ambas as turmas, pode-se afirmar que o AVA contribui na estruturação de TCC. As atividades realizadas na turma 2015-

2017 impulsionaram o desenvolvimento do pré-projeto de pesquisa acarretando, de acordo com o quadro comparativo, crescimento de aproximadamente 40% na turma 2015-2017. As atividades de metodologia da pesquisa científica ocasionaram aumento na utilização do Moodle no processo de interação entre os atores envolvidos, incentivando também a definição do tema, orientador, e a comunicação presencial e (ou) por meio das TIC entre aluno e orientador.

Além da comunicação presencial ou por meio das TIC, em comparação à turma 2013-2015 houve crescimento da utilização do fórum como tecnologia mediadora no processo de interação entre aluno e orientador. Esse item demonstra a positiva interferência de técnicas de Ead no processo de comunicação (assíncrona) para elaboração da estrutura da monografia.

Alguns pontos importantes demonstrados nos dados coletados que cabe maior investigação é decorrente ao uso do AVA no processo de interação entre os atores envolvidos e o declínio da utilização de dispositivos móveis no processo de comunicação. Mesmo com a realização das atividades pelo recurso “fórum”, essa TIC não foi a mais utilizada nesse processo, sendo constatado o uso de outras tecnologias, por maior porcentagem dos pesquisados.

## 6 CONSIDERAÇÕES FINAIS

Após a execução do estudo de caso e realização de análise comparativa entre os dados coletados de ambas as turmas, pode-se confirmar a hipótese criada nesse trabalho, sobre a contribuição do AVA e técnicas de Ead no processo de estruturação de TCC no ensino superior presencial. Planejar a pesquisa por meio de uma estrutura clara, bem definida, e adquirir conhecimento em metodologia científica são itens essenciais indicados por Medeiros *et al.* (2015) para a elaboração de TCC.

A utilização de técnicas de Ead por meio dos recursos do AVA no processo de estruturação de monografias possibilitou a definição e delimitação do tema de pesquisa (pré projeto), o planejamento de estudo e maior interação entre os atores envolvidos (orientando e orientador). Além do aumento na comunicação presencial, o uso do AVA impulsionou a interação entre os protagonistas envolvidos por meio das TIC disponibilizadas nesse ambiente como, por exemplo, o aumento no uso da ferramenta “fórum”.

O AVA, inicialmente utilizado em Ead, visa possibilitar por meio de suas ferramentas de comunicação (síncrona e assíncrona) maior interação e mediação no processo de ensino aprendizagem. Nesse contexto cabe utilizar esses recursos de TIC do ambiente como estratégia no ensino superior presencial para maior efetividade no processo de elaboração de trabalhos científicos. Segundo Silva, Sihrlei e Silva (2012) o TCC é causador de desistências em cursos de graduação e pós-graduação, sendo um dos motivos a necessidade de comunicação constante entre os atores envolvidos.

De acordo com a pesquisa houve crescimento na utilização do AVA no processo de interação entre orientando e orientador, mas essa tecnologia não foi a mais utilizada. Com base nessa questão indicada e estendendo a discussão para trabalhos futuros, identifica-se a necessidade de maior investigação de métodos de interação entre aluno e professor para estruturação de TCC no AVA.

Visando maior eficiência e eficácia na utilização do ambiente nesse processo é necessário estudo sobre a Gestão do Conhecimento – GC em AVA. Cada vez mais as práticas de GC vêm sendo aplicadas no contexto educacional, por meio principalmente dos AVA. Neles são elaborados espaços colaborativos onde a construção e compartilhamento do conhecimento tanto tácito (conhecimento pessoal) como explícito (conhecimento registrado de forma tangível) é seu principal objetivo.

Segundo Dalkir (2005), a GC incorpora tanto a captura e armazenamento da perspectiva do conhecimento como a valorização dos ativos intelectuais. Cabe estudo sobre a forma de criação e compartilhamento desse conhecimento por meio do AVA tendo como base os modos de conversão de conhecimento elaborado por Takeuchi e Nonaka (2009) modelo SECI – Socialização, Externalização, Combinação e Internalização.

