

Fernando J. Spanhol • Giovani M. Lunardi
Márcio Vieira de Souza
organizadores

TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NA SEGURANÇA PÚBLICA E DIREITOS HUMANOS



COLEÇÃO MÍDIA, EDUCAÇÃO, INOVAÇÃO e CONHECIMENTO

VOLUME 2

Blucher Open Access

Fernando José Spanhol
Giovani Mendonça Lunardi
Márcio Vieira de Souza
(organizadores)

Tecnologias da informação e comunicação na segurança pública e direitos humanos



Blucher

Tecnologias da informação e comunicação na segurança pública e direitos humanos

© 2016 Fernando José Spanhol / Giovani Mendonça Lunardi / Márcio Vieira de Souza (organizadores)

Editora Edgard Blücher Ltda.

Blucher

Rua Pedroso Alvarenga, 1245, 4º andar

04531-934 – São Paulo – SP – Brasil

Tel 55 11 3078-5366

contato@blucher.com.br

www.blucher.com.br

Segundo Novo Acordo Ortográfico, conforme 5. ed.
do *Vocabulário Ortográfico da Língua Portuguesa*,
Academia Brasileira de Letras, março de 2009.

É proibida a reprodução total ou parcial por quaisquer
meios, sem autorização escrita da Editora.

Todos os direitos reservados pela Editora
Edgard Blücher Ltda.

FICHA CATALOGRÁFICA

Tecnologias da informação e comunicação na
segurança pública e direitos humanos / organização
de Fernando José Spanhol, Giovani Mendonça
Lunardi, Márcio Vieira de Souza. – São Paulo: Blucher,
2016.

206 p.; pdf.

Bibliografia

ISBN 978-85-8039-176-3 (e-book)

ISBN 978-85-8039-177-0 (impresso)

Open Access

1. Tecnologia da informação 2. Segurança pública
3. Direitos humanos I. Spanhol, Fernando José II.
Lunardi, Giovani Mendonça III. Souza, Márcio Vieira de

16-0587

CDD 004

Índice para catálogo sistemático:

1. Tecnologia da informação

Agradecimentos

Esta obra foi elaborada com recursos da Secretaria Nacional de Segurança Pública (SENASP), do Ministério da Justiça (MJ), por meio do Edital SENASP nº 006/2012, vinculado à Rede Nacional de Altos Estudos em Segurança Pública (RENAESP).

Os temas aqui apresentados são frutos de pesquisas executadas por professores e alunos do curso de especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos (turma 2013-2015), da Universidade Federal de Santa Catarina – *Campus* Araranguá, pertencente ao Programa de Pós-Graduação do Mestrado Interdisciplinar em Tecnologias da Informação e Comunicação (PPGTIC).

A organização desta obra coube aos pesquisadores do Laboratório de Mídia e Conhecimento do *Campus* Araranguá (UFSC/SC).

Conselho editorial da coleção “mídia, educação, inovação e conhecimento”

COORDENADOR DO CONSELHO EDITORIAL

Dr. Marcio Vieira de Souza – Universidade Federal de Santa Catarina (UFSC)

CONSELHO EDITORIAL

Dr. Alexandre Marino Costa – Universidade Federal de Santa Catarina (UFSC)

Dr.^a Alexandra Okada – Open University (Inglaterra)

Dr.^a Araci Hack Catapan – Universidade Federal de Santa Catarina (UFSC)

Dr. Carlos Alberto de Souza – Universidade Estadual de Ponta Grossa (UEPG)

Dr.^a Clarissa Stefani – Universidade Federal de Santa Catarina (UFSC)

Dr.^a Eliane Schlemmer – Universidade do Vale do Rio dos Sinos (Unisinos)

Dr. Francisco Antonio Pereira Fialho – Universidade Federal de Santa Catarina (UFSC)

Dr. Pablo Lucas – University College Dublin (Irlanda)

Dr. Fernando Jose Spanhol – Universidade Federal de Santa Catarina (UFSC)

Dr. Giovani Mendonça Lunardi – Universidade Federal de Santa Catarina (UFSC)

Dr.^a Greicy K. Spanhol Lenzi – Faculdade AEROTD (Faero)

Dr. José Manuel Moran – Universidade de São Paulo (USP)

Dr. Kamil Giglio – Teltec Solutions/Faculdade AEROTD (Faero)

Dr.^a Karina Marcon – Universidade do Estado de Santa Catarina (Udesc)

Dr. Luiz Palazzo – Universidade Católica de Pelotas (UCPEL)

Dr. Marcio Vieira de Souza – Universidade Federal de Santa Catarina (UFSC)

Dr.^a Mara Lucia Fernandes Carneiro – Universidade Federal do Rio Grande do Sul (UFRGS)

Dr.^a Margarita Victoria Gomez – Universidade Federal do Rio de Janeiro (UFRJ)

Dr.^a Marina Keiko Nakayama – Universidade Federal de Santa Catarina (UFSC)

Dr.^a Ofelia Morales – Universidade Estadual de Ponta Grossa (UEPG)

Dr.^a Patricia Lupion Torres – Pontifícia Universidade Católica do Paraná (PUC-PR)

Dr.^a Patricia Jantsch Fiuza – Universidade Federal de Santa Catarina (UFSC)

Dr.^a Ricardo Azambuja Silveira – Universidade Federal de Santa Catarina (UFSC)

Dr. Robson Rodrigues Lemos – Universidade Federal de Santa Catarina (UFSC)

Dr.^a Roselaine Ripa – Universidade do Estado de Santa Catarina (Udesc)

Dr.^a Silvia Quevedo – Universidade Federal de Santa Catarina (UFSC)

Dr. Tarcisio Vanzin – Universidade Federal de Santa Catarina (UFSC)

Dr.^a Vânia Ribas Ulbricht – Universidade Federal de Santa Catarina (UFSC)

Sobre os autores

Alexandre Leopoldo Gonçalves – Doutor em Engenharia de Produção 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.

Alberto Felipe Friderichs Barros – Mestrando do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (PPGTIC/UFSC). Graduado em Tecnologia em Telecomunicações pela Universidade do Extremo Sul Catarinense. Atualmente, é coordenador de Tecnologia da Informação e Comunicação no Instituto Federal de Santa Catarina (IFSC) – *Campus* Criciúma.

Daiane Oliveira João – 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 Ciência da Computação pela Universidade do Extremo Sul de Santa Catarina. Atualmente, é analista de sistemas.

Eduardo Santos Acosta – 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 de Santa Cruz do Sul. Atualmente, é bombeiro militar do Rio Grande do Sul.

Elbio Carlos Bock – 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 Luterana do Brasil. Atualmente, é agente da Polícia Civil do Rio Grande do Sul.

Eliane Pozzebon – Doutora em Engenharia Elétrica com ênfase em Automação e Sistemas pela Universidade Federal de Santa Catarina (UFSC). Atualmente, é

professora adjunta e professora permanente do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC), ambos na UFSC.

Emerson Wendt – Mestre em Direito pelo Centro Universitário La Salle (UnilaSalle), de Canoas (RS). Graduado em Ciências Jurídicas e Sociais/Direito pela Universidade Federal de Santa Maria (UFSM). Atualmente, é chefe de Polícia na Polícia Civil do Rio Grande do Sul.

Fernanda Todesco Nunes – Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina (Pós TIC Senasp). Licenciada em Matemática pela UFSC. Atualmente, é agente da Polícia Civil de Santa Catarina.

Fernando Henrique Borges 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 pela UFSC. Atualmente, é escrivão da Polícia Civil.

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/Unisinos de Direitos Humanos e ao Grupo de Pesquisa Ética, Biopolítica e Alteridade. Atua como professor adjunto e professor permanente dos Programas de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC) e em Energia e Sustentabilidade (PPGES), todos na UFSC.

Herbson de Carvalho – 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 Administração pela Universidade Norte do Paraná. Atualmente, é soldado qpm-1 – Brigada Militar do Rio Grande do Sul.

João Bosco da Mota Alves – Doutor em Engenharia Elétrica pela coordenação dos cursos de Pós-Graduação em Engenharia da Universidade Federal do Rio de Janeiro (COPPE/UFRJ). Atualmente, é professor voluntário nos Programas de Pós-Graduação em Engenharia e Gestão do Conhecimento (PPGEGC) e em Tecnologias da Informação e Comunicação (PPGTI), ambos na UFSC.

Joel Souza de Oliveira – Mestrando 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 UFSC (Pós TIC Senasp). Bacharel em Ciên-

cias Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS). Atualmente, é delegado de Polícia da Polícia Civil do Estado do Rio Grande do Sul.

Josiel Pereira – Mestrando do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (PPGTIC/UFSC). Bacharel em Tecnologias da Informação e Comunicação pela UFSC. Atualmente, é bolsista pela Fundação de Apoio à Pesquisa Científica e Tecnológica do Estado de Santa Catarina (Fapesc).

Juarez Bento da Silva – Doutor em Engenharia e Gestão do Conhecimento pela Universidade Federal de Santa Catarina (UFSC). Atua como professor adjunto e professor permanente do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC) na UFSC.

Laudelino Joaquim – 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 Ciência da Computação pela Universidade do Sul de Santa Catarina. Atualmente, é soldado da Polícia Militar de Santa Catarina.

Leandro da Silva dos Reis – 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 Sul de Santa Catarina. Atualmente, é agente da Polícia Civil de Santa Catarina.

Lorielcio da Silva Peres – 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 Administração pela UFSC. Atualmente, é gerente de projetos e consultor.

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.

Márcio Giani Rosa de Matos – Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina (Pós TIC Senasp). Licenciado em História pela Universidade Luterana do Brasil. Atualmente, é sargento da Polícia Militar de Santa Catarina.

Márcio Vieira de Souza – Doutor em Engenharia de Produção pela Universidade Federal de Santa Catarina (UFSC). É professor adjunto e professor permanente nos Programas de Pós-Graduação em Tecnologia da Informação e Comu-

nicação (PPGTIC) e em Engenharia e Gestão do Conhecimento (PPGEGC), todos na UFSC.

Marta Adriana da Silva Cristiano – Doutoranda em Engenharia e Gestão do Conhecimento pela Universidade Federal de Santa Catarina (PPGEGC/UFSC). Graduada em Ciência da Computação pela Universidade do Sul de Santa Catarina. Atualmente, é pesquisadora do Laboratório de Experimentação Remota (RExLab) e do Grupo de Pesquisa INOVAmid – Subjetividade e Inovação em Mídias do Conhecimento na Sociedade em Rede (UFSC).

Natana Lopes Pereira – Bacharelanda em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (UFSC). Atualmente, é bolsista do curso Pós TIC Senasp – Especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos.

Norton Meidel Karam – Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos pela Universidade Federal de Santa Catarina (Pós TIC Senasp). Graduado em Engenharia Química pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS). Atualmente, é perito criminal do Instituto Geral de Perícias do Rio Grande do Sul.

Paulo Cesar 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.

Priscila Cadorin Nicolete – Mestranda do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação pela Universidade Federal de Santa Catarina (PPGTIC/UFSC). Bacharel em Tecnologias da Informação e Comunicação pela UFSC. Atualmente, é bolsista pelo Centro Anhanguera de Promoção e Educação Social (Capes).

Rangel Machado Simon – Mestrando do Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento pela Universidade Federal de Santa Catarina (PPGEGC/UFSC). Bacharel em Tecnologias da Informação e Comunicação pela UFSC. Atualmente, é professor do Instituto Mix e pesquisador laboratório de mídia e informação da UFSC.

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.

Rosinei Freitas da Rosa – Especialista em Tecnologias da Informação e Comu-

nicação 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 do Estado de Santa Catarina.

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.

Sônia 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.

Thabata Clezar de Almeida – Mestranda pelo Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento (PPGEGC/UFSC). Bacharel em Direito pela Universidade do Sul de Santa Catarina. Atualmente, é advogada da Ordem dos Advogados do Brasil de Santa Catarina (OAB-SC).

Vilson 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.

Sobre os organizadores

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/Unisinos de Direitos Humanos e ao Grupo de Pesquisa Ética, Biopolítica e Alteridade. É professor adjunto e professor permanente dos Programas de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC) e em Energia e Sustentabilidade (PPGES), todos na UFSC.

Márcio Vieira de Souza – Doutor em Engenharia de Produção pela Universidade Federal de Santa Catarina (UFSC). É professor adjunto e professor permanente nos Programas de Pós-Graduação em Tecnologia da Informação e Comunicação (PPGTIC) e em Engenharia e Gestão do Conhecimento (PPGEGC), todos na UFSC.

Prefácio

Muito me honra o convite para prefaciар um livro escrito por dezenas de mãos e mentes brilhantes e ávidas pelo debate acadêmico. Não poderia deixar de atender à convocação do Prof. Dr. Giovanni M. Lunardi, da Universidade Federal de Santa Catarina (UFSC), *Campus* de Araranguá/SC, local onde tive o privilégio de palestrar.

Os autores inovam em seus escritos, abrangendo o uso da tecnologia dentro de um contexto – de Segurança Pública – em que o seu desuso já não pode ser vislumbrado, mas, por outro lado, não é privilegiado, incentivado ou, em outros termos, não tem a atenção que merece, seja pelos atores da segurança pública, seja pelos políticos que a usam como meio de promessa, principalmente se aliada ao contexto da atividade de inteligência. Aliás, os investimentos em tecnologias novas geralmente são colocados em segundo plano e as verdadeiras inovações e utilizações saem de aplicações parciais ou de iniciativas pessoais.

As políticas de segurança, embora tenham uma contemplação e diretriz nacional, nem sempre atendem às demandas regionais ou locais de cada Estado, principalmente quando estipulam apenas orientações teóricas e não vêm acompanhadas de incentivos financeiros, ou relativos a recursos materiais, ou em relação à formação dos profissionais de segurança pública. Os gestores contemporâneos têm, por isso, que se adequar às condições locais de produção de conhecimentos e, com base nas necessidades e demandas existentes, procurar atuar frente a uma conjuntura nacional e buscando, aliado às bases tecnológicas, a padronização de conceitos, estruturas e procedimentos relativos ao seu nicho de atuação, seja de polícia ostensiva, seja de polícia investigativa, seja de perícia, seja de atuação de defesa civil ou atuação em catástrofes naturais ou situações humanas provocadas.

Questões atuais, como a (a) agregação do laudo digital ao procedimento policial, eletrônico ou físico, (b) a identificação biométrica dos investigados, maiores ou adolescentes, (c) a utilização de aplicações que auxiliem na tarefa dos policiais, não só na busca de informações e na facilitação dos trabalhos policiais, mas

também na organização de ações e procedimentos, (d) a busca de identificação automatizada através de sistemas de reconhecimento facial, (e) a criação de mecanismos de gestão para situações complexas da atualidade, tal qual o meio ambiente, (f) a incorporação de tecnologias embarcadas nas frotas veiculares, (g) a utilização de redes sociais como forma de aproximação comunitária e facilitação da comunicação, e, (h) a disseminação dos conhecimentos através de cursos não presenciais, foram muito bem analisadas pelos nossos autores.

Verifica-se, de outra sorte, que o sistema de Segurança Pública só evolui com a evolução dos seus subsistemas, das polícias militares e civis, das perícias, do sistema prisional, do corpo de bombeiros etc. A comunicação e a tecnologia que a amplia é, de acordo com o idealizador da Teoria dos Sistemas, Niklas Luhmann, o mecanismo de acoplamento estrutural entre os subsistemas e, também, meio de interação com seu entorno, seja com o sistema mãe, a Sociedade, seja com os demais sistemas, o do Direito, o da Política, o da Moral, dentre outros. Certo é que o sistema social acabou por gerar a demanda de um formato de controle dos seres humanos e que a parte criminal primária (de atuação) tenha ficado a cargo das polícias, sobre as quais recai a principal demanda atual: aumento da sensação de segurança.

O ponto de partida da análise sistêmica com base em Luhmann tem por princípio a diferença entre sistemas e seu entorno, sendo aqueles estruturalmente orientados para sua autoorganização, porém não podem existir sem o entorno. Assim, os sistemas se constituem e se mantêm mediante a criação e a conservação da diferença com seu entorno, utilizando de seus limites (código e programação) para regular (e preservar) dita diferença. Assim, os sistemas são autopoieticos autorreferenciais, pois são unidades fechadas e sua organização é tal que o único produto é ele mesmo, evoluindo por seus próprios meios, referem-se a si mesmos e produzem seus elementos constitutivos a partir dos elementos dos quais são compostos. Produzem-se e se reproduzem a si mesmos e suas operações e o modo de reprodução são por natureza autônomos, sendo que a relação que entabulam com o entorno (meio ambiente) é estabelecida (por sua diferenciação funcional) segundo a medida de sua forma operativa. Assim, por serem autopoieticos, os sistemas são autorreferenciais, auto-organizados e autorreprodutivos. Essa relação – do sistema – estabelecida com o entorno é realizada por meio da comunicação, como referido, que é mecanismo de acoplamento estrutural entre ambos, em estímulos constantes e processamento autoestruturado da informação resultante da diferença sistema/entorno. A comunicação, assim, é o meio pelo qual é possível acesso ao sentido, indispensável para o processo coevolutivo dos sistemas sociais: a comunicação é que faz possível a diferença sistema/entorno.

Aplicando-se essa lógica ao sistema de segurança pública, este sistema não pode existir sem o seu entorno: o indivíduo e, num contexto de estar abrangido,

a sociedade. O código binário do sistema de segurança pública, por esta teoria, deve estar entre seguro/inseguro ou insegurança/segurança, porém com meandros que vão além dos aspectos objetivos, porquanto a sensação de segurança ou insegurança é algo que pode não ser objetivado e, aliás, amplificado por sistemas comunicacionais e midiáticos.

Assim, o livro, embora não refira diretamente a teoria sistêmica, num contexto de análise de terceira ordem acaba por nos trazer pesquisas que, avaliadas conjuntamente, enfocam aspectos fundamentais do sistema de Segurança Pública e seus aspectos fundamentais diante das tecnologias da informação e da comunicação da contemporaneidade.

Delegado Emerson Wendt
Chefe de Polícia na Polícia Civil do Estado do Rio Grande do Sul

Apresentação

Este livro é o resultado das pesquisas realizadas por professores e alunos do curso de especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos (turma 2013-2015), da Universidade Federal de Santa Catarina – *Campus* Araranguá, financiado pela Secretaria Nacional de Segurança Pública do Ministério da Justiça (Senasp/MJ), 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 convergem basicamente para a discussão de três temas fundamentais para a sociedade brasileira: segurança pública, direitos humanos e desenvolvimento das Tecnologias da Informação e Comunicação (TIC).

A convergência destes temas segue 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, são relevantes à 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 ao desenvolvimento tecnológico e ao crescimento econômico do Brasil no horizonte temporal até 2025 os investimentos estratégicos em TIC em Sistemas de Segurança Pública.

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

Esperamos que 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 a inovação tecnológica direcionada à redução das desigualdades econômicas e à inclusão social.

Boa leitura.

Os organizadores

Sumário

CAPÍTULO 1 – POLÍTICAS DE SEGURANÇA PÚBLICA E DIREITOS HUMANOS EM SANTA CATARINA	25
1 INTRODUÇÃO	25
2 PLANOS NACIONAIS DE SEGURANÇA PÚBLICA.....	27
3 POLÍTICAS DE SEGURANÇA PÚBLICA: FHC, LULA E DILMA	28
3.1 Secretaria Nacional de Segurança Pública	28
3.2 Plano Nacional de Segurança Pública.....	29
3.3 Sistema Único de Segurança Pública.....	30
3.4 Programa Nacional de Segurança Pública com Cidadania.....	31
4 SANTA CATARINA: IMPACTOS DOS PLANOS NACIONAIS – 2005 A 2013	32
5 RESULTADOS.....	33
6 CONSIDERAÇÕES FINAIS.....	38
REFERÊNCIAS.....	40
CAPÍTULO 2 – AS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NA GESTÃO ADMINISTRATIVA E OPERACIONAL DA SEGURANÇA PÚBLICA	43
1 INTRODUÇÃO	43
2 PROCEDIMENTOS METODOLÓGICOS.....	45
3 RESULTADOS E DISCUSSÕES	45

4	CONSIDERAÇÕES FINAIS.....	52
	REFERÊNCIAS.....	53
CAPÍTULO 3	– LAUDO DIGITAL – A QUEBRA DE PARADIGMAS ..	55
1	INTRODUÇÃO	55
2	PROCEDIMENTOS METODOLÓGICOS.....	56
3	SISTEMAS DE INFORMAÇÃO.....	57
4	FLUXO DE TRABALHO – <i>WORKFLOW</i>	58
5	CONSIDERAÇÕES FINAIS.....	60
	REFERÊNCIAS.....	63
CAPÍTULO 4	– IDENTIFICAÇÃO BIOMÉTRICA DIGITAL NA	
	GESTÃO DO ATENDIMENTO DE ADOLESCENTES INFRATORES ...	65
1	INTRODUÇÃO	65
2	CONCEITO E OS TIPOS DE BIOMETRIA.....	66
2.1	Impressões digitais.....	67
3	METODOLOGIA	68
4	RESULTADOS E DISCUSSÃO.....	69
4.1	Comparação dos processos: antes e depois da identificação biométrica.....	72
4.2	Implantação da identificação biométrica	73
5	CONSIDERAÇÕES FINAIS.....	74
	REFERÊNCIAS.....	74
CAPÍTULO 5	– TECNOLOGIAS PARA PREVENÇÃO DE	
	INCÊNDIOS: A TRAGÉDIA DA BOATE KISS	77
1	INTRODUÇÃO	77
2	ANTECEDENTES: A HISTÓRIA DE UMA TRAGÉDIA.....	78
3	CONCLUSÃO DO INQUÉRITO	81

4	TECNOLOGIAS PARA PREVENÇÃO DE INCÊNDIOS.....	82
4.1	Tecnologias preventivas: <i>sprinkler</i>	82
4.2	Sistema de exaustão de fumaça	83
4.3	Detectores de fumaça, térmicos e acionadores manuais.....	83
4.4	Sistema de gestão integrado da prevenção de incêndios	84
5	CONSIDERAÇÕES FINAIS.....	89
	REFERÊNCIAS.....	91
	CAPÍTULO 6 – APLICATIVOS PARA DISPOSITIVOS MÓVEIS APLICADOS À SEGURANÇA PÚBLICA.....	93
1	INTRODUÇÃO	93
2	DESENVOLVIMENTO.....	95
3	CONSIDERAÇÕES FINAIS.....	101
	REFERÊNCIAS.....	102
	CAPÍTULO 7 – UM MODELO DE DADOS VOLTADO AO SERVIÇO DE INTELIGÊNCIA POLICIAL	103
1	INTRODUÇÃO	103
2	MODELO PROPOSTO.....	105
2.1	Modelagem conceitual	106
3	UTILIZAÇÃO DO MODELO.....	107
3.1	Exemplos de consultas e discussões.....	108
4	CONSIDERAÇÕES FINAIS.....	109
	REFERÊNCIAS.....	110
	CAPÍTULO 8 – UM ESTUDO SOBRE TÉCNICAS DE BIOMETRIA BASEADAS EM PADRÕES FACIAIS E SUA UTILIZAÇÃO NA SEGURANÇA PÚBLICA	113
1	INTRODUÇÃO	113
2	SISTEMAS BIOMÉTRICOS.....	115

3	RECONHECIMENTO FACIAL	116
3.1	Métodos de reconhecimento de rostos	118
3.2	Métodos holísticos	120
3.3	Métodos estruturais.....	121
4	APLICAÇÕES	122
5	USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA	123
5.1	No exterior	123
5.2	No Brasil.....	125
6	CONSIDERAÇÕES FINAIS.....	128
	REFERÊNCIAS.....	129

CAPÍTULO 9 – APLICAÇÃO DE IDENTIFICAÇÃO BIOMÉTRICA POR IMPRESSÃO DIGITAL NA LAVRATURA DO AUTO DE PRISÃO EM FLAGRANTE

1	INTRODUÇÃO	133
2	AUTO DE PRISÃO EM FLAGRANTE.....	134
3	BIOMETRIA	136
4	CONCEITO E FUNCIONAMENTO	136
5	IMPRESSÃO DIGITAL COMO IDENTIFICADOR BIOMÉTRICO	137
6	SISTEMAS FORENSES DE IDENTIFICAÇÃO DIGITAL.....	140
7	EXTRAÇÃO DE CARACTERÍSTICAS, COMO É FEITO NO BRASIL?	141
8	CONCLUSÃO.....	143
	REFERÊNCIAS.....	144

CAPÍTULO 10 – PROPOSTA DE UM SISTEMA DE GESTÃO PARA FISCALIZAÇÃO AMBIENTAL

1	INTRODUÇÃO	147
2	METODOLOGIA	148

3	FUNDAMENTAÇÃO TEÓRICA.....	149
4	GESTÃO AMBIENTAL NA POLÍCIA MILITAR DE MARACAJÁ.....	150
5	SISTEMA PROPOSTO.....	152
6	CONCLUSÕES.....	155
	REFERÊNCIAS.....	156
	CAPÍTULO 11 – PROPOSTAS PARA INFORMATIZAÇÃO DE VIATURAS POLICIAIS COMO INSTRUMENTO DE SEGURANÇA PÚBLICA.....	157
1	INTRODUÇÃO.....	157
2	METODOLOGIA.....	158
3	ANÁLISE DA PESQUISA.....	158
4	PROPOSTA DA VIATURA POLICIAL IDEAL.....	162
5	CONCLUSÕES.....	164
	REFERÊNCIAS.....	165
	CAPÍTULO 12 – REDES SOCIAIS E A POLÍCIA COMUNITÁRIA: ESTUDO DE CASO DOS CONSEGS DO VALE DO ARARANGUÁ	167
1	INTRODUÇÃO.....	167
2	OS CONSEGS E AS REDES SOCIAIS.....	169
3.	CONSIDERAÇÕES FINAIS.....	175
	REFERÊNCIAS.....	176
	CAPÍTULO 13 – TECNOLOGIAS DA INFORMAÇÃO APLICADAS NA PMSC E BPMA.....	179
1	INTRODUÇÃO.....	179
2	PROCEDIMENTOS METODOLÓGICOS.....	182
3	TIC UTILIZADAS PELA PMSC.....	182
4	CONSIDERAÇÕES FINAIS.....	184
	REFERÊNCIAS.....	187

CAPÍTULO 14 – EDUCAÇÃO A DISTÂNCIA, TECNOLOGIA E LEGISLAÇÃO PRISIONAL..... 189

1 INTRODUÇÃO	189
2 REFERENCIAL TEÓRICO	190
3 CONSIDERAÇÕES FINAIS.....	194
REFERÊNCIAS.....	195

CAPÍTULO 15 – O USO DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NA MEDIAÇÃO DA ESPECIALIZAÇÃO EM TIC APLICADAS À SEGURANÇA PÚBLICA E DIREITOS HUMANOS 197

1 INTRODUÇÃO	197
2 FUNDAMENTAÇÃO.....	198
3 PROCEDIMENTOS METODOLÓGICOS.....	200
3.1 Coleta de Dados.....	200
4 AMBIENTES COMPUTACIONAIS DA UFSC.....	201
5 AMBIENTES UTILIZADOS	201
6 RESULTADO DA PESQUISA APLICADA.....	202
7 CONCLUSÃO.....	203
REFERÊNCIAS.....	204

1 CAPÍTULO

POLÍTICAS DE SEGURANÇA PÚBLICA E DIREITOS HUMANOS EM SANTA CATARINA

Daiane Oliveira João

Giovani Mendonça Lunardi

Marta Adriano da Silva Cristiano

1 INTRODUÇÃO

O debate e as agendas em torno dos temas da Segurança Pública e Direitos Humanos no Brasil estão, hoje, entre as questões mais importantes no que tange a consolidação dos direitos civis e sociais dos cidadãos brasileiros. Neste sentido, o Governo Federal vem ao longo dos últimos anos desenvolvendo várias políticas públicas nacionais de Segurança e Direitos Humanos (BRASIL, 2015).

Destacam-se como ações estratégicas: a consolidação do Sistema Único de Segurança Pública (Susp), os programas da Secretaria Nacional de Segurança Pú-

blica 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 a Matriz Curricular Nacional para Ações Formativas dos Profissionais da Área da Segurança Pública. Da mesma forma, são relevantes 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, a prestação de serviços públicos de segurança inclui o policiamento ostensivo, a apuração de infrações penais e a guarda e recolhimento de presos. O foco das políticas de segurança pública é proteger a cidadania, prevenindo e controlando manifestações da criminalidade e da violência, efetivas ou potenciais, garantindo o exercício pleno da cidadania nos limites da lei (SANTA CATARINA, 2015). Então, como se fala tanto em políticas de segurança pública e, ainda assim, temos uma sensação crescente de aumento da violência urbana?

Devido a este questionamento, o problema da violência tornou-se objeto de interesse e discussão de especialistas e da população em geral. A sociedade brasileira tem acompanhado o aumento da violência e da criminalidade e também observado a falta de respostas por parte das polícias e da Justiça quanto ao enfrentamento do crime e das altas taxas de impunidade.

Trata-se de um problema social que gera ampla mobilização da opinião pública, além de causar impacto sobre o sistema de justiça criminal, que precisa formular e implementar políticas públicas penais, e também no Estado, que precisa adequar suas políticas de segurança pública de modo a diminuir não somente o crime, mas principalmente a insegurança generalizada da sociedade. No Estado de Santa Catarina, a situação não é muito diferente do quadro geral do País: os ataques criminosos vêm aumentando consideravelmente, mesmo com as iniciativas do governo e as novas políticas de segurança pública.

A mídia tem apresentado uma série de atentados criminosos pelo estado, o que faz parecer que a violência se tornou o meio padrão de protesto. Em 2013, ocorreram mais de 82 atentados a ônibus em 26 municípios. Em 2014, os números foram ainda piores: além de ocorrerem em maior número, os atentados também foram mais violentos e duraram mais dias. Pessoas suspeitas de cometerem crimes foram linchadas em diversos municípios de Santa Catarina e os agressores eram familiares e amigos de vítimas, que decidem agir por conta própria.

Florianópolis passou por vários episódios nos quais que toda a população foi afetada não somente pela violência, mas também pela reclusão, por não po-

der ir e vir livremente, por ter toque de recolher, pelos ônibus que deixaram de circular entre às 23 horas e às 6 horas. Penalidade para a sociedade e não para os criminosos.

Em vista dos inúmeros projetos de segurança pública que visam inibir a prática criminosa e agilizar o tempo de resposta no atendimento às ocorrências, busca-se com esta pesquisa entender porque os fatos divulgados pela mídia e as incidências de crimes cada vez mais constantes indicam o contrário do que é proposto pelos programas instituídos. Essas políticas de segurança pública estão realmente sendo aplicadas? A partir deste questionamento, neste capítulo serão examinadas as políticas de segurança pública e os direitos humanos implantados no Brasil e no Estado de Santa Catarina a partir dos Planos Nacionais no período de 2005 a 2013.

2 PLANOS NACIONAIS DE SEGURANÇA PÚBLICA

A Constituição brasileira de 1988, em seu artigo 5º, apresenta o direito à segurança como um dos direitos fundamentais, de igual importância ao direito à vida, à liberdade, à igualdade e à propriedade. O legislador constituinte também expressou a prioridade do tema da segurança enquanto preocupação da sociedade em geral.

Entretanto, os governantes, no sentido de responder a esta preocupação relacionada com a segurança enquanto política pública, apresentaram ações de caráter restritivo e aporético aos demais direitos fundamentais, como: sistemas de vigilância, leis penais mais severas, controle de imigração etc. Estas ações polarizam duas reivindicações da sociedade, que são a garantia dos direitos individuais e a emergência do direito à segurança.

De certa forma, colocam-se como opostos aquilo que possuem a mesma essência. De um lado, tem-se a criação de uma série de mecanismos para garantia dos direitos individuais, como a inviolabilidade do domicílio, a proibição de prisões ilegais, o instituto do *habeas corpus*, a garantia de ampla defesa aos acusados etc. De outro lado, o direito à segurança enquanto política pública teve como principais ações a militarização do policiamento preventivo e ostensivo, transformando “os agentes policiais em uma facção deslocada da sociedade civil, exorbitando em sua prática de vigilância e defesa para a agressão e extermínio” (BRAGA JÚNIOR, 2009, p. 453).

Todas as promessas de repressão à violência endêmica na sociedade brasileira não conseguem ir além do imediatismo eleitoreiro de fácil assimilação. Braga Júnior cita a aplicação de penas mais severas, o aumento do policiamento ostensivo, a elevação dos sistemas de vigilância, entre outros exemplos que remetem a promessas de campanha eleitoral. Ou seja, são ações que vão de encontro aos

direitos individuais. Assim, a situação social brasileira referente à segurança pública, divide as atividades do Estado em positivas e negativas, restando ao aparato policial somente as de caráter negativo (BRAGA JÚNIOR, 2009, p. 453).

3 POLÍTICAS DE SEGURANÇA PÚBLICA: FHC, LULA E DILMA

Questões de segurança pública passaram a ser consideradas de fundamental importância para a sociedade nos últimos anos e têm recebido atenção especial do Governo Federal. A visibilidade pública que a segurança ganhou é inédita neste país; até então, não se tinha visto tamanha repercussão nem estado tanto em destaque na mídia e em debates como tem sido atualmente. O aumento considerável da criminalidade despertou o interesse de muitos estudiosos e colocou a segurança como principal desafio para o Estado. Os problemas a se resolver são muitos, e na tentativa de solucioná-lo, o governo cria planos e estratégias que visam reprimir a criminalidade e manter a segurança pública.

Trata-se, pois, a política pública, de uma estratégia de ação pensada, planejada e avaliada, guiada por uma racionalidade coletiva na qual tanto o Estado como a sociedade desempenham papéis ativos. Eis porque o estudo da política pública é também o estudo do Estado em ação (Meny e Toenig) nas suas permanentes relações de reciprocidade e antagonismo com a sociedade, a qual constitui o espaço privilegiado das classes sociais (Ianni) (PEREIRA, 2009, p. 96).

Outra definição ainda para política pública é a colocada por Souza, em que destaca:

Pode-se, então, resumir política pública como o campo do conhecimento que busca, ao mesmo tempo, “colocar o governo em ação” e/ou analisar essa ação (variável independente) e, quando necessário, propor mudanças no rumo ou curso dessas ações (variável dependente). A formulação de políticas públicas constitui-se no estágio em que os governos democráticos traduzem seus propósitos e plataformas eleitorais em programas e ações que produzirão resultados ou mudanças no mundo real (SOUZA, 2006, p. 26).

Por estas razões, foram criados alguns programas no intuito de diminuir as recorrentes reivindicações da sociedade por segurança, possibilitando a tradução de Políticas Públicas de Segurança em Programas de Trabalho, como são apresentados na sequência.

3.1 Secretaria Nacional de Segurança Pública

Em 1995, por meio da Medida Provisória nº 813, foi criada pelo Governo Federal a Secretaria de Planejamento de Ações Nacionais de Segurança Pública

(Seplanseg), no âmbito do Ministério da Justiça. Em decorrência de transformação da Seplanseg, foi criada a Senasp, pelo Decreto nº 2.315, de 4 de setembro de 1997, tendo como perspectiva atuar de forma articulada com os estados da Federação para a implementação da Política Nacional de Segurança Pública (PNSP). A instituição da Senasp como órgão executivo significou a estruturação de mecanismos de gestão capazes de modificar o arranjo institucional da organização administrativa da segurança pública no âmbito do Governo Federal.

3.2 Plano Nacional de Segurança Pública

Em 1996, o governo Fernando Henrique Cardoso criou o Programa Nacional de Direitos Humanos (PNDH), tendo por base os fundamentos da Conferência Mundial de Direitos Humanos, ocorrida em Viena, em 1993. O foco do programa era, principalmente, a preservação das liberdades civis em função das recorrentes reclamações da sociedade frente ao uso de violência por parte de policiais. Este programa foi substituído mais tarde pelo II Programa Nacional de Direitos Humanos, instituído no segundo governo FHC, em 2000. Surgiu então, neste mesmo ano, o PNSP, que tem o objetivo de aperfeiçoar as ações dos órgãos de segurança pública, com propostas que integram políticas de segurança, políticas sociais e ações comunitárias, buscando reprimir e prevenir o crime e reduzir a impunidade, elevando o índice de segurança do cidadão.

Para dar apoio financeiro aos projetos do PNSP e à prevenção à violência, foi instituído no âmbito do Ministério da Justiça, também no ano 2000, o Fundo Nacional de Segurança Pública (FNSP). O FNSP apoia projetos na área de segurança pública destinados ao reequipamento, ao treinamento e à qualificação das polícias civis e militares, corpos de bombeiros militares e guardas municipais; sistemas de informações, de inteligência e de investigação, bem como de estatísticas policiais; estruturação e modernização da polícia técnica e científica; programas de polícia comunitária e programas de prevenção ao delito e à violência, entre outros. Ainda assim, esses avanços na formatação da política de segurança pública não produziram os resultados concretos esperados. De acordo com Fernando Salla:

[...] o Plano Nacional de Segurança Pública [...] compreendia 124 ações distribuídas em 15 compromissos que estavam voltadas para áreas diversas como o combate ao narcotráfico e ao crime organizado; o desarmamento; à capacitação profissional; e ao reaparelhamento das polícias, à atualização da legislação sobre segurança pública, à redução da violência urbana e ao aperfeiçoamento do sistema penitenciário. Uma novidade é que no plano, além dessas iniciativas na área específica de segurança, eram propostas diversas ações na esfera das políticas sociais. O plano, no entanto, não fixava os recursos nem as metas para ações. Ao mesmo tempo, não estavam estabelecidos quais seriam os mecanismos de gestão, acompanhamento e avaliação do plano (SALLA, 2003, p. 430).

O PNSP do governo Fernando Henrique Cardoso, assim como a política de segurança pública adotada no primeiro governo do presidente Luiz Inácio Lula da Silva, não teve os resultados esperados. Questões relacionadas à segurança pública, diante de sua amplitude e complexidade, não podem ser tratadas como política limitada de governo. Para ter êxito, elas devem ser enfrentadas tanto pelo Estado quanto pela sociedade.

As políticas públicas de segurança, justiça e penitenciárias não têm contido o crescimento dos crimes, das graves violações dos direitos humanos e da violência em geral. A despeito das pressões sociais e das mudanças estimuladas por investimentos promovidos pelos governos estaduais e federal, em recursos materiais e humanos e na renovação das diretrizes institucionais que orientam as agências responsáveis pelo controle da ordem pública, os resultados ainda parecem tímidos e pouco visíveis (ADORNO, 2002, p. 8).

3.3 Sistema Único de Segurança Pública

O Sistema Único de Segurança Pública (Susp), lançado em abril de 2003, foi criado com o objetivo de promover a integração e a articulação das ações federais, estaduais e municipais nas áreas de Segurança Pública e da Justiça Criminal. A articulação seria por meio da integração desses órgãos, e não pela unificação; a autonomia federativa, assegurada pela Constituição Federal, é preservada. Estados, Polícia Civil e Polícia Militar permanecem cumprindo suas responsabilidades, de forma autônoma, porém passam a utilizar um sistema único, com intuito de prevenir e planejar ações estratégicas. A participação do Estado no SUSP dá-se por meio da criação de um Comitê de Gestão Integrada, do qual fazem parte o secretário estadual de Segurança Pública, representantes da Polícia Federal, Rodoviária Federal, Civil e guardas municipais. A função desse comitê é definir as ações a serem tomadas para combater o crime, atuando principalmente contra o crime organizado (tráfico de drogas e de armas, contrabando, lavagem de dinheiro, pirataria).

As polícias Civil e Militar passaram a integrar a mesma academia e ter acesso à formação prática e teórica de igual conteúdo. Também foi estimulada pelo governo a criação de unidades policiais integradas, com forças das polícias civil e militar, em um mesmo espaço físico.

De acordo com a Senasp, o Susp está definido sob seis eixos:

- **Gestão unificada da informação:** todas as demandas na área de segurança pública são recebidas por uma central, que as coleta e registra em um banco de dados único, auxiliando na redução da violência e na prevenção ao crime.
- **Gestão do sistema de segurança:** institui perícia em delegacias, polícia civil e polícia militar, que deverão ser implantadas para cuidar de determinadas áreas geográficas das cidades.

- **Formação e aperfeiçoamento de policiais:** treinamento para policiais civis e militares em academias integradas.
- **Valorização das perícias:** como fase relevante da investigação dos crimes.
- **Ações concretas para a prevenção e redução da violência:** nos estados, essas ações serão prioritárias, com papel fundamental da polícia comunitária nesse processo.
- **Criação de ouvidorias independentes e corregedorias unificadas:** as ouvidorias receberão as reclamações da população e identificar possíveis abusos da ação policial, e as corregedorias deverão fiscalizar os atos dos policiais civis e militares.

3.4 Programa Nacional de Segurança Pública com Cidadania

A partir de 2007, já no segundo mandato do presidente Lula, foi apresentado um novo programa na área da segurança pública, o Programa Nacional de Segurança Pública com Cidadania (Pronasci), aprovado por unanimidade no Congresso Nacional. O Pronasci foi instituído pela Lei nº 11.530, de 24 de outubro de 2007, e traz a violência como um fenômeno decorrente de diversos fatores, colocando como origens da violência e da criminalidade áreas como a educação, saúde e cultura (BRASIL, 2007).

Art. 1º – Fica instituído o Programa Nacional de Segurança Pública com Cidadania – PRONASCI, a ser executado pela União, por meio da articulação dos órgãos federais, em regime de cooperação com Estados, Distrito Federal e Municípios e com a participação das famílias e da comunidade, mediante programas, projetos e ações de assistência técnica e financeira e mobilização social, visando à melhoria da segurança pública.

Art. 2º – O Pronasci destina-se a articular ações de segurança pública para a prevenção, controle e repressão da criminalidade, estabelecendo políticas sociais e ações de proteção às vítimas.

O Pronasci marca uma iniciativa relevante no enfrentamento ao crime no país. O programa tem a finalidade de articular ações de segurança pública, priorizando a prevenção, o controle e a repressão da criminalidade, e estabelecendo políticas sociais e ações de proteção às vítimas da violência. Busca atingir as causas que levam à violência, na intenção de evitá-la.

Muitos pontos merecem destaque no Pronasci, como a valorização dos profissionais de segurança pública, a reestruturação do sistema penitenciário, o combate à corrupção policial e o envolvimento da comunidade na prevenção da

violência. O programa é dividido em 94 projetos que, para sua execução, contam com atuação da União, dos estados, dos municípios e da comunidade. A seguir, detalham-se alguns deles:

- a) **Mulheres da Paz:** destina-se à capacitação de mulheres socialmente atuantes nas áreas geográficas atendidas pelo Pronasci.
- b) **Proteção de Jovens em Território Vulnerável – Proteção:** Voltado à formação e inclusão social de jovens e adolescentes expostos à violência doméstica ou urbana nas áreas abrangidas pelo Pronasci.
- c) **Bolsa-Formação:** benefício concedido aos profissionais de segurança pública como incentivo ao estudo e à atuação junto às comunidades. Policiais civis e militares, bombeiros, peritos e agentes penitenciários de baixa renda que participarem e forem aprovados em cursos de capacitação promovidos, credenciados ou reconhecidos pela Senasp, do Ministério da Justiça, terão acesso a uma bolsa de até R\$ 400.
- d) **Plano Nacional de Habitação para Profissionais de Segurança Pública:** os profissionais na segurança pública também podem contar com o benefício no valor de até R\$ 50 mil, para aqueles que recebam até R\$ 4.900,00, em forma de unidades populares e cartas de crédito para a compra da casa própria.
- e) **Formação Policial:** oferta, por meio da Renaesp, de cursos para a qualificação das polícias, que inclui práticas de segurança cidadã, como a utilização de tecnologias não letais, direitos humanos, entre outros.
- f) **Sistema Prisional:** criação de novas vagas no sistema penitenciário do país destinadas a públicos específicos. O objetivo é separar os detentos por faixa etária e por natureza do delito, para impedir que aqueles que cometeram pequenas infrações fiquem sob a influência dos líderes do crime organizado.

O Estado de Santa Catarina aderiu ao Pronasci em 2011, durante o governo Raimundo Colombo.

4 SANTA CATARINA: IMPACTOS DOS PLANOS NACIONAIS – 2005 A 2013

No Estado de Santa Catarina, são inúmeros os projetos em andamento que visam reduzir o número de crimes e a insegurança. O governo estadual tem dado atenção especial à Segurança Pública. Em 2012, por exemplo, foi lançado o **Pacto pela Segurança Pública, Justiça e Cidadania**, com a proposta de modernizar e ampliar o serviço das polícias civil e militar, corpo de bombeiros e

do Instituto Geral de Perícias. Entre as medidas do programa, destacam-se os investimentos com vídeomonitoramento por câmeras de segurança na maioria das cidades catarinenses, cujo objetivo é reduzir o índice de criminalidade no Estado.

O Governo do Estado declarou, em 2012, que estava investindo constantemente na ampliação do sistema de vídeomonitoramento por câmeras de segurança. A proposta do Pacto previa a instalação de câmeras principalmente em locais com grande circulação de pessoas, como praças e nas proximidades de agências bancárias e de escolas. A parceria foi feita com os municípios, que firmaram convênio com o governo e escolheram o projeto para a instalação de seis a dez câmeras, com valores que variavam entre R\$ 80 mil a R\$ 105 mil.