## REFERÊNCIAS

CAETANO, Camila Barreto Rodrigues Cochia; MORAES, Lucélia Leite de; ZANIM, Rosana Ruiz. **Tutoria e Docência na Modalidade a Distância**: Definição de Papéis. In: CIAED- CONGRESSO NACIONAL DE EDUCAÇÃO A DISTÂNCIA 2014, Paraná. **Anais**. Maringá: Ciaed, 2014. p. 1 - 10. Disponível em: <<http://www.abed.org.br/hotsite/20-ciaed/pt/anais/pdf/258.pdf>>. Acesso em: 12 abr. 2016.

DALKIR, Kimiz. **Knowledge management in theory and practice**. Amsterdam: Elsevier Butterworth-heinemann, 2005. 372 p..

FREIRE, Patrícia de Sá. **Aumente qualidade e quantidade de suas publicações científicas**: Manual para elaboração de projetos e artigos científicos. 1. ed. - Curitiba, PR: CRV, 2013.

GIL, Antônio Carlos Como Elaborar Projetos de Pesquisa. 5. ed. São Paulo: Atlas, 2010.

MACHADO, Andrea de Bem et al. **COMUNICAÇÃO NA EAD: UMA ANÁLISE NO PROCESSO DE ORIENTAÇÃO DE MONOGRAFIA**. In: CIAED- CONGRESSO NACIONAL DE EDUCAÇÃO A DISTÂNCIA, 20, 2014a, Florianópolis. **Anais**. Disponível em: <<http://www.abed.org.br/hotsite/20-ciaed/pt/anais/pdf/98.pdf>>. Acesso em: 15 out. 2016.

MACHADO, Andreia de Bem et al. **ORIENTAÇÃO NA EDUCAÇÃO A DISTÂNCIA: UMA ANÁLISE DA REALIDADE BRASILEIRA**. **Revista da Universidade Vale do Rio Verde**, Três Corações, v. 2, n. 12, p.149-158, dez. 2014b. Disponível em: <[http://revistas.unincor.br/index.php/revistaunincor/article/view/1419/pdf\\_196](http://revistas.unincor.br/index.php/revistaunincor/article/view/1419/pdf_196)>. Acesso em: 17 abr. 2016.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologias científica**. 7.ed. São Paulo: Atlas 2010.

MEDEIROS, B. C. et al. **DIFICULDADES DO PROCESSO DE ORIENTAÇÃO EM TRABALHOS DE CONCLUSÃO DE CURSO (TCC): UM ESTUDO COM OS DOCENTES DO CURSO DE ADMINISTRAÇÃO DE UMA INSTITUIÇÃO PRIVADA DE ENSINO SUPERIOR**. **Holos**, Rio Grande do Norte, v. 5, n. 31, p.242-255, set. 2015. Disponível em: <<http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/1011/1147>>. Acesso em: 20 jun. 2016.

MOORE, Michael; KEARSLEY, Greg. **Educação a Distância: Uma Visão Integrada**. São Paulo: Cengage Learning, 2010. 398 p.

POPPE, Maria da Conceição Maggioni. **TCC NA EAD: PROCESSO DE LETRAMENTO ACADÊMICO E DE PRODUÇÃO DO CONHECIMENTO NO ENSINO SUPERIOR**. In: CIAED- CONGRESSO NACIONAL DE EDUCAÇÃO A DISTÂNCIA, 21, 2015, Rio de Janeiro. **Anais**. Disponível em: <[http://www.abed.org.br/congresso2015/anais/pdf/BD\\_32.pdf](http://www.abed.org.br/congresso2015/anais/pdf/BD_32.pdf)>. Acesso em: 15 out. 2016.

ROCHA, Henrique Martins. **Abordagem metodológica na análise de dados de estudos não-paramétricos, com base em respostas em escalas ordinais**. Gepros, São Paulo, v. 3, n. 6, p.77-91, abr. 2011. Disponível em: <<http://revista.feb.unesp.br/index.php/gepros/article/view/649/358>>. Acesso em: 11 nov. 2016

SALDANHA, Camila Teixeira. **Interação nos Fóruns de Discussão: Uma análise Linguística**. 2011. 201 f. Dissertação (Mestrado) - Curso de Pós-graduação em Educação, Universidade Federal de Santa Catarina, Florianópolis, 2011.

SILVA, Ana Paula Costa e; SIHLER, Anelise Pereira; SILVA, Chris Alves da. **ORIENTAÇÃO DE TRABALHOS DE CONCLUSÃO DE CURSO A DISTÂNCIA: UMA EXPERIÊNCIA FUNDAMENTADA NA INTERAÇÃO**. Renote, UFRGS, v. 10, n. 1, p.1-07, jul. 2012. Disponível em: < [seer.ufrgs.br/renote/article/download/30855/19211](http://seer.ufrgs.br/renote/article/download/30855/19211) >. Acesso em: 15 maio 2016.

SILVA, Robson Santos da. **MOODLE para autores e tutores**. 2. ed. São Paulo: Novatec Editora, 2011.

SIMÃO NETO, Antonia. **Cenários e Modalidades da Ead**. Curitiba: Iesde Brasil S. A., 2010. 219 p.

SOUSA, Robson Pequeno de et al (Org.). **Tecnologias Digitais na Educação**. 21. ed. Campina Grande: Eduepb, 2011. 274 p.

TAKEUCHI, Hirotaka; NONAKA, Ikujiro. **Gestão do Conhecimento**. Porto Alegre: Bookman, 2009. 320 p.

# Sobre os organizadores

**Angelita Darela Mendes** – Licenciada em Letras - Língua Italiana pela Universidade Federal de Santa Catarina (1993), mestrado em Linguística e Letras pela Universidade Federal de Santa Catarina (2000) e doutorado em Educação pela Universidade de São Paulo (2009). Experiência nas modalidades de ensino presencial e a distância nas áreas de: Linguística Aplicada - atuando principalmente com ensino de leitura e escrita, formação de professores, Metodologia científica e Letramentos.

**Fernando José Spanhol** – Doutor em Mídia e Conhecimento pela Universidade Federal de Santa Catarina (UFSC). Atualmente, é professor adjunto e professor permanente dos Programas de Pós-Graduação em Engenharia e Gestão do Conhecimento (PPGEGC) e em Tecnologias da Informação e Comunicação (PPGTIC), todos na UFSC.

**Giovani Mendonça Lunardi** – Pós-doutor em Filosofia (PPG Filosofia) pela Unisinos junto à Cátedra Unesco de Direitos Humanos. É professor associado e professor permanente do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC). Foi coordenador das turmas de Especialização em Tecnologias da Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos, em convênio UFSC-SENASP/MJ.

**Márcio Vieira de Souza** – Doutor em Engenharia de Produção pela Universidade Federal de Santa Catarina (UFSC). É professor Adjunto da Universidade Federal de

Santa Catarina (UFSC) onde é um dos líderes do Grupo de Pesquisa de Mídia e Conhecimento da UFSC (CNPq) e atua no Departamento de Engenharia e Gestão do Conhecimento (DEGC-UFSC). É professor permanente no Programa de Pós-graduação em Engenharia e Gestão do Conhecimento, todos na UFSC.

**Natana Lopes Pereira** – Mestranda em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (PPGTIC/UFSC) Possui graduação em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (2016).

## Sobre os autores

**Angelita Darela Mendes** – Licenciada em Letras - Língua Italiana pela Universidade Federal de Santa Catarina (1993), mestrado em Linguística e Letras pela Universidade Federal de Santa Catarina (2000) e doutorado em Educação pela Universidade de São Paulo (2009). Experiência nas modalidades de ensino presencial e a distância nas áreas de: Linguística Aplicada - atuando principalmente com ensino de leitura e escrita, formação de professores, Metodologia científica e Letramentos.

**Antônio Altino de Farias** – Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina (Pós TIC SENASP). Especialização em Políticas e Gestão em Segurança Pública - FESDB (2015), Graduação de Gestão Empreendedora pela Faculdade de Tecnologia Radial de Curitiba (2007). Atualmente é agente penitenciário - Secretaria de Estado da Justiça e Cidadania - SC. Tem experiência na área de administração, planejamento estratégico, tecnologias da Informação e comunicação aplicadas a segurança pública e direitos humanos.

**Alexandre Leopoldo Gonçalves** – Possui graduação em Ciência da Computação pela Fundação Universidade Regional de Blumenau, mestrado e doutorado em Engenharia de Produção pela Universidade Federal de Santa Catarina. Atualmente é Professor Adjunto lotado no Campus Araranguá/UFSC e Professor Permanente do Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento/UFSC. Tem experiência nas áreas de Ciência da Computação e Engenharia do Conhecimento.

**Bruna da Silva Pires** – Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina (Pós TIC SENASP). Bacharel em Direito pela Universidade do Extremo Sul Catarinense. Atualmente, é Soldado da Polícia Militar de Santa Catarina.