Preocupado com o aumento elevado dos índices de criminalidade no Estado, o governo criou uma série de programas que visa à prevenção do crime, e não apenas a atuação imediata e corretiva de crises. Dentre esses programas, que são reflexos da preocupação nacional com a segurança, destacam-se: Programa Município Seguro, Polícia Comunitária, Programa Segurança Mirim, Programa De Olho Na Rua etc.

Por sua vez, os investimentos em Segurança Pública ficaram a cargo do programa Pacto por Santa Catarina, que reúne obras e aquisições para atender às principais demandas da sociedade. É um programa de gestão dos projetos, alguns já implantados ou em vias de implantação, que vem recebendo investimentos consideráveis. O Pacto foi lançado em julho de 2012, no governo Raimundo Colombo, com o intuito de abranger os projetos em andamento em um único programa de gestão.

Seus recursos destinam-se a investimentos em áreas estruturantes da Segurança Pública. A proposta foi de que, nos anos de 2013 e 2014, o governo estadual, por meio da Secretaria de Segurança Pública, destinaria R\$ 265 milhões para investimentos essa área. Por ser um programa aberto, o Pacto pode agregar novas iniciativas e recursos, sendo que inicialmente o foco são a mobilidade policial, os equipamentos, a estrutura e o monitoramento urbano. Esses investimentos potencializam os serviços no enfrentamento da violência, em que a comunidade será beneficiada com o aumento da segurança e a diminuição dos índices de criminalidade.

5 RESULTADOS

Controlar a ordem pública é cada vez mais difícil e complexo. O aumento das taxas de criminalidade, a sensação de insegurança que de forma generalizada toma conta do país, os inúmeros registros de violência policial e violação de direitos humanos, a superlotação dos presídios, a falta de programas de ressocialização

lização, as rebeliões, os atos violentos cometidos por populares, a degradação do patrimônio público, a corrupção, a morosidade judicial, o descrédito na investigação policial, entre outros fatores, representam verdadeiros desafios ao Estado na formulação de políticas públicas.

A participação social na construção da política de segurança pública se faz primordial, uma vez que Estado e sociedade devem agir em conjunto para reforçar a construção de uma nova política, que se afaste dos paradigmas tradicionais. Este pode ser considerado o maior desafio da área de segurança pública para os governos federal, estaduais e municipais e para sociedade.

Nos últimos anos, muitos investimentos foram feitos em Segurança Pública. Por outro lado, é um período marcado por diversas crises, uma vez que o número de rebeliões e de mortes em presídios foi grande, além dos diversos casos de linchamentos, reflexo da sensação de impunidade que leva a sociedade a “fazer justiça com as próprias mãos”. A falta de segurança para exercer suas atividades e o número reduzido de policiais gerou greves por todo o país. A revolta da população contra as ações do governo Dilma Rousseff gerou inúmeras manifestações contra a realização da Copa do Mundo. Hoje, o país ainda enfrenta a crise da rejeição para com o atual governo.

Os dados publicados pelo Fórum Brasileiro de Segurança Pública, de 2014, reforçam que o país convive com taxas absurdas e que o sistema judicial e de segurança são ineficientes. Embora tenha se investido muito na segurança pública, os números aumentaram consideravelmente.

O total de crimes violentos letais intencionais cometidos no Brasil no ano de 2009 foi de 44.518 ocorrências; já em 2013, mesmo com todo esforço para redução da criminalidade, o número subiu para 53.646 ocorrências. Segundo o Fórum Brasileiro de Segurança Pública, de 2014, do total investido em segurança pública na área de Informação e Inteligência em 2012, somente 0,01% foram para o Estado de Santa Catarina e, em 2013, esse percentual foi de 0,07%, valor ainda muito baixo. Em 2013, do total investido com Segurança Pública, somente 1,36 % foram em Informação e Inteligência.

Da mesma forma, os números sobre criminalidade no Brasil são assustadores. Dados indicam que nosso país representa 10% dos casos mundiais de homicídios. Em termos absolutos, é aqui que mais pessoas morrem vítimas de agressão. A marca de um milhão de homicídios foi atingida em 2009, sendo atualmente a principal causa de mortes no país. O apontamento do Mapa da Violência, publicado em 2014, diz que o Brasil, com sua taxa de 27,4 homicídios por 100 mil habitantes, supera largamente os índices dos 12 países mais populosos do mundo.

Hoje, a estatística de homicídio é o principal indicador de criminalidade utilizado no mundo. Entre os vários fatores que explicam sua utilização, em primeiro lugar, entende-se que o homicídio é um crime que afronta o maior bem jurídico protegido pelo ordenamento pátrio, ou seja, a vida.

Segundo Beato (2012), o Brasil é um dos países mais violentos do mundo, mas sabemos pouco sobre as razões dessa supremacia. Beato afirma ainda que o paradoxo nessa evolução negativa na segurança pública é que ela ocorreu justamente em um período de melhoria generalizada dos indicadores sociais, bem como de fortalecimento das instituições democráticas brasileiras. Sua avaliação é que “todos os esforços de nosso sistema de justiça e de organizações às voltas com segurança pública parecem proteger justamente aqueles que estão menos expostos à violência. A concentração de equipamentos de proteção social, bem como de recursos de segurança pública, se dá de forma desigual” (BEATO, 2012).

Por sua vez, em Santa Catarina, segundo dados da Secretaria de Segurança Pública (SSP), em 2011, o Estado apresentou taxa de 6,34 homicídios para cada 100 mil habitantes no primeiro semestre de 2011, enquanto, no primeiro semestre de 2012, apresentou taxa de 5,78 homicídios. Apesar da redução da taxa de homicídios, na região de Criciúma, onde está localizado o *campus* Araranguá da Universidade Federal de Santa Catarina (UFSC), houve acréscimo de 11% no número de ocorrências, que acabou por incluí-lo no rol das piores taxas do Estado.

O que se pode concluir, e que também já foi apontado pelo Mapa da Violência de anos anteriores, é a interiorização do crime. O aumento antes registrado nas capitais e nos grandes centros urbanos, até 2003, na última década começou a atingir as cidades do interior, as taxas nas capitais ficam estagnadas enquanto no interior continuam crescendo, e isso é agravado pelo fato de essas regiões serem menos protegidas, estarem menos preparadas para a onda de crimes. Esse é o fato que torna essas regiões mais atrativas: a insuficiência da segurança pública em áreas de baixos índices de violência, pois essas regiões não estão preparadas para ações repressivas nem têm efetivos para isso. Isso é agravado pelo fato de que, nas capitais e nos grandes centros, o investimento com segurança é maior, o que proporciona mais eficiência nas ações policiais nessas regiões.

Recentemente, um jovem menor de idade proveniente de Porto Alegre (RS) foi preso em Criciúma, acusado de realizar vários assaltos a prédios comerciais da cidade. Ao ser questionado sobre sua vinda para a região, ele respondeu que “soube” que aqui havia muitos locais de fácil acesso no centro da cidade, com

pouca ou nenhuma vigilância.¹ De 2003 a 2011, as taxas das capitais, antes tidas como mais violentas, caíram de 41,6 homicídios por 100 mil para 36,4 em 2011. Em contrapartida, nas cidades do interior, os índices continuam crescendo – houve aumento de 23,6% no período, segundo dados do Mapa da Violência, de 2014.

Assim como ocorre em nível nacional, também ocorre em Santa Catarina, onde as principais vítimas de homicídio são, de forma exponencial, do sexo masculino, com idades entre 18 e 24 anos e com antecedentes policiais. Perfil idêntico foi identificado no estudo semestral do ano de 2011. Frisa-se também a similaridade de perfis entre o autor e a vítima. Esse perfil da criminalidade aplica-se a quem está mais vulnerável a cometer um crime, tanto a quem está vulnerável a ser vítima dele. Inclui-se ainda a este perfil que estes jovens do sexo masculino são, em sua maioria, moradores de periferia e com baixa escolaridade.

Concordando com Beato (2012), apesar de todas as políticas públicas e investimentos em segurança realizados, existe muito a ser executado em termos de pesquisas, educação e gestão na área de Segurança Pública e Direitos Humanos.

Citando aqui um pouco da história do nosso país, até os anos 1950, o Brasil tinha uma população predominantemente rural; já em 1970, mais da metade da população vivia nas cidades, número que atualmente ultrapassa os 80%. Em pouco tempo, quem trabalhava no campo foi substituído por máquinas e migrou para os grandes centros urbanos, onde a indústria e a construção civil tinham oferta de empregos. Com isso, as cidades cresceram desordenadamente e muito rápido, o que fez crescer a periferia. As cidades não tinham condições de acolher todos, e isso fez surgirem grandes problemas sociais: falta de infraestrutura, saúde, transporte, educação, segurança, ou seja, falta quase tudo. Se o Estado não cria condições de gerar isso tudo, aumenta a criminalidade.

O Mapa da Violência de 2014 aponta Santa Catarina como o estado com os menores índices em relação a outros estados brasileiros, com taxa de 12,6 homicídios por 100 mil habitantes, em 2011. Mas a pesquisa mostra também dois outros índices muito relevantes: que a violência cresceu em relação aos anos anteriores e o crescente aumento da violência dentro do estado, como é o caso da região de Criciúma. Mesmo diante desses dados, não é possível uma acomodação no sentido de se acostumar com o crime, acreditar que a população dessa região está vivendo bem por estar num Estado com um dos menores índices do país, é preciso estar ciente de que a criminalidade cresce a cada dia, e que há um número cada vez maior de presos nos presídios, pois viver na insegurança não pode ser considerado algo comum ou trivial. Pesquisas mostram o aumento das taxas de

1 Notícia veiculada no portal de notícias Engeplus Telecom. Disponível em: <<http://www.engeplus.com.br/categoria/seguranca>>. Acesso em: 16 maio 2016.

homicídio em Santa Catarina, cujos registros de homicídios passaram de 653 em 2003 para 816 em 2012.

Ainda com base no Mapa da Violência de 2014, ao se traçar o perfil do crime, aponta-se alguns fatos marcantes que contribuíram para o crescimento da criminalidade na última década em todo o país, como o desarmamento e as estratégias políticas adotadas nos estados mais violentos, no período de 2003 a 2007, gerando assim queda nos índices, seguida de estabilização. Já no período de 2007 a 2012, as taxas voltaram a crescer, com aumento de 15,3% para o país, passando de 25,2 homicídios em 2007 para 29,0 em 2012. Em Santa Catarina, o aumento foi de mais de 23%, passando de 10,4 em 2007 para 12,8 em 2012.

Fica claro, pelos dados encontrados durante esta pesquisa, que existem esforços no sentido de reduzir a criminalidade, mas que os dispêndios efetuados são insuficientes e que ainda há muito o que se fazer neste campo. As políticas de segurança pública implantadas no estado são eficazes, mas elas, por si só, não resolverão o problema, uma vez que o estado não está sequer conseguindo estabilizá-los. Os números mostram o aumento exponencial e a sociedade amedrontada clama por ações urgentes.

No que diz respeito ao sistema prisional, também é possível apontar problemas sérios no estado. O governo de Santa Catarina divulgou, em janeiro de 2014, o balanço do sistema prisional, em que aponta que o estado fechou 2013 com 17.200 detentos em suas 48 unidades prisionais, sendo 1.300 mulheres e 15.900 homens, dos quais 57% com idade entre 18 e 29 anos. No balanço, foi divulgado que, dos 17.200 detentos, 6.600 estão em regime fechado, 3.700 em regime semiaberto, 1.700 em regime aberto e 5.200 são presos que aguardam julgamento (SANTA CATARINA, 2015).

O Tribunal de Contas do Estado de Santa Catarina realizou em 2014, entre os dias 24 de julho e 8 de agosto, uma auditoria operacional com intuito de avaliar a gestão do sistema carcerário do estado. Entre os principais problemas encontrados e citados no relatório técnico da auditoria estão a superlotação, a inexistência de cálculo do custo mensal por preso e de informações sobre reincidência, e a carência de recursos humanos.

Segundo o relatório (SANTA CATARINA, 2013) da Diretoria de Atividades Especiais (DAE), em 2012, existiam 49 estabelecimentos prisionais, sendo 44 deles administrados exclusivamente pela Secretaria de Justiça e Cidadania (SJC), autogestão² e cinco operados por cogestão³. A auditoria indicou população car-

2 **Autogestão:** forma de gestão do estabelecimento prisional em que a SJC é integralmente responsável pela administração da unidade.

3 **Cogestão:** a SJC contrata empresa para realizar a execução de serviços técnicos e materiais para a operacionalização das unidades, mas a Secretaria permanece com a direção do estabelecimento penal.

cerária de 14.905 presos naquele período, sendo que 44 dos estabelecimentos apresentaram superlotação, gerando déficit de 4.474 vagas, além de apontamentos quanto à carência de 931 agentes prisionais e de 131 profissionais da área da saúde e assistência social para que fossem cumpridos os padrões definidos pelo Conselho Nacional de Política Criminal e Penitenciária.

Os dados apontam ainda que há uma série de inversões de valores no país, daí os desafios em erradicar os fatores que originam a violência. Esses atos intimidam a sociedade, que vive em situação de risco, em um Estado Democrático de Direito. O que assusta não é somente a falta de identificação do autor de um crime, mas também a ausência de uma punição coerente com o crime cometido. O fato de criminosos rapidamente estarem livres para repetirem atos criminosos faz com que a população se sinta encarcerada: é a sociedade que quem está ficando reclusa, sem poder exercer seu direito de ir e vir.

6 CONSIDERAÇÕES FINAIS

São muitas as consequências que este aumento da violência urbana tem causado. É fato que a solução para esses problemas não envolve apenas a segurança pública; é preciso melhorias no sistema público como um todo. Em uma sociedade em que não se recebe boa educação, não tem moradia, oportunidades de emprego, acesso ao sistema de saúde, entre outros fatores, certamente haverá aumento no índice criminal. A solução envolve, portanto, mudanças nas políticas públicas e na sociedade.

As cidades são locais de convivência humana, de troca de experiências, de contato direto com outras pessoas, enfim, são espaços que promovem o acesso à informação, e para que isso aconteça, é preciso criar condições e fornecer a segurança necessária. Porém, a realidade dos últimos anos é bem diferente disso: a divulgação intensiva de crimes e da violência urbana promove a insegurança, gera o medo e a sensação de desamparo, que comumente são vinculados ao estado, tido como ausente no provimento de segurança pública.

Esse sentimento da população reflete também no governo, que acaba criando leis na base do imediatismo, tomado pela emergência da situação. São ações que não são de prevenção, aspecto que é fundamental para a redução da violência.

Conclui-se, com este estudo, que as políticas de segurança pública precisam mais do que investimentos no setor. Não basta construir novos presídios, tem que haver uma reforma penal, a legislação precisa caminhar junto com a segurança, é preciso criar meios para que as forças policiais possam combater e prevenir ações criminosas. Vale destacar que não há investimentos com planejamento estratégico em gestão da tecnologia, informação e conhecimento direcionados à segurança pública.

A ausência ou omissão do Estado é uma das principais causas da criminalidade, por deixar faltar os direitos básicos do cidadão. A desigualdade social também é uma causa importante, assim como a má distribuição de renda do país só vem agravar a situação. Os jovens da periferia também querem ter roupas de marca, acesso as tecnologias da “moda” e, como não conseguem por meio do trabalho, acabam partindo para o lado do crime, no qual esses itens podem ser adquiridos.

Outra causa importante do aumento da violência é a ação dos traficantes de drogas. A relação do tráfico com o crime é extensa, não somente pela ação do traficante, mas também pelo fato de esses traficantes estarem cientes das leis do país, que acabam por colocar os jovens menores de idade na mira dos traficantes. Eles são, de certa forma, obrigados a cometer o crime. Não há como restabelecer a ordem pública se os autores de graves delitos não forem punidos.

É preciso urgentemente uma reforma no Código Penal, pois os criminosos estão se valendo das leis atuais, nas quais predomina a impunidade. Medidas preventivas devem ser tomadas para combater a criminalidade. E para que possam existir tais medidas, a lei precisa ser atualizada, pois hoje não se cometem somente os crimes que existiam em 1988. Se o crime é culpa das desigualdades sociais, é preciso lutar para acabar com elas e não colocar jovens que cometem crimes de volta às ruas só porque eles são vítimas da sociedade.

Os poucos investimentos na segurança pública geraram impactos para o Estado de Santa Catarina. O aumento da criminalidade reflete-se não apenas nas ocorrências registradas pela polícia, mas também no número de efetivos na rua em determinados horários e localidades, programas em locais de maior incidência de crimes e voltados para as pessoas mais vulneráveis a ele. Porém, o mais importante é que a garantia dos direitos previstos na Constituição Federal para os detentos não pode, em nenhum momento ou situação, prevalecer sobre a garantia dos direitos dos cidadãos e dos profissionais de segurança pública.

Sapori (2012) reitera com a seguinte afirmação:

A reversão desse triste quadro exige que a sociedade brasileira transforme a segurança pública em verdadeira prioridade política. Não se trata apenas de alocação de mais recursos públicos para o setor. A tarefa que se apresenta é a reforma do arranjo institucional da segurança pública previsto na Constituição Federal, que se mostra anacrônico diante da realidade atual. Necessitamos de um esforço coletivo similar àquele empreendido para o controle da inflação em meados da década de 1990 (SAPORI, 2012, p 157).

Reconhecer que o Estado deve investir ainda mais em segurança é um fato, porém, espera-se que os direitos dos cidadãos, previstos na Constituição Federal, sejam resguardados e que os direitos daqueles que cometem crimes não se sobreponham em qualquer situação aos direitos dos profissionais da segurança pública e dos cidadãos.

REFERÊNCIAS

ADORNO, S. Insegurança *versus* direitos humanos: entre a lei e a ordem. *Tempo Social Rev. Sociol. USP*, São Paulo, v.11, n.2, p.129-153, out. 1999 (edit. fev. 2000).

_____. Exclusão sócio-econômica e violência urbana. In: TAVARES DOS SANTOS, J. V.; BAUMGARTEN, M. (ed.). *Sociologias – Violências, América Latina. Revista Semestral do Programa de Pós-Graduação em Sociologia da UFRGS*, Porto Alegre, n.8. jul./dez. 2002, p. 84-135. Disponível em: <http://www.nevusp.org/portugues/index.php?option=com_content&task=view&id=1060&Itemid=96> Acesso em: 7 jun. 2015.

BEATO, C. *Crime e Cidades*. Belo Horizonte: UFMG, 2012.

BRAGA JÚNIOR, M. O conceito de polícia e a noção de segurança no contexto atual dos direitos Humanos. In: BITTAR, E. C. B. (Org.) *Direitos Humanos no século XXI: Cenários de Tensão*. Rio de Janeiro: Forense Universitária, 2009.

BRASIL. Ministério da Justiça Secretaria Nacional de Segurança Pública/SENASP. *Matriz Curricular Nacional: Para Ações Formativas dos Profissionais da Área de Segurança Pública*. 2009. Disponível em: <<http://posticsenasp.ufsc.br/files/2014/02/2009MatrizCurricular.pdf>> Acesso em: 7 jun. 2015.

_____. Ministério da Justiça. Secretaria Nacional de Segurança Pública. *Programa de Ciência e Tecnologia aplicada na Área de Segurança Pública*. Brasília: 2007.

_____. Presidência da República. Secretaria de Direitos Humanos. *Plano Nacional de Educação em Direitos Humanos*. 2015. Disponível em: <<http://www.sdh.gov.br/sobre/participacao-social/cnedh>>. Acesso em: 7 jun. 2015.

_____. Presidência da República. Secretaria de Direitos Humanos. *Programa Nacional de Direitos Humanos 3*. 2010. Disponível em <<http://www.sdh.gov.br/assuntos/direito-para-todos/programas/pdfs/programa-nacional-de-direitos-humanos-pndh-3>>. Acesso em: 7 jun. 2015.

_____. Secretaria Geral da Presidência da República. *Mapa da Violência 2012: os novos padrões da violência homicida no Brasil*. 1.ed. São Paulo: Instituto Sangari, 2011. Disponível em: <<http://www.mapadaviolencia.org.br/>>. Acesso em: 20 jun. 2015.

_____. Secretaria-Geral da Presidência da República. *Mapa da Violência 2014*. 2014. Brasília: 2014. Disponível em: <<http://www.mapadaviolencia.org.br/>>. Acesso em: 20 jun. 2015.

FELTRAN, G. S. *Fronteiras de Tensão: Política e Violência nas Periferias de São Paulo*. São Paulo: Unesp, 2012.

LOPES, E. *Política e segurança pública: uma vontade de sujeição*. Rio de Janeiro: Contraponto, 2009. Disponível em: <http://www.sapientia.pucsp.br/tde_arquivos/3/TDE-2007-06-13T09:38:59Z-3474/Publico/Edson%20Lopes.pdf>. Acesso em: 7 jun. 2015.

LUNARDI, G. M. O direito à segurança enquanto direito humano: liberdade *versus* segurança pública. 8º Encontro da ANDHEP – Políticas Públicas para a Segurança Pública e Direitos Humanos, São Paulo, 28-30 abr. 2014. Faculdade de Direito USP, 2014.

PEREIRA, P. A. P. Discussões conceituais sobre política social como política pública e de direito de cidadania. In: BOSCHETTI, I. (Org.). *Política social no capitalismo: tendências contemporâneas*. São Paulo: Cortez, 2009.

SALLA, F. Os impasses da democracia brasileira: o balanço de uma década de políticas para as prisões no Brasil. **Revista Lusotopie**, Paris, v.10, p. 419-435, 2003.

SANTA CATARINA. Secretaria de Estado de Comunicação. **Balanço do Sistema Prisional 2013**. Disponível em: <<http://www.sc.gov.br/mais-sobre-seguranca-publica/sc-divulga-balanco-do-sistema-prisional>>. Acesso em: 20 jun. 2015.

_____. Secretária de Estado e do Planejamento. **Pacto por SC**. Disponível em: <<http://www.pactoporsc.sc.gov.br/>>. Acesso em: 7 jun. 2015.

_____. Tribunal de Contas do Estado. **Auditoria no Sistema Prisional Catarinense**. Florianópolis. 10 dez. 2014. Disponível em: <<http://www.tce.sc.gov.br/acom-intranet/noticia/23413/tcesc-faz-radiografia-do-sistema-prisional-catarinense>>. Acesso em: 20 jun. 2015.

SAPORI, L. F. **Segurança pública no Brasil: desafios e perspectivas**. Rio de Janeiro: Editora FGV, 2007.

_____. Avanço no socioeconômico, retrocesso na segurança pública: paradoxo brasileiro? **Revista de Ciências Sociais da PUC-Rio**, n.11, ago./dez. 2012, p. 133-158.

SOARES, L. E. A Política Nacional de Segurança Pública: histórico, dilemas e perspectivas. **Estudos Avançados**, São Paulo, v.21, n.61, 2007, p. 91-92.

SOUZA, C. Políticas Públicas: uma revisão da literatura. **Sociologias**, Porto Alegre, ano 8, n.16, jul./dez. 2006, p. 20-45.

2

CAPÍTULO

AS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NA GESTÃO ADMINISTRATIVA E OPERACIONAL DA SEGURANÇA PÚBLICA

Joel Souza de Oliveira

Vilson Gruber

Roderval Marcelino

Giovani Mendonça Lunardi

1 INTRODUÇÃO

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 industrial, de saúde, de ensino etc., e não seria diferente na segurança pública. Talvez esteja nesta área a maior contribuição da inovação na atualidade, devido ao fato de que, com o advento da globalização e com o avanço sistêmico das mais diversas tecnologias, o crime também inova, principalmente o crime organizado, que antes ficava restrito a determinadas regiões. Hoje, com as facilidades e a instantaneidade das comunicações, essas práticas delituosas são divulgadas quase instantaneamente para o mundo todo.

A informação não escolhe lugar determinado para chegar; ela está disponível para ser acessada em todo lugar e a qualquer momento. Para isso, basta que façamos uso de equipamentos com boa capacidade tecnológica e já estamos de posse da informação que nos interessa. Nos dias atuais, isso pode ser feito na palma da mão dos usuários dessas tecnologias: é o caso daquele que possui um *smartphone*, o que o torna habilitado a receber e a transmitir informações de qualquer lugar em que esteja. Sem falar, é claro, dos produtos que estão sendo desenvolvidos a todo o momento e que podem ser acessados a baixo custo, e até mesmo gratuitamente. Agora, imagine aqueles que estão segregados nos sistemas penitenciários do nosso país, por exemplo, onde quase todos os presos possuem em suas celas um aparelho de televisão, um microcomputador, seja ele um notebook ou netbook, um smartphone, um terminal celular de boa qualidade etc., e com todo o tempo e “segurança” do mundo para aprender a praticar o mal. Hoje, o cidadão que está em sua residência talvez não esteja tão seguro quanto aquele que está recolhido a um presídio de uma cidade qualquer do nosso país. As Tecnologias da Informação e Comunicação (TIC) levam o conhecimento a qualquer lugar do mundo, bastando, para isso, que se disponha de equipamentos integrantes de sistemas computacionais e com acesso à internet, que levam ao usuário qualquer tipo de informação desejada e que seja suficiente para aumentar seu conhecimento.

Verificou-se, em determinada ocasião, no Estado do Rio Grande do Sul, que da massa carcerária composta por aproximadamente 24 mil presos (na época da realização da pesquisa), que 10% destes conheciam eletrônica, ou seja, 2.400 presos conheciam eletrônica e 800 conheciam informática. Imagine o que se pode fazer com esse conhecimento, haja vista que nos nossos dias, com a eletrônica e a informática avançadas, pode-se fazer muita coisa, e em determinadas oportunidades até à distância, – como se tem notícia seguidamente –, em que criminosos de outros países praticam fatos criminosos aqui no Brasil e criminosos brasileiros cometem delitos em outros países, – os chamados crimes cibernéticos – que para serem descobertos exigem que os investigadores possuam um bom nível de conhecimento técnico.

Como é possível notar, o criminoso está inovando a todo o momento e os gestores da segurança pública não procedem da mesma forma, muitas vezes devido à própria legislação. Para citar um exemplo, a Lei nº 8.666 (Lei das Licitações, ou a Lei do Diabo, como é vulgarmente conhecida por causa do seu número final 666). Na área pública, esta lei gera uma série de transtornos em razão da necessidade de cumprimento de prazos. A lei é ótima, mas, no serviço público, ela acaba travando muitos processos, haja vista que quando se solicita algum equipamento de tecnologia de ponta, quando se recebe o que foi solicitado, este equipamento já está ultrapassado, devido ao avanço tecnológico, que é muito rápido. Para exemplificar, para a sorte dos órgãos que tratam com a segurança pública, as impressoras 3D, pelo que se sabe, ainda não chegaram ao submundo do crime, pois se lá estivesse, os criminosos certamente já estariam consertando e fabricando seu próprio armamento, em razão do potencial tecnológico deste equipamento.

2 PROCEDIMENTOS METODOLÓGICOS

A metodologia utilizada para tornar possível esta pesquisa foi a de cunho bibliográfico. “Pesquisa bibliográfica: quando elaborada a partir de material já publicado, constituído principalmente de livros, artigos de periódicos e atualmente com material disponibilizado na internet”. (GIL, 1991 apud SILVA; MENEZES, 2001, p. 21). Na oportunidade, também se utilizou a experiência dos autores, uma vez que o mesmo é servidor da Polícia Civil do Estado do Rio Grande do Sul, onde atuou como diretor de vários departamentos que compõem a estrutura orgânica da Polícia Civil, exercendo, inclusive, o cargo de Subchefe de Polícia.

3 RESULTADOS E DISCUSSÕES

As Nações Unidas definem segurança pública como: “o termo que consegue conjugar as dimensões de paz, segurança e desenvolvimento”. Isso pode ser interpretado como a ausência da violência em sociedade e a não existência de conflitos violentos, sendo que a expressão evoca os direitos fundamentais, a governança e o acesso à saúde e à educação. Ou seja, cada indivíduo terá oportunidades e liberdade de escolha para alcançar seu próprio potencial. Pode-se lembrar de Celso Furtado que, em sua premissa, lembra: “o desenvolvimento é uma construção coletiva. Não basta anunciar um novo paradigma de segurança pública no Brasil, é preciso mobilizar a sociedade em torno dele” (BRASIL, 2009, p. 14).

Da premissa de Furtado, verifica-se que a participação da sociedade é importante nas questões relacionadas à segurança pública em razão não apenas da prevenção, uma vez que, sem prevenção, não se faz segurança pública. Pode-se

até ir mais longe e afirmar que a prevenção reduz custo na gestão da segurança pública, fato que muitos “ditos” gestores da segurança não conseguem perceber, principalmente aqueles que vêm de órgãos operacionais de instituições encarregadas da prestação de serviços de segurança pública e que, por causa disso, acabam não fazendo gestão e, ao mesmo tempo, não fazem segurança; continuam fazendo ações como se estivessem no comando dos órgãos operacionais que dirigiam antes de assumir a gestão da instituição policial a qual pertencem. Pode-se concluir que o conceito de participação social da Constituição Federal de 1988 não é em vão, pois implica, no que se refere às políticas públicas, o envolvimento de muitos autores sociais, nas suas distintas etapas: elaboração de planejamento, implementação, execução, monitoramento e avaliação dos processos e políticas selecionadas nas áreas mais diversas dos serviços públicos e que podem contribuir para melhorias na segurança pública.

Do exposto, pode-se chegar à seguinte conclusão: no cenário global, a segurança dos indivíduos e da vida em sociedade passa a ser vista como uma etapa essencial ao desenvolvimento das nações, independentemente de situação econômica, pois começa a se tornar prioridade nas agendas políticas a criação de condições para que todos tenham o direito de conviver em liberdade e sem violência. Daí, conclui-se o motivo pelo qual não se faz investimentos em regiões muito violentas. As grandes indústrias e empresas, antes de se instalarem em determinados municípios, fazem uma sondagem sobre vários aspectos e um deles refere-se à segurança na localidade na qual pretendem se instalar. As TIC podem contribuir com as organizações que prestam serviços de segurança pública, principalmente na gestão administrativa e operacional desses órgãos, uma vez que a inovação tecnológica oportuniza a adoção de vários sistemas de comunicações, haja vista que se tem em mente que essas tecnologias, além de melhorar a qualidade dos serviços prestados à sociedade, traz motivação ao funcionários, resultando em aumento da produtividade nas áreas administrativas e operacionais das empresas públicas encarregadas da prestação de serviços de segurança. Para citar algumas tecnologias que podem ser empregadas com sucesso na segurança pública, pode-se começar pela teleconferência e pela videoconferência, tecnologias que facilitam as tomadas de decisões na gestão administrativa e operacionais das instituições, pois podem ser utilizadas para a realização de reuniões à distância entre os mais diversos órgãos que compõem a estrutura orgânica das organizações policiais. Isso reduz as despesas do Estado com diárias de viagem, gastos com combustível e desgaste dos veículos policiais, aumentando consideravelmente sua vida útil; diminui o risco de acidentes em viagens, no qual, muitas vezes, os envolvidos ficam impossibilitados de trabalhar por algum tempo ou até mesmo definitivamente, em razão de sequelas dos acidentes, podendo aposentar-se por acidente do trabalho ou precocemente, onerando os cofres públicos.

Na área operacional, a videoconferência tem uma importância significativa, representando ganho de qualidade, rapidez, eficácia e eficiência nas atividades de competência dos órgãos encarregados deste mister, mesmo que se tenha que alterar a legislação vigente, pois essa tecnologia possibilita a realização de oitivas, interrogatórios, reconhecimentos de pessoas, coisas e criminosos à distância, facilitando, assim, o trabalho dos órgãos operacionais das instituições encarregadas da prestação de serviços de segurança pública. O investimento em telefonia IP (Protocolo de internet) nesta área elevaria a qualidade dos serviços da instituição, tornando-a mais qualificada administrativa e operacionalmente e com importante redução de custos. O ensino à distância também tem sua importância na segurança pública, visando à qualificação dos funcionários e à formação do capital intelectual das instituições que operam na área. Essa tecnologia possibilita que funcionários do interior do Estado possam se atualizar com a participação em cursos de reciclagem, sem a necessidade de deslocamentos para a capital para frequentar cursos que possam ser ministrados à distância. No caso dos policiais, isso se torna ainda mais complicado, pois, para fazer um curso, ele não apenas se deslocaria, como diminuiria o efetivo da segurança de sua localidade.

Um provedor de internet é importante por ser um instrumento que agrega valor, principalmente no que se refere à utilização do tempo, em razão do interesse da administração na solução das mais diversas situações, uma vez que a informação é a principal matéria-prima com as quais as organizações policiais trabalham. A adoção de um sistema de terminais leves agrega muito valor na execução dos trabalhos desenvolvidos pelos organismos de segurança pública em razão do reduzido custo operacional desses terminais, ainda mais quando se necessita da aquisição de softwares e hardwares, além de oportunizar o aumento da produtividade administrativa e operacional.

Quando se refere à gestão operacional das instituições que lidam com segurança pública, com a utilização de TIC não se pode ficar alheio à inteligência, uma vez que esta destina-se à produção de conhecimento e é a que mais necessita de inovação tecnológica. Daí a importância que se dá a essa ferramenta, até mesmo porque se entende que: sem tecnologia da informação e comunicação não se tem inteligência.

A inteligência é um instrumento de grande importância para a atividade de segurança pública. Ela deve ser bem empregada pelos gestores, porém muitos deles não se dão conta disso e até a confundem com investigação. Aliás, esse é um dos principais problemas encontrados pelos gestores de órgãos encarregados da segurança pública na atualidade; por terem vindo da área operacional, muitos não conseguem distinguir uma da outra e quase sempre dispensam a inteligência e ficam com a investigação. Acabam jogando fora uma das melhores ferramentas que têm à sua disposição.

A inteligência como ferramenta de ampliação do conhecimento se alicerça, principalmente, na Análise Criminal, uma vez que esta tem por finalidade estabelecer correlações para a detecção de padrões criminais, como data, hora e característica do local em que ocorreu o crime; perfil das vítimas de interesse dos criminosos; o *modus operandi*, entre outros fatores significativos que podem contribuir para a identificação de padrão de determinada atividade criminosa ou do conjunto de atividades delituosas. Esse trabalho de análise é facilitado quando se utilizam meios computacionais para sua execução.

Os resultados ou os produtos oriundos da análise criminal são imprescindíveis para o bom desenvolvimento da atividade de polícia, pois favorecem não só a tomada de decisões, mas também o planejamento organizacional e o planejamento operacional, possibilitando a distribuição mais adequada de recursos materiais e humanos, direcionados às operações especiais de unidades táticas e de operações preventivas, subsidiando, assim, o desenvolvimento das ações de segurança pública com vistas à redução dos índices de violência e criminalidade. As principais fontes de informações e de dados, utilizadas atualmente com maior frequência pelos órgãos de segurança pública para a elaboração dos seus relatórios de análise criminal, são os registros de ocorrências policiais, as oitivas contidas nos inquéritos policiais, os relatórios das autoridades policiais e que integram os mesmos inquéritos policiais, as informações oriundas dos disque-denúncias, entre outras atividades internas e externas, sendo que estas podem ser acessadas a partir da utilização de softwares destinados a esta finalidade e que estão à disposição no mercado. Há softwares que facilitam a busca em diversos bancos de dados, em fontes abertas e fechadas. O Estado de Santa Catarina possui indústrias que desenvolvem produtos de excelente qualidade nesta área, por exemplo, sendo um polo industrial muito forte na produção de softwares.

Também se pode utilizar de sistemas de monitoramento de incidentes criminais a partir de mapas. Os mapas podem fornecer uma grande variedade de informações que incluem, mas não se limitam, à localização, à distância e à direção, bem como ao padrão de apresentação de dados pontuais ou de área. Cada tipo de dado significa coisas diferentes para usuários diferentes. Para a segurança pública, os mapas têm importância significativa, principalmente na formação de bancos de dados, com a utilização de mapas digitais georreferenciados, visando ao armazenamento de diversas informações sobre criminosos, grupos de criminosos (quadrilhas) e o crime organizado como um todo. A localização é, na perspectiva do analista criminal, o tipo mais importante de informação a ser apresentado ou reunido em um mapa. Os locais em que as coisas acontecem, aconteceram ou podem acontecer são as informações mais procurada e potencialmente úteis para a segurança pública, pois têm diversas implicações e aplicações para os agentes de inteligência e para os investigadores, bem como para a alocação dos recursos

do órgão policial com atuação no local em que está situada a comunidade para a qual devem prestar serviço, além da sua significativa utilidade no campo do planejamento organizacional, operacional e das políticas públicas de segurança. Na análise criminal, é importante levar em consideração o perfil geográfico de determinado ambiente. Por isso, considera-se de suma importância o georreferenciamento do local, por exemplo, se o local onde o grupo se reúne, reside ou está homiziado pode favorecer o oferecimento de alguma resistência à ação policial; identificar suas entradas e saídas e se há possibilidade de fuga no local e por onde estas podem ocorrer, bem como outras informações referentes ao terreno e que sejam interessantes, uma vez que esta é uma metodologia de inteligência e de investigação que utiliza a localização do conjunto de crimes ocorridos em determinado local, os quais devem estar conectados para determinar a provável região de atuação de um determinado criminoso ou grupo de criminosos, embora normalmente aplicado em casos de homicídios, estupros, incêndios criminosos, assaltos e atentados à bomba, seriais e outros. Nesses casos, pode ser produzido, com o auxílio de um software, o que se conhece por análise de vínculo, por meio da qual toda a quadrilha grupo ou organização criminosa tem o mapeamento de seus integrantes, assim como a identificação e os seus contatos.

Os locais dos crimes geralmente são subdivididos segundo o tipo de prática criminosa (por exemplo: encontro com a vítima, homicídio e local de desova dos corpos das vítimas), e como estão sendo utilizado, segundo os endereços, latitude/longitude ou digitalização. Nestes casos, podem-se utilizar fotos tiradas por satélites, tecnologia muito valiosa para o mapeamento e o georrefenciamento de locais de homicídio e/ou desova de cadáveres; ou um equipamento do tipo GPS para a marcação das coordenadas geográficas, importantes para a atividade policial. Ou seja, são oportunidades em que são criados e examinados os mais diversos cenários, nos quais os locais de práticas criminosas são pensados com base em certos princípios teóricos e metodológicos de interesse da inteligência, visando dar contribuição para a solução de um determinado caso delituoso.

O geoprocessamento “é um conjunto de técnicas de coleta, tratamento, manipulação e apresentação de informações que estão situadas dentro de um determinado espaço geográfico” (FURTADO, 2005, p. 49-50). Entre as mais relevantes formas de geoprocessamento, destacam-se: cartografia automatizada, processamento de imagens de satélite, digitalização de mapas e sistemas de informações (GIS – *Geographic Information System*) (GONÇALVES, 2001 apud FURTADO, 2005). O principal objeto do geoprocessamento, quando utilizado para subsidiar ações de segurança pública, é a geoinformação, ou seja, corresponde a uma informação unida com um atributo geográfico e que é identificado com auxílio de um equipamento do tipo GPS. Uma informação que tem como aliada sua posição geográfica é também chamada de informação georreferenciada, no

sentido de ter referência, por meio das coordenadas geográficas, a algum ponto da Terra. O tratamento da geoinformação permite o controle do meio ambiente e o planejamento de cidades e de redes de infraestrutura (FURTADO, 2005). No mapa, torna-se possível visualizar com mais facilidade a posição das informações coletadas. Essas visualizações das informações localizadas em um mapa, por si só, já esclarecem muito, pois dão noção espacial ao dado, trazendo este para o mundo concreto. Mas, além de facilitar a visualização, o mapa, aliado aos softwares e outros equipamentos de análise, também permite que o analista calcule as distâncias entre elas para tirar dessas informações tudo o que elas podem dar quanto ao lugar a que se referem.

Outra área bastante interessante que se verifica na segurança pública e que tem uma importância significativa nos dias atuais é a de radiocomunicações, ou seja, a utilização de sistemas de rádio. Cavalcante (2014, p. 62) apresenta aos leitores um artigo sobre as comunicações via rádio na segurança pública, introduzindo o assunto com um pequeno resumo histórico das comunicações através dos tempos, no mundo e no Brasil. O autor menciona que:

na década de 1990, as polícias brasileiras (Polícia Federal, Rodoviária Federal, Militar e Civil) começaram a trilhar caminhos diferentes para a aquisição de seus equipamentos de rádio, que, embora atendessem às especificidades de cada uma, em geral, não permitiam uma comunicação direta entre elas.

Essa é uma grande verdade: os órgãos que cuidam da segurança pública não falam entre si em nosso país. Imagine isso ocorrendo em uma situação de risco, de crise ou de emergência. Pelo que se sabe, é obrigação exclusiva do Estado proporcionar essa comunicação a partir da aquisição de equipamentos adequados e modernos, assim como exigir de todas as organizações, suas subordinadas, que os utilizem diariamente, possibilitando inclusive, de tempo em tempo, o treinamento simulado em conjunto de todas essas instituições. O treinamento deveria ocorrer nas unidades menores das instituições citadas anteriormente, preferencialmente nas Regiões Metropolitanas e também nas cidades do interior dos Estados e que hoje são aquelas que mais sofrem com a quantidade de assaltos a banco e com a utilização de explosivos (dinamite), em que os criminosos, muitas vezes, não possuem treinamento nem conhecimento sobre a carga de explosivos que devem utilizar, o que pode trazer sérias consequências, como derrubar um edifício inteiro, bem como as instituições que tratam com a segurança, que também não estão preparadas para o enfrentamento de uma situação de emergência desta natureza.

Cavalcante (2014) também comenta o ataque às Torres Gêmeas, no dia 11 de setembro de 2001, em Nova York, nos Estados Unidos, no qual ocorreu uma “falha na comunicação” – palavras mágicas que servem, muitas vezes, para minimizar uma situação que poderia ter um desfecho menos crítico ou até mesmo

salvar várias vidas. No dia em questão, quando os bombeiros de Nova York se dirigiam às torres em chamas, os sistemas de radiocomunicações não funcionaram, inclusive o sistema do Corpo de Bombeiros. Isso ocorreu em razão de estes profissionais nunca terem feito um treinamento para verificar o funcionamento dos seus equipamentos de telecomunicações, haja vista que eles haviam recebido transeptores novos, mas nunca os colocaram em uso, pois estavam guardados nos armários do Corpo de Bombeiros de Nova York ou nos porta-malas das suas viaturas.

Com a polícia aconteceu o contrário: os sistemas de rádio estavam funcionando, mas, por falta de treinamento conjunto, não conseguiam se comunicar com os bombeiros, sendo que estes não se entendiam entre si mesmo, pois os subordinados do Corpo de Bombeiros não conseguiam sequer ouvir as ordens emanadas de seus superiores via rádio. Pane em um sistema de comunicação via rádio é muito difícil de acontecer, ainda mais quando ele é utilizado constantemente, pois qualquer problema que ocorre é reclamado pelos usuários e logo o sistema é consertado. É bem isso que acontece em muitos dos nossos estados e municípios, com polícias civis e militares, corpos de bombeiros, guardas municipais, os institutos gerais de perícias, defesas civis, guardas de trânsito, entre outros, que, não estando preparados para o enfrentamento de uma crise, emergência ou caso de necessidade, não falam entre si por esses meios de comunicações, pois as frequências de operação utilizadas pelos rádios desses órgãos não são compatíveis.

O bom gestor deve estar atento a tudo e ser inovador. Por isso, são interessantes as frases de Vegetius, que diz “*Si vis pacem, para bellum*” (Se queres paz, prepara-te para a guerra) e de Sun Tzu: “Na paz, prepara-te para a guerra. Na guerra, prepara-te para a paz”. Fica subentendido que devemos estar sempre preparados para o enfrentamento de casos de crise ou de emergência, que pode ocorrer a qualquer momento e em qualquer lugar. O atentado às Torres Gêmeas ceifou a vida de mais de 2 mil pessoas, fato que não teria ocorrido se os sistemas de comunicação via rádio tivessem funcionado a contento naquele dia. Entre as mortes ocorridas, estavam muitos bombeiros, que perderam a vida em consequência do não funcionamento de seus equipamentos.

No Estado do Rio Grande do Sul vive-se um fato gravíssimo relacionado à gestão da segurança pública, que é o caso do Centro de Comando e Controle. Esse centro faz parte da estrutura orgânica da Secretaria da Segurança Pública, o que entendemos como completamente errado, haja vista que a Secretaria é um órgão de supervisão e não um órgão de execução. Por isso, não poderia ter em sua estrutura um órgão de execução, assim como também não poderia estar de posse do Sistema Guardião, equipamento do sistema computacional e que deveria ser de uso exclusivo do órgão que detém a competência da investigação policial, ou seja, a Polícia Civil. No entanto, também está sediado no âmbito da Secretaria e,

assim como o Centro de Comando e Controle, também faz parte da sua estrutura orgânica, só para citar os problemas de gestão que se pode encontrar nesta área no nosso Estado. O interessante seria o Centro de Comando e Controle, que está instalado na Secretaria, funcionar junto à inteligência, sendo um órgão integrante do Departamento de Inteligência de Segurança Pública, para subsidiar o secretário da Segurança em suas tomadas de decisão. Já os demais órgãos vinculados à Secretaria deveriam possuir seus próprios centros, como era em outras épocas, em que a Polícia Militar possuía a Central de Operações Policiais Militares (COPOM) e a Polícia Civil possuía seu Centro de Operações. Só para se ter uma ideia, naquela oportunidade, a Polícia Militar, após um trabalho de implantação de um sistema de controle de qualidade, atendia a uma ocorrência em menos de cinco minutos, fato que hoje não ocorre.

Assim, imagine o que pode ocorrer em uma situação de crise ou de emergência. É interessante que se tenha outros centros, até mesmo como um sistema de contingência, para atuação em casos de extrema necessidade, para que não ocorra o que aconteceu no 11 de Setembro. A todo o momento surgem novas TIC, que auxiliam na solução das necessidades dos órgãos que atuam na segurança pública, como é o caso de balões, drones (VANTs), nanodrones, chips, REFIDs (abreviação de *Radio Frequency Identification*, Identificação por Rádio), Biometria, novas formas de monitoramento eletrônico, investigação eletrônica à distância e equipamentos eletrônicos embarcados (tecnologia embarcada), principalmente na área das telecomunicações.

4 CONSIDERAÇÕES FINAIS

Ante ao exposto, verifica-se o quanto é importante a inovação associada às Tecnologias da Informação e Comunicação na segurança pública do nosso país, uma vez que se entende a informação como a principal matéria-prima utilizada pelos órgãos policiais, que detêm a competência para tratar a segurança pública, principalmente quando necessitam esclarecer práticas delituosas e que, em muitas situações, envolvem até mesmo o crime organizado, controlado por quadrilhas qualificadas e com tentáculos, em alguns casos, até no exterior.

A grande dificuldade encontrada atualmente está na cabeça dos gestores das instituições encarregadas dessa prestação de serviço, que devem sair da mesmice e praticar inovação a qualquer custo. Para atuar na segurança pública, os gestores devem ser criativos, verdadeiros empreendedores, caso contrário, estarão fadados ao insucesso e serão cobrados pelas principais lideranças da sociedade em que atuam.

O que acontece atualmente, e que acaba criando problemas para os gestores desta área, é o fato de que eles têm dificuldade de lidar com novidades. Procuram fazer, e até mesmo atuar, olhando sempre para o retrovisor, ou seja, continuam

praticando os mesmos atos que eram praticados por seus antecessores, não criam nem investem em novos modelos e esquecem-se de que possuem uma grande aliada, as TIC, que se bem utilizadas, facilitarão todo o tipo de trabalho que é realizado pelos órgãos encarregados da prestação desse serviço tão importante para a sociedade.

REFERÊNCIAS

- BRASIL. Ministério da Justiça. Texto-base. In: CONFERÊNCIA NACIONAL DE SEGURANÇA PÚBLICA, 1., 2009, Brasília, DF. **Texto-base...** Brasília, DF, 2009. Disponível em: <http://www.ipea.gov.br/participacao/images/pdfs/conferencias/Seguranca_Publica/texto_base_1_conferencia_seguranca_publica.pdf>. Acesso em: 20 jun. 2016.
- CAVALCANTE, V. D. Comunicação na segurança. **Revista Segurança e Defesa**, Rio de Janeiro, n. 116, p. 62-66, 2014.
- DANTAS, G. F. L.; SOUZA, N. G. **As bases introdutórias da análise criminal na inteligência policial**. Disponível em: <http://www.justica.gov.br/central-de-conteudo/seguranca-publica/artigos/art_as-bases-introductorias.pdf/view>. Acesso em: 16 mar. 2015.
- DWYWE, J., FLYNN, K. **102 minutos: a história inédita da luta pela vida nas Torres Gêmeas**. (Tradução de Maria Lúcia de Oliveira). Rio de Janeiro: Jorge Zahar, 2005.
- FURTADO, V. **Tecnologia e gestão da informação na segurança pública**. Rio de Janeiro: Garamond, 2005.
- GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2008.
- KING, D. W.; TENOPIR, C. A publicação de revistas eletrônicas: economia da produção, distribuição e uso. **Ciência da Informação**, Brasília, DF, v. 27, n. 2, p. 176-182, maio-ago. 1998. Disponível em: <<http://www.scielo.br/pdf/ci/v27n2/2729810.pdf>>. Acesso em: 28 set. 2015.
- MEADOWS, A. J. **A comunicação científica**. Brasília, DF: Briquet de Lemos, 1999.
- OLIVEIRA, F. B. et al. **Desafios da gestão pública de segurança**. Rio de Janeiro: Editora FGV, 2009.
- SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. Florianópolis: UFSC, 2005.
- VALLE, A. B. **Gestão da tecnologia da informação**. Rio de Janeiro: Editora FGV, 2013.

3

CAPÍTULO

LAUDO DIGITAL – A QUEBRA DE PARADIGMAS

Norton Meidel Karam

Vilson Gruber

Roderval Marcelino

Giovani Mendonça Lunardi

1 INTRODUÇÃO

O grande desafio é implantar esse novo procedimento em um ambiente no qual, há alguns anos, a forma de trabalho é totalmente diferente. Desde as máquinas datilográficas, o rascunho do laudo era produzido em papel, com as fotografias em anexo, muitas vezes ainda reveladas e coladas a um suporte de papel que acompanhava a parte escrita – o corpo do laudo. Esse rascunho era passado ao revisor, que ali mesmo anotava seus comentários, riscava os erros, colocava acentos e vírgulas esquecidas etc., devolvendo ao relator para correção. Com o conteúdo do laudo devidamente corrigido, esse vai-e-vem se repetia para a assinatura do documento. De repente, aquele “sempre foi assim” muda.

Todos sabem que o ser humano tende a ser resistente às mudanças, pois isso demanda a saída de sua zona de conforto. Então, qual é a forma menos dolorosa de fazer com que, da noite para o dia, todos, incluindo os peritos mais antigos com sua aposentadoria já próxima, comecem a trabalhar de forma diferente? Quais são os artifícios administrativos, tecnológicos, para convencer a utilização dessa nova ferramenta? Como passar, com o mínimo de trauma, do papel para a tela de um computador, na qual não se precisa de caneta para a assinatura do laudo?

A monografia completa, produzida como trabalho de conclusão do curso de Especialização em TI na Segurança Pública, versa, após uma breve explicação sobre todo o processo, desde a solicitação da perícia e a elaboração do laudo até a entrega do documento (o laudo pericial, com ou sem devolução de material), que esclarece a persecução penal e parte dos órgãos envolvidos, além de estabelecer as principais carências captadas por meio de pesquisa de campo, compor um tutorial (uma espécie de manual do usuário) e propor sua utilização pelos novos usuários do sistema. Este artigo pretende discutir somente a implantação de um novo sistema de informação, suas consequências, suas adversidades e suas peculiaridades, por meio de pesquisa realizada em seções do Departamento de Criminalística do Instituto Geral de Perícias (IGP/RS), no qual a implantação já foi iniciada. Dessa forma, aqui são expostos os procedimentos utilizados, considerações sobre a implantação e manutenção de novos sistemas de informação, com mudança radical nos processos utilizados até então, discutindo a melhor forma de fazê-lo.

2 PROCEDIMENTOS METODOLÓGICOS

A técnica de levantamento de dados e informações utilizada foi a pesquisa documental (questionário), com enfoque exploratório, que consiste na coleta, classificação e seleção difusa no emprego de toda espécie de informações. O estudo pressupõe uma abordagem qualitativa, com o desafio de apreender, sob a ótica daqueles que participam do universo pesquisado, o sentido da experiência vivenciada, buscando compreensão dos fenômenos sociais para além de sua explicação, em termos de relação causa-efeito.

Pode-se observar que não houve a necessidade de identificação pessoal dos pesquisados, o que os deixou livres para exporem, de forma não comprometedora, suas visões sobre o que lhes fora oferecido até então. O resultado alcançado com a aplicação do questionário não poderia ser outro: havia insatisfação generalizada sobre a forma como o novo sistema foi colocado em prática.

Sabe-se que, para o sucesso de uma implantação de um novo sistema de informação, é necessário o atendimento de um requisito conhecido hoje em dia por *Enterprise Resource Planning* (ERP). Um ERP bem estruturado exige que sejam cumpridas todas as etapas do processo, que vão desde a aquisição de hardware e

software adequados ao sistema, desenvolvimento de documentação, treinamento de usuário final, acompanhamento, manutenção e *feedback* dos operadores ou usuários finais.

3 SISTEMAS DE INFORMAÇÃO

O desenvolvimento e a manutenção dos sistemas de informação (SI) empresariais englobam princípios de TI e sua infraestrutura; a administração dos recursos de hardware e de software, com a utilização preferencial de software livre; o uso de telecomunicações e de redes; suporte gerencial e organizacional, apoiando os gestores nos processos de tomada de decisão; segurança e controle; além de questões políticas, éticas e sociais. As transformações dependem dos avanços tecnológicos, da busca constante por mais qualidade, das mudanças na economia e no comportamento das pessoas, bem como do aumento da competitividade e da globalização.

Estamos na Era da Informação, com pessoas passando a maior parte do seu tempo criando, usando e distribuindo informação. Na nova economia, a informação e o conhecimento são as fontes do poder. O profissional da era do conhecimento tem a capacidade de transformar os dados e as informações em conhecimento, conhecimento que gera ação.

No âmbito da Segurança Pública não poderia ser diferente. Observa-se que, em um ambiente que muda constantemente, as filosofias operacionais e administrativas precisam se adaptar às exigências do mercado. É necessário estar consciente de que a participação ativa do funcionário da ponta – os *knowledge workers* – é imprescindível no desenvolvimento e na manutenção dos sistemas de informação. Só assim pode-se obter conhecimento suficiente acerca da dinâmica e da realidade da instituição. Deve haver uma orientação sistêmica para definir problemas e oportunidades e desenvolver soluções. Os sistemas de informação dependem da Tecnologia da Informação (TI). Sistemas eficazes e eficientes têm grande impacto na estratégia corporativa e no sucesso organizacional, proporcionando segurança, disponibilidade de recursos, melhores serviços, aperfeiçoamento no controle e na tomada de decisões, e na redução de custos. Independentemente do tamanho, cada vez mais organizações precisam de sistemas de informação para reagir aos problemas. Esses sistemas vêm se tornando, ao longo dos últimos anos, cruciais para as operações do dia a dia das organizações, nos níveis operacional, de conhecimento, gerencial e estratégico. São eles que dão suporte aos gerentes organizacionais no acompanhamento de atividades e transações elementares das organizações, seja ajudando a empresa a integrar novos conhecimentos, fornecendo relatórios periódicos ou informações instantâneas sobre as transações internas e externas, ou ainda apoiando as atividades de planejamento, conciliando altera-

ções no ambiente externo com a capacidade organizacional existente.

Este artigo pretende abordar o sistema de processamento de transações – um sistema básico que serve para o nível operacional da organização. Ele realiza e grava as transações rotineiras necessárias para conduzir o negócio – a perícia oficial. É utilizado pelo IGP/RS, o Protocolo Geral de Perícias (PGP). Apesar de ser utilizado por pessoas com pouca ou nenhuma responsabilidade, são os dados ali inseridos que alimentarão o *business information* (BI), que auxiliará os gestores nas tomadas de decisões. A conscientização dos usuários deve ser implementada pelas chefias, notificando os erros de procedimento, para que estes sejam minimizados. A adoção de um novo sistema ou a realização de mudanças radicais, como a utilização da *web service* para registro das atividades e encaminhamento dos trabalhos, conhecido como *workflow*, afetam sobremaneira, positiva ou negativamente, seus usuários colaboradores da instituição.

Estudos de sistemas de informação de processamento de transações que tiveram sucesso mostram que raramente eles são planejados, mas evoluem vagarosamente em longos períodos de tempo e quase sempre se originam de problemas práticos operacionais. Em vez de brotarem de alguma metodologia mágica, os sistemas estratégicos que atingiram bons resultados vieram de observações de situações reais. Por essa razão, e também devido às peculiaridades da Região Sul, o IGP/RS optou por desenvolver seu próprio sistema, com o auxílio da empresa Procergs, em vez de adquirir uma ferramenta pronta disponível no mercado. Além disso, foi observado que um dos maiores obstáculos para as transições é a resistência em mudar a cultura operacional. Isso foi notado tanto em colaboradores veteranos como em servidores mais jovens, inclusive os da geração Y, que já nasceram com a internet.

4 FLUXO DE TRABALHO – WORKFLOW

O IGP só trabalha se provocado. A Polícia Civil responde por cerca de 95% das solicitações de perícias. Outros órgãos, como a Brigada Militar, o Ministério Público e a Justiça Estadual, também podem solicitar perícia ao IGP/RS. É a partir da solicitação de perícia que é gerado um novo protocolo no sistema. Por enquanto, esse registro ainda é realizado no sistema antigo (PGP Desktop). Após o preenchimento de algumas etapas, migra-se para o novo sistema (PGP Web). A utilização desse novo sistema está entre as principais diretrizes do IGP/RS. Esse sistema dispensa parte da mão de obra administrativa, carência comum em diversos órgãos públicos. O registro, a tramitação e o encaminhamento interno, como o envio para a revisão e assinatura dos laudos, assim como seu envio para o órgão solicitante ou de difusão, por meio da integração do Sistema da Polícia Judiciária (SPJ), foram automatizados. O novo processo termina definitivamente

com a utilização de papel, impressora e cartucho de impressão nesse trâmite. É uma mudança radical em procedimento. Este trabalho, após constatar a carência de um manual, o produz.

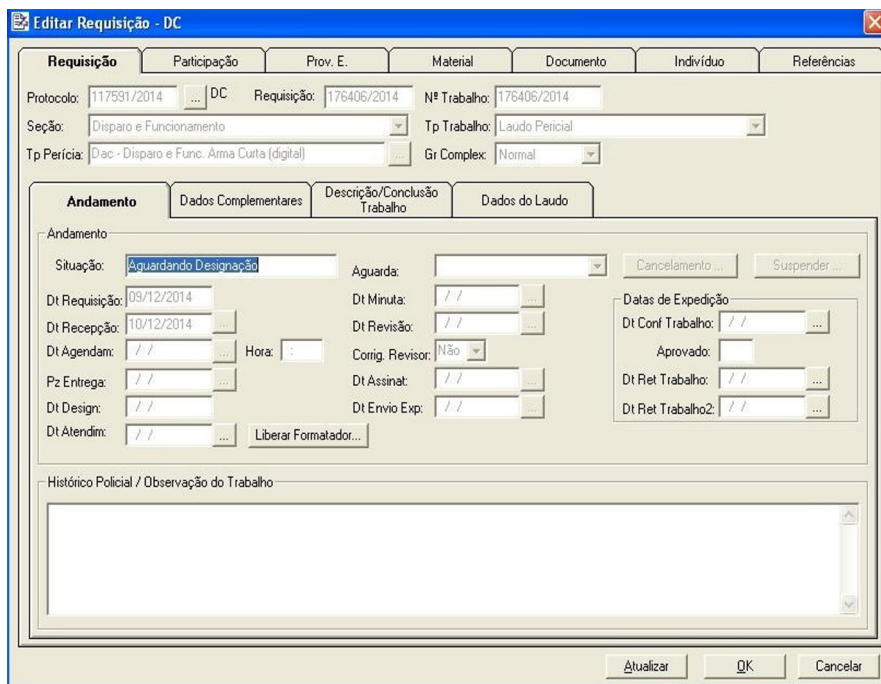


Figura 3.1 Tela de tramitação do trabalho pericial no PGP Desktop.

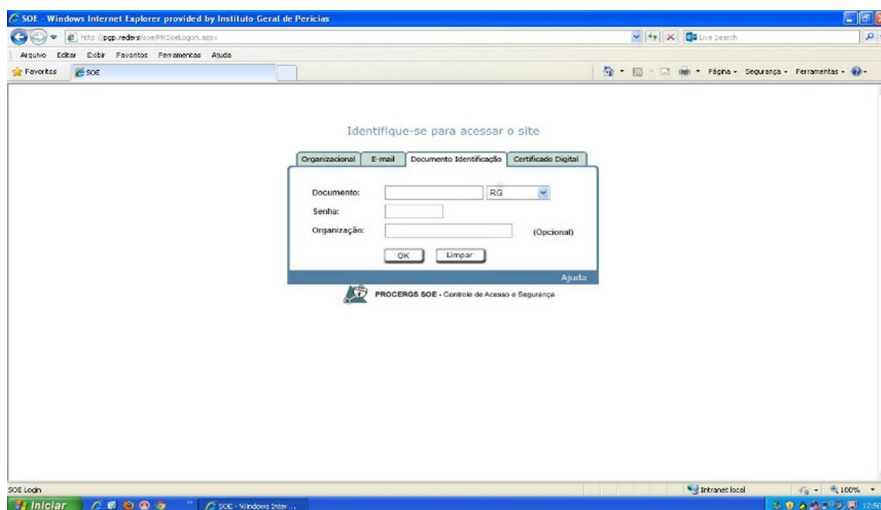


Figura 3.2 Tela de acesso ao novo sistema PGP Web.

O manual é um tutorial sobre como os novos usuários deverão proceder no sistema PGP Web. Esse tutorial demonstra todos os passos necessários no novo processo, desde o login no sistema, a escolha do módulo (Módulo de Laudos), as guias *Formatador de Laudos* e *Tarefas em Lote*, gerar um arquivo, editá-lo, enviar ao revisor (se for o caso), recebê-lo de volta, corrigi-lo, assiná-lo digitalmente, até enviar novamente ao revisor para finalmente ser enviado por meio da integração dos sistemas PGP e SPJ, caso não haja material a ser retirado preliminarmente.

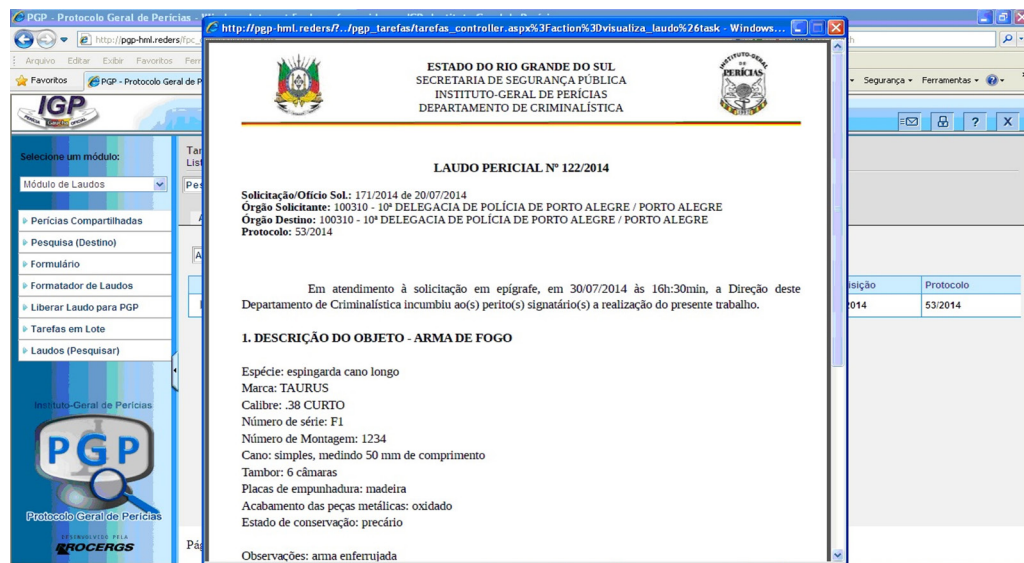


Figura 3.3 Parte de um laudo pericial digital.

Uma vez esclarecido, pelo manual, o passo a passo de todo o processo de solicitação de perícia até o envio do laudo digital assinado eletronicamente, passamos à questão de como difundir esse conhecimento, modificando totalmente a forma de trabalho, por meio da implantação do novo sistema de informação. Essa é a proposta da monografia: verificar a melhor maneira de “sugerir” aos colaboradores do Departamento de Criminalística, em suas diversas seções e cerca de 130 tipos de perícias diferentes, a colaboração no sentido, de juntos, desenvolver a forma menos traumática de utilização do novo sistema de informação.

5 CONSIDERAÇÕES FINAIS

Não há como contrariar que a não utilização do papel, impressora e cartuchos, até a necessidade de menos mão de obra administrativa na tramitação dos trabalhos periciais, são os principais efeitos da implantação do laudo digital. Além dessa vantagem, o imediatismo do envio do documento, apesar de condicio-

nado à retirada física do material periciado, quando houver, “corre parelho nessa cancha reta”, como dizem metaforicamente os gaúchos, pois existem milhares de resultados de exames periciais que não devolvem material e poderão ser prontamente conhecidos pelas partes interessadas. Por fim, o armazenamento digital dos laudos, terminando com os depósitos lotados de caixas de papelão com folhas de papéis mofados, mal conservados e com difícil acesso, acaba com qualquer dúvida no sucesso dessa nova tecnologia.

É inerente a toda implantação de novos sistemas de informação causar certa resistência por parte do usuário final. Porém, esse problema pode ser minimizado com a efetivação de todas as etapas da implantação bem realizadas. Disponibilização de hardware e software adequados, documentação do processo, treinamento de usuário final, acompanhamento, manutenção e *feedback* são imprescindíveis. Notadamente, em todos os órgãos públicos existem carências de recursos e, sem a implantação correta, os resultados serão insatisfatórios, causando a impressão de que “antes era melhor, mais fácil e mais rápido”, o que não é verdade. Quantas pessoas, não necessariamente as mais idosas, resistem à utilização de telefones celulares para o envio de mensagens, arquivos de imagens e vídeos? Mas todos concordam que é uma tecnologia inquestionável. Mais cedo ou mais tarde, quem não se adaptar ficará defasado, “por fora”. Devem ser tomadas todas as medidas necessárias para que esse processo de mudança seja o menos traumático possível. Existem inúmeros estudos sobre implantação de sistemas, mas todos concordam no ponto em que se fala que só obterá sucesso na implantação de um novo sistema de informação aquelas empresas que compreenderem a exigência de todas as etapas necessárias.

Grande parte da iniciativa deve vir da TI, entendida como o setor da empresa que proporcionará, de forma sistêmica ou esporádica, todos os recursos tecnológicos e computacionais para geração, tratamento e uso da informação. A TI é a base do gestor na tomada de decisão com rapidez e dinamismo. O desconhecimento elementar ou a falta de valorização da TI e de seus recursos debilita o planejamento estratégico. Essa área atua no desenvolvimento e na melhoria do sistema de informação, auxiliando a organização em seus processos e suas atividades-fim. Os níveis de decisão obedecem à hierarquia (política, no caso de empresas públicas) existente na empresa, algumas vezes segmentado em níveis estratégico, tático e operacional. A tecnologia ERP são pacotes (software) de gestão empresarial ou de sistemas integrados, com recursos de automação e informatização, que visam contribuir com o gerenciamento dos negócios. Quanto mais preciso e ágil for o fluxo de informações, maior será a velocidade com que a informação será processada. Integrar esses processos de maneira que permita que a informação flua imediatamente, sem o auxílio da tecnologia da informação, é humanamente impossível.

O desenvolvimento de documentação que seja de fácil compreensão (manual do operador) é de suma importância na implantação de um SI. O manual deve compreender os procedimentos operacionais com amostras de telas de exibição, formulários e relatórios de entrada e saída de dados. O treinamento dos usuários finais, o acompanhamento e a manutenção do SI, principalmente na fase de implantação, são etapas necessárias para corrigir falhas e problemas que surgem durante a operação do sistema. A avaliação compreende eficiência, flexibilidade, segurança, conectividade, linguagem, documentação, hardware etc. A falta de experiência em virtude da ausência de treinamento e de capacitação adequada dos novos usuários muitas vezes acaba levando-os a ter medo de serem julgados como incompetentes.

A resistência das pessoas em trocar o velho controle feito com papel e caneta por um software funcional e preciso será inevitável por muito tempo ainda. O que precisa ser feito é preparar os indivíduos para tais mudanças, tendo como objetivo principal a melhoria e o aperfeiçoamento do processo. As novas tecnologias sempre provocarão mudanças no ambiente social da organização e o gestor precisa preparar-se para saber o que fazer diante dessas mudanças. Hoje, é claro e notório que é difícil imaginar alguma inovação tecnológica que possa ser introduzida sem provocar algum efeito, visto que o principal objetivo das organizações ao adquirirem inovações tecnológicas é a forte preocupação com seu desempenho.

A perícia do Rio Grande do Sul deve desempenhar um processo agressivo de crescimento e modernização em virtude da alta qualidade da mão de obra empregada, produzindo um laudo digital condizente com seus colaboradores, pautada nas diretrizes da norma ISO 9001. Maior importância, estrutura e autonomia deverão ser aplicadas à Divisão de Tecnologia da Informação (DTI), para a efetiva e eficaz implantação do PGP Web.

Com a utilização do Manual do Laudo Digital, as dúvidas corriqueiras na utilização do novo sistema (PGP Web), “cairão por terra”. Haverá mais aceitação das mudanças, desde que todas as etapas, já citadas, na implantação de novos sistemas de informação sejam observadas e a devida valorização à TI do Departamento de Criminalística (DC) seja dada.

Esperamos dos gestores a compreensão de que não existe gestão sem informação. Os formulários serão desenvolvidos, um a um, conforme os procedimentos operacionais padrão (POP) elaborados pela Senasp e adaptados à realidade gaúcha por meio de uma comissão que deverá ser formada no Departamento de Criminalística. Esse formulário não é rígido, engessado. Pode ser modificado e aperfeiçoado a qualquer instante por desenvolvedores do sistema.

O sistema PGP Web tem tudo para dar certo. É o futuro, ou melhor, já é o presente. O Manual do Laudo Digital já é realidade. A iniciativa individual

atingiu o objetivo de sua produção. O aprendiz do novo procedimento já terá essa nova ferramenta em suas mãos e não precisará ficar anotando em pedaços de papel ou cadernos como utilizá-lo, o que pode incorrer em erros devido ao grande volume de informações, em função da falta do manual. Temos certeza de que a Direção Geral do IGP/RS compreenderá a importância desta ferramenta de trabalho, tomando as medidas necessárias para sua utilização plena.

Fica clara e evidente a necessidade de mais investimentos em pessoal na área de TI, tanto em nível de DC quanto em nível de IGP como um todo. O mais importante da conclusão deste trabalho é que o IGP/RS, especialmente o DC, ganhou uma ferramenta imprescindível – o Manual do Laudo Digital –, o Fluxo Digital no PGP Web, com diversas ilustrações e imagens com setas indicando onde clicar e como fazer para desenvolver esse novo procedimento que, sem dúvida alguma, só tem a qualificar o serviço da perícia rio-grandense.

Esperamos a compreensão dos diversos aspectos elencados neste artigo para a melhoria do trabalho técnico de perícia desenvolvida pelos colaboradores do Departamento de Criminalística, com a certeza de que posicionamentos políticos não interferirão na qualificação desses profissionais.

REFERÊNCIAS

BRASIL. Defesa e Segurança. **Portaria define normas a serem seguidas pelas perícias criminais**. Disponível em: <<http://www.brasil.gov.br/defesa-e-seguranca/2014/07/portaria-define-normas-a-serem-seguidas-pelas-pericias-criminais>>. Acesso em: 6 fev. 2015.

_____. Diário Oficial da União nº 143, 29/07/2014, Seção 1, p. 46, ISSN 1677-7042. Portaria nº 89, de 28/07/2014. SENASP/MJ.

_____. Ministério da Justiça. Secretaria Nacional de Segurança Pública. **Procedimento Operacional Padrão – Perícia Criminal**. Brasília/DF, 2013.

CONSELHO DE JUSTIÇA FEDERAL. **O que é assinatura digital?** Disponível em: <<http://www.cjf.jus.br/cjf/tecnologia-da-informacao/identidade-digital/o-que-e-assinatura-digital>>. Acesso em: 13 fev. 2015.

ESPINDULA, A. Laudo pericial e outros documentos técnicos. **Conteúdo Jurídico**, Brasília, 20 dez. 2008. Disponível em: <<http://www.conteudojuridico.com.br/artigo,laudo-pericial-e-outros-documentos-tecnicos,22509.html>>. Acesso em: 6 fev.2015.

RABELLO, E. **Curso de Criminalística**. Porto Alegre: Sagra/Dc Luzzatto, 1996.

RIO GRANDE DO SUL. **Lei nº 13.601**, de 1 de janeiro de 2011. Dispõe sobre a estrutura administrativa do Poder Executivo do Estado do Rio grande do Sul e dá outras providências. Art. 33, p 10.

STUMVOLL, V. P.; TOCCHETTO, D. **Criminalística**. 6. ed. São Paulo: Millenium, 2009.

TOURINHO FILHO, F. C. **Processo Penal**. 24. ed. São Paulo: Saraiva, 2002.

WIKIPEDIA. **Sistema integrado de gestão empresarial**. Disponível em: <https://pt.wikipedia.org/wiki/Sistema_integrado_de_gest%C3%A3o_empresarial>. Acesso em: 26 abr. 2016.

WIKIPEDIA. **Web service**. Disponível em: <https://pt.wikipedia.org/wiki/Web_service>. Acesso em: 10 fev. 2015.

4

CAPÍTULO

IDENTIFICAÇÃO BIOMÉTRICA DIGITAL NA GESTÃO DO ATENDIMENTO DE ADOLESCENTES INFRATORES

Sônia Maria Dall'Igna

Alberto Felipe Friderichs Barros

Paulo Cesar Leite Esteves

Vilson Gruber

Giovani Mendonça Lunardi

1 INTRODUÇÃO

De acordo com Santin (1999), a segurança pública é considerada pela população como um dos serviços mais importantes e essenciais, provavelmente pela sensação de insegurança que decorre da crescente criminalidade nas grandes cidades, o que influencia diretamente no sentimento de liberdade dos cidadãos. O

Departamento Estadual da Criança e Adolescente (DECA), da Polícia Civil do Rio Grande do Sul (RS), tem em sua estrutura um plantão para o atendimento de adolescentes que entram em conflito com a lei.

Por questões de várias ordens, o adolescente que se torna reincidente adquire uma etiqueta no sistema, que reforça a continuidade das práticas delitivas, eis que se autodefine como identificado com o crime. Porém, diante da perspectiva de se livrarem dos registros policiais, repassam seus delitos para nomes que o liberam de inúmeros antecedentes (TEJADAS, 2007).

Em razão desse panorama, de 1990 até 2005, em vista da precária tecnologia, os adolescentes, quando apresentados à autoridade policial, faltavam com a verdade quanto às suas identidades e, caso não fossem localizados seus responsáveis, eram registrados na ocorrência com os nomes que declarassem em razão da ausência de confrontação de dados. Entretanto, ficavam erroneamente identificados, muitas vezes incriminando seus irmãos, primos, tios, parentes ou vizinhos, de quem utilizavam o nome na identificação, ou simplesmente mencionando nomes imaginados, não existentes na realidade.

Era comum um único adolescente possuir identificações diferentes e, em algum momento, ser identificado de forma correta pela memória do policial que já o atenderá em outros episódios, pois a reincidência entre adolescentes infratores é alta. Diante dessa abordagem, justifica-se a realização desta pesquisa, que objetiva apresentar as melhorias no processo de gestão de modo a contribuir com outras unidades de identificação em todo o país.

No presente trabalho, apresenta-se um estudo de caso sobre a implantação da biometria no Departamento Estadual da Criança e do Adolescente da Polícia Civil do Rio Grande do Sul. Para tanto, este artigo está estruturado em quatro seções, inclusive introdução. A seção 2 traz o referencial teórico e aborda a literatura sobre biometria. A seção 3 apresenta os procedimentos metodológicos que conduziram esta pesquisa. A seção 4 aponta os resultados e o processo de implantação biométrica e, por fim, têm-se as considerações finais do trabalho.

2 CONCEITO E OS TIPOS DE BIOMETRIA

Um controle biométrico pode ser definido como um método automatizado para verificar a identidade de uma pessoa, com base em características físicas e comportamentais. A maioria das pessoas compara alguma característica pessoal com um perfil armazenado (MONK, 2013). “A biometria, em sentido amplo, trata da mensuração e avaliação estatística das estruturas dos seres vivos. É muito antiga, mas as tecnologias de informação e comunicação geraram avanços significativos na área” (ABDI, 2010, p. 60).

As características biométricas podem ser divididas em duas classes principais, conforme pode-se observar na Figura 4.1.

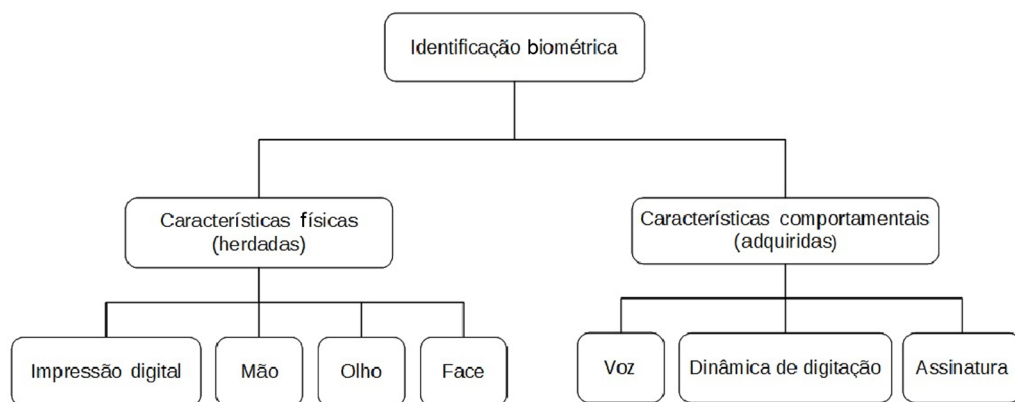


Figura 4.1 Classificação e tipos de biometria.

Fonte: adaptada de <http://www.acessoseguro.com.br/biometricas.asp>.

As características físicas estão relacionadas com a forma do corpo. Como exemplos de características físicas destacam-se: as impressões digitais, a aparência facial, o padrão da íris, a geometria das mãos, o DNA, o padrão de veias das mãos, a retina e a geometria das orelhas. Já as características relacionadas ao comportamento de uma pessoa, diferentemente das características físicas, podem ser aprendidas ou treinadas ao longo do tempo, como: o modo de andar, a assinatura, o padrão de voz, a dinâmica de digitação, os movimentos faciais e os movimentos labiais (KAMI, 2011).

2.1 Impressões digitais

Conforme Campos (2005), a impressão digital é o método de biometria mais utilizada no mundo, tecnicamente chamada de datilograma ou dermatóglifo. É o desenho formado pelas papilas, elevações da pele, presentes nas polpas dos dedos das mãos, deixado em uma superfície lisa. As impressões digitais são únicas em cada indivíduo, sendo distintas inclusive entre gêmeos univitelinos. Tal característica, chamada unicidade, faz com que elas sejam utilizadas como forma de identificação de pessoas há séculos.

As papilas são formadas durante a gestação e acompanham a pessoa até a morte, sem apresentar mudanças significativas. Esta propriedade é conhecida como imutabilidade. A impressão digital apresenta pontos característicos e formações que permitem que um perito ou um papiloscopista identifique uma pessoa de forma bastante confiável. Uma das tecnologias biométricas comercialmente

disponível são os dispositivos de reconhecimento de impressões digitais. Com esses dispositivos, os usuários não precisam digitar senhas; em vez disso, com apenas um toque, o sistema oferece acesso instantâneo (PATRÍCIA, 2014).

Segundo Muniz (2007), os aparelhos biométricos funcionam por meio da captura de amostras do ser humano: íris, retina, dedo, rosto, veias da mão, voz e até odores do corpo. Essa amostra é transformada em um padrão, que poderá ser comparado para futuras identificações. A biometria baseia-se na ideia de que alguns traços físicos são exclusivos de cada ser e os transforma em padrões. Não existe um consenso quanto à tecnologia biométrica mais adequada para cada tipo de aplicação, mas existem aplicações que só são viáveis com determinada tecnologia.

A identificação por impressão digital ainda é a preferida para a maioria das aplicações por ser mais simples e madura e também pela tradição de uso anterior às tecnologias digitais, principalmente pela polícia. Além disso, é a única tecnologia que permite identificação posterior de pessoas por meio da coleta da impressão digital deixada em objetos (ABDI, 2010).

As aplicações principais estão relacionadas à identificação para autenticidade da pessoa e controle de acesso. Sua utilização, porém, é possível em uma infinidade de situações como: autorização de acesso a locais físicos, controle de ponto, identificação de clientes em sistemas de cobrança automática de consumo, identificação de pessoas em hospitais, controle de acesso a informações confidenciais em quaisquer tipos de instituições e empresas, ativação de equipamentos, identificação em presídios, liberação de transações financeiras, entre outras (ABDI, 2010).

3 METODOLOGIA

Este trabalho caracteriza-se basicamente como uma pesquisa de campo, pois o objetivo principal foi avaliar a mudança ocorrida na gestão do Departamento Estadual da Criança e Adolescente (DECA), da Polícia Civil do Rio Grande do Sul, após a implantação da identificação biométrica para a identificação dos jovens infratores.

Collis e Hussey (2005), ao classificarem o tipo de pesquisa baseando-se em seu processo, ou seja, a maneira pela qual se coletam e analisam os dados, os estudos qualitativos envolvem o exame e a reflexão das percepções para obter um entendimento de atividades sociais e humanas. Ademais, não há a busca e a análise estatística de dados quantitativos. As pesquisas qualitativas referem-se ao significado, à definição, ao modelo que caracteriza alguma coisa, buscando, portanto, “o que” e não “o quanto”.

A técnica utilizada para a coleta de dados foi uma entrevista estruturada, conduzida por meio de roteiro, contendo oito perguntas abertas, na qual o entre-

vistado responde livremente a cada questão. A entrevista foi aplicada ao senhor Tiago Melo, chefe da seção de Perícias Externas no Departamento de Identificação do Instituto Geral de Perícias do Rio Grande do Sul (IGP-RS), que se reportou aos serviços desenvolvidos nas dependências do DECA, ao recepcionar adolescentes infratores, firmando um panorama da gestão tecnológica. As questões de 1 a 8 priorizaram mapear os processos da gestão, sendo elas:

- 1) Como é realizada a identificação do adolescente infrator quando apresentado após o cometimento de ato infracional?
- 2) Desde quando esse processo é utilizado?
- 3) Existem casos de identidade falsa, ausência de identidade ou utilização de identidade de outra pessoa quando apresentado à Autoridade Policial?
- 4) Como são solucionados os casos em que pessoa inocente é apontada como autora de um ato infracional?
- 5) Existe procedimento padrão para resolver os problemas desse tipo?
- 6) Quanto tempo é necessário para que o erro de registro seja corrigido?
- 7) Nos casos de reincidência do adolescente infrator, os delitos que foram registrados em nome de pessoas nas quais ele indicou foram transferidos para sua ficha de antecedentes?
- 8) Quais foram as melhorias após a implantação da Identificação Biométrica Digital?

4 RESULTADOS E DISCUSSÃO

As respostas obtidas na entrevista são apresentadas a seguir, enumeradas pela ordem do questionário.

- 1) Fazemos o cadastramento biométrico, tanto civil quanto criminal, do adolescente. Ele é encaminhado ao plantão da papiloscopia do IGP para cadastramento dos dados que foram fornecidos na acareação pela autoridade policial e que nos chegam por meio do ofício de solicitação. Esses dados, e outros, como tatuagens e medidas, são cadastrados em nosso Sistema de Identificação de Indivíduos. Posteriormente, é feita a fotografia criminal, coleta de assinatura e digitais no sistema. Após analisadas as impressões digitais pelo papiloscopista, é gerado o cadastro do indivíduo, não prejudicando ou alterando os dados de cadastro civil caso o indivíduo tenha e seja diverso do que foi fornecido, pois o cadastro criminal guarda os dados biográficos no protocolo criminal e apenas atualiza foto e digital.
- 2) Desde novembro de 2006.
- 3) Sim. Existem todos esses casos. Apesar de ser um sistema seguro, ainda é possível o estelionato. Com a entrada do novo sistema em 2006, o Sis-

- tema Automático de Comparação de Impressões Digitais (AFIS) reconhece as digitais dos indivíduos em cadastros posteriores a 2006 e que estejam tentando se identificar com outros dados. Há também a possibilidade da falsificação externa, na qual o documento foi falsificado sem ter sido encaminhado pelo Departamento de Identificação. Restando ainda dúvida, é encaminhado ao Departamento de Identificação. Restando ainda dúvida, é encaminhado ao Departamento de Criminalística, onde o perito fará análise.
- 4) Em um primeiro momento, o caso deve ser encaminhado ao Departamento de Identificação, para, com base nos registros, verificar se o documento foi realmente encaminhado por nós. Para tanto, é importante manter o documento original, pois caso não tenha sido feita no Departamento de Identificação, deve-se tratar como falsificação externa. O documento original em sua posse deverá ser remetido aos peritos do Departamento de Criminalística para análise. Quando são constatadas anormalidades no banco de dados, os cadastros são bloqueados para verificação, pois nessa hora só sabemos que há, por exemplo, duas pessoas diferentes com mesmo nome, mas não sabemos quem é vítima e quem é estelionatário. Será feita análise, e caso não se chegue a uma conclusão, será remetido para a Polícia Civil, para responder com base em investigações e diligências.
 - 5) Cada caso é um caso, e para cada um há um procedimento. Por exemplo: quando há dois RGs civis para mesmo indivíduo, com todos os dados biográficos iguais: unificação de cadastros. Quando há duas pessoas diferentes com o mesmo RG, é realizado o bloqueio de RG e seu encaminhamento à Polícia Civil para investigação. Quando há uma pessoa e dois RGs com dados biográficos diferentes, é realizado o bloqueio dos RGs e seu encaminhamento à Polícia Civil para investigação.
 - 6) Quando o registro no banco de dados é suficiente para identificarmos os dois indivíduos, a correção é feita rapidamente. No caso em que há cadastros para os dois indivíduos, em que um usa o RG do outro em uma identificação criminal, também é resolvido com rapidez. Casos mais complexos, que colocam em dúvida, são encaminhados à Polícia Civil e ela envia o inquérito à Justiça. O tempo de resposta é o tempo transcorrido entre a investigação policial e conclusão do juiz e pode levar semanas.
 - 7) Sempre que se faz a verificação do RG, transfere-se todos os antecedentes cometidos.
 - 8) O sistema biométrico tem ajudado muito, não substituindo, porém, o papiloscopista. Tem sido uma ferramenta muito útil de trabalho, não sendo mais possível trabalhar no sistema manual anterior. Fragmentos encontrados em local de crime e veículos recuperados de furto e roubo são submetidos ao sistema de reconhecimento e auxiliam o papiloscopista, sem a necessidade do envio de suspeitos, contribuindo, assim, para a prova da

autoria tão almejada pela autoridade policial. Para atingir a precisão necessária para identificar autores de atos infracionais, bem como diminuir a margem de erro quanto ao sujeito, verdadeiro autor do delito, fazia-se imprescindível a evolução tecnológica do sistema aplicado na década de 1990.

Além do questionário, foram coletadas via sistema informações referentes ao número de atendimentos realizados por ano. Essas informações foram obtidas no Departamento Estadual da Criança e do Adolescente, apresentando um panorama da quantidade de usuários beneficiados por esta tecnologia, conforme segue apresentado no Gráfico 4.1.

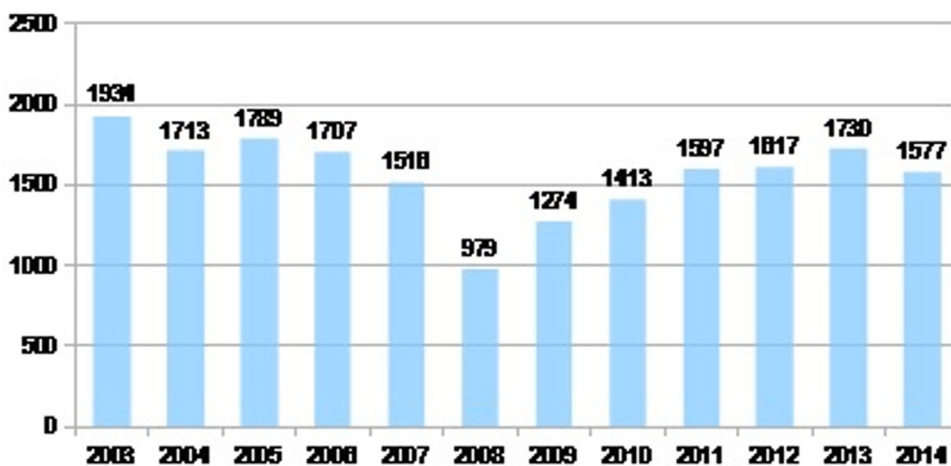


Gráfico 4.1 Atendimento realizados.

Fonte: DECA/RS.

A intensa demanda de adolescentes infratores apresentados ao plantão do DECA, já em 2005, alertou os gestores da instituição para a necessidade de implantar processos de aceleração no atendimento dos flagrantes. Como a forma de identificação era morosa e muitas vezes imprecisa (face às falsas informações fornecidas pelos autores de atos infracionais), devido às várias consultas necessárias ao banco de dados, na tentativa de identificar corretamente os apresentados, tornou-se premente um método que colaborasse com a modernização do processo empregado, acelerando a coleta de informações e, desta forma, melhorando a prática dos atos relacionados ao flagrante.

Assim, após as providências administrativas cabíveis e a concretização da parceria unindo os esforços do DECA e do IGP, nas dependências do próprio Departamento, em sala especialmente montada para a identificação, foi designado um perito permanente, que se utiliza do sistema AFIS ali instalado e, quando de-

mandado, procede aos atos identificatórios, confirmando a identificação daquele que já possui carteira de identidade ou já possui antecedentes policiais, ou promove a identificação daquele que não tem seu RG ou ainda não havia cometido atos infracionais.