**Deivis Noal Ferreira** – Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina (Pós TIC Senasp). Bacharel em Direito pelo Centro Universitário Metodista de Porto Alegre. Atualmente, é Policial Militar do Rio Grande do Sul.

**Edna Gusmão de Góes Brennand** – Possui Pós-Doutorado pela Université Catholique de Louvain-UCL Bélgica (2005) e na Universidade Lusófona de Humanidades e Tecnologias- ULHT -Portugal (2012). Doutorado em Sociologia - Université Paris I Panthéon Sorbonne. Mestrado em Educação pela Universidade Federal da Paraíba. Atualmente é Professora Titular da Universidade Federal da Paraíba. Coordenadora do Programa de Pós-Graduação em Gestão nas Organizações Aprendentes- MPGOA.

**Eliane Pozzebon** – Professora de graduação e pós-graduação da Universidade Federal de Santa Catarina (UFSC). Fez o Doutorado na Engenharia Elétrica com ênfase em Automação e Sistemas na Universidade Federal de Santa Catarina (2008). Possui mestrado em Ciências da Computação pela Universidade Federal de Santa Catarina (2003), especialização em Engenharia de Software (1999) e graduação em Processamento de Dados (1998). Coordenadora do curso de Engenharia da Computação da UFSC. Coordenadora do Laboratório de Tecnologias Computacionais (LabTeC-UFSC). Líder do grupo de pesquisa de Tecnologias Computacionais (CNPQ). Pesquisadora na área de inteligência artificial, jogos digitais, dispositivos móveis.

**Fernando José Spanhol** – Doutor em Mídia e Conhecimento pela Universidade Federal de Santa Catarina (UFSC). Atualmente, é professor adjunto e professor permanente dos Programas de Pós-Graduação em Engenharia e Gestão do Conhecimento (PPGEGC) e em Tecnologias da Informação e Comunicação (PPGTIC), todos na UFSC.

**Fernando Lúcio Mendes** – Delegado de Polícia Civil. Formado em Direito pela Pontifícia Universidade Católica de Minas Gerais. Especialista em Ciências Criminais pela Universidade Cândido Mendes. Especialista em Tecnologias da Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos pela UFSC. Mestrando em Tecnologias da Informação e Comunicação na UFSC.

**Giovani Mendonça Lunardi** – Pós-doutor em Filosofia (PPG Filosofia) pela Unisinos junto à Cátedra Unesco de Direitos Humanos. É professor associado e professor permanente do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC). Foi coordenador das turmas de Especialização em Tecnologias da Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos, em convênio UFSC-SENASP/MJ.

**Juarez Bento da Silva** – Possui graduação em Administração de Empresas pela Pontifícia Universidade Católica do Rio Grande do Sul (1991), mestrado em Ciências da Computação pela Universidade Federal de Santa Catarina (2002) e doutorado em Engenharia e Gestão do Conhecimento pela Universidade Federal de Santa Catarina (2007). Atualmente é professor adjunto da Universidade Federal de Santa Catarina onde atua como docente nos cursos de graduação em Engenharia de Computação e Tecnologias da Informação e Comunicação e também no Programa de Pós-Graduação em TIC.

**Luciana Bolan Frigo** – Doutora em Engenharia Elétrica pela Universidade Federal de Santa Catarina (UFSC) e doutora em Informática pela Université de Toulouse 1 (2007). Atualmente, é professora adjunta e professora colaboradora do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC) na UFSC.

**Macon dos Santos Borges** – Especialista em Tecnologias da Informação e Comunicação aplicadas a Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina Pós TIC SENASP. Possui graduação em Marketing pela Universidade Norte do Paraná (2014). Atualmente é soldado - Polícia Militar do Estado de Santa Catarina.

**Milena Petters Melo** – Possui graduação em Direito, UFSC (Brasil, 1999); Formação em Direitos Humanos junto ao Instituto Interamericano de Derechos Humanos, IIDH (Costa Rica, 2001); Doutorado em Direito, Università degli Studi di Lecce, UNISALENTO (Itália, 2004). Atualmente é Professora Titular de Direito Constitucional e “ Direitos Humanos e sustentabilidade ” da Universidade Regional de Blumenau - FURB. Coordenadora Local do Doutorado Interinstitucional em Direito DINTER FURB/UNISINOS. Professora e Coordenadora para a área lusófona do Centro Didático Euro-Americano sobre Políticas Constitucionais - CEDEUAM, UNISALENTO, Itália. Professora da Academia Brasileira de Direito Constitucional - ABDConst. Professora do Programa de Doutorado em Ciências Jurídicas e Políticas, Universidade Pablo de Olavide - UPO, Espanha. Professora no Programa Máster-Doutorado Oficial da União Européia Derechos Humanos, Interculturalidad y Desarrollo, Universidade Pablo de Olavide - UPO/Univesidad Internacional da Andaluzia - UNIA, Espanha.