4.1 Comparação dos processos: antes e depois da identificação biométrica

Conforme levantamento colhido a partir de testemunhos de funcionários da época, verificou-se que o processo anterior à identificação biométrica digital, além da incerteza quando às identidades dos adolescentes, passava, em caso de dúvida, por dois tipos de situações:

- 1) O adolescente seguia seu processo com o nome que informou, sem qualquer contestação em razão da ausência do nome fornecido no banco de dados, pois, em geral, não apresentava documento de identidade. Desta forma, era encaminhado às demais instâncias com identidade equivocada, até que a fraude fosse descoberta. Tal fato causava insegurança e custo adicional face à necessidade de correções posteriores.
- 2) O adolescente, ao informar nome fictício, era descoberto em sua falsidade e levado ao Instituto de Identificação (em prédio distante do DECA), que realizava, pelo método de digitais colhidas e impressas com tinta, a comparação dessas digitais com as fichas lá existentes, demonstrando o equívoco e, muitas vezes, a utilização, pelo adolescente, de nomes de pessoas alheias ao ato infracional cometido.

Este trajeto de ida e volta demandava em torno de duas a três horas a mais no fechamento do processo e encaminhamento aos demais segmentos de atendimento (Ministério Público e Juizado de Infância e Juventude). Com essa demora, todos os que faziam parte do flagrante (policiais militares, vítima, testemunhas etc.) ficavam aguardando a finalização dos atos policiais, gerando significativo tumulto, já que os envolvidos permaneciam no local até dispensa de sua presença, ou seja, tinham que aguardar o retorno do autor, que voltaria somente após a conclusão de sua identificação.

Porém, em 2006, após a implantação de sala específica do IGP e, por consequência, de perito utilizando o sistema AFIS de identificação biométrica digital, o trabalho sofreu grande facilitação, com significativa diminuição da demora na identificação dos adolescentes apresentados no plantão, modernizando e aperfeiçoando o processo identificatório, propiciando a certeza da autoria e expressiva melhora nos dados lançados no banco de dados, que teve um salto de qualidade na confiabilidade necessária para futuras consultas e para a realização de estatísticas mais precisas.

4.2 Implantação da identificação biométrica

O Sistema Automatizado de Identificação pela Impressão Digital (AFIS) permitiu que as análises das impressões digitais fossem melhoradas por meio de filtros de imagem e, após o perito delimitar a área útil do fragmento e confirmar quais minúcias serão utilizadas, o sistema cria uma matriz e realiza a busca no banco de dados. Em seguida, uma série de adolescentes são apresentados, cabendo ao papiloscopista verificar a coincidência.

Sistemas desse tipo são ferramentas de trabalho e auxiliam o profissional nas suas atividades de perícia com relação ao seu convencimento e tomada de decisões. A grande vantagem é o tempo reduzido necessário para pesquisa no banco de dados (DIAS; DE PAULA, 2013).

Tecnicamente, sistemas biométricos são vantajosos frente às tradicionais senhas em razão da maior segurança para confiar em características próprias do corpo humano, o que facilita a vida do usuário e dificulta tentativas de invasão. Na prática, um sistema biométrico analisa uma amostra de corpo do usuário. No caso do olho, ele analisa 265 pontos diferentes para formar uma imagem que será usada para comparação toda vez que o usuário tentar se autenticar. Caso apenas um ponto na íris do usuário à frente do sensor não bata com o molde guardado, o sistema biométrico barra sua entrada. O mesmo exemplo acontece com as outras tecnologias disponíveis no mercado, como reconhecimento de voz, geometria da palma da mão, leitura do rosto, posicionamento das veias dentro da mão e a tradicional impressão digital. Portanto, um sistema biométrico é, essencialmente, um sistema de reconhecimento de padrões, que busca extrair o padrão mais distintivo de uma pessoa, armazená-lo para depois comparar como novas amostras e determinar a identidade de cada amostra dentro de uma população (ABDI, 2010).

Assim, a partir da implantação de uma unidade do IGP, dentro do prédio do DECA, que identifica digitalmente o adolescente quando ele entra no plantão policial, extinguindo longos anos de inculpação de inocentes, eis que os nomes falsamente informados geravam antecedentes criminais a jovens primários, isto é, que não cometeram crime algum.

A autoridade policial, por interesse em ver tais distorções resolvidas, já que não havia obrigação formal, elaborava um levantamento dos vários nomes criados por cada adolescente infrator que assim agia, na tentativa de organizar um cadastro confiável.

Após o aperfeiçoamento do sistema, surgiu a identificação biométrica, por meio das impressões digitais. Em linhas gerais, esse sistema captura as impressões digitais de uma pessoa para posterior processamento, incluindo comparação entre as impressões obtidas e um banco de dados de impressões arquivadas (KASIENKO, 2003).

Esse sistema conferiu segurança às formas de reconhecer os adolescentes que já tiveram seus nomes inseridos no cadastro de atos infracionais, bem como aqueles que, pela primeira vez, apresentam-se ao banco de dados. Nos dias de hoje, o sistema está implantado na capital Porto Alegre. Entretanto, no interior, essa melhoria do processo ainda é inexistente.

5 CONSIDERAÇÕES FINAIS

Com base no histórico traçado pela autoridade entrevistada, foi possível detectar a importância da gestão tecnológica, atualmente representada pela precisão na identificação de adolescentes infratores, não ocorrendo mais os equívocos de registros, já que o jovem autor de delitos apresentava-se com o nome que lhe ocorria, muitas vezes utilizando-se de nomes de conhecidos, irmãos, primos ou o que a sua imaginação apontasse.

Com o advento e implantação da tecnologia embasada nas impressões digitais, denominada identificação biométrica, foi possível melhorar o processo de gestão, com alta precisão na identificação de adolescentes infratores, com a inserção dos dados em banco específico, ao qual é possível realizar consultas que aceleram os processos administrativos, demonstrando claramente a evolução do sistema.

O objetivo desse sistema era atestar a veracidade na relação indivíduo *versus* ação criminosa, garantindo o acerto na identificação, criando um banco de dados a ser compartilhado na rede de Delegacias Especializadas de Atendimento ao Adolescente Infrator (DPCAS) do Estado para assegurar a aplicação das medidas socioeducativas, sem correr o risco de erro nas identificações.

A implantação da identificação biométrica se tornaria uma ferramenta de gestão valiosa, vez que evitaria a imputação de crime a alguém que não fez parte do ato infracional.

É necessário, portanto, implantar a identificação digital em todo o interior e, ainda, que tais identidades sejam lançadas em banco de dados, proporcionando abrangência estadual, para que as delegacias possam compartilhar as mesmas informações, agilizando o processo de inserção de dados, tornando-se uma ferramenta de pesquisa confiável, em razão da eficiência da identificação biométrica.

REFERÊNCIAS

ABDI – AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL. *Sistemas Aplicados à Segurança Pública*. Brasília, DF, 2010.

ACESSO SEGURO. *Tipos de tecnologias biométricas*. Disponível em: <<http://www.acesseseguro.com.br/biometricas.asp>>. Acesso em: 22 dez. 2014.

BARROS, A. J. S. *Fundamentos de metodologia científica*. 3. ed. São Paulo: Pearson Prentice Hall, 2007.

- CAMPOS, J. B. **Como funcionam os sistemas de biometria: um estudo geral**. 23 abr. 2006. Disponível em: <<https://www.vivaolinux.com.br/artigo/Como-funcionam-os-sistemas-de-biometria-um-estudo-geral>>. Acesso em: 16 maio 2016.
- COLLIS, J.; HUSSEY, R. **Pesquisa: um guia prático para alunos de graduação e pós-graduação**. 2. ed. Porto Alegre: Bookman, 2005.
- DIAS, G. O.; DE PAULA, C. AFIS: uma ferramenta tecnológica sobre o crime. **Anais do 3º Congresso de Iniciação Científica do Centro Universitário do Distrito Federal**. UDF, 2013. Disponível em: <http://revista.udf.edu.br/index.php/congresso_ic/article/view/5/5>. Acesso em: 10 abr. 2016.
- GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.
- IENH – INSTITUIÇÃO EVANGÉLICA DE NOVO HAMBURGO. **Manual de normatização para trabalhos técnico-científicos**. Novo Hamburgo, 2012. Disponível em: <http://www.ienh.com.br/files/downloads/1331576650_51.pdf>. Acesso em: 16 maio 2016.
- KAMI, G. J. C. **Análise de técnicas de reconhecimento de padrões para a identificação biométrica de usuários em aplicações WEB utilizando faces a partir de vídeos**. Dissertação de mestrado – Ciência da Computação. Universidade Estadual Paulista Júlio de Mesquita Filho. São Paulo, 2011.
- KASIENKO, J. F. **Assinatura digital de documentos eletrônicos através da impressão digital**. Dissertação de mestrado – Ciência da Computação. Universidade Federal de Santa Catarina. Florianópolis, 2003.
- MONK, S. **Tecnologia da informação para gestão: em busca de um melhor desempenho estratégico e operacional**. 8.ed. São Paulo: Bookman, 2013.
- MUNIZ, D. Entenda o que é e como funciona a biometria. **Folha de S.Paulo**. 27 jan. 2007. Disponível em: <<http://www1.folha.uol.com.br/folha/informatica/ult124u21496.shtml>>. Acesso em: 8 nov. 2014.
- PATRÍCIA, K. **Impressões digitais têm importância biológica?** Disponível em: <<http://diariodebiologia.com/2011/11/impressoes-digitais-tem-importancia-biologica/>>. Acesso em: 5 dez. 2014.
- SANTIN, V. F. A participação do ministério público e do cidadão na política de segurança pública. **13º Congresso Nacional do Ministério Público**. Curitiba, 26-29 out. 1999. Disponível em: <http://www.apmp.com.br/juridico/santin/artigos/art_segpublica1.htm>. Acesso em: 16 dez. 2014.
- TEJADAS, S. S. **Juventude e ato infracional: as múltiplas determinações da reincidência**. Porto Alegre: EDIPUCRS, 2007.

5

CAPÍTULO

TECNOLOGIAS PARA PREVENÇÃO DE INCÊNDIOS: A TRAGÉDIA DA BOATE KISS

Eduardo Santos Acosta

Giovani Mendonça Lunardi

Solange Maria da Silva

1 INTRODUÇÃO

A tragédia da boate Kiss vitimou 242 pessoas e feriu, pelo menos, outras 680. O incêndio ocorreu na madrugada do dia 27 de janeiro de 2013 e teve início pelo acendimento de um artefato pirotécnico por um integrante de uma banda que se apresentava na casa noturna. Esta foi a segunda maior tragédia no Brasil em número de vítimas em um incêndio, sendo superado apenas pelo episódio do Grande Circo Norte-Americano, que ocorreu em 1961, em Niterói, no Rio de Janeiro, que vitimou 503 pessoas e teve características semelhantes às do incêndio ocorrido na Argentina, em 2004, na casa noturna República *Cromañón*. Rotula-se também como o quinto maior desastre da história do Brasil, o maior do Rio Grande do

Sul, o de maior número de mortos nos últimos 50 anos no Brasil e o terceiro maior desastre em casas noturnas no mundo.

Diante do exposto, este capítulo apresenta a investigação sobre a tragédia em si e, mais especificamente, se as tecnologias disponíveis para prevenção de incêndios poderiam tê-la impedido ou minimizado. Para isto, na seção 1, faz-se uma reconstituição da tragédia em todos os seus aspectos. Na seção 2, um exame das tecnologias disponíveis para prevenção de incêndios. E, por fim, um exame crítico com encaminhamentos.

2 ANTECEDENTES: A HISTÓRIA DE UMA TRAGÉDIA

Grande sucesso empresarial, com filas que dobravam a esquina da Rua dos Andradas, em Santa Maria (RS), a boate Kiss foi inaugurada no dia 31 de julho de 2009, fazendo com que os proprietários organizassem a entrada devido ao elevado número de pessoas, que passava 1.500 pagantes em cada evento.

Apesar da capacidade do local ser para 691, havia de 1.000 a 1.500 pessoas na noite do fato, segundo a perícia. A catástrofe vitimou 242 pessoas e feriu outras 680. Às 23 horas do dia 26 de janeiro de 2013, iniciava-se a festa “Agglomerados”, na boate Kiss. A festa foi idealizada e preparada por estudantes de seis cursos universitários e técnicos da Universidade Federal de Santa Maria (UFSM). Após análise, técnicos estimaram que havia no local entre 500 a 1.000 pessoas. A maioria dos estudantes era dos cursos de Pedagogia, Agronomia, Medicina Veterinária e Zootecnia (2)

Aproximadamente às 2h30 do dia 27 de janeiro, durante a apresentação da banda Gurizada Fandangueira, a segunda banda a se apresentar na noite, um sinalizador de uso interno proibido foi utilizado pelo vocalista da banda. O artefato soltou faíscas que atingiram o teto da boate, incendiando a espuma de isolamento acústico, que não tinha resistência ao fogo. Esse sinalizador, chamado *sputnik*, que era de uso rotineiro da banda. Segundo a Associação Brasileira de Pirotecnia (ABP), por desprender chamas e faíscas que alcançam até 4 metros de distância, seu uso é recomendado para ambientes externos, salientando que a altura do teto da boate era inferior aos 4 metros indicado. A ABP orienta ainda que, para o uso correto, esse sinalizador deve ser colocado no chão para ser aceso, uma vez que libera grande quantidade de fumaça, e os usuários devem ficar a pelo menos 10 metros do objeto. Seu uso é proibido em ambientes fechados e próximo a materiais inflamáveis, e seu custo fica em torno de R\$ 5,00. Sua venda não é fiscalizada (TERRA, 2013).

Não houve comunicação no início do incêndio entre os seguranças que estavam localizados no palco e os seguranças que estavam na saída da boate. Estes, inicialmente, não permitiram que os jovens saíssem pela única porta da boate, por

acreditarem tratar-se de uma briga. O pagamento do consumo na casa noturna dava-se a partir de comandas, que eram pagas na saída, fazendo com que os seguranças interpretassem que as pessoas estavam tentando sair sem pagar. Muitas vítimas tentaram sair pelas portas dos banheiros, pois, no tumulto, confundiram-se com portas de saída de emergência que, depois, foi constatado não existirem na casa noturna. Em decorrência disso, 90% das vítimas estariam nos banheiros. Na maioria das vezes, as pessoas automaticamente relacionam as mortes e as lesões às queimaduras pelo fogo quando o assunto é incêndio. Contudo, a principal *causa mortis* de indivíduos expostos a incêndios ocorre devido aos males causados pela inalação de fumaça. Em certas situações, cerca de 80% dos óbitos são por inalação de vapores e produtos químicos, principalmente monóxido de carbônico e cianeto. O grande vilão da história, apontado por laudos técnicos como a causa de 100% das mortes dos estudantes, junto com o monóxido de carbono, foi o cianeto, substância encontrada na natureza e que também é um produto da atividade humana, que foi liberado na queima do isolamento acústico (BARRUCHO, 2013).

O isolamento acústico era muito usual em toda a cidade, uma vez que inúmeras vezes os vizinhos de casas noturnas da cidade formalizaram reclamações nos órgãos competentes, relatando o barulho emitido por estas. A forma usada na maioria dos locais que emitiam som era isolar com uma espuma de colchão. Isso não era utilizado só para minimizar os efeitos do som, mas também era usada a pedido dos DJs e das bandas, porque aumentava a qualidade dos sons graves e agudos, a nitidez e ainda eliminava o eco. Contudo, foi novamente instalada para impedir o eco de som. Os órgãos de fiscalização não notaram a instalação dessa espuma inadequada. A fiscalização do município não era treinada para reconhecê-la e mesmo o Conselho Regional de Engenharia e Agronomia do Rio Grande do Sul só a constatou a partir de uma denúncia, que destacava a existência desse material. Quanto ao Corpo de Bombeiro, apenas vistoriavam as instalações inerentes ao combate ao incêndio, como iluminação e saídas de emergência e hidrantes, entre outros. Lixeiros encontravam enormes quantidades dessas espumas próximas às casas que a tinham instaladas. Segundo a imprensa, dois deles relataram ter coletado 50 sacos para vender às recicladoras. A Banda Gurizada Fandangueira mesclava ritmos sertanejos e música gaúcha e titulava-se como “inovadores de ritmos e na tecnologia”, como foi visto após a tragédia em sua página na rede social Facebook. Era usual pela banda a utilização de dispositivos pirotécnicos, apesar de garantir que acidente algum até então houvesse ocorrido. Raro era o mês que não houvesse show da banda na casa. Segundo informaram clientes rotineiros, a banda sempre utilizava artefatos como aquele que iniciou o incêndio.

A seguir, apresenta-se uma lista de erros e de omissões que foram apurados:

- Documento emitido pelos bombeiros foi usado como Plano de Prevenção e Combate a Incêndio (PPCI), em 26 de junho de 2009. Este documento era emitido de forma quase automática, uma vez que o sistema era eletrônico e simplesmente emitia um relatório do que deveria ser instalado, conforme informações dadas pelo próprio cliente. Não tinha *status* de alvará. Apesar das fragilidades do documento, o primeiro alvará de incêndio foi concedido pelo Corpo de Bombeiros, em agosto de 2009, com vigência de um ano. O alvará foi emitido após inspeção e verificação do local, conforme a planta anexada no plano. A casa iniciou suas atividades em 31 de julho de 2009, somente com o alvará de incêndio, mas sem o alvará de localização da prefeitura, emitido apenas em 2010. De agosto de 2010 a agosto de 2011, a Kiss ficou sem o alvará dos bombeiros, que só foi renovado em 9 de agosto de 2011. O alvará estava novamente vencido na data do fato.
- A empresa de engenharia responsável pelo PPCI disse ter elaborado o plano conforme uma planta-baixa, em 2009, mas não acompanhou a execução das obras.
- Em 1º de agosto de 2009, devido à falta do alvará de localização, a boate foi notificada para fechar as portas.
- Pelo menos quatro vezes, entre agosto e dezembro de 2009, em vez de ser fechada, a boate foi somente multada.
- Sem que o alvará fosse expedido e com a boate em funcionamento, as multas foram aplicadas sucessivamente.
- Em 1º de agosto de 2009 foi emitida a primeira notificação, por uma fiscal da prefeitura, mandando fechar as portas, nestes termos: “Cessar as atividades até a regularização junto ao município e apresentar alvará no prazo de cinco dias a contar da data da notificação”. Ignorando a notificação, a boate seguiu seu funcionamento, quando a mesma fiscal retornou em agosto, em 8 de setembro de 2009 e aplicou a primeira multa.
- Em 7 de outubro, com a casa ainda em funcionamento, sem alvará e sem interdição, aplicaram a segunda sanção. Houve nova fiscalização em 27 de novembro de 2009, gerando a terceira multa, uma vez que a casa permanecia em funcionamento. No dia 11 de dezembro de 2009, a boate sofre nova sanção, baseada no descumprimento das anteriores, mesmo assim a boate permaneceu aberta (WAGNER, 2013).
- Em 14 de abril de 2010, depois de oito meses de funcionamento, o alvará de localização foi finalmente expedido.

- Em 9 de abril de 2012, a fiscalização da prefeitura fez uma vistoria e descobriu que o alvará de incêndio estava prestes a vencer.
- Em 27 de janeiro de 2013 acontece o incêndio.
- A Polícia Civil efetuou a prisão dos sócios da casa e dois integrantes da banda Gurizada Fandangueira no dia 29 de janeiro, pela manhã. O juiz concedeu o pedido de prisão temporária ainda na madrugada. Na mesma tarde, além do outro sócio da casa se entregar, foi decretado o bloqueio dos bens dos proprietários.
- No mesmo dia, o delegado regional listou pelo menos quatro irregularidades pontuais na boate:
 - **saída única:** uma só porta e pouco espaçosa;
 - **sinizador em local fechado:** causou faíscas, que iniciaram o incêndio;
 - **excesso de pessoas:** 1.300 pessoas em local com capacidade para 691;
 - **material de revestimento inadequado.**
- Em 4 de fevereiro de 2013, o Conselho Regional de Engenharia e Agronomia (CREA) publicou um relatório oficial que apontou as causas da tragédia. O uso de um revestimento acústico inflamável exposto na zona do palco e a realização de um show com artefatos pirotécnicos em ambiente impróprio foram as duas principais causas. Devido à falta de extintores de incêndio, o fogo se propagou, e a falta de saídas de emergência, junto com a superlotação, aumentou consideravelmente o número de vítimas. O relatório também indicou que a casa não possuía um Plano de Prevenção Contra Incêndio (PPCI) e que os proprietários se aproveitaram da fragilidade do sistema informatizado dos bombeiros para obterem alvarás sem estarem em acordo com a legislação. Luiz Carlos Filho, coordenador da comissão do CREA-RS, falou ao Jornal Zero Hora, que o brasileiro se sentia seguro demais por causa das medidas contra incêndios tomadas na década de 1970, quando houve muitos sinistros desse tipo no país.

3 CONCLUSÃO DO INQUÉRITO

Com os depoimentos finais das vítimas que sobreviveram à tragédia e com a montagem de uma maquete 3D da boate, feita por peritos de Brasília, o inquérito policial entrou em sua última semana com mais de 2 mil páginas e com a oitiva de 240 pessoas. A Polícia Civil havia recebido os celulares das vítimas para perícia e 33 pessoas seguiam internadas na capital e em Santa Maria.

A situação real da casa noturna quanto ao alvará de localização foi conhecida no dia 21 de fevereiro. A Kiss iniciou suas atividades sem o alvará e, por isso, foi multada seis vezes pelo município. Quatro meses depois de abrir, em julho de

2009, o empreendimento foi embargado, porém a medida durou apenas cinco dias. Apenas em 14 de abril de 2010 foi expedido o alvará, contudo, com multas que passavam de R\$ 15 mil. O Ministério Público, em 26 de fevereiro, indiciou quatro pessoas: dois sócios da boate, o produtor do grupo e um membro da banda Gurizada Fandangueira, que estavam presos provisoriamente. Os crimes foram transformados em homicídio qualificado, por causa das mortes por asfixia, com penas de 12 a 30 anos. Após o término do inquérito a denúncia seria apresentada.

O laudo do Instituto Geral de Perícias havia concluído que o gás cianeto foi realmente a causa da morte das vítimas na Kiss. A partir daquela data, o Ministério Público teria 10 dias para denunciar ao Poder Judiciário. Feita a denúncia pelo MP, os indiciados formalmente se tornariam acusados e, uma vez recebido o processo pelo Judiciário, eles se tornariam réus. Eram 13 mil páginas, 52 volumes e mais de 800 depoimentos. Por homicídio com dolo eventual qualificado, foram nove pessoas indiciadas (G1, 2013).

4 TECNOLOGIAS PARA PREVENÇÃO DE INCÊNDIOS

Vamos examinar a seguir as tecnologias para prevenção de incêndios que poderiam ter minimizado ou impedido os acontecimentos registrados na boate Kiss. Inicialmente, descreveremos algumas tecnologias e, em seguida, vamos nos deter na investigação do sistema Integrado de Gestão da Prevenção de Incêndio (SIGPI), software desenvolvido para desburocratizar e agilizar o processo administrativo da prevenção de incêndio.

4.1 Tecnologias preventivas: *sprinkler*

A instalação do sistema de *sprinklers* consiste basicamente em uma rede de bicos, adequadamente distribuídos e interligados por tubulações aéreas e conexões. A rede deve ser fixada como suportes em quantidade suficiente, conforme determinação das normas pertinentes. O objetivo de *sprinkler* é extinguir um incêndio de maneira rápida e automática logo no princípio, antes que o fogo se propague e provoque danos mais relevantes.

O sistema de *sprinklers* automáticos atua na extinção do fogo na área, pela pronta e contínua descarga de água diretamente sobre o material em combustão. Eles são projetados na rede com espaçamentos regulamentados para cada tipo de risco a ser protegido. Cada instalação, com um determinado número de *sprinklers*, é controlada por uma válvula de governo e alarme. Os componentes básicos dos bicos de *sprinklers* são: orifício de entrada, ampola (elemento sensor) e o defletor. O elemento sensível dos *sprinklers* é a ampola de vidro transparente, caracterizada pela sua resistência e rigidez. Essa ampola e seu conteúdo são de na-

tureza permanente e invariável, e não sofrem alteração com a passagem do tempo ou condições atmosféricas. A ampola de vidro é hermeticamente fechada e selada, e contém um líquido altamente expansível e sensível ao calor, capaz de exercer uma força de rompimento elevada. No caso de a temperatura se elevar acima de um limite predeterminado, a pressão criada pela expansão do líquido rompe a ampola, dando passagem à água que se espalha ao chocar-se contra o defletor, sendo espargida em forma de chuva sobre o foco de incêndio. Existem, ainda, os modelos de *sprinklers* no qual o elemento sensor é constituído de um elo fusível metálico, em substituição à ampola de vidro. A principal vantagem desse sistema sobre os demais é a redução ao mínimo dos danos causados pelo fogo e também pela água. É importante observar que os *sprinklers* somente funcionarão sobre o local do incêndio, empregando, assim, apenas a quantidade de água estritamente necessária (ROCHA, 2013).

4.2 Sistema de exaustão de fumaça

Após um grande incêndio ter destruído completamente a fábrica da General Motors, em Michigan, nos Estados Unidos, iniciou-se o controle de fumaça, em 1965, gerando um prejuízo superior a US\$ 55 milhões. Com isso, sua filial na Inglaterra resolveu inovar e adotou pela primeira vez o conceito. Em terras tupiniquins, não é compulsório, no entanto, a instalação de mecanismos de expulsão da fumaça em PPCIs, com exceção das escadas enclausuradas.

Em declaração, o presidente do CREA-RS apontou os gargalos da legislação gaúcha. A legislação estadual é claramente omissa quanto às exigências de sistemas de controle de fumaça nos ambientes de reunião de público, quer seja pela aplicação de materiais de revestimento com características de pouca geração de fumaça, quer seja por sistemas naturais ou forçados de exaustão. O grande número de mortos por asfixia na tragédia santa-mariense destacou a importância e a necessidade de soluções de controle de fumaça nas estratégias de segurança contra incêndio das edificações. O sistema de exaustão de fumaça consiste basicamente em prover meios pelos quais o calor e a fumaça possam ser retirados da edificação, impedindo que se espalhem pelos demais ambientes. Esse sistema possibilita ainda a ventilação do ambiente e permite a visualização da rota de fuga, quando corretamente instalada e integrada, reduzindo significativamente à temperatura interna (ROCHA, 2013).

4.3 Detectores de fumaça, térmicos e acionadores manuais

Esse sistema tem a finalidade de detectar imediatamente o princípio de incêndio, por meio de detectores de fumaça e/ou detectores térmicos ou, ainda, por

acionadores manuais, distribuídos de acordo com a norma NBR 17.240. Esses detectores de fumaça e térmicos de incêndio devem ser localizados em intervalos regulares, capazes de detectar a área afetada sem a intervenção humana, e são interligados a uma central de alarme por meio de um sistema de fiação, permitindo o controle do sistema e a identificação da área em sinistro.

Os dispositivos de atuação manual (acionadores manuais) são incorporados ao sistema, permitindo a operação manual quando o princípio de incêndio é percebido antes da atuação automática. Esses acionadores são distribuídos na área a ser protegida segundo recomendação da norma brasileira ABNT NBR 17.240. Para avisar as pessoas sobre a necessidade de desocupação da área, no caso da ocorrência de incêndio, o sistema possui dispositivos de sinalização que podem ser do tipo sonoro (sirene), visual (*flash*) ou combinado (sinalizador audiovisual). Esses sinalizadores devem ser distribuídos da mesma forma que os demais.

Em ambos os casos, a central de alarme deverá possuir uma fonte de alimentação de emergência constituída por baterias, destinada a manter o funcionamento do sistema na falta de energia elétrica normal (ROCHA, 2013).

4.4 Sistema de gestão integrado da prevenção de incêndios

Após a tragédia ocorrida em Santa Maria na madrugada de 27 de janeiro de 2013, no que diz respeito à legislação de Prevenção e Proteção contra Incêndio, quase nada foi alterado. Apesar de toda a pressão feita por familiares, vítimas e pela imprensa, que condenou o software utilizado mesmo sem entender mais a fundo seu funcionamento, passados mais de dois anos desde o acidente na boate Kiss, as regras continuam praticamente as mesmas. São muitas as leis de prevenção e de combate a incêndio, umas contradizendo as outras; partes dessas normas já estão ultrapassadas, mesmo com as “novas” normas de 2014. Sem falarmos da ausência de legislações específicas para sistemas de prevenção contra incêndios mais atuais.

A legislação atual já nos proporciona uma boa base para analisarmos, com um nível razoavelmente bom, os planos de prevenção de incêndio. Contudo, deparamo-nos com outros grandes problemas, como a falta de bombeiros qualificados para trabalhar nas Assessorias de Análises Técnicas (AATs) e nas Seções de Prevenção de Incêndios (SPIs). A falta de efetivo do Corpo de Bombeiros do Rio Grande do Sul é histórica; devido a isso, inspeções são realizadas por militares com conhecimento reduzido na área de prevenção, uma vez que são combatentes do fogo, gerando assim inspeções muitas vezes imprecisas. Outro fator importante é que atualmente a nossa legislação está sendo alterada praticamente todos os meses. Isso torna necessária a atualização constante dos militares, e como esses

bombeiros não estão diariamente discutindo e vendo essas alterações, fica potencialmente aumentado o risco de erros nas vistorias. Além da situação descrita, temos ainda o fato de os arquitetos e os engenheiros que confeccionam os PPCIs, na maioria das vezes, não dominarem o conhecimento específico sobre as leis de prevenção de incêndio.

4.4.1 Mudança no processo de análise de projetos de prevenção de incêndios

O Sistema Integrado de Gestão da Prevenção de Incêndio (SIGPI) é um software concebido e desenvolvido para desburocratizar e agilizar o processo administrativo da prevenção de incêndio. Trata-se de uma ferramenta múltipla de Tecnologia da Informação (TI), que permite a padronização nos procedimentos, das normas legais e técnicas, autocorreção, atualização de dados em tempo real e memória. Com o SIGPI, tornou-se possível mensurar a evolução e a produtividade da atividade prevencionista, além de obter informações estatísticas, geoespaciais, históricas e técnicas das edificações.

Com o surgimento de nova atribuição legal para o Corpo de Bombeiros da Brigada Militar, no Rio Grande do Sul, por meio da Lei nº 10.987,¹ de 11 de agosto de 1997, iniciou-se grande mudança cultural interna na corporação, com reflexos significativos no público externo, pois se passou ao atendimento de balcão. Essa lei obriga o Corpo de Bombeiros a fiscalizar os sistemas de segurança contra incêndio nos prédios, conforme seu Art. 1º. Todos os prédios com instalações comerciais, industriais, de diversões públicas e edifícios residenciais com mais de uma economia e mais de um pavimento deverão possuir plano de prevenção e proteção contra incêndio, aprovado pelo Corpo de Bombeiros da brigada militar do Rio Grande do Sul. O novo sistema legal exige mais preparo profissional por parte dos bombeiros e também provoca mudança cultural dentro da própria instituição pública. A população brasileira é bastante crítica em relação ao serviço público prestado nos mais diferentes órgãos. É público e notório que alguns possuem atendimento de baixa qualidade, e os motivos para tal são os mais variados possíveis. Por outro lado, encontramos excelentes procedimentos, inspirados na iniciativa privada, no qual a prioridade é o cliente. O Corpo de Bombeiros, após identificar suas principais deficiências no atendimento ao público, precisavam mudar o enfoque de seu serviço, sem perder o foco. Assim, o esforço principal da corporação passou a ser o cumprimento da lei, mas não somente isso. Era preciso

1 A Lei nº 10.987, de 11 de agosto de 1997, estabelece normas sobre sistemas de prevenção e proteção contra incêndios, dispõe sobre a destinação da taxa de serviços especiais não emergenciais do corpo de bombeiros e da outras providências.

levar em consideração o novo serviço a ser prestado e tratar o cidadão envolvido no processo como “cliente”. Todos os procedimentos na busca da legalidade e cumprimento de normas não podem ser abandonados, pois são estes que garantem as atividades preventivas e exigem que o serviço técnico dos bombeiros seja aperfeiçoado. Com isso, busca-se envolver na doutrina ou em suas diretrizes mais atenção ao cidadão, pois é ele quem arca com os tributos públicos. Este é o grande desafio: a mudança de enfoque ou sua aplicação.

4.4.2 Sistema de análise de PPCI anterior ao SIGPI (projeto de prevenção)

No processo convencional praticado, verificou-se que o Corpo de Bombeiros em relação ao cumprimento da lei somente emite o parecer após o cidadão dar entrada com o PPCI, propondo o sistema de segurança a ser instalado no seu prédio. Esses sistemas são identificados por meio de desenhos e plantas e inúmeros documentos complementares (memoriais). Dessa forma, identifica-se que a administração pública desempenha uma sistemática de prestação de serviço de reação, mas somente age após o cidadão ter encaminhado os documentos na seção pertinente. Esse é o momento de muitos conflitos existentes no processo de análise ou exame da documentação, isso por se tratar de interpretação de lei e normas que são carregadas de subjetividades e intensa presença da personalidade na aprovação do PPCI. Outro fato não menos importante é a morosidade no processo de análise, pois são muitos os prédios a serem fiscalizados, em termos de documentação. Para se ter uma ideia, somente em Caxias do Sul (RS), são quase 30 mil, o que levaria o Corpo de Bombeiros a analisar aproximadamente 1.330 processos por mês. Esse fato é praticamente impossível, pois, à medida que forem necessárias correções nos processos, estes serão devolvidos ao cidadão, corrigido pelo mesmo, e reapresentados. Um fato que não pode ser desprezado é que aproximadamente 20% dos projetos apresentados no Corpo de Bombeiros são devolvidos para correções mais de duas vezes.

4.4.3 Mudança de processo de análise de PPCI

O SIGPI surgiu da necessidade de aumentar a agilidade dos processos relativos à Prevenção de Incêndios e Pânico, relacionados a Legislação Estadual (Lei nº 10.987/97), e os Decretos nº 37.380/97 e nº 38.273/98. Esse sistema possibilita o controle e a visão de todos os passos relativos à implementação e à execução dos sistemas de prevenção de incêndio, desde a notificação de adequação até a concessão do alvará, gerando gráficos e mapas estatísticos, e que também serve de suporte para a operacionalidade, principalmente para as guarnições de serviço a partir das informações indispensáveis sobre a edificação ante o atendimento de incêndios.

Atualmente, o SIGPI abrange a todos os municípios do interior do Estado do Rio Grande do Sul. Esse projeto-piloto teve início em fevereiro de 2006, quando o 5º Comando Regional de Bombeiros (CRB), com sede em Caxias do Sul, identificou um problema da execução da prevenção de incêndio, conforme previsto em lei. Havia uma demanda reprimida de processos, ao ponto de comprometer as atribuições do Corpo de Bombeiros, com análise de projetos (plantas, memoriais e demais informações relativas à segurança contra incêndio do prédio). Diante disso, iniciou-se a busca pela solução desse problema. Após exaustivas discussões e longo período de estudos, chegou-se à conclusão de que a solução passaria pela mudança de PPCI, deixando o processo manual para a adoção da informatização (RS, 1997).

4.4.4 Como funciona o novo processo de aprovação de PPCI

Foi criado um software que responde e define quais são as exigências específicas para cada prédio, de acordo com as suas variáveis (altura, ocupação, área de maior pavimento etc.). O cidadão vai até o setor competente do Corpo de Bombeiros e fornece as informações necessárias ao preenchimento do formulário, que é realizado pelo atendente da corporação. Para isso, foram extraídos das Normas Técnicas citadas pela Legislação Estadual – registrem-se as Normas da Associação Brasileira de Normas Técnicas (ABNT) e Normas Regulamentadoras do Ministério do Trabalho –, aqueles dispositivos de real interesse para a execução da missão do Corpo de Bombeiros. Com isso, todo o tempo de análise de projeto de prevenção foi reduzido para cinco minutos em média. É somente o tempo de preenchimento do requerimento e de informações ou variáveis do prédio. A seguir, o cidadão recebe o emolumento a ser recolhido na rede bancária e o apresenta no Corpo de Bombeiros para retirada do documento oficial e determinativo chamado Certificado de Conformidade.

De posse desse documento, o cidadão está em condições de implementar a sua execução, ficando a seu critério a quem recorrer para tal. Normalmente, o cidadão contrata a pessoa ou empresa que projetará sua obra e esta deve inserir no projeto as especificações constantes no Certificado de Conformidade expedido pelo Corpo de Bombeiros. É importante salientar que toda a responsabilidade que a corporação tinha no momento da análise das plantas se transferirá para o momento da vistoria final dos sistemas instalados no prédio. Ocorre que, para os bombeiros, interessa muito mais que os prédios nasçam com os sistemas de segurança contra incêndios, instalados sem perda de tempo com trâmites burocráticos antes de suas construções. Sem dúvida poderão ocorrer problemas de execução de sistemas preventivos, necessitando correções, porém, é preferível essa situação a ver o cidadão deixar de procurar o bombeiro pela burocracia que enfrentará ou

pela morosidade na prestação do serviço. Importante salientar a grande mudança interna das instituições nessa área pela nova preparação técnica, que deverá ser implementada tendo como público-alvo seus vistoriadores. Estes deverão ser possuidores de elevado conhecimento técnico, pois, muitas vezes, terão que saber medir se o sistema preventivo existente é eficiente e eficaz, porque não basta somente estar instalado no local, mas é preciso verificar se seu funcionamento atende às necessidades de sua colocação.

4.4.5 Sistema de Gestão Integrado da Prevenção de Incêndios

Há de se salientar que, provavelmente, todas as corporações dos bombeiros do Brasil possuam seu sistema de Gestão da Prevenção de Incêndios, seja informatizada, seja com fichários e pastas. O que se está apresentando é um sistema de gestão via web, pois pode ser apresentado pelo gestor ou cliente a partir de qualquer máquina que tenha acesso à internet. A grande mudança e quebra de paradigma foi à alteração no processo de análise dos PPCI, abolindo-se as plantas para a obtenção da aprovação junto ao Corpo de Bombeiros. Porém, não se abre mão de nenhum detalhe necessário ao atendimento das normas em rigor, que é detidamente conferido após a execução dos sistemas previamente determinados. Muitos questionamentos foram impostos, mas o principal é: “Depois de pronto o prédio, quem deixou de construir uma escada de emergência não poderá corrigir esse erro?”. Pois bem, não se viu, na prática, esse fato nesses quase dez anos de implantação do sistema e processo. Entendemos que quem está predisposto a descumprir a lei, independentemente da forma com que foi notificado para fazê-lo, se por meio de planta aprovada nos bombeiros ou se a partir de certidão emitida pelo mesmo órgão. Para ilustrar, seguem tópicos com as principais características na mudança de processo de análise com o advento SIGPI:

- instituição do SIGPI como ferramenta básica e primordial para a Prevenção de Incêndio;
- migração de todas as informações técnicas, administrativas e operacionais relativas à prevenção e combate a incêndio para o SIGPI, transformando-o em ferramenta multifuncional;
- manutenção de equipes de trabalho para permanente melhoria do sistema, com o incremento na área de ensino aos vistoriantes;
- manter-se aberto a novas ideias, contando com a participação de todos (público interno e externo) para melhoria da ferramenta e gestão;
- manutenção dos níveis de acesso por servidor e aprimoramento da segurança interna e externa;

- organização do setor técnico de Prevenção de Incêndio em chefia, secretaria, protocolo e inspeção, porém em um sistema integrado que permita o inter-relacionamento administrativo e operacional, tanto dos setores, como dos servidores;
- constante aprimoramento do treinamento do efetivo por meio de instruções cotidianas em nível local, regional e estadual; e
- foco no cliente (sociedade).

5 CONSIDERAÇÕES FINAIS

O presente trabalho apresenta a pesquisa sobre tecnologias, tendo como fato histórico uma das maiores tragédias do Brasil. Pelo exposto, fica claro que não se tratou de um erro isolado, independentemente de quem o cometeu, mas sim de um grande número de erros ou desatenções que, somadas, transformou a vida de famílias e até de uma cidade inteira.

Como apontado no estudo, vimos que além do número e da largura das portas de saídas, a superlotação, a ausência de vários sistemas de prevenção e as atitudes heróicas dos frequentadores que já estavam em zona segura, contribuíram consideravelmente para o inacreditável número de mortos na boate Kiss. O CREA, juntamente com o Corpo de Bombeiros, analisou a tragédia de forma sistemática e concluíram que 100% das vidas poderiam ter sido salvas se a casa tivesse atendido a todas as solicitações dos órgãos competentes. Dos sistemas mencionados, o de exaustão de fumaça seria, naquela situação, o mais importante. Porém, ainda hoje ele não é exigido pelas normas nacionais. Há uma grande pressão do Corpo de Bombeiro e do CREA para essa exigência, que hoje esbarra em barreiras políticas. Não menos importante, os demais sistemas auxiliariam no aviso de incêndio. Os detectores de fumaça ou de temperatura, ao serem acionados, emitiriam um sinal sonoro ou alarme, dependendo da configuração. Com esse aviso, que ocorreria na fase de princípio de incêndio, as pessoas poderiam ser evacuadas com calma, com o auxílio de funcionários previamente treinados com o PPCI. Caso os detectores automáticos ainda não tivessem sido acionados, os acionadores manuais poderiam ser ativados pela primeira pessoa que visualizasse o incêndio, assim como também anunciado o início do incêndio, potencializando as chances de os jovens saírem em segurança. Quanto ao sistema de *sprinklers*, além de possivelmente apagar o incêndio, ele ainda teria a grande valia de inibir a convecção, que consiste na ascensão do ar quente, enquanto o ar frio tende a descer. Isso torna muito mais lento o deslocamento da fumaça, graças à diminuição da temperatura da edificação proporcionada pela água esguichada pelo sistema.

A sinalização, que era precária na casa, também teve sua parcela de culpa. Como falado anteriormente, os banheiros estavam lotados de corpos, um sob os

outros, pois uma luminária que sinalizava os banheiros foi, no meio da fumaça e do desespero, confundida com a placa de saída. Além da confusão, foi posteriormente verificado que não havia na Kiss a indicação de rota de fuga em caso de pânico. A mídia, não só local como mundial, como sempre, fez seu papel de polemizar, apontar culpado e induzir o Poder Público a adotar medidas emergenciais como forma de solucionar e prevenir novos acontecimentos. Não obstante os meios de comunicação, a Polícia Civil, por meio de seu delegado, que aproveitou seu momento de fama, prometeu em praça pública de Santa Maria fazer justiça, com um megafone, no meio da primeira manifestação dos familiares e amigos – mesmo sendo de conhecimento popular que a Polícia Civil, e principalmente o delegado, não faz justiça e, sim, aponta indícios de autoria e prova de materialidade. Com esse intuito, o delegado apontou 28 pessoas inicialmente. O Ministério Público, após solicitar novas diligências e analisar de forma menos espetacular, deixou de denunciar grande parte dessas pessoas, principalmente os bombeiros, que inicialmente, no entendimento do delegado, deveriam responder por homicídio qualificado, por não impedir os populares de ajudar a retirar os feridos. Com esse clamor público, o Legislativo tinha que tomar alguma atitude, pois até para ele a imprensa atribuiu a culpa, por deixar defasar as leis, mesmo que estas não tenham sido o problema. A Lei Complementar nº 14.376, de 26 de dezembro 2013, que entrou em vigor na data de sua publicação, veio como resposta imediata para tragédia, porém, foi feita às pressas e sem consultar operadores da área. Com toda a pressa, a nova legislação apresentou inúmeras falhas em suas “inovações”, obrigando a criação da Lei nº 14.555, de 2 de julho de 2014. Ainda assim, não supriu todas as lacunas, uma vez que prevenção de incêndio virou preocupação primordial dos órgãos públicos e das sociedades de classe, principalmente do CREA, que também sofreu represália em um primeiro momento. Finalmente, em 10 de setembro de 2014, entrou em vigor o Decreto nº 51.803, para regulamentar as leis anteriormente citadas. Mas ele não é definitivo, pois não sana todos os problemas que vão aparecendo conforme o uso pelos operadores de prevenção de incêndio. Será um fato que jamais será esquecido, de inegável importância social, pública e familiar, e um marco na história, como nos casos dos edifícios Joelma e Andraus, em São Paulo, que alterou legislação e as tecnologias na prevenção de incêndio da época.

Todos esperam o final desta história, uns buscando absolvição, outros justiça, mas o que sabemos, além das vidas perdidas e das famílias desfeitas, é que esta novela está muito longe do final.

REFERÊNCIAS

- ANTONELLO, L. Dois bombeiros são condenados e seis são absolvidos por envolvimento na tragédia da boate Kiss. **Diário de Santa Maria**. Santa Maria, jun. 2015. Disponível em: <<http://diariodesantamaria.clicrbs.com.br/rs/geral-policial/noticia/2015/06/dois-bombeiros-sao-condenados-e-seis-sao-absolvidos-por-envolvimento-na-tragedia-da-boate-kiss-4774124.html>>. Acesso em: 10 abr. 2015.
- BARRUCHO, L. G. Punição a responsáveis por tragédia deve demorar anos, dizem advogados. **BBC Brasil**. São Paulo, jan. 2013. Disponível em: <http://www.bbc.com/portuguese/celular/noticias/2013/01/130130_justica_punicao_culpados_tragedia_lgb.shtml>. Acesso em: 10 abr. 2015.
- G1. **Bombeiro indiciado por fogo na Kiss divulga carta aberta à população**. Porto Alegre, mar. 2013. Disponível em: <<http://g1.globo.com/rs/rio-grande-do-sul/noticia/2013/03/bombeiro-indiciado-por-fogo-na-kiss-divulga-carta-aberta-populacao-leia.html>>. Acesso em: 10 abr. 2015.
- LOPES, G. H. Incêndio na Boate Kiss em Santa Maria foi premeditado? **E-Farsas.com**. jan. 2013. Disponível em: <<http://www.e-farsas.com/incendio-na-boate-kiss-em-santa-maria-foi-premeditado.html>>. Acesso em: 10 abr. 2015.
- RIO GRANDE DO SUL. **Lei nº 10.987**, de 11 de agosto de 1997. Estabelece normas sobre sistemas de prevenção e proteção contra incêndios.
- ROCHA, A. P. Fumaça sob controle. **Revista Técnica**. São Paulo, abr. 2013. ed.193. Disponível em: <<http://techne.pini.com.br/engenharia-civil/193/fumaca-sob-controle-adequadamente-dimensionados-sistemas-de-exaustao-natural-287001-1.aspx>>. Acesso em: 10 abr. 2015.
- TERRA. **Fotos mostram que uso de artefatos pirotécnicos na boate era comum**. São Paulo, jan. 2013. Disponível em: <<http://noticias.terra.com.br/brasil/cidades/tragedia-em-santa-maria/fotos-mostram-que-uso-de-artefatos-pirotecnicos-na-boate-era-comum,81a9e6013eb8c310VgnVCM5000009cceb0aRCRD.html>>. Acesso em: 10 abr. 2015.
- TREZZI, H. Desespero de familiares marca reconhecimento de corpos de vítimas da tragédia em Santa Maria. **ZH Notícias**. Porto Alegre, jan. 2013. Disponível em: <<http://zh.clicrbs.com.br/rs/noticias/noticia/2013/01/despero-de-familiares-marca-reconhecimento-de-corpos-de-vitimas-da-tragedia-em-santa-maria-4024472.html>>. Acesso em: 10 abr. 2015.
- WAGNER, C. Boate Kiss funcionou seis meses sem alvará em Santa Maria. **ZH Notícias**. Porto Alegre, fev. 2013. Disponível em: <<http://zh.clicrbs.com.br/rs/noticias/noticia/2013/02/boate-kiss-funcionou-seis-meses-sem-alvara-em-santa-maria-4051624.html>>. Acesso em: 10 abr. 2015.

6

CAPÍTULO

APLICATIVOS PARA DISPOSITIVOS MÓVEIS APLICADOS À SEGURANÇA PÚBLICA

Lorielcio da Silva Peres

Roderval Marcelino

Vilson Gruber

João Bosco da Mota Alves

1 INTRODUÇÃO

A informação é um dos recursos mais importantes para a tomada de decisão. A grande questão é: como adquirir informação? A tecnologia é atualmente utilizada para os mais diversos objetivos, entre eles a busca e organização da informação. Somente ter informação não basta; é necessário que ela seja divulgada, comunicada às partes interessadas, para que seja útil em tomadas de decisão,

que nos dias de hoje requerem rapidez e eficiência. Para isso, faz-se necessário ter sempre disponíveis mecanismos de obtenção, processamento e divulgação de informações ABDI (2010).

As Tecnologias de Informação e Comunicação (TIC) reúnem todo esse arcabouço de requisitos para prover a comunidade com informações para as tomadas de decisões necessárias ao crescimento e ao desenvolvimento do que chamamos hoje de Sociedade da Informação. “A introdução das TIC em todas as áreas de atividades, de geradora de externalidades positivas, passou nos anos recentes a constituir o cerne do que se vem chamando de Sociedade da Informação” (ABDI, 2010, p. 13).

Foi com o objetivo de gerar e organizar informação que aconteceu, em 2010, a Oficina de Trabalho “Visão de Futuro e Agenda TIC: 2008–2025”, iniciativa da Agência Brasileira de Desenvolvimento Industrial (ABDI) em conjunto com o Centro de Gestão e Estudos Estratégicos (CGEE). O trabalho foi desenvolvido por um grupo de especialistas em aplicações mobilizadoras.

Aplicações mobilizadoras referem-se à oferta de produtos e serviços de informação e comunicação que considerem estratégias globais no acesso e uso de tecnologias de informação e comunicação (TICs) e que demandem desenvolvimentos de novas tecnologias, equipamentos, metodologias, modelos de negócio, em um esforço articulado por parte das instituições acadêmicas, de governo e empresas (ABDI, 2010, p. 12).

Este trabalho tem o objetivo contribuir com os estudos relativos à aplicações mobilizadoras desenvolvidas a partir das TIC aplicadas à segurança pública nacional, visando gerar informações que poderão ser utilizadas em aplicações e que demandem mais estudos, aperfeiçoamento, investimentos e estratégias de uso e gerenciamento.

Existe um conjunto de processos que podem ser melhorados a partir de novas aplicações e tecnologias como:

- Atendimento e interação com o cidadão, envolvendo todos os canais de comunicação e troca de informações diretamente com a sociedade, seja para registro de ocorrências, difusão de informações ou prestação de serviços ao cidadão.
- Sistemas de tratamento de ocorrências, envolvendo todos os trâmites desde os registros do incidente até a finalização de processos judiciais.
- Tratamento de informações relativas à identificação civil e criminal, incluídas aí todas as formas de coleta, armazenamento e processamento de dados de identificação.
- Tratamento de informações coletadas por serviços de inteligência e integração dos sistemas de informação das diversas organizações policiais.

- Acompanhamento e avaliação dos procedimentos realizados pelos órgãos de segurança. (ABDI, 2010 p. 56)

Foi baseando neste conjunto de processos que este trabalho se orientou para buscar mais informações relacionadas às aplicações tecnológicas para a segurança pública.

No desenvolvimento de software, atualmente está acontecendo uma revolução nos termos do que entendemos por computação móvel, os smartphones como o iPhone e outros que utilizam o sistema operacional Android redefiniram o que entendemos por computação móvel.

Uma aplicação móvel pode ter milhões de descarregamentos em pouco tempo e esse mercado potencial gerou uma nova forma de distribuição e entrega de software a partir das lojas virtuais de *apps* (aplicativos), que reduzem significativamente os custos de distribuição e de comercialização. “Os mercados para aplicativos móveis criaram um mecanismo totalmente novo para a distribuição de conteúdo, estimulando investimentos consideráveis no desenvolvimento de software para dispositivos móveis” (UNESCO, 2014, p. 23).

Diante da realidade atual, em relação às aplicações móveis, optou-se por limitar a investigação a tecnologias disponíveis para dispositivos móveis do tipo smartphones e tablets.

2 DESENVOLVIMENTO

As aplicações mobilizadoras referem-se à oferta de produtos e serviços de informação e comunicação, relacionando com estratégias para acesso e uso que demandem desenvolvimentos de novas tecnologias, equipamentos e metodologias. A ideia para este trabalho se consolidou com a perspectiva de pesquisar uma tecnologia bastante atual, que é a utilização de dispositivos móveis como smartphones e tablets a partir de aplicativos (softwares) desenvolvidos para atender a objetivos específicos. Os objetivos norteadores deste trabalho foram identificar o cenário nacional deste conjunto de tecnologia, equipamentos e metodologia e sua capacidade em gerar informação que podem ser úteis à segurança pública e obter mais conhecimentos quanto aos aplicativos e aos dispositivos móveis e suas destinações junto à sociedade.

Segundo a ABDI (2010), existe um conjunto de processos que podem ser melhorados a partir de novas aplicações e tecnologias, e está relacionado ao atendimento e à interação com o cidadão, envolvendo todos os canais de comunicação e troca de informações diretamente com a sociedade, seja para registro de ocorrências, difusão de informações ou prestação de serviços. Paralelo à questão

das aplicações mobilizadoras, a pesquisa exploratória apontou para um novo cenário em termos de desenvolvimento de software, no qual, atualmente, está acontecendo uma revolução em termos do que se pode entender por computação móvel. Por meio de tablets e smartphones, uma aplicação móvel pode ter milhões de descarregamentos em pouco tempo e esse mercado potencial gerou uma nova forma de distribuição e entrega de software por meio das lojas virtuais de *apps*. Esse formato de distribuição reduz significativamente os custos de distribuição e comercialização, o que aponta para uma nova metodologia tanto no sentido de busca de ferramentas, quanto na própria utilização. O mercado também abre um novo leque de tecnologia a ser investido pelos órgãos públicos e pelo governo federal por meio de pesquisa e de desenvolvimento.

A ABDI e o CGEE selecionaram como ponto de partida para a construção da visão de futuro sete aplicações, considerando os objetivos dos cinco subprogramas do Programa Mobilizador em TIC, da Política de Desenvolvimento Produtivo, e pelo menos três destes subprogramas que estão relacionados ao que foi pesquisado neste trabalho, que são: software e serviços de TI, infraestrutura para inclusão digital e adensamento da cadeia produtiva. Entre as sete aplicações encontram-se os sistemas aplicados à segurança pública, ou seja, no cenário nacional de aplicativos móveis foi possível identificar aplicativos que correspondem aos objetivos dos subprogramas.

A rotina de trabalho relacionada à segurança pública é bastante dinâmica e precisa de agilidade. Uma tecnologia que disponha de mobilidade com certeza trará facilidades e praticidade para o dia a dia. A mobilidade ou computação móvel refere-se basicamente à capacidade de um dispositivo poder ser movimentado fisicamente enquanto ele está em uso. Aplicativos móveis são softwares específicos para dispositivos móveis como tablets e smartphones; alguns aplicativos vêm instalados nos dispositivos e outros podem ser adquiridos nas lojas de aplicativos na internet como, *App Store*, *Google Play* ou *Windows Phone Store*. Os aplicativos pesquisados e ofertados pelo governo estão disponíveis nestas lojas e, em sua maioria, disponíveis para pelos menos dois sistemas operacionais: Android e IOS.

A pesquisa procurou se embasar em aplicativos ofertados pelo Governo Federal para traçar um cenário nacional. O governo criou um guia de aplicativos, um catálogo de aplicativos para dispositivos móveis desenvolvidos por órgãos do Poder Executivo federal. Esse guia é um portal centralizador no qual o cidadão pode obter informações e conhecer os aplicativos que o governo oferece. Todos os aplicativos disponibilizados são gratuitos e de responsabilidade de órgãos de governo. Para acessar a relação, basta acessar o link: <<http://www.aplicativos.gov.br/>>, no qual é possível fazer uma busca por órgãos, conhecer e acessar links para download. Este portal é fácil de localizar a partir de uma busca no Google ou outro sistema de busca, e a forma de apresentação dos aplicativos também é

simples e objetiva. No portal, os aplicativos podem ser agrupados a partir dos destaques, por categoria, por órgão ou pela plataforma.

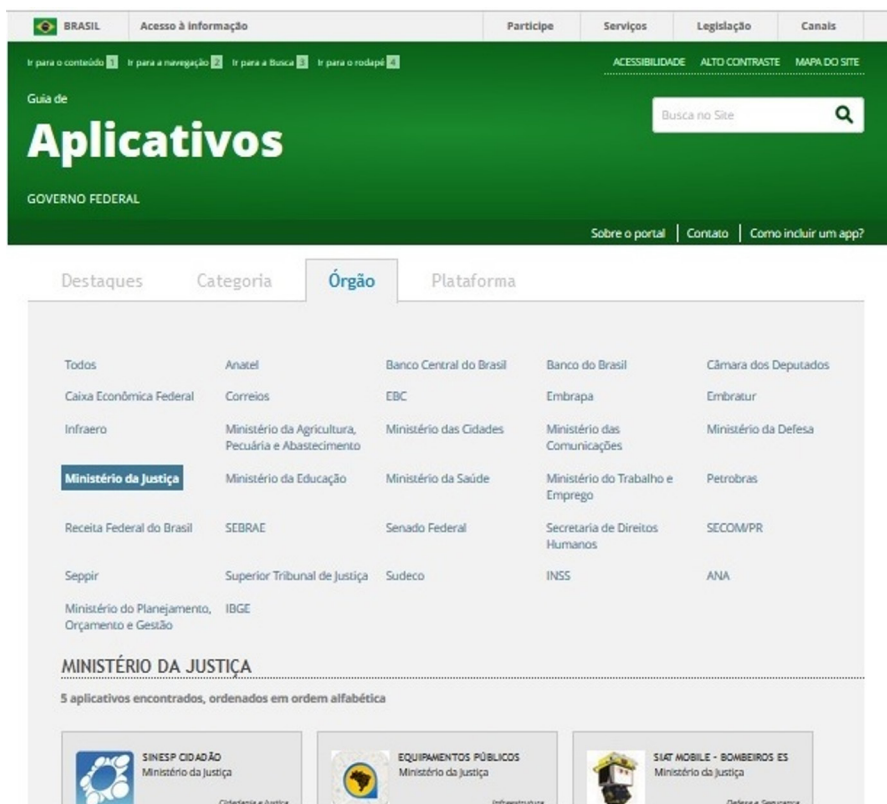


Figura 6.1 Guia de aplicativos do Governo Federal – agrupamento por órgão.

Fonte: <http://www.aplicativos.gov.br/orgaos?filtro=Orgao&valor=123f54b21bf066a578a889e932d9ef11>.

As considerações a seguir, relacionadas aos aplicativos, buscam, além de pontuar questões observadas nesses aplicativos, apresentar alguns aplicativos similares ofertados ao mercado por outros órgãos públicos e até por algumas iniciativas privadas. Complementando o cenário nacional ofertado pelo governo, o estudo visa orientar escopos de novas pesquisas, mais direcionadas à análise de conteúdo, e recursos para procurar aperfeiçoar os aplicativos já existentes e direcionar a pesquisa e desenvolvimento de novos aplicativos.

O aplicativo do Ministério da Justiça (Sinesp Cidadão), por exemplo, tem uma série de outros aplicativos que se assemelham. Foi possível identificar, por meio da pesquisa, que uma das funções do aplicativo do Governo Federal é auxiliar o cidadão na consulta a veículos a partir da placa e tem vários similares desenvolvidos pelos Departamentos Estaduais de Trânsito (Detran), como:

Aplicativo Detran.SP

Aplicativo utilizado para consultar informações sobre seu próprio veículo ou de terceiros, e para consulta de informações de Carteira Nacional de Habilitação (CNH). É oferecido pela Companhia de Processamento de Dados do Estado de São Paulo (Prodesp). Disponível em: <<https://play.google.com/store/apps/details?id=br.gov.sp.detran.consultas>>.

Com o novo aplicativo do Detran.SP para tablets e smartphones, ficou ainda mais fácil verificar a pontuação de sua CNH e possíveis multas registradas em seu veículo. Para ter acesso às consultas, basta utilizar a mesma senha do portal do Detran.SP.

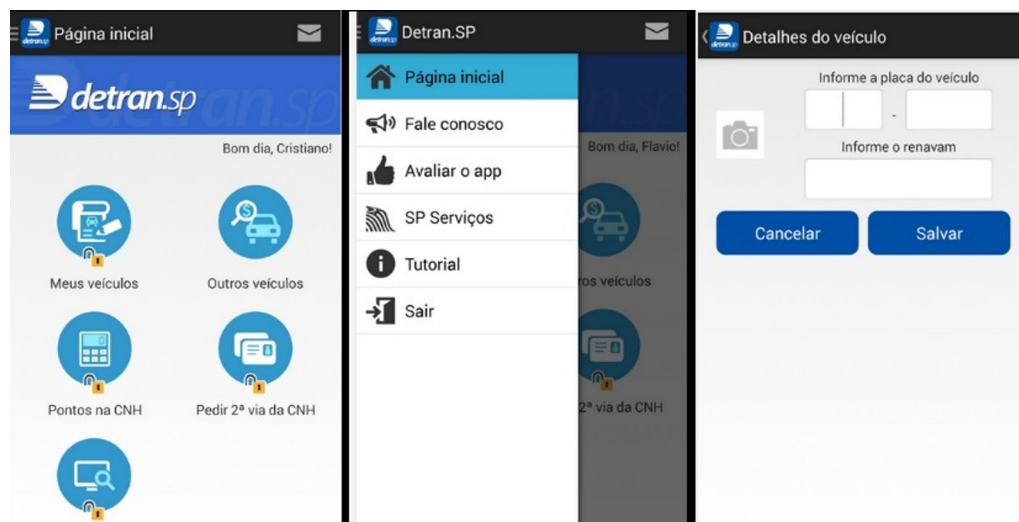


Figura 6.2 Aplicativo Detran.SP.

Fonte: <https://play.google.com/store/apps/details?id=br.gov.sp.detran.consultas>.

Aplicativo Detran CE Mobile

Aplicativo utilizado para consultar a situação de veículos a partir da placa e/ou RENAVAM, entre outros. É oferecido por Detran Ceará. Disponível em: <<https://play.google.com/store/apps/details?id=br.gov.ce.detran.mobile>>.

Este é o mais novo aplicativo do DETRAN Ceará. Com ele, os usuários de smartphones e tablets obtêm acesso rápido e amigável a:

- Informações da Carteira Nacional de Habilitação (pontuação, vencimento e renovação).
- Consulta de veículos pela placa e/ou Renavam.

- Geração de código de barras para pagamento de taxas via internet Banking.
- Informações sobre transporte rodoviário intermunicipal de passageiros (ônibus e vans)
- Envio de críticas, reclamações e denúncias diretamente para a ouvidoria do órgão [...].



Figura 6.3 Aplicativo Detran CE.

Fonte: <https://play.google.com/store/apps/details?id=br.gov.ce.detran.mobile>.

Analisando os aplicativos dos órgãos estaduais e comparando com o aplicativo do governo, foi possível levantar algumas considerações importantes, iniciando pela questão de existirem vários aplicativos diferentes, mas basicamente com a mesma destinação de uso para cada estado. A primeira consideração a ser feita é em relação aos custos de pesquisa e desenvolvimento despendidos por todos os órgãos estaduais. Nesta mesma linha de raciocínio, segue a questão da informação, que é descentralizada e limitada por estado, ou seja, cada aplicativo estadual consulta bases de dados diferentes dos veículos do seu estado, como Detran e Prodesp, enquanto o aplicativo do governo consulta uma base nacional do Departamento Nacional de Trânsito (Denatran).

Outra observação que cabe é em relação às funcionalidades acessórias, ou seja, o que um aplicativo do governo oferece em relação ao que cada aplicativo estadual oferece. No aplicativo do governo (Sinesp Cidadão), é possível, além da consulta de veículos, consultar desaparecidos e mandados de prisão. Nos aplicativos do Detran dos estados, além da consulta de veículos, comum a todos, outras destinações são apresentadas, como consultar informações sobre seu próprio veículo, sobre CNH e pontuação, solicitar segunda via de CNH, informações sobre transporte, geração de código de barras para pagamento de taxas, entre outros.

É importante ponderar a respeito de como o resultado da consulta é apresentada: alguns aplicativos apresentam os dados de forma bem sintética, enquanto outros o fazem com um nível de detalhamento mais aprofundado, o que oferece mais subsídios e informações tanto para o trabalho dos agentes de segurança pública como para a utilização do cidadão civil.

Com isso, é possível afirmar que não existe um padrão de informação, e que se houvesse uma interação entre o governo e os estados seria possível otimizar tanto a questão de investimentos em pesquisa e desenvolvimento, quanto outras questões relacionadas às fontes de informações, formas de apresentação e destinações de uso dos aplicativos.

Outro aplicativo do governo ao qual também cabe a mesma linha de considerações é o STJ – Consulta Processual, que é um aplicativo oficial do Superior Tribunal de Justiça (STJ) e permite acesso à consulta processual. Com funcionalidades e destinação de uso muito semelhantes a este aplicativo, existem vários outros aplicativos gratuitos ofertados por empresas privadas, destinados à consulta processual para vários estados. Em relação aos órgãos públicos, o Tribunal de Justiça do Estado do Pará lançou, por meio da Secretaria de Informática, o TJPA – Mobile .

Aplicativo TJPA – MóBILE

Aplicativo utilizado para consulta processual e acompanhamento de processos. É oferecido por Tribunal de Justiça do Estado do Pará. Disponível em: <<https://play.google.com/store/apps/details?id=br.jus.tjpa.androidlawsuit>>.

Realizar a Justiça buscando a excelência jurisdicional, contribuindo com o efetivo fortalecimento do Estado democrático de Direito.

- Consulta processual;
- consulta por número do processo;
- leitura por código de barras;
- consulta por nome da parte;
- consulta por número da OAB;
- informações gerais, partes envolvidas, movimentações, custas, audiências, documentos [...].

Como é possível observar, a destinação e as funcionalidades são muito semelhantes ao aplicativo do Governo Federal. Neste caso, o que se pode ponderar é a respeito do padrão na apresentação das informações, dos recursos que podem ser incorporados a um ou a outro e, ainda, da base de pesquisa e desenvolvimento

que pode servir como base para outros órgãos públicos investirem na tecnologia e metodologia de aplicações móveis.

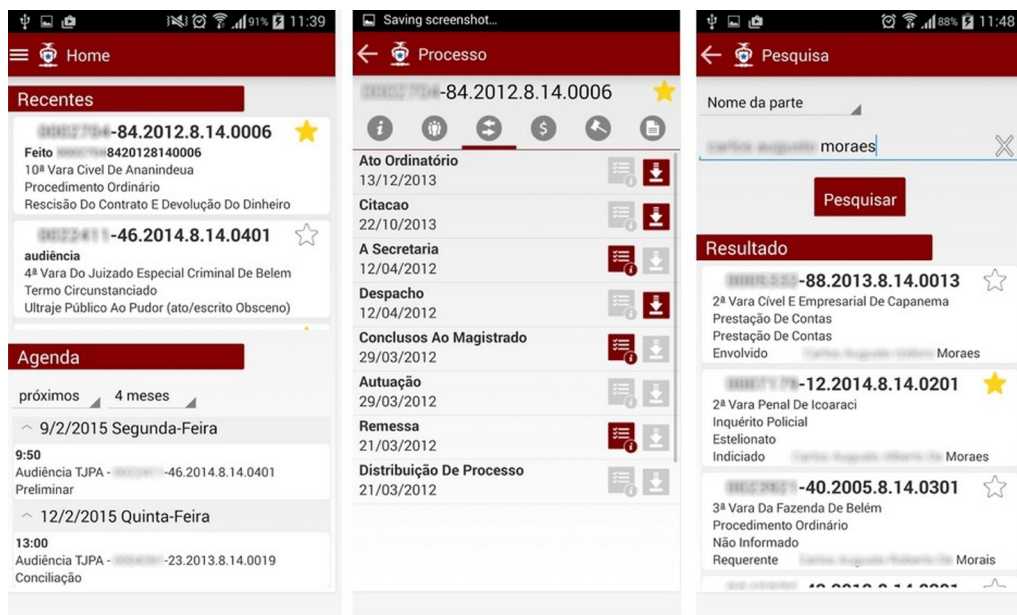


Figura 6.4 Aplicativo TJPA – Mobile.

Fonte: <https://play.google.com/store/apps/details?id=br.jus.tjpa.androidlawsuit>.

3 CONSIDERAÇÕES FINAIS

Muitas considerações importantes podem ser apontadas em relação à pesquisa. Uma delas é o quanto às pequenas empresas e iniciativas de profissionais independentes aparecem com várias diversificações de aplicativos, com destinações muito semelhantes aos pesquisados, sendo ofertados, na maioria das vezes, gratuitamente nas lojas de aplicativos. Uma pesquisa que poderia ser feita é em relação às possíveis parcerias destes com os órgãos públicos para o desenvolvimento de aplicativos oficiais.

Outra característica importante nos aplicativos apresentados nesta pesquisa está relacionada à plataforma em que o *app* foi desenvolvido. A maioria dos aplicativos está disponível para os sistemas operacionais Android, utilizado por várias marcas de smartphones e tablets, baseado no núcleo Linux e atualmente desenvolvido pela Google; e IOS, da Apple. Também foi possível observar que, em relação aos sistemas operacionais, ainda não existe um padrão definitivo estabelecido, mesmo que maioria deles sendo desenvolvida para IOS e Android, alguns funcionam melhor em uma plataforma do que outra e as atualizações algumas vezes passam a ser geradas em apenas uma das plataformas.

Como considerações finais, pode-se afirmar, pelo que foi encontrado nas pesquisas, que os dispositivos móveis e seus aplicativos vieram para ficar e estão compondo um novo cenário em termos de computação móvel, que a segurança pública já está inserida neste contexto, ainda que de forma embrionária, e que existe um campo bastante amplo para outras pesquisas, que possibilitam aprofundar o desenvolvimento de aplicações mobilizadas das TIC para os sistemas de segurança pública.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL – ABDI. **Cadernos Temáticos – Tecnologias de Informação e Comunicação – TIC: Sistemas Aplicados a Segurança Pública**. Brasília: Abdi, 2010.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

_____. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. (Tradução de Maria Luiza X. A. Borges; revisão técnica de Paulo Vaz). Rio de Janeiro: Jorge Zahar, 2003.

EVANS, D. **A internet das coisas: como a próxima evolução da internet está mudando tudo**. 2011. Disponível em: <http://www.cisco.com/web/BR/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf>. Acesso em: 29 maio 2015.

FURTADO, V. **Tecnologia e gestão da informação na segurança pública**. Rio de Janeiro: Garamond, 2003.

RICHARDSON, R. J. **Pesquisa social: métodos e técnicas**. 3.ed. São Paulo: Atlas, 1999.

TORRES, C. E. **Mobilidade: computação móvel, dispositivos e aplicativos**. 2013. Disponível em: <<http://pt.slideshare.net/cetorres/palestra-mobilidade-computao-mvel-dispositivos-e-aplicativos-2013>>. Acesso em: 14 maio 2015.

UNESCO. **O futuro da aprendizagem móvel: implicações para planejadores e gestores de políticas**. Brasília: Unesco, 2014. 64 p. ISBN: 978-85-7652-188-4.

7

CAPÍTULO

UM MODELO DE DADOS VOLTADO AO SERVIÇO DE INTELIGÊNCIA POLICIAL

Herbson de Carvalho

Alexandre Leopoldo Gonçalves

1 INTRODUÇÃO

Segundo o Dicionário Michaelis, o vocábulo inteligência, do latim *intelligentia*, significa a faculdade de entender, pensar, raciocinar e interpretar; entendimento, intelecto; o que se pode entender também por habilidade para escolher os métodos e obter um bom resultado. Neste trabalho, o foco reside na atenção à inteligência policial, que é atividade realizada pelo Estado por meio de suas instituições policiais. As instituições tradicionalmente responsáveis por realizarem as atividades de inteligência são conhecidas como Serviços de Inteligência e definidas por Cepik (2003, p. 13) como: “[...] agências governamentais responsáveis pela coleta, pela análise e pela disseminação de informações consideradas relevantes para o processo de tomada de decisões e implementação de políticas públicas nas

áreas de política externa, defesa nacional e provimento de ordem pública”.

De acordo com Martins (2011), inteligência, no contexto policial, é entendida como uma atividade proativa, caracterizada pela busca de informações, com a finalidade de possibilitar ao gestor público um supedâneo mínimo para seu poder decisório. Com base em informações contextualizadas, o destinatário final da atividade de inteligência poderá propor e comandar ações concretas em termos de segurança pública.

No Brasil, as instituições policiais, sejam elas civis, militares ou federais, possuem em suas estruturas serviços de inteligência responsáveis pela coordenação e realização das atividades afins. Segundo Pacheco (2005), o serviço de inteligência policial pode ser subdividido em três áreas: análise, contra-inteligência e operações.

As instituições que atuam em segurança pública, em especial as polícias militares, possuem, entre seus departamentos, Agências de Inteligência (AI) que integram do Sistema Brasileiro de Inteligência (Sisbin). Os órgãos de inteligência possuem como atividade o exercício de ações especializadas para identificação, acompanhamento e avaliação de ameaças reais ou potenciais na esfera da segurança pública. Atuam ainda na obtenção, produção e salvaguarda de dados, informações e conhecimentos que subsidiem ações da Polícia Militar para neutralizar, coibir e reprimir atos criminosos de qualquer natureza.

Um dos principais desafios para as pessoas e para as organizações é saber detectar e gerenciar a informação de maneira eficaz, conforme citado por Lira et al. (2008), pois a busca e coleta de dados para a produção de conhecimento gera uma grande quantidade de dados e informações. O enorme volume de dados acaba, muitas vezes, por dificultar a produção de um conhecimento, ao passo que exige que cada analista tenha que rever e confrontar diversos dados de diversas fontes diferentes.

Para tentar organizar e armazenar esses dados, faz-se necessário o uso de sistemas que possam tornar a grande quantidade de dados existentes em informação. Adiciona-se ainda a necessidade de aprimorar determinado contexto por meio da transformação de informações em conhecimento. Sistemas são importantes para auxiliarem os gestores na tomada de decisão. No caso da inteligência policial, a utilização de sistemas informatizados são uma ferramenta para essencial para o analista.

O ponto de partida para este trabalho considera que cada AI adota sua maneira de armazenar dados sobre potenciais alvos de investigação. Esses alvos podem ser indivíduos, veículos ou locais. Em muitos casos, são confeccionados Relatórios de Inteligência em formato de texto e repassados por meio de mensagens eletrônicas, sendo arquivados em computadores. O principal desencontro de informações é que cada AI arquiva seus documentos de uma forma. Pode-se

dizer que cada agência busca maneiras individuais de organizar melhor seus dados e informações. Esse problema é recorrente em diversos órgãos de inteligência. Gabrielli (2007), em seu trabalho sobre os núcleos de inteligência da Polícia Rodoviária Federal de Santa Catarina, destaca que, apesar da grande quantidade de atribuições dos núcleos, eles não possuem sistemas que realmente possam auxiliar em suas atividades.

Adiciona-se a isso o fato de que parte da informação sobre um indivíduo está, no máximo, apenas na memória do agente que participou de determinada operação. Muitas vezes, um agente coletou dados e informações acerca da mesma pessoa em diferentes momentos e isto poderia auxiliar na identificação de ações criminosas, mas é desconhecido por outros agentes que possuem o mesmo alvo. Em muitos casos, não há sequer um banco de dados que reúna informações sobre esses indivíduos, como locais que frequenta, pessoas com quem se relaciona, veículos que utiliza e outros dados. O mais comum é a existência de banco de dados dispersos, que armazenam somente ocorrências policiais incompletas.

Neste sentido, existe uma lacuna nos órgãos de inteligência, ou seja, a inexistência de um banco de dados sobre informações adquiridas pelos agentes. Um banco de dados com tais características poderia armazenar esses dados e informações, compartilhando com as demais agências, que teriam acesso ao conhecimento já produzido por um conjunto de agentes de inteligência. Isso resultaria, claramente, em uma redução de trabalho e em mais qualidade nos relatórios produzidos, auxiliando no processo de tomada de decisões com maior precisão.

Neste sentido, este trabalho tem por objetivo propor um modelo de dados capaz de promover subsídios à tomada de decisão no contexto da inteligência policial, bem como demonstrar o potencial por meio de exemplos de sua utilização.

2 MODELO PROPOSTO

O presente trabalho propõe um modelo de dados, sendo este uma representação de determinada realidade, domínio ou contexto. Pretende-se, a partir da proposta, apresentar os principais elementos para suportar a captura e o armazenamento de dados no contexto da inteligência policial.

Inicia-se pela modelagem, ou seja, pelo processo de representar o mundo observado real ou imaginário (COUGO, 1997) considerando um conjunto de requisitos. Em seguida, tais requisitos devem ser apresentados em uma linguagem que permita analisar mais facilmente os componentes do domínio, bem como os relacionamentos entre os mesmos. Para tal, a modelagem conceitual caracteriza-se como um ferramental capaz de transcrever as necessidades em um diagrama com o intuito de deixar claro o que se deseja com o modelo de dados.

A modelagem conceitual concentra-se em um nível de abstração e deve ser usada para envolver o usuário final, pois o objetivo é discutir os aspectos do banco de dados e não da tecnologia. Os exemplos de modelagem de dados vistos ao nível do modelo conceitual são mais fáceis de compreender, já que não há limitações ou aplicação de tecnologia específica.

Segundo Heuser (2009), o modelo conceitual captura as necessidades da organização em termos de armazenamento de dados independentemente de implementação. A modelagem conceitual é o primeiro estágio para um projeto de banco de dados que visa suportar sistemas capazes de gerir os dados e, a partir destes, fornecer informações que possam ser utilizadas na tomada de decisão. Após a modelagem conceitual, tornam-se necessárias as modelagens lógica e física, estando estas mais voltadas ao próprio banco de dados.

Existem muito modelos ou tipos de bancos de dados. Entre os mais utilizados atualmente encontra-se o modelo relacional. Um banco de dados relacional é um mecanismo de armazenamento que permite a persistência de dados e, opcionalmente, a implementação de funcionalidades. O que caracteriza o modelo relacional é a maneira como os dados são armazenados e organizados no banco de dados. No contexto deste trabalho, o foco está voltado aos Sistemas de Gerenciamento de Banco de Dados Relacional (SGBDR – do inglês *Relational Database Management System* [RDBMS]), que se apresentam ou são percebidos pelo usuário na forma de tabelas (GRAD, 2012; CAMPBELL-KELLY, 2012).

2.1 Modelagem conceitual

Pensando na criação de um banco de dados voltado ao uso na inteligência policial, a primeira entidade a ser criada é a **Informacao**. Esta entidade contém um atributo identificador (atributo identificado por uma bolinha azul), além dos campos de texto **Descricao**, no qual será descrito o dado/informação que se deseja armazenar. O campo **DataFato** é responsável por armazenar a data em que ocorreu o descrito na informação. Existem ainda os campos **TipoInformacao** e **DataCadastro**, que armazenaram, respectivamente, o tipo de informação e a data do cadastro.

Outras quatro entidades são necessárias para completar a entidade **Informacao**, sendo elas: **Veiculo**, **Individuo**, **Geo** e **Ocorrencia**. A entidade **Veiculo** é responsável por armazenar os dados referentes a veículos, como **Placa**, **MarcaModelo**, **Ano**, **Cor** e **Chassi**. O atributo identificador é determinado por meio do atributo **IdVeiculo**.

A entidade **Individuo** armazena dados sobre pessoas, tendo como atributo identificador **IdIndividuo**. Já a entidade **Geo** é responsável por armazenar dados sobre locais como endereços e coordenadas geográficas, tendo como atributo identificador **IdGeo**. A entidade **Ocorrencia** armazenará todos os tipos de ocor-

rências policiais existentes. A Figura 7.1 apresenta o modelo conceitual proposto neste trabalho.

A entidade **Informacao** poderá ter mais de um indivíduo e mais de um veículo relacionado, bem como, pode estar associado a mais de um local e mais de um tipo de ocorrência. Também pode existir um relacionamento com outra tupla cadastrada anteriormente. Isto ocorre através do conceito de auto-relacionamento, representado no modelo por um losango anexo a própria entidade **Informacao**.

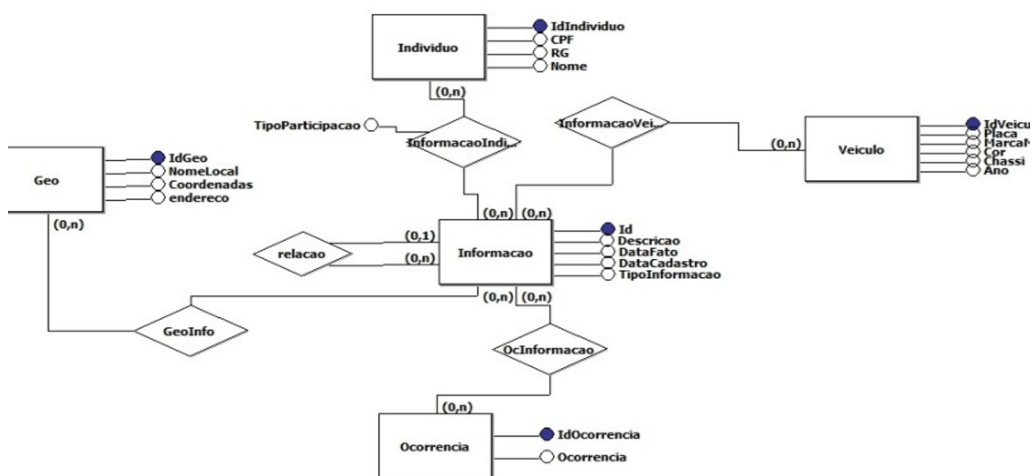


Figura 7.1 Modelo conceitual proposto.

3 UTILIZAÇÃO DO MODELO

O cenário proposto para a avaliação do modelo é baseado nos órgãos de inteligência da Brigada Militar (BM) do Estado do Rio Grande do Sul. Para dimensionar o tamanho real que o modelo proposto de banco de dados poderia trabalhar, utiliza-se o número de ocorrência do ano de 2014, com base nas informações fornecidas pela Secretária de Segurança Pública do Estado do Rio Grande do Sul (SSP/RS). Conforme dados estatísticos da SSP em atendimento à Lei nº 11.343/99 e à Lei nº 12.954/08, em 2014, a BM/RS realizou 759.715 atendimentos de crimes consumados e 20.458 tentativas de crimes (RS, 2014).

Neste estudo, foram incluídos alguns dados para possibilitar a simulação da utilização do banco de dados. Sendo assim, foram cadastrados 1.425 relatórios de inteligência, 21 indivíduos, sete veículos e 519 locais de ocorrências.

Esses dados foram utilizados como forma de permitir a utilização de uma aplicação que possibilitasse, a partir de consultas, demonstrar a viabilidade do modelo proposto. A quantidade de dados, conforme mencionado, foram cadas-

trados com base no número médio de ocorrências de um período de três meses em apenas uma cidade de pequeno porte.

3.1 Exemplos de consultas e discussões

A partir do modelo proposto é possível realizar diversas consultas. Com a finalidade de facilitar a demonstração dos resultados que podem ser obtidos, foi desenvolvida uma aplicação em Linguagem PHP® (PHP: *Hypertext Preprocessor*). A seguir, serão demonstrados e discutidos alguns resultados obtidos a partir do modelo proposto e povoado conforme descrito anteriormente.

Entre as possíveis resultados, cita-se a possibilidade de relacionar todas as informações de determinado indivíduo, apresentando também quais outras pessoas foram citadas conjuntamente. Demonstra ainda os veículos e os locais identificados com um indivíduo em questão (Figura 7.2).

Indivíduo

Nome	Mario [redacted] Junior
Alcunha	Mario
RG:	1 [redacted]
CPF:	

Relatório onde é citado:

Relatório	Fato	Participação	Data
Registro Policial nº 1.366/2015	Fato em tese Atípico,	Só comunicante	26/04/2015 14:30:00
Registro Policial nº 1.364/2015	Exercício arbitrário da própria razão,	Acusado	26/04/2015 12:00:00
Registro Policial nº 1.406/2015	Injúria,	Vítima	14/10/2014 18:30:00
Registro Policial nº 1.402/2015	Desobediência,	Acusado	14/10/2014 18:30:00
Registro Policial nº 1.373/2015	Outros Crimes,	Acusado	11/08/2009 15:00:00
Registro Policial nº 1.394/2015	Lesão Corporal Culposa Art.303,	Autor	18/11/2008 14:00:00
Registro Policial nº 1.356/2015	Retenção de veículo,	Acusado	03/05/2007 16:00:00
Registro Policial nº 1.378/2015	Perda de Documento,	Só comunican:e	01/12/1999 00:01:00
Registro Policial nº 1.365/2015	Dirigir s/habilitação Art.309,	Só comunican:e	09/09/1999 12:45:00
Registro Policial nº 1.411/2015	Dirigir s/habilitação Art.309,	Adolescente infrator	07/04/1998 22:00:00

Pessoas que foram citadas junto com este indivíduo:

Pessoa	RG	Quantidade
Roberto [redacted] (Beto)	RG: 1 [redacted]	2x
Fabiano C [redacted] (Camelo)	RG: 1 [redacted]	1x

Locais onde foi citado:

Local	Endereço	Quantidade
-------	----------	------------

Veículos com os quais foi citado:

Placa	Marca Modelo - Cor	Quantidade
KEE-7 [redacted]	Ford Ranger 13d - Azul	1x

Gerar Grafo

Gerar Mapa

Figura 7.2 Relatório de informações do indivíduo.

Como todos os registros possuem informações sobre a localização em que ocorreu o fato, é possível, com base nesta mesma pesquisa, exibir um mapa que mostrará os locais por onde este indivíduo passou (Figura 7.3). Para produzir o mapa, é necessário recuperar os registros nos quais foi citado o indivíduo em questão e resgatar os dados do endereço que foram cadastrados junto àquele registro. Os dados referentes à localização estão disponíveis na tabela **Geo**, na qual é efetuada a consulta para recuperar a informação do endereço e, utilizando ferramentas de georeferenciamento, apresentar um mapa.

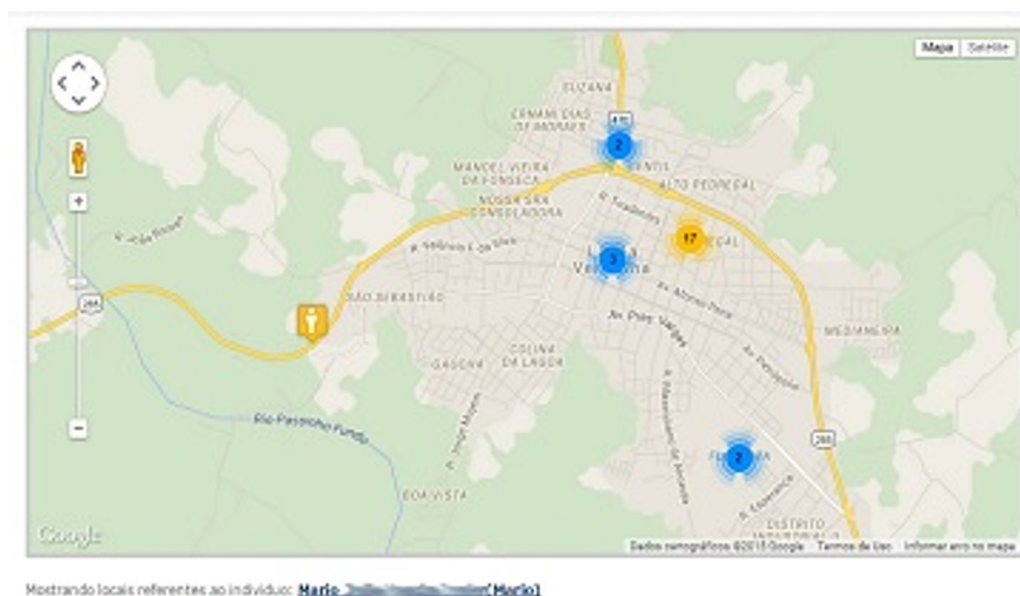


Figura 7.3 Mapa de ocorrências de indivíduo.

Estas duas representações (relatório de informações agregadas e mapa de circulação de determinado indivíduo) obtidas a partir do banco de dados podem ser vistas como relevantes para o uso na inteligência policial, pois, com elas, torna-se possível visualizar, de forma fácil, todos os registros de informações que foram efetuados relacionando determinado alvo.

4 CONSIDERAÇÕES FINAIS

O objetivo geral deste trabalho foi o desenvolvimento de um modelo de banco de dados para a aplicação na gestão da informação com foco em ações de inteligência policial. Neste sentido, foi proposto o modelo de dados detalhando os principais elementos capazes de criar uma especificação ao desenvolvimento de sistemas de informação voltados à inteligência policial. Especificou-se o modelo

conceitual, sendo este o primeiro passo para a criação dos esquemas de relações que no banco de dados são implementadas como tabelas.

Após a concepção do banco de dados, foi elaborado um cenário envolvendo um conjunto de relatórios de inteligência, indivíduos, veículos e locais de ocorrência. O cenário teve como objetivo permitir a execução de consultas e a obtenção de informações consolidadas. Para tal, foi desenvolvida uma aplicação ao nível de protótipo capaz de apresentar, a partir de determinado indivíduo de interesse, informações direta ou indiretamente relacionadas. Essas informações visam auxiliar no entendimento do contexto de inserção de determinado indivíduo alvo.

Os resultados obtidos, ainda que iniciais, demonstram que o modelo de banco de dados proposto pode ajudar muito na confecção de Relatórios de Inteligências por parte dos agentes. De certo modo, isso promove mais credibilidade aos relatórios e mais segurança ao tomador de decisão. A agregação da informação, bem como a confiabilidade da informação utilizada na tomada de decisão, pode produzir melhores resultados e, por consequência, melhorar a efetividade das ações de inteligência policial.

REFERÊNCIAS

- CAMPBELL-KELLY, M. The RDBMS Industry: A Northern California Perspective. *IEEE Annals of the History of Computing*, v.34, n.4. 2012.
- CEPIK, M. A. C. *Espionagem e Democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência*. Rio de Janeiro: FGV, 2003.
- COUGO, P. *Modelagem conceitual e projeto de bancos de dados*. Rio de Janeiro: Elsevier, 1997.
- GABRIELLI, B. V. *Desenvolvimento de um sistema de apoio a inteligência policial*. Departamento de Informática e Estatística – Universidade Federal de Santa Catarina (UFSC). 2007. Disponível em: <https://projetos.inf.ufsc.br/arquivos_projetos/projeto_681/artigoVentorim.pdf>. Acesso em: 27 abr. 2015.
- GRAD, B. Relational Database Management Systems: the formative years. *IEEE Annals of the History of Computing*, v.34, n.4, 2012.
- HEUSER, C. A. *Projeto de banco de dados*. 6.ed. Porto Alegre: Bookman, 2009.
- LIRA, W. S.; CANDIDO, G. A.; ARAÚJO, G. M.; BARROS, M. A. A busca e o uso da informação nas organizações. *Perspect. ciênc. inf.* [online]. v.13, n.1, 2008. ISSN 1413-9936. Disponível em: <<http://dx.doi.org/10.1590/S1413-99362008000100011>>. Acesso em: 26 abr. 2015.
- MARTINS, A. F. *Inteligência policial e investigação*. 2011. Disponível em: <<https://blogdodelegado.wordpress.com/2011/04/13/inteligencia-policial-e-investigacao/>>. Acesso em: 10 mar. 2015.