**Natana Lopes Pereira** – Mestranda em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (PPGTIC/UFSC) Possui graduação em

Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (2016).

**Paulo César Leite Esteves** – Doutor pelo Programa de Pós-Graduação do Departamento de Engenharia de Produção e Sistemas da Universidade Federal de Santa Catarina (UFSC). Atualmente é professor adjunto e professor permanente da Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC), ambos na UFSC.

**Roberto Hideo Omomo** – Especialista em Tecnologia de Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos da Universidade Federal de Santa Catarina campus Araranguá Médico graduado pela Universidade Federal do Rio Grande do Sul (UFRGS), Cirurgião Geral pelo Hospital de Clínicas do Porto Alegre (HCPA), Bacharel em Direito pela Universidade do Sul de Santa Catarina (UNISUL) campus Araranguá. Atua como cirurgião geral do Hospital São Donato de Içara, Perito Médico Legista do IML de Araranguá.

**Roderval Marcelino** – Doutor em Engenharia de Minas, Metalúrgica e de Materiais pela Universidade Federal do Rio Grande do Sul (UFRGS). Atua como professor adjunto e professor permanente do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC), ambos na UFSC.

**Ronnie Carlos Tavares Nunes** – Mestrando em Engenharia e Gestão do Conhecimento pela UFSC. Especialista em TIC aplicada à Segurança Pública e Direitos Humanos e em Gestão Estratégica de TIC. Graduação em Processamento de Dados - Uni-Anhanguera (1995). Atuou como oficial R/2 do Exército Brasileiro. Atualmente é servidor público. Tem experiência na área de TIC, com ênfase em Administração de Redes.

**Samuel Nunes Juliani** – Especialista em TIC aplicados à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina – UFSC, e Pós-graduando em Engenharia de Software pela ESUCRI. Bacharel em Sistemas de Informação pela Escola Superior de Criciúma – ESUCRI.

**Solange Maria da Silva** – Doutora em Engenharia de Produção e Sistemas pela Universidade Federal de Santa Catarina (UFSC). Atualmente, é professora adjunta na mesma instituição.

**Sonia Maria Dall’Igna** – Mestranda em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (PPGTIC/UFSC). Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina (Pós TIC SENASP). Bacharel em Ciências Jurídicas e Sociais pela Universidade do Vale do Rio dos Sinos. Atualmente, é diretora da Divisão de Prevenção e Educação (Dipe), do Departamento Estadual de Investigação do Narcotráfico da Polícia Civil do Rio Grande do Sul.

**Thiago Marcos Ferreira** – Especialista em Tecnologias da Informação e Comunicação aplicados à Segurança e os Direitos Humanos pela Universidade Federal de Santa Catarina (2017), cursando Pós-graduação em Gestão Pública Municipal pelo Instituto Federal de Santa Catarina (2017). Possui graduação em Direito pela Universidade do Extremo Sul Catarinense (2010). Atualmente é servidor público de carreira da Polícia Civil de Santa Catarina.

**Wilson Gruber** – Doutor em Engenharia de Minas, Metalúrgica e de Materiais pela Universidade Federal do Rio Grande do Sul (UFRGS). Atua como professor adjunto e professor permanente do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC), ambos na UFSC.

**Vladmir Braga de Lima** – Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina (Pós TIC SENASP). Tecnólogo em Redes de Computadores pelo Instituto Brasileiro de Gestão de Negócios. Atualmente, é Policial Militar e Administrador de Redes de Computadores no Departamento de Informática da Brigada Militar do Rio Grande do Sul.



**LA MÍDIA**  
GRUPO DE PESQUISA  
MÍDIA E CONHECIMENTO UFSC



**SENASP**

**Renaesp**  
Rede Nacional de Altos Estudos em Segurança Pública



**UFSC**



**PPGTIC**



**FAPEU**

ISBN 978-85-5881-007-4



9 788556 810074