PACHECO, D. F. Atividades de inteligência e processo penal. **IV Jornada Jurídica da Jurídica da Justiça Militar da União**. Auditoria da 4ª CJM. Juiz de Fora, 30 set. 2005. Disponível em: <<http://www.advogado.adv.br/direitomilitar/ano2005/denilsonfeitozapacheco/atividadedeinteligencia.htm>>. Acesso em: 15 dez. 2014.

RIO GRANDE DO SUL – RS. SECRETARIA DA SEGURANÇA PÚBLICA. DEPARTAMENTO DE GESTÃO DA ESTRATÉGIA OPERACIONAL. **Sistema Estatístico da SSP/RS**. Dados estatísticos da Secretaria da Segurança Pública em atendimento à Lei nº 11.343/99 e à Lei nº 12.954/08, contendo os dados do primeiro semestre de 2014. 2014. Disponível em: <http://www.ssp.rs.gov.br/upload/201409111110442014s01_lei_postal_e_lei_stela_farias_1__semestre_de_2014.pdf>. Acesso em: 26 abr. 2015.

8

CAPÍTULO

UM ESTUDO SOBRE TÉCNICAS DE BIOMETRIA BASEADAS EM PADRÕES FACIAIS E SUA UTILIZAÇÃO NA SEGURANÇA PÚBLICA

Fernanda Todesco Nunes

Juarez Bento da Silva

Priscila Cadorin Nicolete

Josiel Pereira

Marta Adriana da Silva Cristiano

1 INTRODUÇÃO

Muito se fala a respeito dos possíveis benefícios das TIC na área de Segurança Pública, assim como da eficiência e da transparência que estas podem aportar à Administração Pública e ao governo em todos os níveis e áreas. Sem dúvida que, para falar sobre a utilização das TIC na Segurança Pública, deve-se levar em conta o contexto, tanto político-administrativo, quanto social no qual se pretende inseri-las, a fim de não se deixar cair em “soluções mágicas” ou “receitas universais”.

Um dos processos que caracteriza a sociedade atual é a crescente densidade das relações sociais, produto, entre outras coisas, da ingerência que possuem as novas tecnologias. Aqui, densidade refere-se à capacidade de relacionamentos pessoais de uma maneira mais complexa, em que as ações de uma pessoa repercutem direta ou indiretamente em uma maior quantidade de indivíduos, criando relações de interdependência mais dinâmicas. Também está ligada à capacidade de

relacionamentos com maior número de pessoas, no mesmo sentido que levantou Durkheim (1987) quando falou sobre “densidade dinâmica”. Essa maior densidade gera novos desafios aos estados, pois a maneira de relacionar-se com e entre seus cidadãos modifica-se constantemente. Neste contexto, as TIC aplicadas à Segurança Pública devem ser englobadas em um processo mais amplo de mudanças sociais e das maneiras de relacionamentos entre todos os atores.

Devido à importância e ao valor que podem obter alguns dos recursos físicos e informáticos (dados) utilizados em diferentes áreas da sociedade, torna-se necessária a criação de mecanismos de proteção, tanto de acesso como de integridade desses recursos. Por exemplo, são empregados processos para restringir o acesso somente a determinadas pessoas. Esses processos buscam utilizar mecanismos altamente confiáveis e seguros.

Diante do aumento da criminalidade, todos os setores da sociedade têm discutido soluções para minimizar os prejuízos sofridos. Visualiza-se mais investimentos por parte das pessoas e das empresas em tecnologias de segurança, como: sistemas de monitoramento, alarmes, escoltas armadas, equipamentos de rastreamento etc. A Segurança Pública também tem recebido maiores fatias de recursos financeiros para aprimorar seus sistemas tecnológicos, principalmente com a aquisição de equipamentos de vídeomonitoramento instalados nas áreas urbanas (RIBEIRO, 2013).

Diante disso, a identificação de pessoas a partir do emprego de técnicas de reconhecimento de padrões faciais pode tornar-se uma alternativa segura e pouco invasiva, que provê a informação biométrica dada as características únicas que possui o rosto de cada pessoa. O desenvolvimento de tecnologias de reconhecimento facial, em conjunto com os sistemas de vídeomonitoramentos já existentes, poderá ser uma ferramenta eficaz no combate à criminalidade, principalmente na localização e na identificação de foragidos, criminosos, desaparecidos etc.

Entretanto, a pouca informação disponível a respeito de sistemas de reconhecimento facial tem dificultado e limitado a possibilidade de sua implantação de maneira massiva (PEREZ; AGUDELO, 2012), bem como o desenvolvimento de projetos que utilizam esse tipo de alternativa nos sistemas de segurança privada ou pública. O que se encontra são projetos que buscam a aplicação do reconhecimento facial para reforçar a segurança orgânica e patrimonial das instalações em geral privadas, que produzem conhecimento ou guardam informações de segurança institucional.

Nesse sentido, seria possível, então, reunir técnicas que permitam conhecer e desenvolver um sistema de segurança baseado na biometria estática por meio de padrões faciais para identificação de rostos humanos nos órgãos de Segurança Pública, e aplicá-los na resolução de crimes de forma massiva?

Desse modo, este estudo pretendeu relacionar as diferentes técnicas existentes para o tratamento de imagens e que permitam a identificação ou reconhecimento de padrões faciais em seres humanos. Para isso, o estudo apresenta um breve panorama sobre a utilização das TIC por parte do Estado, suas possíveis aplicações na área de Segurança Pública, seus entraves e soluções, e os desafios que o Estado enfrenta para acompanhar a evolução tecnológica, bem como discutir a utilização das tecnologias de reconhecimento biométrico, em especial o reconhecimento facial.

2 SISTEMAS BIOMÉTRICOS

Nas civilizações antigas, as pessoas viviam em pequenas comunidades, nas quais as pessoas reconheciam-se sem dificuldade. Com a rápida expansão da população, a identificação converteu-se em um processo complexo, de maneira que, nas sociedades modernas, tem sido necessária a implementação de sofisticados sistemas de gestão de identidade. A identidade refere-se ao conjunto de informações associadas a uma pessoa, como seu nome, sobrenome, data de nascimento, endereço, entre outros.

Os sistemas de gestão de identidade são utilizados em diferentes aplicações, como: em aduanas, na restrição de acesso às instalações, no controle de acesso a recursos informáticos, nas transações financeiras, na abordagem de voos comerciais, entre outros. Dentro dos sistemas de gestão de identidade são encontrados os que baseiam seu funcionamento na biometria; são sistemas os que realizam a análise dos traços característicos do corpo humano.

A biometria tem origem no idioma grego – *bio* (vida) e *metron* (medida) – e refere-se a todas aquelas técnicas que permitem identificar e autenticar as pessoas por meio de suas características fisiológicas e de comportamento (GUGLINSKI, 2013). A biometria foi utilizada pela primeira vez na China, em meados do século XIV, e foi a partir do século XIX que começou a ser utilizada nas culturas ocidentais. O explorador e escritor espanhol João de Barros relatou que os comerciantes chineses usavam papel com tinta para que as pudessem estampar suas impressões digitais com finalidade de poder diferenciá-las (SAEED; NAGASHIMA, 2012).

No ocidente, a identificação baseava-se apenas na “memória fotográfica”, até que Alphonse Bertillon, chefe do departamento fotográfico da Polícia de Paris, desenvolveu o sistema antropométrico, em 1883. Esse foi o primeiro sistema preciso, amplamente utilizado cientificamente para identificação criminal e que converteu a biometria em um campo de estudo. Funcionava medindo, de forma precisa, certos comprimentos e larguras da cabeça e do corpo, assim como registrava marcas individuais como tatuagens e cicatrizes (MAERSA, 2010).

O sistema de Bertillon foi adotado extensamente no ocidente, até que se passou a detectar defeitos no sistema, principalmente, problemas com os diferentes métodos de medidas e mudanças de medida (LI; JAIN, 2009). Posteriormente, foi colocada em prática a impressão digital como método de reconhecimento por parte das autoridades policiais (LI; JAIN, 2009), muito parecido com o sistema utilizado pelos chineses há muitos anos. Atualmente, a biometria não está somente centrada na identificação por meio da impressão digital, mas por diversas outras técnicas de reconhecimento, que levam em conta várias medidas físicas e também comportamentais.

O reconhecimento biométrico corresponde a um sistema automático baseado na inteligência artificial e no reconhecimento de padrões, que permite a identificação e/ou verificação da identidade de pessoas a partir de características morfológicas ou de comportamento, próprias e únicas de cada indivíduo, conhecidas como identificadores. Atualmente, as tecnologias biométricas mais utilizadas são: biometria de impressão digital, geometria da mão e dedos, facial, de íris e de voz (JAIN; ROSS; NANDAKUMAR, 2011).

3 RECONHECIMENTO FACIAL

O conceito de identificação ou reconhecimento facial automatizado foi introduzido nos anos 1960. “Durante os anos 1964 e 1965, Woodrow Wilson Bledsoe, Helen Chan Wolf e Charles Bisson trabalharam no reconhecimento facial humano fazendo uso do computador e desenvolveram o primeiro sistema semiautomático de reconhecimento” (TRASLAVIÑA, 2015).

Nos anos 1970, Goldstein, Harmon e Lesk (2013) usaram 21 características físicas específicas, como a cor do cabelo e a espessura dos lábios, para automatizar o reconhecimento facial, porém identificar estas características continuava requerendo um processo manual. Ao final dos anos 1980, eles produziram um ponto de referência quando Kirby e Sirovich aplicaram uma técnica padronizada de álgebra linear, a análise dos principais componentes (PCA) (TURK; PENTLAND, 1991).

No início da década de 1990, Turk e Pentland (1991), utilizando a técnica de *eigenfaces*, nome que recebeu o método descoberto por Kirby e Sirovich, demonstraram que “o erro residual podia ser utilizado para detectar rostos nas imagens, uma descoberta que permitiu desenvolver sistemas de reconhecimento confiáveis em tempo real”.

Porém, foi no ano 2001 que o uso de câmeras de vigilância chamou a atenção de uma grande quantidade de público na partida do Super Bowl da NFL (Liga Nacional de Futebol Americano), pois naquela ocasião o processo consistiu na captura de imagens por meio das câmeras de vigilância para depois serem

contrastadas e identificadas com uma base de dados que armazenavam imagens digitalizadas de delinquentes. (SUCAR, 2010; MACEDO, 2013).

A partir desta demonstração, originou-se um importante debate sobre como usar a tecnologia para satisfazer necessidades, principalmente governamentais, porém, levando em consideração as preocupações sociais e de privacidade das pessoas. Atualmente, por exemplo, a tecnologia de reconhecimento facial vem sendo muito utilizada para evitar fraudes de identificação, realizar buscas por pessoas desaparecidas, controle de acesso de funcionários em empresas entre outras aplicações. (DE PAULO; PEREIRA, 2015; MONTIBELER; FERNANDES, 2012). Nos últimos anos, foram realizados estudos mais detalhados devido à necessidade de encontrar meios para reconhecer as pessoas a partir de seus traços característicos, sendo o campo da segurança o que tem exigido os maiores avanços (VALLEJO; NEIRA, 2005).

Nesse sentido, o reconhecimento facial é a capacidade de identificar as pessoas por suas características faciais. É uma tecnologia mais avançada e baseada em algoritmos. Por exemplo, o Eigenfaces mapeia as características do rosto de uma pessoa em um espaço multidimensional. Os computadores podem realizar buscas em bases de dados faciais e/ou efetuarem verificações ao vivo um-a-um ou um-para-muitos, com uma precisão sem precedentes e o processamento em uma fração de segundo. Os usuários podem ter acesso seguro em seu computador, dispositivo móvel ou para comércio eletrônico on-line simplesmente olhando para sua câmera web. (LI; JAIN, 2009; TURK; PENTALAND, 1991).

Em geral, um sistema automático de verificação facial é composto de duas etapas principais: detecção de rosto e verificação do rosto. Na detecção de rosto, o objetivo é determinar se existe um ou mais rostos em uma imagem ou vídeo e, se for o caso, retornar sua posição e escala (OLIVEIRA, 2006). O termo localização é empregado quando existe unicamente um rosto na imagem. A detecção do rosto é um aspecto muito importante na pesquisa, porque serve como um primeiro passo necessário para qualquer sistema de processamento facial, como reconhecimento do rosto, acompanhamento e análise de expressões. A maioria das técnicas utilizadas assume que a região do rosto tenha sido localizada perfeitamente. Portanto, o rendimento desse sistema depende significativamente da precisão da etapa da detecção facial (OMAIA, 2009).

Uma fator importante para sistemas de detecção de rostos é a capacidade para separar o rosto do restante da imagem. Para isso, o sistema faz o reconhecimento dos pontos altos, pontos baixo e contornos presentes no rosto, e trata esses nós para medir (Figura 8.1) e comparar com aqueles armazenados no sistema de banco de dados (BORJA; BUENO, [20??]).

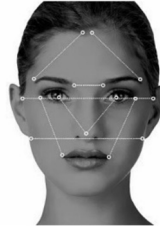


Figura 8.1 Pontos-chave da estrutura de tecidos rígidos do rosto.

Fonte: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf.

Entretanto, algumas dificuldades são encontradas na detecção de rostos. O algoritmo não somente deve detectar o rosto para a identificação ou verificação de pessoas, como também deve levar em conta outros aspectos que poderiam dificultar o processo de detecção do rosto (OTEGUI et al., 2006), como:

- estado de ânimo da pessoa/reconhecimento de expressões (triste, alegre, enojado etc.);
- localização de características relevantes: olhos, boca, sobrancelhas, queixo, orelhas etc.;
- tamanho do rosto;
- presença de lentes, barba, gorros etc.;
- expressão do rosto;
- problemas de iluminação;
- condições da imagem;
- quantidade desconhecida de rostos na imagem (OTEGUI et al., 2006 ; GOLDSTEIN; HARMON; LESK, 1971).

3.1 Métodos de reconhecimento de rostos

O reconhecimento de rostos tem sido estudado por várias disciplinas, como a Psicologia, assim como se estuda o reconhecimento de padrões e redes neurais, as quais dividem o reconhecimento de rostos duas abordagens para extração de características das imagens da face: “Abordagem global – Aparência da face” e “Abordagem local – geometria da face” (COSTA; OBELHEIRO; FRAGA, 2006; OTEGUI et al., 2006).

Na abordagem global, a ideia básica é reduzir uma imagem de milhares de pixels para um conjunto de número (COSTA; OBELHEIRO; FRAGA, 2006). A vantagem dessa abordagem é que as características podem ser identificadas independentemente dos “ruídos” que uma imagem pode ter, como luminosidade, textura da pele, reflexos etc. (COSTA; OBELHEIRO; FRAGA, 2006). Os métodos

para tratamento utilizando essa abordagem é chamado de Métodos Holísticos (COSTA; OBELHEIRO; FRAGA, 2006; OTEGUI et al., 2006).

Já na abordagem local são extraídas as características locais do rosto (olhos, nariz, boca, sobrancelhas etc.) a partir da sua localização geométrica, ou seja, suas posições, que formam a entrada do sistema de reconhecimento (OTEGUI et al.; 2006). Dessa forma, o reconhecimento de face é feito a partir da comparação dos sistemas geométricos obtidos (COSTA; OBELHEIRO; FRAGA, 2006). Para a utilização dessa abordagem, são empregados Métodos Estruturais (COSTA; OBELHEIRO; FRAGA, 2006), também denominados Métodos Baseados em Características Locais (OTEGUI et al., 2006).

Ainda pode-se explorar uma abordagem híbrida, que combina os dois métodos anteriores. Para Costa, Obelheiro e Fraga (2006), os métodos híbridos oferecem o melhor dos dois métodos.

Cada método possui técnicas para o reconhecimento de rostos. Essas técnicas determinam as características a serem extraídas das imagens e as possíveis medidas de similaridade para a etapa de comparação (COSTA; OBELHEIRO; FRAGA, 2006). A Figura 8.2 mostra a classificação de alguns dos métodos de reconhecimento de rostos.

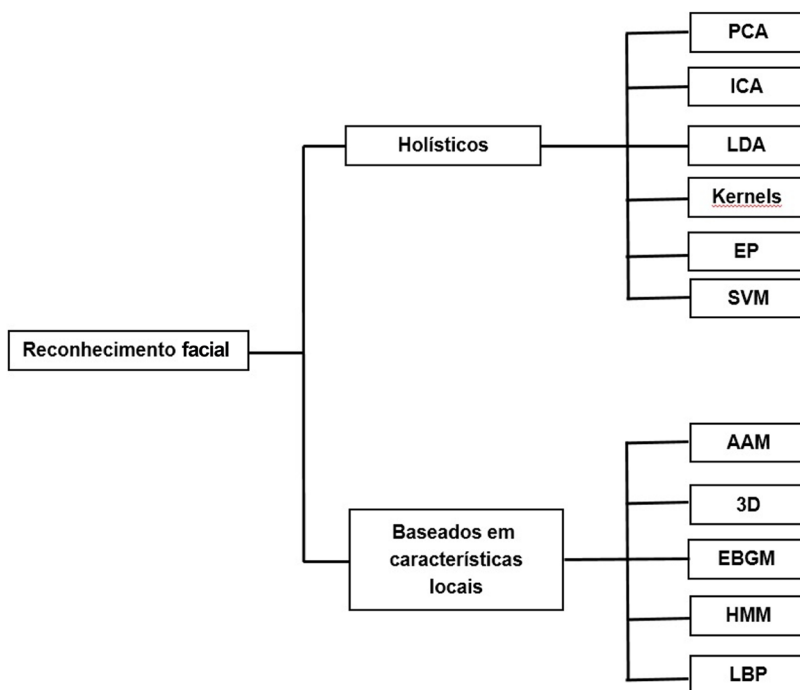


Figura 8.2 Classificação de alguns métodos de reconhecimento de rostos.

A seguir será apresentando de modo geral os métodos e algumas técnicas utilizadas no reconhecimento de rostos.

3.2 Métodos holísticos

Os métodos holísticos são classificados em: Análise de Componentes (PCA, ICA e LDA) e métodos baseados em *Kernels*, *Evolutionary Pursuit* (EP) e *Support Vector Machine* (SVM).

Nos métodos de componentes, é construído um subespaço que cumpre determinadas restrições e, a partir disso, escolhe-se uma base que gerará de alguma maneira particular componentes de maior potência, melhor discriminação etc. (OTEGUI et al., 2006). Os métodos de Análise de Componentes podem ser: Análise de Componentes Principais (PCA), Análise de Componentes Independentes (ICA) e Análise de Discriminante Linear (LDA).

O PCA considera a distribuição de imagens de um rosto e tenta capturar variabilidade destas, buscando a independência de qualquer rosto ou característica particular. É denominado PCA porque busca extrair de um conjunto de imagens de treinamento um subespaço cuja base maximize a variância do espaço original. Esses vetores gerados são chamados de *Eigenfaces*. (TURK; PENTALAND, 1991). Já os métodos baseados em ICA tentam representar o espaço das faces em um subespaço que minimize a dependência de segunda e de maior ordem entre seus componentes. Assume que os sinais de entrada são combinações de fontes não observáveis estatisticamente independentes (HAVRAN et al., 2002). E o algoritmo LDA tenta levar o espaço dos rostos para um subespaço de baixa dimensionalidade e que possa aumentar a separabilidade das classes presentes (ZHAO; CHELLAPPA; KRISHNASWAMY, 1998).

Existem também os métodos baseados em *Kernels*, que são uma generalização dos métodos de análise de componentes (PCA, ICA, LDA). Esses métodos têm a capacidade de trabalhar com mais dados sem ter um custo computacional muito expressivo, pois buscam levar o problema de classificação para um espaço de dimensão maior, no qual as classes possam ser linearmente separadas (YANF, 2001).

Já os métodos denominados *Evolutionary Pursuit* (EP), de forma similar ao PCA, ICA e LDA, baseiam-se na análise de componentes. O EP propõe uma nova maneira de obtenção de uma base de vetores eficientes para a representação das imagens de rostos. Para encontrar a base, é realizada uma busca para maximizar uma função *fitness*, que mede ao mesmo tempo a precisão da classificação e a habilidade de generalização do sistema. Como a busca por uma base ótima é um problema de alta dimensão, utiliza-se para o modelo Algoritmos Genéticos (GA), que são chamados de *Evolutionary Pursuit*. Essa técnica pode ter mais vantagens

do que a PCA, sempre e quando o treinamento das imagens seja for de forma balanceada (LIU; WECHSLER, 2000).

Por fim, o *Support Vector Machine* (SVM) é uma ferramenta genérica para resolver problemas de reconhecimento de padrões e foi proposta na década de 1990 por Cortes e Vapnik. Dado um conjunto de pontos em um determinado espaço que pertencem a duas classes distintas, o SVM encontra o hiperplano que separa a maior quantidade de pontos da mesma classe do mesmo lado. (CORTES; VAPNIK, 1995).

3.3 Métodos estruturais

Os métodos baseados em características locais podem ser do tipo: *Active Appearance Model* (AAM), Modelagem 3D, *Elastic Bunch Graph Matching* (EBGM), Modelos Escondidos de Markov (HMM) e *Local Binary Patterns* (LBP).

O *Active Appearance Model* (AAM) é um modelo estatístico da forma e da aparência, em níveis de cinza, do objeto de interesse. Pode ser gerada a qualquer tempo. Ajustar o modelo de uma imagem implica em encontrar os parâmetros do modelo para minimizar a diferença entre a imagem e uma síntese do modelo projetado na imagem (COOTES; WALKER; TAYLOR, 2000).

Já na modelagem 3D, a ideia central é a construção um modelo genérico tridimensional para cada imagem que se deseja analisar. Existem diversas técnicas de aquisição de imagens (ou de reconstrução) 3D, entre elas: câmeras, escâneres, *Structure Light System* (SLS), sequências de imagens 2D etc. (BLANZ; VETTER, 2003).

Os algoritmos baseados em *Elastic Bunch Graph Matching* (EBGM) visam extrair uma representação do rosto em forma de grafo e o reconhecimento se realiza comparando os grafos correspondentes a diferentes imagens (OTEGUI et al., 2006). Esse algoritmo é selecionado graças a robustez da informação na rotação do plano e pela habilidade de classificar rostos demarcando zonas importantes do rosto. Dentro dessas zonas distintivas são tomadas mais de 80 características que permitem localizar as semelhanças notáveis e as diferenças das imagens de treinamento (WISKOTT et al., 1999). Essas zonas estão compostas pelas seis regiões mais predominantes de rosto humano, são agrupadas em: duas seções para os olhos, duas seções para as sobrancelhas, uma seção para as fossas nasais e uma seção para a região que rodeia a boca.

Outro método baseado em características locais é o Modelo Escondido de Markov (HMM), que é um conjunto de modelos estatísticos utilizados para caracterizar as propriedades estatísticas de um sinal. Esses modelos são de grande utilidade para a representação de dependências estatísticas em problemas que tem uma temporalidade inerente. Esse modelo tem alcançado sucesso em aplicações como o reconhecimento de voz e de gestos (NEFIAN, 1999).

Por fim, o *Local Binary Patterns* (LBP) é uma ferramenta interessante como descritor de textura. Esse operador recorre à imagem e ao *label* dos pixels da mesma, estabelecendo uma vizinhança de 3 x 3 em relação ao valor do pixel no qual se encontra, considerando o resultado como um número binário. Assim, o histograma dos *labels* pode ser utilizado como um descritor de textura (AHONEN; HADID; PIETIKÄINEN, 2004).

4 APLICAÇÕES

A técnica de identificação e reconhecimento facial adquire um novo uso em entidades governamentais, satisfazendo suas necessidades. Atualmente, pode-se ver o grande impacto que essa tecnologia tem conseguido, sendo utilizada em locais em que se deseja levar um controle de acesso e lugares em que seja requerida identificação plena de todas as pessoas, como aeroportos e terminais de transporte. A tecnologia pode, inclusive, ajudar em atividades tão importantes como encontrar pessoas desaparecidas ou em fraudes cometidas muitas vezes ao suplantam a identificação de outra pessoa (DE PAULO RESENDE; PEREIRA, 2015; OMAIA, 2009). A Tabela 8.1 apresenta algumas áreas e aplicações específicas com reconhecimento facial.

Tabela 8.1 Aplicações com reconhecimento facial

Área	Aplicações específicas
Biometria	Carteiras de habilitação, Imigração, passaportes, registro eleitoral, fraude, telefones inteligentes, acesso às instalações restritas.
Segurança da informação	Início de sessão, Segurança de Aplicações, segurança em bases de dados, codificação de informação, segurança na internet, acesso à internet, registros médicos, terminais de comércio seguro, caixas automáticos.
Lei e vigilância	Vídeo vigilância avançada, controle CCTV, controle de portais, análises <i>post-event</i> , furto, acompanhamento de suspeito, investigação.
Tarjetas inteligentes	Valor armazenado, autenticação de usuários.
Controle de acesso	Acesso às instalações, acesso aos veículos.

A seguir será tratada a utilização de reconhecimento facial especificamente na segurança pública.

5 USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

Embora as pesquisas científicas relacionadas ao reconhecimento facial tenham iniciado por volta da década de 1960, um fato relevante, o ataque terrorista de 11 de setembro nos Estados Unidos, alavancou a indústria e a sociedade acadêmica na construção, busca e aprimoramento de sistemas de segurança que utilizem o reconhecimento facial (TUCKER, 2014).

Segundo Almeida (2009), são muitas as áreas de aplicação do reconhecimento facial, como: ações contra o terrorismo, no controle parlamentar, no controle da circulação, na busca por crianças desaparecidas em meio a multidões, na segurança residencial, na verificação da identidade dos eleitores, nas atividades bancárias, entre outros. Porém, é na Segurança Pública que sua implantação é mais requerida.

É preciso salientar que o reconhecimento facial não é algo novo nos órgãos de segurança pública; o que está surgindo com os novos programas é a automação do processo, uma vez que o processo de reconhecimento facial é análogo ao reconhecimento por fotografia ou mesmo o retrato falado, em que autores ou suspeitos de cometimento de crime têm suas características confrontadas com um banco de dados pré-existente nos órgãos de segurança pública.

Neste sentido, Grue (2003) relata que o reconhecimento facial já existia há tempos sob a forma de identificação por foto, que é razoavelmente confiável em nossa sociedade. Até hoje, o processador que decide se uma pessoa é igual a uma foto tem sido o cérebro humano e nunca um computador. No entanto, os computadores introduzidos neste tipo de identificação não servem simplesmente para substituir o raciocínio humano, mas ampliar a possibilidade de buscas. Já não é mais possível comparar uma pessoa à sua própria identidade, mas com o reconhecimento facial em um computador você pode comparar uma pessoa a um banco de dados de imagens armazenadas, permitindo-lhe identificar uma pessoa que nunca foi vista antes ou procurar por milhares de pessoas simultaneamente e encontrar pelo menos uma delas.

Conforme Azevedo e Faria (2014), as fotos publicadas nas redes sociais podem revelar muito sobre uma pessoa, e afirmam que softwares de reconhecimento facial, aliados aos imensos bancos de imagens dessas redes, podem não só revelar o nome de um usuário, mas informar ainda o endereço, telefone e profissão, colaborando e muito com as forças de segurança pública no combate preventivo da criminalidade.

5.1 No exterior

Na área de segurança pública nos Estados Unidos, foram implementados alguns monitoramentos utilizando sistemas de reconhecimento facial, porém até

o momento não mostraram resultados satisfatórios ou que levassem a impedir um ataque terrorista, que foi a principal causa de sua utilização pelas forças de segurança americana. Mesmo assim, os produtos de reconhecimento facial estão começando a surgir nos aplicativos da vida real e vêm chamando especialmente a atenção da população norte-americana desde a crescente ameaça do terrorismo.

Na cidade de Tampa, na Flórida, em 2001, foi feito o monitoramento de cada frequentador do Super Bowl a partir do uso de um popular aplicativo de reconhecimento facial, o *FaceIt*, criado pela Visionics Corporation. Entretanto, conforme Grue (2013), nenhum suspeito foi identificado, apesar do público de 71.000 pessoas. Além de Tampa, algumas outras cidades e aeroportos instalaram softwares de reconhecimento facial que se apresentaram ineficazes na identificação de qualquer suspeito criminal até hoje.

A principal causa da aparente ineficiência dos sistemas está ligada ao fato de que existe a necessidade de um banco de dados para confrontar todos os rostos capturados pelo sistema. Um exemplo prático desta afirmação é o fato que, dos 19 terroristas envolvidos nos ataques de 11 de setembro, apenas dois eram conhecidos do sistema de segurança americano, sendo que apenas um possuía fotografia. Evidentemente, poderia o sistema estar em funcionamento naquele dia e não impediria os ataques, pois existe a necessidade de um banco de dados.

Entretanto, a colocação em funcionamento dos sistemas estimulou uma enorme discussão relativa à confiança nos sistemas de reconhecimento facial e se eles interferem ou não na liberdade individual, já que o reconhecimento facial pode ser utilizado de forma passiva ao contrário de muitas outras técnicas de identificação biométrica. Mesmo utilizando um discurso focado no aumento da segurança e de um país mais protegido na era do terrorismo, a recente transição do reconhecimento facial do laboratório para a realidade ainda necessita de limitações em sua utilização.

Embora exista o argumento de que a tecnologia está em constante aperfeiçoamento e seu fim seja a identificação precisa de indivíduos que representem ser ameaças à coletividade, a verdade é que tem se despendido muito tempo e recursos para tentar resolver as mazelas da proteção e da segurança para o qual o sistema de reconhecimento facial foi idealizado, e não se tem mostrado eficaz, resultando em críticas severas a invasão da privacidade que produz.

O governo está interessado na tecnologia para combater o crime em geral e no mundo, após 11 de setembro, porque o público está se perguntando por que o governo falhou em evitar o ataque. Por essa razão, o governo vem procurando uma solução tecnológica para um problema sério, que não pode ser completamente corrigido por meio do monitoramento de toda a população americana com sistemas de reconhecimento facial. Não obstante, a Agência de Projetos de

Pesquisa Avançada de Defesa (DARPA) iniciou seu programa de financiamento Identificação Humana à Distância (*Human ID at Distance*), que propiciou uma verba para a Visionics, entre outras empresas, para continuar suas pesquisas. A DARPA está procurando uma tecnologia que consiga identificar pessoas em multidões e em grandes extensões. Eles acreditam que essa tecnologia lhes permitiria identificar mais adequadamente os suspeitos em áreas dentro e fora do solo americano.

De acordo com a ABDI (2010), o FBI opera atualmente sob a tecnologia de reconhecimento de impressão digital e está em processo de adoção de um sistema de nova geração, incluindo outras tecnologias biométricas. A iniciativa mostra uma tendência à utilização de diversas tecnologias biométricas em conjunto para manutenção de registros de identidade pessoal. Uma aplicação direta de uma base de dados com múltiplas informações é a possibilidade de busca de pessoas a partir de seus registros por diversos meios diferentes, como reconhecimento facial em fotografias e reconhecimento por meio de câmeras de vídeo.

5.2 No Brasil

Em nosso país, em 2002, foi desenvolvido de forma experimental um sistema de retrato falado, chamado *fotocrim*, utilizando como base o banco de dados de fotos digitais do sistema de Segurança Pública do Rio de Janeiro, com capacidade de inclusão de características das etnias que formam a população brasileira.

Azevedo e Faria (2014) afirmam que o objetivo de um retrato falado é auxiliar uma investigação policial, diminuindo o número de suspeitos e apresentando um rosto com características semelhantes às do indivíduo procurado. A parte principal de um retrato falado é o rosto. Desta forma, o reconhecimento facial, somado às demais tecnologias já empregadas no dia a dia policial, é de suma importância para o aprimoramento das técnicas investigativas, e contribuiria para o aumento de efetividade na resolução de crimes, principalmente no elemento tempo. Entretanto, não há registros no Brasil de integrações entre softwares de produção de retrato falado e banco de dados criminais. A falta desta interligação, entre a composição de um retrato falado e a base de dados comparativa, tem diminuído a efetividade da investigação policial.

A ABDI (2010), em virtude da variedade de tecnologias, classifica os sistemas biométricos em três grupos: Sistemas de Impressão Digital (T3a1); Sistemas de Identificação de Íris, DNA e Face (T3a2); e Sistemas de Reconhecimento de Voz (T3a3). Os dois primeiros são baseados em características fisiológicas do ser humano e o último, em características comportamentais.

Não existe um consenso quanto à tecnologia biométrica mais adequada para cada tipo de aplicação, mas existem aplicações que só são viáveis com de-

terminada tecnologia. A identificação por impressão digital ainda é a preferida para a maioria das aplicações por ser mais simples e madura e também pela tradição de uso anterior às tecnologias digitais, principalmente pela polícia. Além disso, é a única tecnologia que permite identificação posterior de pessoas por meio da coleta da impressão digital deixada em objetos. Mas as tecnologias de reconhecimento de voz e face também abrem possibilidades para outras aplicações, além da identificação para autenticação da pessoa, que somente elas podem viabilizar.

Segundo a ABDI (2010) o reconhecimento facial possibilita a busca de pessoas desaparecidas ou procuradas a partir de fotografias ou combinando a tecnologia de reconhecimento de face com reconhecimento de padrões em vídeo, sem que a pessoa seja chamada para identificação.

Conforme a ABDI (2010) a tecnologia de reconhecimento de impressões digitais (T3a1), por estar em um estágio mais avançado de desenvolvimento, já está saindo da fase de pesquisa e desenvolvimento para ser incorporada a diversos projetos experimentais, devendo atingir as fases de inovação, produção, comercialização e assistência técnica em larga escala ainda no período 2008-2010. As tecnologias de reconhecimento de íris, face e DNA (T3a2) e as tecnologias de reconhecimento de voz (T3a3) ainda estão em amadurecimento, devendo sair da fase de pesquisa e desenvolvimento e atingir as fases de inovação e produção em larga escala ainda no período 2011-2015. A comercialização e assistência técnica em larga escala devem ocorrer somente no período 2016-2025 (Figura 8.3).

O Brasil encontra-se equiparado ao cenário mundial na utilização de tecnologias de reconhecimento de impressão digital (T3a1), embora não como gerador de novas tecnologias e inovações, mas como seguidor na utilização das tecnologias de reconhecimento de íris, face e DNA (T3a2) e voz (T3a3).

A utilização de tecnologias de reconhecimento de impressão digital está difundida em aplicações de controle de acesso físico, acesso a sistemas de informação e algumas aplicações experimentais. Entre elas estão a Universidade Estadual de Campinas (Unicamp), que utilizou um sistema de reconhecimento de impressões digitais no vestibular; o Detran da Bahia, que instituiu um sistema de controle de frequência em curso de formação de condutores; e o Tribunal Superior Eleitoral (TSE), que testou urnas com reconhecimento de impressão digital nas últimas eleições.

O uso das tecnologias de reconhecimento de íris, face e DNA (T3a2) e voz (T3a3) ainda são incipientes. Um projeto experimental no setor financeiro foi conduzido pelo Unibanco, que realizou um projeto com reconhecimento de íris em caixas eletrônicos. Essas tecnologias devem completar a fase de pesquisa e desenvolvimento no período 2008-2010 e atingir a fase de inovação e produção em larga escala somente no período 2011-2015.

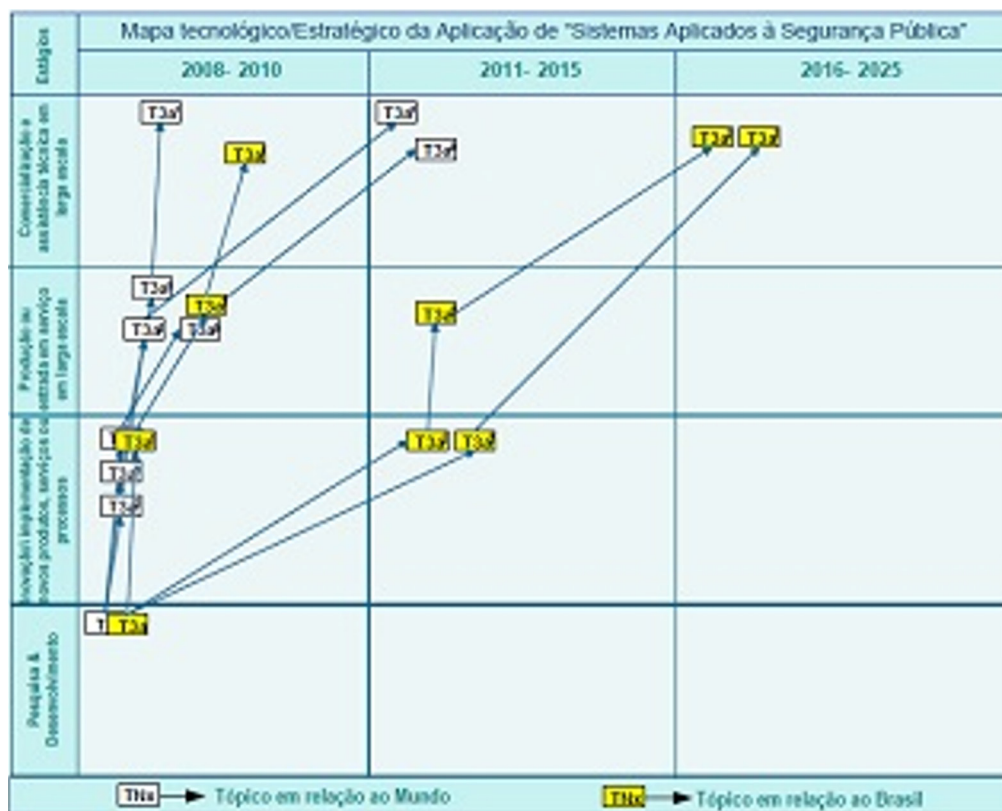


Figura 8.3 Mapa comparativo para biometria.

Fonte: ABDI (2010).

A comercialização e a assistência técnica em larga escala devem viabilizar-se somente no período 2016-2025. Iniciativas de pesquisa são pontuais e descoordenadas no país.

Além dos softwares especializados que a indústria nacional tem condições de produzir, um projeto de envergadura, já em andamento, é o projeto de passaportes, que pretende combinar tecnologias RFID, criptográficas e biométricas, como reconhecimento de impressões digitais e o reconhecimento facial. Outro projeto que pode convergir para a utilização de identificação biométrica é o Registro de Identificação Civil (RIC). Além disso, depois de implantados os projetos que coletam e registram as informações, expande-se o potencial de desenvolvimento de aplicações em segurança pública, que utilizarão essas bases de informação.

Existem algumas organizações atuantes em pesquisas biométricas no Brasil, entre elas a Cognitec Brasil, representante oficial da Cognitec Systems da Alemanha, empresa líder mundial em soluções de biometria de reconhecimento facial.

6 CONSIDERAÇÕES FINAIS

Observando ao nosso redor, seguramente encontra-se uma grande quantidade de sistemas biométricos. A necessidade de aumentar a segurança nos diferentes ambientes nos quais o ser humano interage, convertendo a biometria em uma tecnologia de uso cotidiano. A biometria na área de informática é encontrada em muitas aplicações de uso diário, como em transações bancárias ou em outros ambientes tão complexos como a identificação de civis por parte de entidades governamentais.

A necessidade de melhorar a segurança tanto de pessoas quanto de bens pode ser beneficiada por meio do uso da biometria informática, permitindo capturar informações e características únicas nas pessoas de forma automatizada, comparando-a posteriormente com dados armazenados em alguma base de dados e fornecendo um parecer confiável sobre a semelhança da amostras analisadas.

Conforme foi apresentado neste estudo, existem muitas técnicas utilizadas na biometria. Porém, na hora de implementar um sistema biométrico, algumas técnicas são mais aceitas pelas pessoas do que outras, e isso se deve principalmente ao nível intrusivo que cada técnica biométrica apresentada. Elas normalmente são apontadas em quatro categorias: as que não têm nenhuma interação direta como os usuários; as que apresentam pouca interação; as que requerem alta interação; e aquelas que requerem interação muito alta com os usuários, por exemplo, contato físico.

Outro fator que interfere significativamente na decisão sobre qual técnica biométrica pode ser implementada em cada cenário está relacionada ao ambiente que o rodeia. Ambientes repletos de pessoas são mais difíceis de serem controlados e vigiados, a fim de manter um nível ótimo de segurança, enquanto que em ambientes controlados, no qual o tráfego de pessoas é menor, torna-se mais simples e favorável implementar determinadas técnicas.

Ao estudar as diferentes técnicas de reconhecimento biométrico, foi possível observar que uma das técnicas, que combina maior aceitação por parte dos usuários, confiabilidade na análise e possibilidade de ser implementada eficazmente em ambientes repletos de pessoas e em ambientes controlados, é o reconhecimento de pessoas por meio do uso de padrões faciais.

Aprofundando-se mais nesta técnica, foi possível observar que existe uma grande quantidade de técnicas baseadas no reconhecimento de padrões faciais. Dado que existe uma ampla variedade, o documento ateu-se àquelas mais utilizadas no campo da biometria. Os sistemas apresentados, em sua maioria, trabalham somente com uma técnica na hora de extrair a informação das imagens. Entre as técnicas mais comuns e mais utilizadas estão a PCA e a LDA. Uma conclusão após a realização deste trabalho é que estes tipos de técnicas permitem

melhor desempenho quando trabalham em conjunto, conferindo mais eficácia e rapidez na hora de extrair informações.

É possível observar que há muitas áreas de aplicação do reconhecimento facial, porém, na área da Segurança Pública, em que sua implantação é mais requerida e necessária, ainda é pouco empregada. No exterior, foram implementados alguns monitoramentos utilizando o sistema de reconhecimento facial, porém não mostraram resultados muito satisfatórios. No Brasil, existem poucas referências sobre o uso da biometria facial no ambiente da Segurança Pública. Esse sistema encontra-se ainda em pesquisa, desenvolvimento e inovações, tendo uma previsão de implantação para 2016-2025. Desta forma, observa-se a aplicação do reconhecimento facial basicamente na iniciativa privada.

Considerando a pesquisa realizada, a utilização da biometria facial na Segurança Pública, em especial no meio investigativo-policial, colaboraria para maior resolução de crimes, visto que permitiria ampliar o campo de pesquisa na busca de suspeitos e foragidos da justiça.

Como recomendação, fica a proposta de combinar diferentes técnicas na hora de desenvolver algum tipo de sistema biométrico, pois, desta maneira, aproveitar-se-ia as diferentes funcionalidades que nos brindam estas técnicas na hora de identificar ou reconhecer uma pessoa. Recomenda-se também o estudo sobre o uso da biometria por policiais, por meio de dispositivos móveis e como estes podem auxiliar e facilitar a atividade policial; pesquisa sobre os motivos pelos quais a biometria não alavancou no Brasil; e realização de estudo de caso sobre o uso do reconhecimento facial nos aeroportos nacional e internacional.

REFERÊNCIAS

- AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL – ABDI. **Cadernos Temáticos – Tecnologias de Informação e Comunicação – TIC**. Serviços Convergentes de Telecomunicações. 2010. Disponível em: <<http://j.mp/1TfKKri>>. Acesso em: 1 dez. 2014.
- AHONEN, T.; HADID, A.; PIETIKÄINEN, M. Face recognition with local binary patterns. **Proceedings of the 8th European Conference on Computer Vision**, Prague, ECCV'04, p. 469–481, May 11-14, 2004.
- ALMEIDA, A. F. **Sistemas e tecnologias de informação para serviços policiais: o caso da polícia nacional de Cabo Verde**. 2009. Disponível em: <<http://bdigital.unipiaget.cv:8080/jspui/bitstream/10964/145/1/sistemas%20e%20tecnologias%20de%20informa%C3%A7ao.pdf>>. Acesso em: 1 dez. 2014.
- AZEVEDO, M. G. D.; FARIA, R. A. D. Retrato falado: a evolução do método indiciário para reconhecimento facial. In: **BRAZILIAN CONGRESS ON BIOMEDICAL ENGINEERING**, 24., 2014, Uberlândia. **Proceedings...** Curitiba: UTFPR, 2014. Disponível em: <http://www.canal6.com.br/cbeb/2014/artigos/cbeb2014_submission_757.pdf>. Acesso em: 20 jun. 2016.

- BERTILLON, A. Color of the iris. **Revue Scientifique**. France: IEEE, 2009.
- BLANZ, V.; VETTER, T. Face recognition based on fitting a 3D morphable model. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 25, n. 9, p. 1063-1074, 2003.
- BORJA, C. T.; BUENO, A. G. **Sistemas biométricos**. [S.l.: s.n.], [20??]. Disponível em: <https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo_Biometria.pdf>. Acesso em: 2 jun. 2016.
- CAULKINS, J. P. **Mathematical model of drug policy**. Pittsburgh: Repository Carnegie Mellon University, 1993.
- COOTES, F.; WALKER, K.; TAYLOR, C. J. View-based active appearance models. **Proceedings of the 4th IEEE International Conference on Automatic Face and Gesture Recognition**, Grenoble, France, FG '00, p. 227-232, 2000.
- CORTES C.; VAPNIK V. Support-vector networks. **Machine Learning**, v. 20, n. 3, p. 273-297, 1995.
- COSTA, L. R.; OBELHEIRO, R. R.; FRAGA, J. S. Introdução à biometria. **Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg2006)**. Porto Alegre, v. 1, p. 103-151, 2006.
- DE PAULO, C. A. R.; PEREIRA, M. H. R. Visão computacional aplicada em reconhecimento facial na busca por pessoas desaparecidas. **e-xacta**, v. 8, n. 2, 2015.
- DURKHEIM, E. **As regras do método sociológico**. 3. ed. Lisboa: Editorial Presença, 1987.
- GOLDSTEIN A. J.; HARMON L. D.; LESK A. B. Identification of human faces. **Proceedings of the IEEE**, v. 59, n. 5, p. 748-760, 1971.
- GRUE, A. R. **Reconhecimento facial: aplicação restrita à proteção e segurança**. 2003. Disponível em: <http://mit.universia.com.br/STS/STS035/PDF/anthony_final.pdf>. Acesso em: 10 dez. 2015.
- GUGLINSKI, V. **Leitura sequencial de impressões digitais: diminuição de fraudes em sistemas biométricos**. Teresina: Instituto Brasileiro de Direito da Informática, 2013.
- HAVRAN, C.; HUPET, L.; CZYZ, J.; LEE, J.; VANDENDORPE, L.; VERLEYSEN, M. Independent component analysis for face authentication. **Proceedings of the 6th International Conference on Knowledge-Based Intelligent Information and Engineering Systems**, KES '02, Sep. 2002.
- JAIN, A. K.; ROSS, A. A.; NANDAKUMAR, K. **Introduction to Biometrics**. New York: Springer, 2011.
- LI, S. Z.; JAIN, A. K. **Encyclopedia of Biometrics**. New York: Springer, 2009.
- LIU, C.; WECHSLER, H. Evolutionary pursuit and its application to face recognition. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 22, n. 6, p. 570-582, 2000.
- MACEDO, R. **La gran tendencia: reconocimiento facial**. 2013. Disponível em: <<http://www.cienciaeingenieria.com/2013/09/la-gran-tendencia-reconocimiento-facial.html>>. Acesso em: 24 fev. 2016.
- MAERSA. **Historia de la Biometría y la Huella Digital**. México, 2010. Disponível em: <<http://www.maersa.com.mx/historia.html>>. Acesso em: 22 fev. 2016.

- MONTIBELER, D. C. G. C.; FERNANDES, J. C. L. **Controle de acesso através dos sistemas biométricos como ferramenta de combate a fraudes**. Faculdade de Tecnologia de São Caetano do Sul. São Caetano do Sul, 2012.
- NEFIAN, A. A hidden Markov model-based approach for face detection and recognition. **PhD Thesis**, Atlanta, Georgia Institute of Technology, 1999.
- OLIVEIRA, D. R. **Reconhecimento de Faces Usando Redes Neurais e Biometria**. São José dos Campos: Instituto Nacional de Pesquisas Espaciais, 2006.
- OMAIA, D. **Um sistema para detecção e reconhecimento de face em vídeo utilizando a transformada cosseno discreta**. Departamento de Informática. Universidade Federal da Paraíba. João Pessoa, 2009.
- OTEGUI, C. A. et al. **Proyecto Aguará – Reconocimiento de Caras**. Montevideo: Facultad de Ingeniería Universidad de la República, 2006.
- PEREZ, N. L.; AGUDELO, J. J. T. **Técnicas de biometria basadas en patrones faciales del ser**. 2012. Disponível em: <<http://repositorio.utp.edu.co/dspace/bitstream/11059/2738/1/0053682L864.pdf>>. Acesso em: 3 mar. 2016.
- RIBEIRO, L. Governo financiará videomonitoramento em fronteiras. **O Estado de S.Paulo**. 14 maio 2013. Disponível em: <<http://politica.estadao.com.br/noticias/geral,governo-financiara-videomonitoramento-em-fronteiras,1031668>>. Acesso em: 1 mar. 2016.
- SAEED, K.; NAGASHIMA, T. **Biometrics and Kansei Engineering**. New York: Springer, 2012.
- SUCAR, L. H. **Visión Computacional**. Puebla, México: Instituto Nacional de Astrofísica, Óptica y Electrónica, 2010.
- TRASLAVIÑA, C. M. G. **Introducción a la biometría**. 2007. Disponível em: <http://www.academia.edu/9374109/Introduccion_a_la_biometria>. Acesso em: 24 fev. 2016.
- TUCKER, J. How facial recognition technology came to be The FBI's astonishing new identification system is the product of 175 years of innovation – and paranoia. A visual history. **Boston Globe**. 2014. Disponível em: <<https://www.bostonglobe.com/ideas/2014/11/23/facial-recognition-technology-goes-way-back/CkWaxzozvFcvQ7kvdLHGI/story.html>>. Acesso em: 1 mar. 2016.
- TURK, M.; PENTALEND. Eigenfaces for recognition. **Journal of Cognitive Neuroscience**, v.3, n.1, p. 71-86, 1991.
- VALLEJO, J. A. S.; NEIRA, J. C. S. **Diseño e implementación de un sistema de seguridad basado en reconocimiento de rostros**. 2005. Disponível em: <<http://bibdigital.epn.edu.ec/bitstream/15000/5504/1/T2481.pdf>>. Acesso em: 24 fev. 2016.
- WISKOTT, L.; FELLOUS, J. M.; KRÜGER, N.; MALSBURG, C. Face recognition by elastic bunch graph matching. In: JAIN, L. C.; HALICI, U.; HAYASHI, I.; LEE, S. B. (ed.). **Intelligent Biometric Techniques in Fingerprint and Face Recognition**, chapter 11, p 355-396. CRC Press, 1999.
- YANF, M. H. Face recognition using kernel methods. In: DIETTERICH, T. G.; BECKER, S.; GHAMRANI, Z. (ed.) **Proceedings of the Neural Information Processing Systems Conference, NIPS'01**. Vancouver, Canada: MIT Press, v.14, p. 1457-1464, Dec. 3-8, 2001.
- ZHAO, W.; CHELLAPPA, R.; KRISHNASWAMY, A. Discriminant analysis of principal components for face recognition. **Proceedings of the 3rd International Conference on Automatic Face and Gesture Recognition, FG '98**. Nara, Japan: April 14-16, 1998, p. 336-341.

9

CAPÍTULO

APLICAÇÃO DE IDENTIFICAÇÃO BIOMÉTRICA POR IMPRESSÃO DIGITAL NA LAVRATURA DO AUTO DE PRISÃO EM FLAGRANTE

Fernando Henrique Borges Ferreira

Juarez Bento da Silva

Marta Adriana da Silva Cristiano

Priscila Cadorin Nicolete

1 INTRODUÇÃO

A biometria é uma tecnologia de segurança baseada no reconhecimento de uma característica física e intransferível das pessoas, como a íris, a retina, o rosto, o sistema vascular, a palma da mão, impressão digital e a voz. Graças ao avanço tecnológico na fabricação de sensores que captam imagens digitais a um baixo custo e melhorando cada vez mais suas características, pode-se constatar o crescimento de sua utilização em diversos campos e aplicações. Um dos identificadores

biométricos amplamente utilizados é a impressão digital, principalmente nas áreas forense e policial, bem como no âmbito civil.

As tecnologias biométricas oferecem imagens que são amplamente utilizadas como uma das fontes mais importantes de informação, sobretudo no contexto das aplicações centradas no ser humano, como: vigilância de segurança, desenvolvimento de sistemas biométricos, jogos multimídia de interação homem-máquina, robótica, realidade virtual, videoconferências, indexação e codificação (EKNEL; SANKUR, 2004).

Os fundamentos do reconhecimento de impressões digitais e sua adoção para o uso forense datam do final do século XIX. Seu uso estendeu-se rapidamente e, desde então, vem sendo utilizado de forma rotineira como meio de identificação. A partir da década de 1960, começaram a serem desenvolvidos sistemas de reconhecimento automático de impressões digitais, conhecidos como *Automatic Fingerprint Identification Systems* (AFIS), cujo uso permitiu estender a utilização da impressão digital como meio de identificação para um grande número de aplicações, incluindo aplicações civis (PARZIALE; DIAZ-SANTANA; HAUKE, 2006).

O reconhecimento biométrico desempenha um papel fundamental nos processos de identificação e de verificação de identidade, sobre os quais se baseiam as políticas públicas de segurança. É de fundamental importância, por exemplo, que conste na lavratura do auto de prisão em flagrante as assinaturas das pessoas envolvidas no caso, sobretudo os policiais que efetuaram a prisão e o preso, para a validade da prisão.

A biometria, como ciência da aplicação de métodos de estatísticas quantitativas a fatos biológicos, está hoje cada vez mais sendo usada como forma de garantir a autenticidade e a segurança no reconhecimento de pessoas. Desta forma, entre os métodos de reconhecimento biométricos, pode-se destacar o reconhecimento pela impressão digital, pela voz, pela face e pela íris.

Neste contexto, o reconhecimento pela impressão digital é atualmente o mais usado, inclusive como base de trabalho. A biometria por reconhecimento pela impressão digital é feito por intermédio da leitura de depressões e estrias que formam padrões complexos, que são únicas em cada pessoa e é, assim, um excelente método de verificação.

2 AUTO DE PRISÃO EM FLAGRANTE

Um auto de prisão em flagrante é um ato administrativo que consiste na restrição da liberdade de alguém, independentemente de ordem judicial, desde que

esse alguém esteja cometendo ou tenha acabado de cometer uma infração penal ou esteja em situação semelhante prevista nos incisos III e IV, do Art. 302, do Código de Processo Penal (CPP). Em sentido jurídico, flagrante é uma qualidade do delito, é o ilícito patente que permite a prisão do autor sem mandado judicial. É a autodefesa da sociedade, segundo Mirabeti.

O artigo Art. 302 do Código de Processo Penal assim menciona:

Considera-se em flagrante delito quem:

I – está cometendo a infração penal;

II – acaba de cometê-la;

III – é perseguido, logo após, pela autoridade, pelo ofendido ou por qualquer pessoa, em situação que faça presumir ser autor da infração;

IV – é encontrado, logo depois, com instrumentos, armas, objetos ou papéis que façam presumir ser ele autor da infração.

Portanto, a prisão em flagrante exige, para sua consumação, dois elementos imprescindíveis: a atualidade e a visibilidade. A atualidade é expressa pela própria situação flagrancial, ou seja, algo que está acontecendo naquele momento ou acabou de acontecer; já a visibilidade é a ocorrência externa ao ato, isto é, a situação de alguém atestar a ocorrência do fato ligando-o ao sujeito que o pratica.

No que tange a natureza jurídica da prisão em flagrante, pode-se afirmar que se trata de uma medida cautelar processual que dispensa ordem escrita, pois independe de manifestação jurídica. No entanto, consoante o Art. 5º, LXV, da Constituição Federal (CF), a prisão deverá ser comunicada imediatamente ao juiz, para que verifique a sua legalidade e, caso não aconteça, esta deverá ser relaxada. Com a comunicação ao juiz, o ato se aperfeiçoará e seus requisitos serão homologados.

É importante a observância da formalidade sob pena de nulidade do Auto de Prisão em Flagrante. Havendo o relaxamento do Auto, este perderá sua força coercitiva e servirá como peça de informação a possibilitar, *a posteriori*, o ajuizamento da ação penal. Por isso, ao dar ciência ao preso do motivo de sua prisão, elabora-se a nota de culpa. É um requisito extrínseco do Auto de Prisão em Flagrante, sendo que a ausência da entrega ou omissão desse ato essencial ocasionará o relaxamento da prisão.

Por fim, efetua-se a lavratura do Auto de Prisão em Flagrante, que nada mais é que um ato formal, em que, após capturado, o agente da prática do crime é conduzido à delegacia de polícia, no qual a autoridade policial presente, após análise do fato, no que tange aos seus requisitos, o formalizará. Preso, o agente será comunicado de sua prisão e mencionado seus direitos constitucionais, con-

forme Art. 5º, incisos LXI, LXII, LXIII, LXV e LXVI da CF, e, então, realizar-se-á seu interrogatório. Quanto ao prazo a lei, nada o menciona, mas, por analogia, entende-se que o prazo máximo é de 24 horas, conforme dispõe o Art. 306 do CPP, quando prescreve sobre a nota de culpa. Também pode ser lavrado, inclusive, no dia seguinte à apresentação, desde que não ultrapasse o prazo de 24 horas, sob pena de tornar o ato ilegal por ter decorrido vários dias depois da prisão.

3 BIOMETRIA

O uso prático das impressões digitais como método de identificação de pessoas tem sido utilizado desde o final do século XIX, quando Sir Francis Galton (GALTON, 1892) definiu os axiomas básicos do reconhecimento digital, no qual eram identificados alguns dos pontos ou características por meio das quais as impressões digitais podiam ser identificadas. A digital é uma característica biométrica altamente diferenciada, e este fato, apesar de ser um dado puramente empírico, tem sido amplamente aceito (MALTONI et al., 2009).

Com a expansão do uso dos computadores ao final dos anos 1960, a identificação por meio das impressões digitais iniciou sua transição para a automatização, momento no qual foram criados os sistemas AFIS. Este processo foi também motivado pela expansão do uso das bases de dados forenses, que tornaram a indexação e a comparação manual de digitais cada vez mais complicadas devido ao grande volume de dados (RATHA; KARU; CHEN, 1996).

Com a necessidade de se criar uma tecnologia de desenvolvimento para escaneamento por impressão digital, o FBI contratou serviços da National Bureau of Sander (NBS), atualmente Institute of Standards and Technology (NIST), que veio a dar certo com a criação do escâner, extraíndo os pontos de impressão digital e comparando/confrontando listas de impressões com um banco de dados de impressões digitais. Dessa forma, o FBI criou em 1975, a tecnologia de desenvolvimento para escaneamento de impressão digital. Essa técnica era utilizada para captar e coletar impressão digital (RATHA; BOLLE, 2007).

4 CONCEITO E FUNCIONAMENTO

A palavra *biometria* que vem do grego – *bios* (vida) + *metron* (medida) –, o que significa um estudo das qualidades comportamentais e físicas do ser humano. Atualmente, o termo refere-se ao uso do corpo (impressão digital) em mecanismos de identificação. Segundo o dicionário Michaelis, biometria é a ciência da aplicação de métodos de estatísticas quantitativa a fatos biológicos (MICHAELIS, 2016).

Assim, é possível afirmar que a biometria é uma característica física, única e medível de uma pessoa, ou seja, os seres humanos possuem algumas dessas caracte-

terísticas que podem ser unicamente identificadas, sendo elas, por exemplo, a impressão digital, a retina, a íris, formação da face e a geometria da mão. Portanto, o ponto divergente em relação a outras formas de identificação, como a senha ou o cartão inteligente, é que com a biometria não é possível perder ou esquecer tais características (LIMA, 2016).

Basicamente, todos os sistemas biométricos trabalham da mesma forma: o primeiro passo para o reconhecimento de uma pessoa se dá no cadastro das informações biométricas dessa pessoa, sejam elas dados de impressão digital, íris, voz. Essas informações são coletadas, transformadas em um código digital (numérico ou alfanumérico) e, depois, armazenadas em um banco de dados. Após o armazenamento dessas informações, o sistema já é capaz de reconhecer esta pessoa por meio de uma comparação dos dados recolhidos no instante da solicitação de reconhecimento e dados armazenados no banco de dados (BORJA; BUENO, [20??]).

Esses sistemas devem apresentar três características importantes no que tange ao seu funcionamento, que são: [1] precisão e desempenho; [2] aceitabilidade, que indica o nível de aceitação do sistema de reconhecimento biométrico por parte de seus usuários; e [3] proteção (MACHADO; ALMEIDA JUNIOR, 2015).

O objetivo é determinar a quem pertence uma ou mais impressões a partir da comparação com o banco de dados disponível. Funciona com a captura da imagem da impressão digital por intermédio de um leitor por meios ópticos, imagem digitalizada. Logo em seguida, o sistema compara os dados registrados com aqueles obtidos a partir da digitalização da imagem identificando suas características datiloscópicas.

5 IMPRESSÃO DIGITAL COMO IDENTIFICADOR BIOMÉTRICO

Este artigo se detém à impressão digital, e como tal, vale destacar que as cristas digitais dos dedos, das palmas das mãos e pés são formadas no sexto mês de gestação e permanecem invariantes ao longo de toda a vida de uma pessoa. Isto torna as impressões digitais um traço biométrico muito atraente para os sistemas de reconhecimento. Seu alto grau de aceitação faz com que seu uso seja muito estendido em aplicações comerciais, porém também no âmbito forense, no qual auxilia na identificação de criminosos que deixam suas impressões na cena de um crime. A unicidade das impressões digitais é assumida totalmente, em que pese ser um fato concebido a partir de dados empíricos (JIMENEZ, 2011).

A identificação digital, ou datiloscopia, tem sido um método amplamente utilizado durante as últimas décadas para a identificação de pessoas, quer para fins civis ou policiais. O estudo comparativo das impressões digitais (aquelas tomadas de forma voluntária e com material adequado nos departamentos de polí-

cia ou registro civil) e marcas de digitais (deixadas involuntariamente em um local de crime) tem levado ao auxílio da resolução de casos judiciais, em que tais traços biométricos se constituíram em evidência inegável da presença de um determinado sujeito na cena de um delito.

O padrão da impressão digital, ou datilograma, pode ser analisado a partir de três níveis. O Nível 1 determina a forma geral do datilograma. Para isso, deve ser identificado o núcleo e o delta. O núcleo é o ponto que se encontra mais ao norte da crista mais interna da digital, e o delta corresponde a uma estrutura do tipo triangular, formada por três orientações de cristas, que divergem em um ponto. É produzida pela intersecção das três zonas da impressão digital: a zona basilar, a zona nuclear e a zona marginal (HENRY, 1900).

Segundo a presença e a distribuição de núcleo e deltas, são obtidos diferentes tipos de datilogramas: monodeltos (um único delta), bideltos (dois deltas) e adeltos (não contém deltas) etc. O tamanho e a forma da impressão digital e a orientação do fluxo de cristas são incluídos também como características pertencentes a este nível.

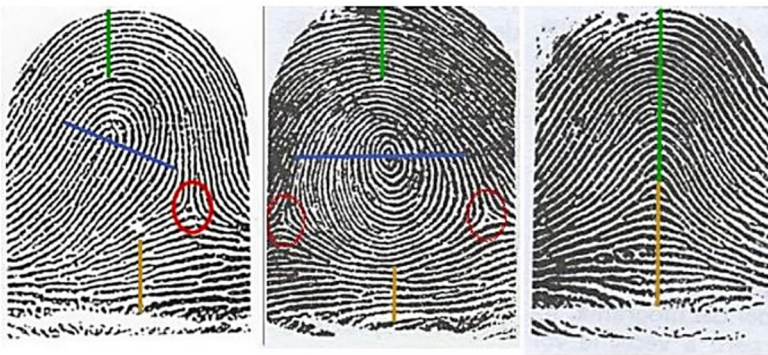


Figura 9.1 Exemplos de digitais do tipo monodelto, bidelho e adelho.

Fonte: Merysnow (2016).

O Nível 2 apresenta alguns tipos de singularidades locais nas impressões digitais, denominadas minúcias (*minutiae*, em inglês). Os tipos de minúcias que aparecem com maior frequência são: bifurcação ou convergência (ponto em que uma crista divide-se em duas) e terminação abrupta (final de uma crista). A localização destes pontos característicos e sua distribuição e orientação são a chave da unicidade das impressões digitais (LLORET, 2013).

O Nível 3 é o mais detalhista e faz uso das características internas de cada crista, que podem ser espessura, localização dos poros da pele dentro destas, forma etc.

Também existem outras formas diferentes de analisar o datilograma dependendo do formato e da situação em que este se apresenta. É possível observar diretamente sobre o dedo, ao natural, ou se pode capturar por meio de diversos métodos sobre uma superfície, quer seja em um ambiente controlado, de forma voluntária e intencionado, para marcar a digital (impressões digitais) ou de forma menos visível e normalmente acidental em uma cena que esteja sendo analisada (latente).

Para a identificação digital no âmbito forense, no campo da datiloscopia, a palavra identificação é sinônimo de individualização e representa a certeza de que uma característica particular foi feita pelas cristas papilares da pele de um determinado indivíduo. A identificação da referida amostra é realizada mediante a análise das características extraídas (CHAMPOD et al., 2004).

Para poder confirmar a identificação de uma impressão digital, é necessário estabelecer alguns critérios prévios que definem o protocolo de atuação. Esse protocolo deve recolher um convênio comum para emparelhar digitais anônimas com outras já identificadas. O objetivo é conseguir que a identificação dos autores das amostras seja justa, imparcial e, principalmente, correta (LÓPEZ GARCÍA, 2009).

O criminalista Edmond Locard enunciou a primeira regra, que estabelecia um número mínimo de minúcias coincidentes necessárias para a identificação de uma impressão digital anônima. Em 1911, ele iniciou um debate para criar um padrão numérico para a identificação forense de impressões digitais. A partir desse debate foram propostas as seguintes regras (CHAMPOD et al., 2004):

- 1) Se forem encontradas mais de 12 minúcias coincidentes e a impressão anônima for nítida, então a identificação será positiva (na ausência de diferenças significativas).
- 2) Se forem constatados entre oito e 12 pontos coincidentes, e a confirmação da identidade dependerá da:
 - a nitidez da marca;
 - a raridade da impressão digital;
 - a presença de núcleo e deltas;
 - a presença de poros;
 - a semelhança da marca e da impressão quanto à largura das cristas e aos vales, sua orientação e o valor angular das bifurcações.
- 3) Se existirem menos de oito minúcias coincidentes, não é possível considerar a identificação da digital, fato pela qual será classificada como não conclusiva.

Estas regras foram amplamente aceitas pela comunidade datiloscópica forense, ainda que, infelizmente, a terceira regra seja constantemente ignorada. Atualmente, o processo de identificação das impressões digitais tem evoluído muito,

geralmente podendo variar entre países ou continentes, em um processo de quatro passos, conhecido no Brasil como “confronto papiloscópico”, no qual o papiloscopista realiza análise, comparação, avaliação e verificação da compatibilidade entre a impressão questionada e a impressão padrão, disponível em um banco de dados de impressões digitais (CHAMPOD et al., 2004).

Em geral, o passo de avaliação pode seguir duas vertentes: limiar qualitativo ou limiar quantitativo. O limiar qualitativo é mais utilizado nos Estados Unidos. É uma abordagem que defende a postura de que cada processo de identificação representa um conjunto único de circunstâncias e não se pode reduzir todo o problema de individualização a um simples número fixo de características coincidentes, fato pelo qual este conceito de identificação não pode ser reduzido apenas a contagem de minúcias das digitais (WEIN; BAVEJA, 2005).

Por outro lado, a abordagem de limiar quantitativo é a tendência mais comum na maioria dos países europeus e sul-americanos. Consiste em fixar um número mínimo de minúcias coincidentes entre duas impressões digitais para a identificação, tal como estabelecem as regras de Locard. Mesmo seguindo este critério, ainda existem variações entre o número de minúcias fixado em cada país, variando entre as sete da Rússia e as 16 da Itália, sendo 12 na maioria dos países (LI, 2009).

6 SISTEMAS FORENSES DE IDENTIFICAÇÃO DIGITAL

Como mencionado anteriormente, os sistemas biométricos utilizados no âmbito forense são, em sua grande maioria, sistemas de identificação. Sua diferença em relação aos sistemas comerciais é que, neste caso, o indivíduo que aporta a característica biométrica não deseja ser identificado, fato pelo qual não há um nome associado à amostra.

Sem dúvida, a única diferença que existe em relação aos sistemas de verificação é o número de comparações que é necessário realizar antes de extrair um resultado. No caso dos sistemas de verificação, ao dispor de uma identidade associada à amostra, somente é necessário realizar uma comparação entre as duas amostras que supostamente pertencem ao mesmo indivíduo, para verificar que efetivamente é assim. Deste tipo de sistema, obtém-se um resultado de confirmação ou de negação.

Porém, no caso dos sistemas de identificação é diferente; são realizadas tantas comparações com amostras quanto se disponha na base de dados. O resultado será uma lista ordenada com o valor do score entre a digital da qual se deseja obter a identidade e o resto das amostras da base de dados. Ou seja, a lista mostrará do maior para o menor, quais são as identidades com as quais mais se parece a digital pesquisada e as que tem maior probabilidade de acerto.

Para poder extrair um resultado ao comparar duas impressões digitais, tanto nos sistemas de verificação como nos de identificação, é necessário realizar um determinado processo composto de várias tarefas. Em geral, um sistema de reconhecimento de impressão digital é composto de duas partes diferenciadas: o extrator de características e o comparador.

No que tange à extração de características, considera-se que a imagem de uma impressão digital é um mapa de cristas e vales papilares da pele. Um sistema de reconhecimento de impressões digitais compara duas impressões por meio de um exame das características das cristas e dos vales para decidir se pertencem ou não à mesma fonte (RATHA; BOLLE, 2007).

Após a extração das características, vem a etapa de comparação ou *matching*, que é uma das fases mais críticas no funcionamento de um sistema de reconhecimento de impressões digitais, em geral em qualquer sistema biométrico. A principal dificuldade é a grande variabilidade que reside na captura da amostra. A característica biométrica em si permanece invariante, porém a forma de capturá-la interfere nas características de cada amostra. Em especial nas imagens das digitais, pode-se variar a espessura das cristas, já que se vê alterada pela pressão exercida sobre a superfície, a orientação, o deslocamento, a curvatura da superfície, o estado da pele, entre outros fatores (RATHA; BOLLE, 2007).

Portanto, um sistema forense de reconhecimento de impressões digitais será um sistema biométrico de identificação, que recebe uma imagem de uma digital sem identificar e devolve, após a extração de características e comparação com uma base, uma lista dos candidatos de maior pontuação obtida e que serão analisados posteriormente por um especialista humano. Esses sistemas são conhecidos como AFIS.

7 EXTRAÇÃO DE CARACTERÍSTICAS, COMO É FEITO NO BRASIL?

No início do século XX, as impressões digitais começam a ser utilizadas profusamente na ciência forense, facilitando a ação policial na identificação criminal. Isto leva à criação de bases de dados contendo digitais em todos os países, que experimentam um aumento considerável no número de digitais e, portanto, requerem um número crescente de especialistas para sua avaliação e comparação. Vários países e governos visualizam a imperiosa necessidade de criar sistemas de reconhecimento automático de impressões digitais (AFIS) e, assim, diversas pesquisas neste âmbito são iniciadas em meados do século XX (FINDLAW, 2016).

Esse conhecimento científico gerado desde cedo, unido à ampla utilização da impressão digital no âmbito forense e policial, impulsionou o estudo e o desenvolvimento dos AFIS. Esse avanço é visualizado, por exemplo, nos sensores

de impressões digitais existentes no mercado, já que existe uma gama de sensores com variedades de qualidade de imagem, técnicas de captura das imagens e preço. Esse avanço técnico e sua ampla aceitação provocaram a ampliação do uso da impressão digital do âmbito forense/policial para o âmbito de aplicações civis, entre as quais se pode destacar o controle de acesso a ambientes.

A imagem é obtida por dispositivos eletrônicos especiais, a qual está baseada em quatro tecnologias: ótica, capacitiva, térmica e ultrassônica. Na ótica, *Frustrated Total Internal Reflection* (FTIR), a superfície da aquisição de 1" × 1" é convertida em imagens de cerca de 500 dpi. Assim, a luz refletida dependerá da pele e das imagens saturadas ou difusas, que podem ser obtidas de peles molhadas e secas. Denota-se que a imagem coletada na forma de ótica é a maneira mais antiga de obtenção de imagens ao vivo (VIOLA, 2006).

Na capacitiva, as cristas e os vales da pele da ponta dos dedos criam diferentes acumulações de carga quando o dedo toca uma rede de chips CMOS. Utilizando uma eletrônica adequada, a carga é convertida em um valor de intensidade de um pixel. A superfície de aquisição de 0,5" × 0,5" é convertida em uma imagem de cerca de 500 dpi. Esses dispositivos são sensíveis e a qualidade das imagens é suscetível a pele seca e molhada.

Já a tecnologia térmica é baseada no fato de que a pele é um condutor de calor melhor do que o ar. O contato com as cristas da pele causa uma alteração observável na temperatura da superfície do sensor. É melhor do que a ótica e capacitiva, no que tange aos problemas de pele seca e molhada. Por outro lado, a imagem de 500 dpi, não é rica em cores preto e cinza.

Por fim, a tecnologia ultrassônica que se baseia em um feixe ultrassônico dirigido à superfície do dedo para medir diretamente a profundidade dos sulcos com base no sinal refletido. A oleosidade da pele não afeta a imagem obtida, que reflete bastante bem a topologia dos sulcos. Mas essas unidades tendem a ser grandes e requerem um tempo de leitura maior do que os leitores óticos.

No tocante ao processo de comparação, este é amplamente baseado em métodos desenvolvidos por especialistas humanos. Os especialistas avaliam três fatores para informar que duas impressões digitais pertencem ao mesmo dedo. São elas: concordância na configuração global do padrão, isto é, distribuição do núcleo e dos deltas, que denota que as impressões digitais são do mesmo tipo; concordância qualitativa, cujos detalhes de minúcias devem ser idênticos; e suficiência quantitativa, que especifica que ao menos determinado número de detalhes de minúcias deve ser encontrado (com mínimo de 12). Ocorrendo similaridade entre duas impressões digitais de um mesmo dedo, a abordagem deve se basear entre: translação, rotação, pressão aplicada e distorção elástica da pele (COSTA; OBELHEIRO; FRAGA, 2006).

Os pontos fortes usados na tecnologia de autenticação biométrica por pressão digital são a precisão e a existência de banco de dados legados de impressões digitais. A impressão digital pode ser colhida facilmente a baixo custo. Quanto aos pontos fracos, estes podem ser, por exemplo, a não aceitação da técnica por questões de higiene, entre outros. Assim, a qualidade das impressões digitais varia enormemente dentro de uma população. Por outro lado, os sensores mais baratos podem comprovadamente ser falsificados e fraudados (BASTOS et al., 2016).

Vale ainda destacar que, no sistema biométrico, há falhas e vantagens no que diz respeito a grau de certeza ou probabilidade de erro, facilidade de aplicação, custos, rapidez de resposta, entre outros parâmetros. Os sistemas biométricos não estão totalmente imunes a falhas de segurança e todos os sistemas de reconhecimento biométrico, em princípio, estão sujeitos a ataques e fraudes em maior ou menor grau. Dessa forma, os módulos de aquisição, extração, comunicação podem representar algum tipo de vulnerabilidade em função de como os sistemas biométricos foram projetado e são utilizados. Os módulos de aquisição são considerados os menos vulneráveis do sistema de identificação (FRÍAS; EDUARDO, 2004).

8 CONCLUSÃO

No caso do Auto de Prisão em Flagrante, a autorização seria concedida ao policial responsável pela lavratura, ou seja, o delegado e o escrivão de Polícia, por sua vez autorizados, seriam registrados nos bancos de dados do sistema. Feita a autorização no sistema, o acesso seria livre para utilização do sistema biométrico por impressão digital, após a lavratura do Auto. O acesso também poderia ser feito de outra forma que não por pessoas, e sim, por exemplo, por um programa acessando um arquivo. Para isso, deverá ser concedido a integridade, a confidencialidade e a disponibilidade da informação, cuja função é garantir que os dados não sejam corrompidos e que somente as pessoas autorizadas os acessem, de modo que eles estejam disponíveis às pessoas competentes sempre que necessário. Com a integridade, garante-se a exatidão dos dados.

Por fim, o uso da biometria por impressão digital na identificação civil está sendo usada no Brasil na maioria dos estados, incluindo Santa Catarina. No entanto, quanto à aplicação na identificação penal, isto ainda não ocorre, pois faltam recursos tecnológicos para seu uso. Embora exista um banco de dados com muitas informações, o sistema ainda não se comunica com os demais órgãos, o que torna prejudicada a aplicação da biometria por impressão digital na identificação penal por enquanto. É bom lembrar que os Estados Unidos, por exemplo, já aplicam o sistema AFIS na identificação de criminosos, elucidando com mais agilidade os delitos que ocorrem.

Diante disso, é possível afirmar que a aplicação da biometria por impressão digital após a lavratura do Auto de Prisão em Flagrante é possível e legal sob o ponto de vista legislativo brasileiro, além de seguro e ágil.

REFERÊNCIAS

- BASTOS, J. M. P. et al. **Biometria Impressões digitais**. Disponível em: <<http://jpconsultoria.com.br/Seguranca/index.html>>. Acesso em: 28 fev. 2016.
- BORJA, C. T.; BUENO, A. G. **Sistemas biométricos**. [S.l.: s.n.], [20??]. Disponível em: <[https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo Biometria.pdf](https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf)>. Acesso em: 28 fev. 2016..
- CHAMPOD, C.; LENNARD, C.; MARGOT, P.; STOILOVIC, M. **Fingerprints and Other Ridge Skin Impressions**. New York: CRC Press, 2004.
- BRASIL. Constituição Federal. **Código Penal e Código de Processo Penal**. 16. ed. São Paulo: Atual, 2014.
- COSTA, L. R.; OBELHEIRO, R. R.; FRAGA. Introdução à Biometria. **Minicursos do VI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'2006)**, Santos, ago. 2006, p. 103-151.
- EKENEL, H.; SANKUR, B. Feature selection in the independent component subspace for face recognition. **Pattern Recognition Letters**, v. 25, n. 12, p. 1377-1388, 2004.
- FINDLAW. **Fingerprints: the first ID**. 2016. Disponível em: <<http://criminal.findlaw.com/criminal-procedure/fingerprints-the-first-id.html>>. Acesso em: 29 fev. 2016.
- FRÍAS, Z.; EDUARDO, X. **Diseño e implementación de un prototipo para autenticación, autorización y conteo (AAA) para el control de asistencia de los empleados de la Escuela Politécnica Nacional por medio de huellas dactilares**. 2004. Disponível em: <<http://bibdigital.epn.edu.ec/bitstream/15000/5487/1/T2349.pdf>>. Acesso em: 29 fev. 2016.
- GALTON, F. **Finger Prints**. London: Macmillan, 1892. Disponível em: <<http://www.clpex.com/Information/Pioneers/galton-1892-fingerprints-lowres.pdf>>. Acesso em: 20 jun. 2016.
- HENRY, E. **Classification and Uses of Finger Prints**. London: Routledge, 1900.
- JIMENEZ, V. E. J. **Crestas papilares**. 2011. Disponível em: <<http://pt.scribd.com/doc/64679879/CRESTAS-PAPILARES#scribd>>. Acesso em: 1 mar. 2016.
- LI, S. Z. **Encyclopedia of Biometrics: I-Z**. New York: Springer Science & Business Media, 2009.
- LIMA, A. C. de. **Biometria**. Monografia. 2016. Disponível em: <<http://superclickmonografias.com/blog/?p=48>>. Acesso em: 28 fev. 2016.
- LLORET, F. R. **Laboratorio Forense**. Espanha: Universidade de Alicante, 2013.
- LÓPEZ GARCÍA, J. **Algoritmo para la identificación de personas basado en huellas dactilares**. 2009. Disponível em: <<http://upcommons.upc.edu/handle/2099.1/8082>>. Acesso em: 1 mar. 2016.
- MACHADO, V. S.; ALMEIDA JUNIOR, J. R. **Sistemas de reconhecimento biométrico**

aplicados à segurança de ambientes físicos. 2015. Disponível em: <<ftp://www.linorg.cirp.usp.br/pub1/SSI/2003/A03.pdf>>. Acesso em: 29 fev. 2016.

MALTONI, D.; MAIO, D.; JAIN, A. K.; PRABHAKAR, S. **Handbook of fingerprint Recognition.** New York: Springer, 2009.

MERYSNOW. **Dime cómo es tu huella dactilar y te diré quién eres.** 2016. Disponível em: <<http://www.mianamnesia.com/2011/12/dime-como-es-tu-huella-dactilar-y-te-dire-quien-eres/>>. Acesso em: 28 fev. 2016.

MICHAELIS. **Biometria.** 2016. Disponível em: <<http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=biometria>>. Acesso em: 28 fev. 2016.

MIRABETE, J. F. **Código de Processo Penal Interpretado.** São Paulo: Atlas, 2001.

MIRABETE, J. F. **Processo Penal.** 3. ed. rev. e atual. São Paulo: Atlas, 1994.

PARZIALE, G.; DIAZ-SANTANA, E.; HAUKE, R. The surround imager: a multicamera touchless device to acquire 3D rolled-equivalent fingerprints, proceedings of international conference on biometrics. Lecture Notes. **Computer Science**, LNCS, v. 3832, p. 244-250. 2006.

RATHA, N.; BOLLE, R. **Automatic fingerprint recognition systems.** New York: Springer Science & Business Media, 2007.

RATHA, N.; KARU, K.; CHEN, S. A real time matching system for large fingerprint database. **IEEE Trans.on Pattern Analysis and Machine Intelligence**, v. 18, p. 799-813, 1996.

VIOLA, F. M. **Estudo sobre formas de melhoria na identificação de características relevantes em imagens de impressão digital.** 2006. 138 f. Dissertação (Mestrado) - Curso de Programa de Pós-graduação em Computação, Instituto de Computação, Universidade Federal Fluminense, Niterói, 2006.

WEIN, L. M.; BAVEJA, M. **Using fingerprint image quality to improve the identification performance of the U.S. Visitor and Immigrant Status Indicator Technology Program.** 2005. Disponível em: <<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1111891/>>. Acesso em: 1 mar. 2016.

10

CAPÍTULO

PROPOSTA DE UM SISTEMA DE GESTÃO PARA FISCALIZAÇÃO AMBIENTAL

*Laudelino Joaquim
Luciana Bolan Frigo
Eliane Pozzebon*

1 INTRODUÇÃO

As organizações responsáveis em preservar o meio ambiente, de modo equilibrado e que forneça qualidade de vida para as pessoas, precisam buscar técnicas para reduzir a degradação e recuperar o dano já ocasionado. Para que isso torne-se possível, são necessárias estratégias que permitam a evolução econômica e financeira sem o comprometimento das fontes de recursos naturais.

Apesar do grande investimento em pesquisas para o desenvolvimento de novas técnicas na agricultura visando ao aumento da produtividade por hectares, muitos agricultores também buscam ampliar sua área de plantio, objetivando a

elevação de sua renda e, em muitos casos, sem que haja qualquer preocupação com o dano ambiental gerado.

Considera-se que na contra mão do mau uso destas técnicas e tecnologias estão os órgãos ambientais de fiscalização. Em Santa Catarina, as duas principais instituições responsáveis pela fiscalização ambiental são a Fundação de Amparo à Tecnologia e ao Meio Ambiente (Fatma) e a Polícia Militar Ambiental (PMA). O principal cenário deste trabalho é a cidade de Maracajá e região, onde não há sistema que registre ou controle a área utilizada no avanço agrícola nem a mensuração dos danos ocasionados. Mesmo quando esses danos são diagnosticados, tais órgãos ambientais não possuem ferramentas computacionais adequadas que os auxiliem no processo de monitoramento das atividades realizadas, como a recuperação dos danos ambientais.

A maioria dos documentos é preenchida manualmente, aumentando a possibilidade de erros e de inconsistência nos dados, o que dificulta o acompanhamento das infrações. Os principais setores produtivos na região de Maracajá, com importante impacto ambiental, são a rizicultura, o agronegócio (frigoríficos de frangos e suínos) e a extração de minerais (carvão, argila e areia), e estes setores estão crescendo e, por vezes, adotando estratégias ilegais que lhes proporcionem vantagens em relação aos órgãos ambientais de fiscalização e controle. A falta de um sistema de gestão para registro, organização e controle das atividades rotineiras da PMA, que forneça informações precisas das áreas que estão sendo mais afetadas, a frequência e expansão do dano, prejudica o desempenho da Polícia Militar Ambiental e facilita a degradação do meio ambiente.

O objetivo deste trabalho é propor um sistema computacional de gestão ambiental, que possa ser aplicado pela Polícia Militar Ambiental em Santa Catarina.

2 METODOLOGIA

Foi realizada uma pesquisa junto aos órgãos ambientais de todo o Brasil que, de alguma forma, possam auxiliar no diagnóstico e contribuir para um sistema de gestão ambiental mais eficaz. Para tanto, serão contactados aos seguintes segmentos de fiscalização:

- a) unidades de Polícia Militar Ambiental, instaladas na Região Sul e em algumas de outras regiões do país;
- b) unidades da Polícia Militar Ambiental de Santa Catarina, instaladas em 18 cidades do estado e que tem como missão atender aos 295 municípios catarinenses;
- c) fundações, secretarias e departamentos de meio ambiente, instalados nos 27 municípios que compõem a Associação dos Municípios do Extremo Sul Catarinense (Amesc) e Associação dos Municípios da Região Carbonífera (Amrec).

3 FUNDAMENTAÇÃO TEÓRICA

Há acerca de 50 anos, grande parcela da população não tinha nenhuma preocupação com a qualidade do meio ambiente, pois entendia que os recursos naturais eram infinitos e que não haveria motivo para preservar ou fazer uso consciente desses recursos. Ao longo dos anos, o homem começou a perceber que dependia, sim, da qualidade do meio ambiente para que sua vida fosse também mantida em boas condições.

Em 1972 aconteceu a Conferência de Estocolmo. Desde então, o Brasil e outros países nunca mais foram os mesmos em relação à preservação ambiental, apesar de, nesta conferência, os países ricos e pobres não terem conseguido entrar em acordo. Passado algum tempo desde o Protocolo de Quioto, foi realizado um acordo para controle na emissão de poluentes e que cada nação deveria realizar ações e cooperar para que o meio ambiente fosse respeitado (CURI, 2012).

Na década de 1990, a gestão ambiental virou assunto para a ISO. Foi nesta época que nasceu a família ISO 14000, com o objetivo de nortear o ciclo de vida dos produtos, as auditorias e o Sistema de Gestão Ambiental (SGA), entre outras questões ligadas ao meio ambiente. As normas ISO 14000 não são leis; elas têm como objetivo principal ajudar as empresas a seguirem o rumo mais adequado para a sustentabilidade. A norma sobre SGA ficou conhecida no Brasil como NBR ISO 14001 – Sistema de Gestão Ambiental, sendo a única norma da série 14000 que oferece certificação (OMETTO; FILHO; PERES, 2013).

Faz parte da gestão ambiental dos órgãos licenciadores o Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (Ibama) e a Fundação de Amparo à Tecnologia e ao Meio Ambiente (Fatma). Em Santa Catarina, há a cobrança de que o interessado na obtenção da licença realize um relatório técnico, chamado Estudo de Impacto Ambiental (EIA), que avalia as consequências para o ambiente decorrente de um determinado projeto. O EIA, ao contrário ao que o nome sugere, não se limita às questões do meio ambiente. No Art. 1º da Resolução do Conselho Nacional do Meio Ambiente (Conama) de 1986, define como impacto ambiental qualquer alteração de natureza química, física e biológica do meio ambiente, bem como contra a saúde, segurança e bem-estar da população (PHILIPPI; ROMÉRO; BRUNA, 2010).

Na Polícia Militar Ambiental de Santa Catarina, existe um setor denominado Gestão de Educação Ambiental (GEA), que é responsável pelo suporte às unidades operacionais instaladas nos municípios, com o objetivo de organizarem e desenvolverem atividades educativas para serem levadas até as escolas conscientizando crianças e adolescentes. Os programas educativos atualmente existentes na PMA/SC são as Palestras em Sala de Aula, com uso de cartilhas de temas voltados ao meio ambiente, bem como o carro-chefe, o Projeto Protetor Ambiental

(Proa), que contempla adolescentes de 12 a 14 anos com aulas no contraturno de seu ensino regular durante um semestre letivo.

4 GESTÃO AMBIENTAL NA POLÍCIA MILITAR DE MARACAJÁ

Na Polícia Militar Ambiental de Maracajá, as ocorrências recebidas via telefone são cadastradas em um base de dados elaborada por integrantes da própria unidade, com auxílio do software e aplicativo de banco de dados denominado Access, parte integrante do pacote Office, da Microsoft. As ocorrências são filtradas para, então, serem encaminhadas a uma guarnição para a fiscalização da referida solicitação.

As ocorrências também podem ser recebidas via ofício do Ministério Público Federal, do Ministério Público Estadual, das Delegacias de Polícia Civil, bem como por meio do Net Denúncia, um serviço disponibilizado no site da Polícia Militar de Santa Catarina, conforme mostra a Figura 10.1, no qual o cidadão pode registrar sua denúncia, de qualquer natureza, inclusive os crimes contra o meio ambiente, não havendo a necessidade de identificação do denunciante.

Você está em: > Cidadão > Contato

Outros ▾

Anônimo

pmapmapma@pm.sc.gov.br

pmapmapma@pm.sc.gov.br

CRIME AMBIENTAL

Presenciei na manhã de hoje, dia 18/06/2015, próximo ao mercado do **Joca**, na localidade de Morro Grande, na cidade de Turvo, o corte de mata nativa. Estão desmatamento um área de dois hectares de figueira, peroba e outras tipos de madeiras.
Solicito providência com urgência.

Digite » 5951 Enviar

Figura 10.1 Formulário para Net Denúncia da PM/SC.

Após o cadastramento, a solicitação é repassada para uma guarnição de serviço que vai até o local do suposto cometimento da infração ambiental. Sendo confirmado o crime ambiental, a equipe de fiscalização confeccionará os documentos de acordo com cada situação.

Os documentos costumeiramente preenchidos em um atendimento que flagram o delito ambiental são:

- 1) Auto de Infração Ambiental (AIA);
- 2) Termos de Embargos e Interdição (TEI);
- 3) Termos de Apreensão e Depósito (TAD);
- 4) Auto de Constatação (AC).

Ao término do atendimento das solicitações, o responsável pela guarnição de serviços confeccionará o relatório de serviço realizado, alimentará o sistema Access do cadastro das denúncias recebidas e fará a inserção dos documentos (AIA, TEI e TAD) em um sistema denominado GAIA, gerido pela Fatma para controle dos processos administrativos. Quando necessário, o AC será devidamente registrado em livros de protocolo da PMA, para posterior envio, via ofício, ao órgão solicitante.

Durante as pesquisas realizadas, não foi possível identificar nenhum estado brasileiro com um sistema computacional de gestão ambiental para o processo de ocorrências ambientais, sendo que cada unidade cria seu próprio meio de cadastro, gerenciamento e controle de suas ocorrências, e que, dessa forma, não há controle da situação atual dos danos ambientais no Brasil. Quando encontramos informativos com alguns dados de danos ambientais, estes dados nunca são reais e, sim, estimativos, pois não há sistema de controle devidamente instalado para gerir tais informações.

Dentre as situações identificadas, destaca-se a PMA de Foz do Iguaçu, no Estado do Paraná, que ainda registra a denúncia de um possível crime ambiental (comércio ilegal de lenha), conforme apresenta a Figura 10.2.

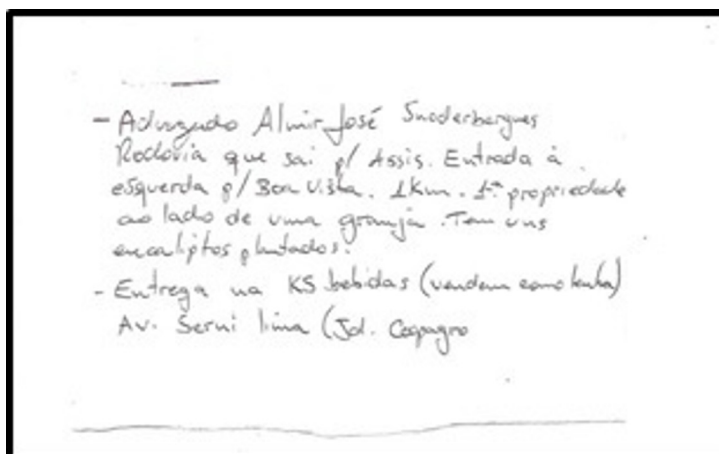


Figura 10.2 Registro de denúncia ambiental.

No 2º Pelotão de Polícia Militar Ambiental de Maracajá, unidade-base para realização das pesquisas, as denúncias chegam de várias formas (Net Denúncia, ofícios do Ministério Público Estadual e Federal, telefone ou diretamente na unidade), e as informações recebidas são gerenciadas da seguinte maneira:

- 1) Net Denúncia e ofícios dos Ministérios Públicos são organizados manualmente e entregues aos agentes para atendimento.
- 1) As denúncias recebidas via telefone ou diretamente na sede da Polícia Militar em Maracajá são cadastradas em uma base de dados. Neste momento, é realizado o cadastramento de informações, imprescindível ao atendimento da denúncia (telefone do solicitante, endereço de onde estaria ocorrendo o dano ambiental e descrição do fato observado pelo solicitante).

Com as informações cadastradas, o coordenador realiza uma filtragem e prioriza o atendimento, designando uma guarnição para realizar o atendimento. Após encerrar o atendimento, o policial realiza o fechamento da denúncia, inserindo no campo “Providências Tomadas” a descrição do que foi constatado no local do fato.

Ao realizar o atendimento das denúncias, e ao ser constatado que o fato configura crime ambiental, a guarnição precisa realizar o procedimento administrativo (multa) e criminal. Vários documentos precisam ser preenchidos para o cumprimento da legislação, que podem alterar o valor da multa a ser aplicada ao autuado pelo cometimento do crime ambiental.

É evidente e urgente a necessidade de um sistema de gestão ambiental voltados aos órgãos de fiscalização.

5 SISTEMA PROPOSTO

Propõe-se um sistema computacional de gestão ambiental voltado aos órgãos de fiscalização ambientais. Os requisitos do sistema foram levantados, usando técnicas de elicitação, como entrevista e análise de documentos (SOMMERVILLE, 2007), junto à Polícia Militar Ambiental de Maracajá, que almeja realizar uma gestão mais eficiente de suas atividades rotineiras.

O sistema deverá permitir o cadastramento de denúncias (Figura 10.3) e, em seguida, o coordenador realizará a filtragem dos fatos, priorizando os atendimentos mais urgentes (vazamento de produto tóxico, desmatamento, caça, extração de minerais etc.), para, então, determinar que uma guarnição desloque-se até o local do suposto dano ambiental e possa apurar os fatos. Neste estágio do processo, o sistema deveria possuir um módulo de sistema móvel (sistema compacto que rodaria com facilidade em um tablet utilizado pela guarnição), sendo que neste

sistema móvel (Figura 10.4) estariam as mesmas funções do sistema principal para fechamento de ocorrência e geração do processo administrativo (AIA, TEI, TAD etc.).

Figura 10.3 Cadastro de denúncia ambiental.

Serão inseridos os dados informados pelo solicitante, que gerarão a base de ocorrências a serem atendidas.

Figura 10.4 Preenchimento de AIA.

Ao inserir as informações no sistema, será possível preencher todos os documentos sem a necessidade de retrabalho que ocorre com o preenchimento manuscrito.

É importante ressaltar que tal sistema deveria ter seu funcionamento também no modo off-line, pois as atividades da PMA, em geral, são realizadas em áreas rurais, nas quais, muitas vezes, não existem conexões com redes de transmissão de dados, sendo que o agente fiscalizador faria todo procedimento em seu equipamento eletrônico como se estivesse na base da PMA e, ao chegar a locais com acesso às redes de comunicação, o sistema automaticamente faria a sincronização e passaria todas as informações aos servidores e o fato apurado estaria liberado ao acesso de todos que possuem privilégio para tal pesquisa.

Para realmente atender à expectativa gerencial da unidade de PMA de Maracajá, é necessário elaborar consultas, relatórios e representações gráficas que possibilitem o mapeamento da atual situação dos crimes ambientais cometido em sua área de atuação. Portanto, será demonstrado a seguir como será realizada esta tarefa de gestão de fiscalização dos danos ambientais.

Apresentam-se as opções de consultas do sistema, sendo que a partir delas será feito o gerenciamento da incidência de crimes ambientais em determinada região de nossa área de atuação.

Será possível realizar consultas gerais por período. Para tanto, deve-se informar o período desejado e receber o resultado geral das denúncias. Há também a possibilidade de realizar consultas por município e por natureza, bem como consulta personalizada.

Para demonstrar a funcionalidade do sistema, foi criada uma tabela com 60 registros fictícios de crimes ambientais comuns na área do 2º Pelotão da Polícia Militar de Maracajá, e foram feitas algumas simulações, conforme Figura 10.5, demonstrando a gestão do cadastro de ocorrências ambientais da região, em que é possível identificar o atendimento de apenas 60% das ocorrências do período.

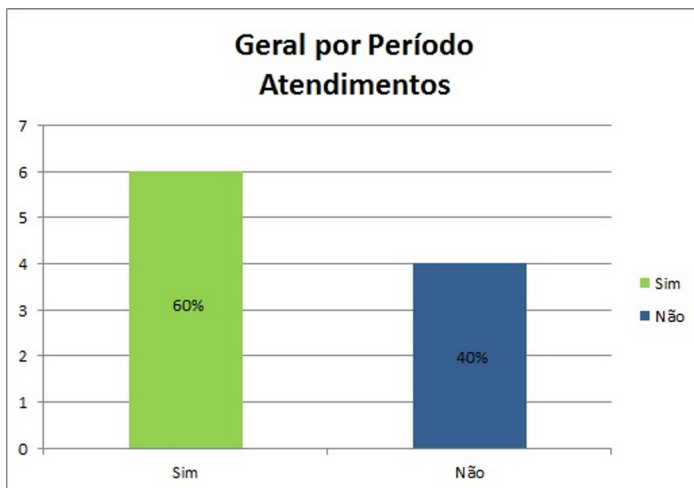


Figura 10.5 Gráfico de ocorrências por período.

Realizando uma consulta ampla, sem filtros, o sistema poderia gerar um gráfico com os 60 registros que temos em nossa base de dados e, assim, demonstrar onde estão os maiores problemas de crimes ambientais, possibilitando elaborar ações para minimizar os danos contra o meio ambiente.

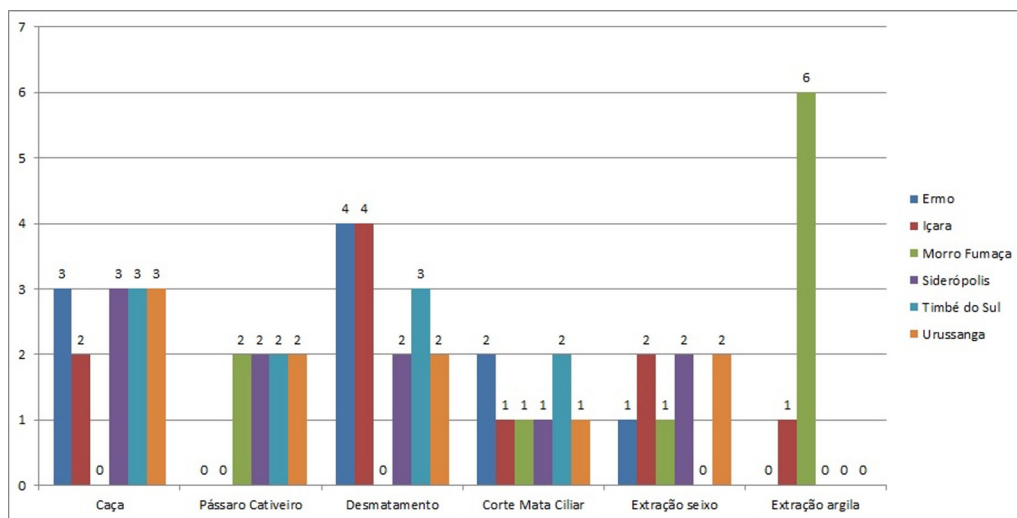


Figura 10.6 Gráfico das ocorrências por natureza e por município.

6 CONCLUSÕES

O objetivo principal deste trabalho foi de propor um sistema computacional que possa ser aplicado pela Polícia Militar Ambiental (PMA) no Estado de Santa Catarina para a gestão da fiscalização ambiental. Para que este objetivo fosse alcançado, foi necessário acompanhar e descrever as principais atividades da PMA no que tange o processo de registro e acompanhamento de processos advindos de denúncias realizadas de diferentes formas, como via web, telefone etc.

Após o levantamento dos requisitos do sistema, foi realizada uma pesquisa junto aos órgãos de fiscalização dos diversos estados da federação, com o intuito de identificar sistemas que atendessem à demanda local e que, porventura, pudessem ser adotados na sua totalidade ou com pequenas adaptações. Neste aspecto, não foi possível localizar um sistema que atendesse às necessidades da Polícia Ambiental de Maracajá e, por este motivo, fez-se necessário propor um protótipo a partir das informações obtidas na etapa de elicitação de requisitos.

É possível verificar que a demanda da Polícia Militar Ambiental é bastante específica para suas atividades diárias e que as políticas públicas não têm acompanhado essas necessidades. Com este trabalho de levantamento de requisitos e

modelagem do sistema, propõe-se como trabalho futuro a implementação de um protótipo funcional para a validação do modelo sugerido.

REFERÊNCIAS

CURI, D. *Gestão ambiental*. São Paulo: Pearson, 2012.

OMETO, A. R.; FILHO, A. G.; PERES, R. B. *Gestão ambiental de empresas*. Rio de Janeiro: Elsevier, 2013.

PHILIPPI, J. A.; ROMÉRO, M. A.; BRUNA, G. C. *Curso de Gestão Ambiental*. 1. ed. Barueri: Manole, 2004.

SOMMERVILLE, I. *Engenharia de software*. 8. ed. v. XIV. São Paulo: Pearson Addison-Wesley, 2007.

PROPOSTAS PARA INFORMATIZAÇÃO DE VIATURAS POLICIAIS COMO INSTRUMENTO DE SEGURANÇA PÚBLICA

Elbio Carlos Bock

Eliane Pozzebon

Luciana Bolan Frigo

1 INTRODUÇÃO

As viaturas policiais são elementos de uso mais efetivo para o desenvolvimento do trabalho policial. No Brasil, as viaturas possuem como equipamentos orgânicos as luzes de emergência e o rádio comunicador, servindo basicamente para o transporte de pessoal, sejam policiais ou pessoas envolvidas em ocorrências. Poucos são os estados que estão equipando suas viaturas com câmeras de vídeo e sistemas de captura de áudio.

Em outros países, como os Estados Unidos, as viaturas têm computadores, programas de registros de ocorrências, comunicação sem fio, entre outras tecno-

logias. Seria uma alternativa como meio de aprimorar a segurança pública no Brasil, colaborando, em um segundo momento, com a manutenção do respeito aos Direitos Humanos.

Este trabalho elabora uma proposta de viatura policial equipada com tecnologia embarcada, que visa possibilitar um atendimento mais qualificado às ocorrências policiais, prestando melhor serviço à população brasileira, tanto em termos de segurança pública, quanto em Direitos Humanos. Para atingir este objetivo, foi realizado um levantamento com policiais civis e militares referente às necessidades de seu cotidiano quanto às tecnologias nas viaturas.

2 METODOLOGIA

Para chegarmos aos objetivos propostos, utilizou-se como metodologia a pesquisa literária, a fim de tomarmos conhecimento das novas tecnologias disponíveis no Brasil e em outros países, e uma pesquisa junto a policiais civis e militares, por meio de questionário, objetivando saber quais são as tecnologias atualmente disponíveis em suas viaturas e as tecnologias julgadas úteis para se chegar a um resultado mais efetivo no atendimento e na resolução das ocorrências policiais.

Após análise dos dados e informações obtidas, elaborou-se uma proposta de um protótipo de aplicação de tecnologia embarcada nas viaturas, que possibilite a dinamização dos trabalhos, com otimização de recursos e diminuição de tempo de atendimento das ocorrências policiais.

3 ANÁLISE DA PESQUISA

Para elaboração do presente trabalho, foi realizada uma pesquisa de campo, a partir da aplicação de um questionário a amostra de policiais civis e militares da cidade de Torres, no Rio Grande do Sul. A amostra consistiu em dez policiais militares, em um universo de 48 policiais, e dez policiais civis, em um universo de 22 policiais. Tal pesquisa visou, basicamente, ao levantamento de como são as viaturas policiais atualmente, quais tecnologias poderiam ser utilizadas para melhorar essas viaturas, e como os policiais imaginam que serão as viaturas no futuro, em um prazo de 20 anos.

As primeiras questões foram para conhecer a qual instituição pertencia o entrevistado e seu tempo de serviço naquela corporação (Gráfico 11.1). A quase totalidade dos policiais militares entrevistados contava com mais de 20 anos na função, variando de seis a 35 anos, ao passo que os policiais civis são, em média, mais jovens e com menos tempo de serviço, entre três a 22 anos de serviços prestados à corporação.

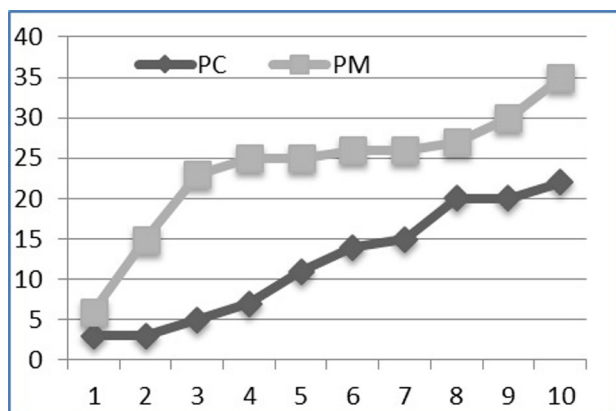


Gráfico 11.1 Instituições e tempo de serviço dos entrevistados.

Em se tratando do principal uso da viatura, elas são utilizadas para o policiamento ostensivo, atendimento de ocorrências e atividades administrativas por parte da Polícia Militar. Já os policiais civis mencionaram que a principal utilização é o transporte de presos e o serviço de investigação.

Todos os policiais entrevistados foram unânimes em afirmar, ao serem questionados sobre os equipamentos de suas viaturas, que elas apenas possuem rádio comunicador, sirenes e luzes de emergências (Gráfico 11.2). Houve uma menção à GPS por parte da Polícia Militar e uma por parte da Polícia Civil. Cabe salientar que, atualmente, cada corporação possui uma viatura com GPS integrante do kit multimídia original de fábrica de cada veículo, e não como acessório disponibilizado pelas corporações.

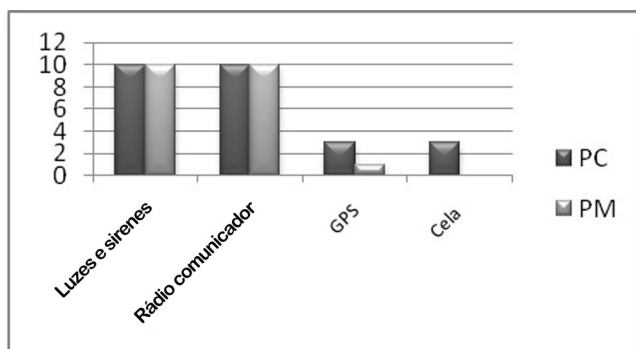


Gráfico 11.2 Equipamentos atualmente existentes nas viaturas.

Em contrapartida, ao serem questionados sobre quais meios julgavam úteis para suas funções, todos aqueles oferecidos como opções de respostas foram citados, sem exceção. Os policiais civis foram quase unânimes ao elenca-

rem a totalidade dos itens de tecnologia, com apenas duas exceções do total de entrevistados. Já entre os policiais militares, houve uma variação maior, tendo, no entanto, igualmente todos os itens sido citados, com ênfase para rádio comunicador, leitor óptico para digitais, programa de reconhecimento facial, computador, cela e GPS.

Ao serem inquiridos acerca de quais tecnologias poderiam ser incluídas no futuro para melhorar as comunicações, os policiais, tanto civis quanto militares, fizeram menção aos dispositivos e programas como reconhecimento facial, escâner de placas etc. Além disso, conforme mostra o Gráfico 11.4, os policiais citaram que equipamentos de comunicação mais avançados passam, obrigatoriamente, por uma conexão sem fio de alta qualidade e velocidade de resposta. Também foi mencionado o uso de computadores com programas de consultas a indivíduos e veículos, que devem estar interligados a diversos bancos de dados em nível nacional.

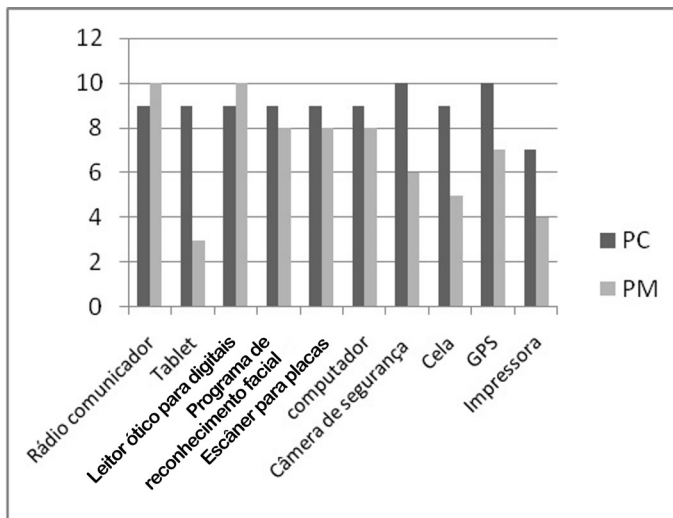


Gráfico 11.3 Equipamentos julgados úteis pelos policiais.

Questionados acerca da segurança das viaturas, mais especificamente sobre o que se poderia incluir nestas a fim de aumentar a segurança, a totalidade dos policiais militares mencionou a blindagem das viaturas como item mais importante a ser adotado. Citaram ainda o uso de armamento mais potente, do tipo fuzil, bem como computadores com sistemas avançados de consultas. Já os policiais civis, pela diversidade maior no uso das viaturas, mencionaram mais elementos ligados à tecnologia, como programas de identificação mais ágeis, sistemas de comunicação mais eficazes, celas e GPS em todas as viaturas. Mais da metade dos policiais civis entrevistados também mencionou a blindagem das viaturas como um item importantíssimo para sua segurança, conforme Gráfico 11.5.

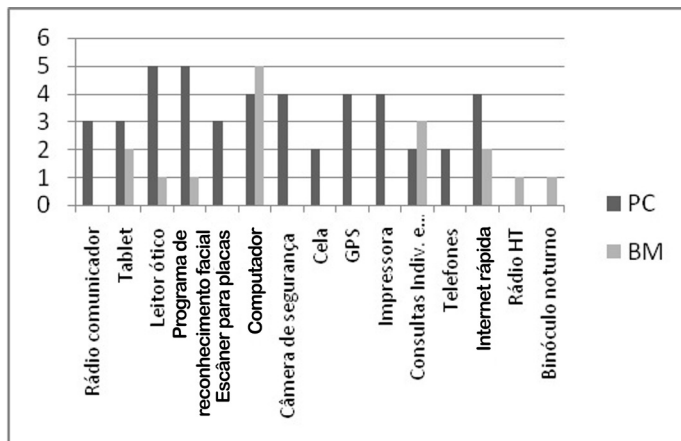


Gráfico 11.4 Tecnologias julgadas úteis em termos de comunicação.

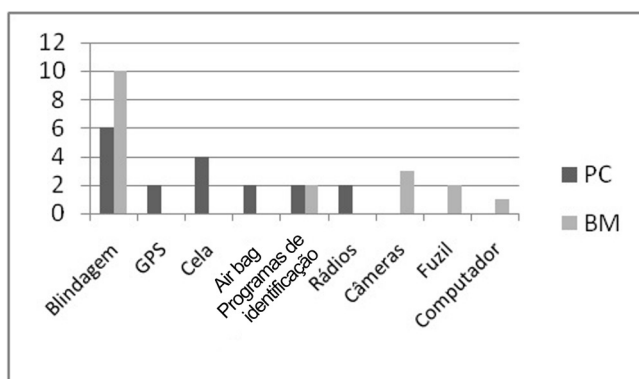


Gráfico 11.5 Tecnologias julgadas úteis para a segurança dos policiais.

A última questão foi a que causou maior surpresa e, ao mesmo tempo, preocupação pelas respostas obtidas. Embora tenham surgido opiniões interessante, como veículos anfíbios, à prova de fogo, com blindagem máxima, flutuantes, motores potentes (sempre os melhores existentes no mercado), com tecnologia que forneça mais segurança aos policiais e aos suspeitos, com comunicação e sistemas de consultas eficazes, com identificação biométrica eficiente, também houve manifestações claras de desesperança em relação ao futuro.

Na polícia militar, cerca da metade dos entrevistados, e na polícia civil cerca de 30% dos consultados, manifestaram-se no sentido de não fazerem sequer uma previsão ou de ter ideia de como seriam as viaturas daqui a 20 anos.

Disso tudo, denota-se claramente a preocupação dos policiais com sua segurança pessoal, ao mencionarem majoritariamente a questão da blindagem das

viaturas e uso de armamento mais potente, bem como se verifica o sentimento de abandono por parte do governo, ao relatar não terem perspectiva de melhora tecnológica, mesmo em uma visão no longo prazo.

4 PROPOSTA DA VIATURA POLICIAL IDEAL

Com base na análise da pesquisa de campo feita por meio de realização de questionário por amostragem junto às polícias civil e militar do Rio Grande do Sul, foi elaborada uma proposta de viatura de uso policial dotada de equipamentos que visam aperfeiçoar a eficiência das polícias, diminuir o tempo de atendimento às ocorrências, bem como reduzir os erros durante esse atendimento. Cabe esclarecer que nem todas as sugestões foram contempladas, eis que algumas delas são dignas de obra de ficção científica, inexecutáveis em termos de realidade em um futuro próximo. Como exemplo disso, tivemos um caso de sugestão de viaturas que voassem/flutuassem ao invés de rodarem.

Da observância da situação atual das viaturas policiais no Brasil, além da análise de uma pequena amostra de como são as viaturas policiais na cidade de Fort Worth, no Texas, nos Estados Unidos, surgiu a ideia de como seria a viatura ideal para o uso em serviço policial, em termos de tecnologia da informação e comunicação, visando sua utilização de maneira mais eficaz, rápida e justa por parte das forças de segurança nas suas mais variadas esferas. Para chegarmos a esse resultado, seria necessário que tais veículos fossem equipados com hardwares e softwares específicos para as atividades de segurança pública.

Em um primeiro momento, o veículo deverá ser equipado com um computador portátil, do tipo *ultrabook*, sendo este orgânico da viatura e ali permanecendo durante as 24 horas do dia. A recomendação é de que seja um equipamento com processador de altas capacidade e velocidade, com conexão à internet, o que facilitará as consultas a serem realizadas nos mais diversos bancos de dados em nível estadual e federal, devendo estes estar perfeitamente integrados e disponíveis para acessos remotos, como um notebook Getac B300 (GETAC, 2015).

A transmissão de dados se daria por meio do sistema *wireless*, ou seja, de ondas de rádio, sem a utilização de fios e, portanto, de maneira remota. Uma das preocupações em utilizar esse sistema é a segurança das transmissões, com a possibilidade da interceptação e captura desses dados e informações por terceiros. Atualmente, a utilização de criptografia é considerado um dos meios mais eficazes para garantir segurança na troca de mensagens, além da utilização de protocolos de segurança baseados nesses métodos. A criptografia transforma a mensagem utilizando uma cifra ou um sistema criptográfico, que codificam a mensagem de modo que este torne-se incompreensível. Desta maneira, existe uma chave (*key*), que funciona como uma senha para a cifra, que torna a mensagem incompreensível para todos

menos para o emissor e receptor daquela mensagem, que terão acesso a essa chave e poderão decodificar aquela mensagem (DEITEL, et al. 2002).

Como um dos meios de entrada de dados, seriam utilizadas câmeras do tipo webcam, com autofoco e alta definição, para que possibilite a utilização dos softwares de detecção de placas e de reconhecimento facial. Tais câmeras permitiriam melhor qualidade de vídeo, por meio do controle automático, com cores vivas e imagens precisas (MAGYAR; SOUZA, 2014).

Um sistema para reconhecimento facial é composto por três momentos ou fases essenciais: mapeamento da face, captura e seleção de características faciais, e reconhecimento da face propriamente dito. Em um primeiro momento, as viaturas poderiam ser dotadas do software Malic – Reconhecimento Facial Open-Source.

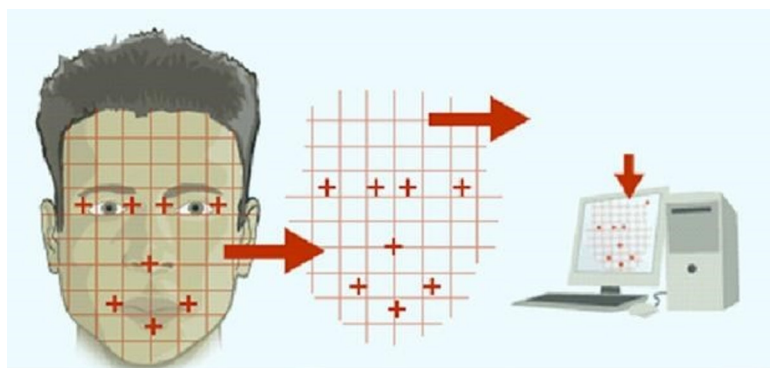


Figura 11.1 Representação de captura da face.

Fonte: Tecmundo.com.br.

O primeiro passo é identificar, por meio de uma câmera (digital, webcam, de celular, entre outras), todos ou alguns desses pontos em comum, como os dois olhos e a distância entre eles, o nariz e seu comprimento, a boca, as bochechas e o queixo, limitando o formato da face e o espaço ocupado por ela (Figura 11.1). Esses pontos são gravados e armazenados no formato de algoritmos em um banco de dados, que os reconhecem a partir de cálculos. Uma vez feitos esses cálculos e reconhecida a face, essa imagem seria submetida a um banco de dados (inicialmente das polícias, institutos de identificação e Detrans) para fins de identificação do indivíduo, bem como de verificação de sua situação junto à Justiça.

Dentre os sistemas de leitura biométrica atualmente existentes, além do reconhecimento facial, outro de fundamental importância é o de leitura de impressão digital. Esse é um sistema que capta a imagem da impressão digital com um leitor biométrico óptico e compara com um banco de dados de imagens com as digitais gravadas. É um método rápido, de alta confiabilidade e baixo custo. E é justamen-

te por essas garantias e facilidades em seu uso que entendemos ser perfeitamente possível seu uso em tecnologia embarcada em viaturas policiais.

5 CONCLUSÕES

No Brasil, não há uma cultura de valorização das polícias ou do serviço por elas prestados, justamente a começar pelos veículos disponibilizados. Por exemplo, na Alemanha, tem-se a cultura de que a polícia tem de estar equipada com melhores e mais potentes veículos do mercado. A explicação dada é, justamente, a valorização do policial. Segundo os alemães, se o policial vai abordar um veículo, que no Brasil seria considerado de luxo, ele não pode estar em situação inferior; ele tem de estar em pé de igualdade com o cidadão abordado, a fim de que não seja humilhado por este.

Por esta razão, entre outras, inclusive pelo desempenho de mais de 20 anos de serviço policial do autor deste artigo, vimos a necessidade de elaborar o presente trabalho, visando ser um marco na modernização das frotas policiais em operação em nosso país. A introdução de tal cultura serviria como instrumento de aprimoramento da prestação de uma função que é obrigação fundamental do Estado, qual seja o fornecimento de um serviço de excelência ao cidadão em termos de segurança.

Todas as tecnologias mencionadas, seja a identificação por reconhecimento facial, seja a identificação biométrica, apenas para citar as mais importantes, já são existentes. Bastaria que houvesse, por parte dos governantes, maior vontade política para melhorar os investimentos realizados nessa área, visto que, em um segundo momento, tais medidas gerariam economia aos cofres públicos. Tal afirmação segue este raciocínio: atualmente, tanto os estados quanto o Governo Federal são alvos de frequentes ações judiciais de indenização, oriundas de erros cometidos por seus agentes por meio de prisões irregulares e/ou ilegais, levando ao cárcere pessoas que não deveriam permanecer ali, justamente por erros de identificação.

Com a implementação das medidas apontadas neste trabalho, tais erros, se não eliminados, seriam reduzidos drasticamente, evitando, por consequência, um sem número de possíveis ações, que seriam fatalmente intentadas junto ao Poder Judiciário ante a manutenção dos moldes atuais das políticas de segurança pública, mais precisamente a utilização de meros veículos comuns, com pintura diferenciada e sirene e luz de emergência como únicos equipamentos disponíveis para abnegados servidores realizarem a segurança de qualidade a qual tanto necessita a nossa sociedade.

Como trabalhos futuros, poderiam ser estudadas novas formas de identificação, por exemplo, a leitura ótica da íris ou a identificação biométrica por meio da

circulação sanguínea das veias das mão, que, assim como as digitais, são únicas nos indivíduos.

Agora, no campo de uma divagação, poder-se-ia também imaginar um incremento tecnológico para as viaturas utilizadas pelas equipes de perícias, para, quem sabe no futuro, podermos agilizar não só o atendimento das ocorrências diversas, mas igualmente sermos prodigiosos na realização de exames periciais. Quem sabe um furgão ou um utilitário com equipamentos e tecnologia que permitissem fornecer, em minutos e *in loco*, os tão aguardados resultados periciais, que hoje demoram de meses até mesmo anos para serem realizados e concluídos.

REFERÊNCIAS

- BOCK, E. C. **Sugestões para a informatização de viaturas policiais como instrumento de segurança pública**. Pós-graduação em Tecnologias da Informação e Comunicação Aplicadas na Segurança Pública e Direitos Humanos. Universidade Federal de Santa Catarina. 2015. Disponível em: <http://posticsenasp.ufsc.br/files/2015/07/Dissertação_Elbio-V13.pdf>. Acesso em: 1 fev. 2016.
- DEITEL, H. M. et al. **Wireless Internet and mobile business: how to program**. Upper Saddle River: Prentice Hall, 2002. (Série How to Program).
- GETAC. **Descrição de computador Getac B300**. Disponível em: <<http://us.getac.com/notebooks/B300/features.html>>. Acesso em: 7 jun. 2015.
- MAGYAR, A. M.; SOUZA, S. Y. **Sistema de monitoramento e gravação para utilização em viaturas de policiamento ostensivo**. Universidade Tecnológica Federal do Paraná. 2014. Disponível em: <<http://repositorio.roca.utfpr.edu.br/jspui/handle/1/2228>>. Acesso em: 14 jul. 2015.
- PASTORINI, A. **Motorola traz viatura do futuro para a Interseg**. Disponível em: <<http://economiasc.com.br/wp-content/uploads/2014/09/carromotorola.jpg>>. Acesso em: 9 jan. 2015.
- SOUZA, M. M. **Siscompm: uma proposta de comunicação entre Copom e viaturas policiais militares utilizando comunicação wireless**. Universidade Federal de Lavras. 2015. Disponível em: <<http://repositorio.ufla.br/jspui/handle/1/9447>>. Acesso em: 7 jun. 2015.

12

CAPÍTULO

REDES SOCIAIS E A POLÍCIA COMUNITÁRIA: ESTUDO DE CASO DOS CONSEGS DO VALE DO ARARANGUÁ¹

Márcio Giani Rosa de Matos

Márcio Vieira de Souza

1 INTRODUÇÃO

A busca por segurança foi um dos motores que levaram os homens a viverem em grupos, ou seja, a segurança tem papel significativo na formação da vida em sociedade.

¹ 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 Marcio Giani Rosa de Matos e orientado pelo Prof. Dr. Marcio Vieira de Souza.

Viver em sociedade – pequenos grupos – gerava proteção contra algum inimigo externo, contudo, exigiam que certas regras, necessárias à sobrevivência do grupo, fossem observadas. Alguns componentes do grupo receberam a competência para policiar o cumprimento das regras sociais. Nascia ali o embrião do que hoje chamamos de Polícia (MARCINEIRO; PACHECO, 2005).

A polícia, ao longo do tempo, desempenhou seu papel das mais variadas formas. Durante sua evolução, o ato de policiar foi influenciado por diversas ideologias de polícia, dentre as quais se podem destacar: Ideologia Militarista, Ideologia de Controle Social, Ideologia Reativa e Ideologia Preventiva.

Baseados nas ideologias de polícia, nas condições de seus Estados e em suas culturas, os países desenvolveram diversos modelos de polícia, cada um com suas características: modelo anglo-saxão de polícia (descentralizado), modelo francês (Maréchaussée – militar), modelo português (influenciado pelo francês) e modelo oriental (proativo).

O modelo oriental 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. (MARCINEIRO, 2005, p. 39)

O Brasil, devido ao fato de ter sido colônia portuguesa, iniciou sua polícia na Ideologia Militarista com um modelo herdado dos franceses. Contudo, ao logo da sua evolução, todos os modelos de polícia apresentados anteriormente influenciaram a polícia brasileira, cada qual com mais ou menos intensidade em diferentes períodos da história.

Todavia, estes modelos não se mostraram eficientes para resolver o crescente problema do crime e da violência, que apresenta índices cada vez mais elevados, contando com criminosos cada vez mais cruéis, atuantes e impunes. Soma-se ao aumento do crime e da violência as mudanças democráticas estabelecidas com a Constituição Federal de 1988, que exigiu das polícias uma nova postura e uma ruptura com os antigos paradigmas da segurança pública.

A busca 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 a uma visão mais ampla dos problemas da Segurança Pública e, conseqüentemente, ao encontro da Filosofia de Polícia Comunitária, na qual todos são corresponsáveis.

O Brasil seguiu, assim, o mesmo caminho que trilharam Estados Unidos da América, Japão, Canadá, Espanha e outros países, que encontraram na democratização das polícias a solução para inúmeros problemas de segurança pública.

A função da polícia dentro da Filosofia Comunitária vai muito além de defender os interesses do Estado por meio do controle social como modelo latino-francês, ou de patrulhar as ruas e controlar o crime atendendo às chamadas de emergência e prendendo criminosos, tal qual o modelo anglo-saxão. Nela, deve-se buscar a prevenção do crime, estabelecendo parcerias com a comunidade, identificando problemas e agregando recursos da polícia, Estado e comunidade na resolução destes.

O caminho democrático levou o Brasil, no ano 2000, a implantar o Plano Nacional de Segurança Pública (PNSP), considerado a primeira política nacional e democrática de segurança do Brasil, seguido em 2007 pelo Programa Nacional de Segurança Pública com Cidadania (Pronasci), que alavancou 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 Secretária Nacional de Segurança Pública (Senasp), vem sendo, paulatinamente, implementada a Filosofia de Polícia Comunitária.

A principal ferramenta utilizada pelas polícias na Filosofia de Polícia Comunitária para estabelecer parceria com as comunidades e agirem juntas na solução de problemas são os Conselhos Comunitários de Segurança (Conseg).

A Senasp (2007) define os Consegs como:

Entidade de direito privado, com vida própria e independente em relação aos segmentos da segurança pública ou a qualquer outro órgão público; modalidade de associação comunitária, de utilidade pública, sem fins lucrativos, constituída no exercício do direito de associação garantido no art. 5º, inciso XVII, da Constituição Federal, e que tem por objetivos mobilizar e congregar forças da comunidade para a discussão de problemas locais da segurança pública, no contexto municipal ou em subdivisão territorial de um município (SENASP, 2007, p. 297).

2 OS CONSEGS E AS REDES SOCIAIS

O Conseg, em Santa Catarina, é o principal meio pelo qual se busca instituir uma polícia democrática e cidadã, ou seja, é a principal ferramenta da Filosofia de Polícia Comunitária. Marcineiro (2009) destaca que para alcançar os objetivos da Filosofia de Polícia Comunitária é preciso que as pessoas que compõem aquela comunidade reúnam-se com os policiais, seja nos Consegs ou em qualquer outra forma de reunir pessoas para discutir soluções para os problemas de segurança pública, inerentes àquela comunidade.

Por sua estruturação, podemos afirmar que os conselhos, por meio de seus conselheiros – cidadãos, polícia, empresas, Poder Legislativo etc. –, que se

relacionam e conectam-se, constituem uma rede social compartilhando o objetivo comum de trocar e gerar informações sobre segurança pública. 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 (MARTINS; LOTTA, 2010).

As redes sociais são, sem dúvida, mecanismos poderosos com potencial para viabilizar a participação democrática do povo na administração do Estado. E os Consegs, enquanto rede social, teoricamente são uma ferramenta fantástica para a efetivação da participação da comunidade nos assuntos de segurança a ela relativos. Contudo, na prática, os Consegs da microrregião de Araranguá (Vale do Araranguá) não desempenham seus papéis satisfatoriamente.

Entrevistas feitas com conselheiros e coordenadores dos Consegs do Vale do Araranguá revelaram sérios problemas que afetam o desempenho dos conselhos:

- **Baixo número de conselheiros e representatividade:** mesmo com os esforços e os apelos das polícias, os Consegs não cooptam pessoas suficientes para que os conselhos sejam órgão representativo da vontade da comunidade.
- **Dificuldade de divulgar sua filosofia e ações.**
- **Curto ciclo de vida:** após ações voltadas para estimular as comunidades à formação dos seus conselhos, os Consegs nascem atuantes e participativos, contudo, aos poucos – em alguns casos, rapidamente – as reuniões mensais se esvaziam e os conselhos sucumbem.;
- **Interesses distintos da segurança:** os conselheiros relataram que muitos se aproximam dos Consegs com objetivo de se autopromoverem, com o intuito de galgar vantagens pessoais e políticas.
- **Descrédito:** são poucos os conselheiros que ainda acreditam que os Consegs são meios eficientes à Filosofia de Polícia Comunitária.
- **Distanciamento das TIC:** os Consegs não utilizam, ou utilizam parcamente, as TIC como ferramentas auxiliadoras ao cumprimento dos seus objetivos. Apenas um, dentre todos os conselhos, possuía um blog; nos outros nem mesmo o e-mail era utilizado.

Tendo como base os problemas expostos, os questionários de pesquisa foram confeccionados. Algumas das questões visavam encontrar as causas e outras possibilitariam a sugestões de possíveis soluções. Mas antes de relatarmos as considerações galgadas a partir das respostas dos participantes, faz-se necessário ressaltar outros dois problemas que a análise dos questionários rutilou:

- **Ausência de jovens:** os conselhos não contam com a participação de jovens com menos de 25 anos de idade.

- **Discrepância entre os gêneros:** os participantes do sexo masculino são a maioria absoluta.

Uma vez que os problemas relativos aos Consegos estão elencados, passa-se à análise dos dados quantitativos e qualitativos, na busca de causas e soluções.

Os questionários aplicados aos conselheiros e não conselheiros foram distintos. O grupo dos não conselheiros foi dividido em três subgrupos: pedestres sem nenhum contato com a Filosofia de Polícia Comunitária, trabalhadores do comércio que participam de um projeto embasado nesta filosofia há um ano, e diretores de escolas que participam de projetos comunitários há dois anos. A divisão em grupos e subgrupos permitiu o cruzamento de dados, que levou às conclusões e considerações acerca dos problemas apresentados.

Comparando o número de não conselheiros conhecedores da Filosofia de Polícia Comunitária e dos Consegos com o número de conselheiros por faixa etária, pode-se constatar que os percentuais são praticamente os mesmos. Entre os mais jovens, o percentual de não conselheiros conhecedores da Filosofia fica próximo de zero, oscila entre aqueles com idade entre 25 e 45 anos e tem seu ápice naqueles com mais de 45 anos.



Figura 12.1 Não conselheiros conhecedores da Filosofia de Polícia Comunitária e conselheiros agrupados por faixa etária.

Fonte: Elaboração do autor.

Inversos a esta tendência são os percentuais dos usuários de redes sociais digitais, em que os mais novos são a maioria em todos os grupos.

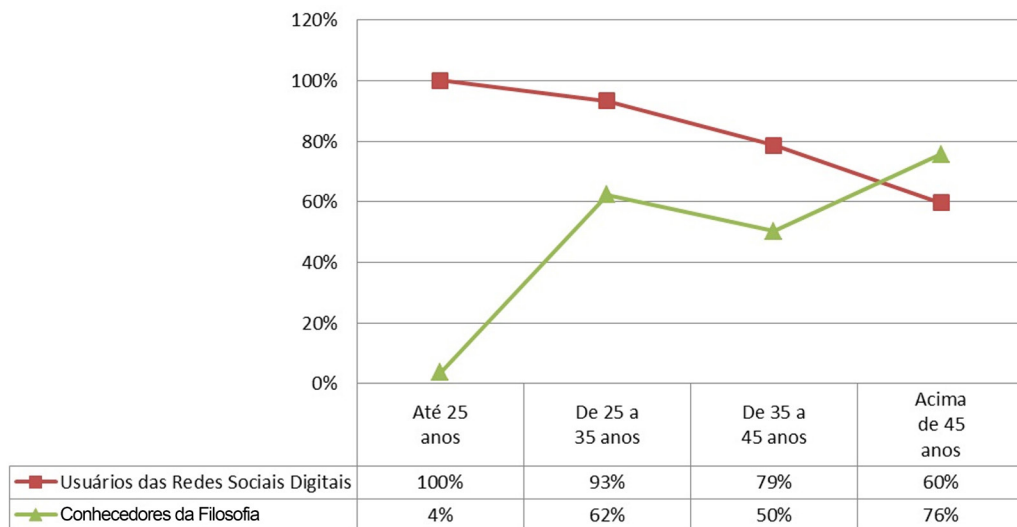


Figura 12.2 Comparativo do percentual dos usuários de redes sociais digitais e conhecedores da Filosofia de Polícia Comunitária por faixa etária.

Fonte: Elaboração do autor.

Mesmo entre os homens com idade acima de 45 anos, que são o grupo com maior percentual de conhecedores da Filosofia e dos Consegs, este percentual ainda é muito baixo, principalmente entre os pedestres. Os percentuais melhoram no grupo dos trabalhadores do comércio e continuam subindo no grupo dos diretores de escolas. Contudo, nem nestes últimos, que possuem dois anos de contato com a Filosofia de Polícia Comunitária, os jovens foram alcançados. A diferença de tempo de participação em projetos de polícia comunitária mostrou-se significativa, pois os trabalhadores do comércio apresentam percentuais de conhecedores de Filosofia e dos Consegs muito menores do que os dos diretores de escolas.

Filtrando os dados pelo gênero dos participantes, as tendências anteriores permanecem: os homens não conselheiros conhecedores da Filosofia e dos Consegs contam com percentual muito maior do que as mulheres do mesmo grupo, e a adesão às redes sociais digitais também segue sentido inverso, sendo as mulheres a maioria dos usuários.

O grupo dos diretores de escolas foi ignorado, na Figura 12.3, devido ao fato de que 86% dos seus participantes são do sexo feminino, o que inviabiliza o uso de tais dados em uma comparação entre sexos.

Enquanto a diferença entre homens e mulheres conhecedores da Filosofia de Polícia Comunitária e Consegs é de 9% a mais para os homens, a diferença entre os gêneros dos conselheiros é de 52% a mais para os homens. Pode-se deduzir, então, que a diferença entre os gêneros dos conselheiros não se assenta, isolada-

mente, na capacidade de se fazer conhecer da Filosofia de Polícia Comunitária e dos Consegs.

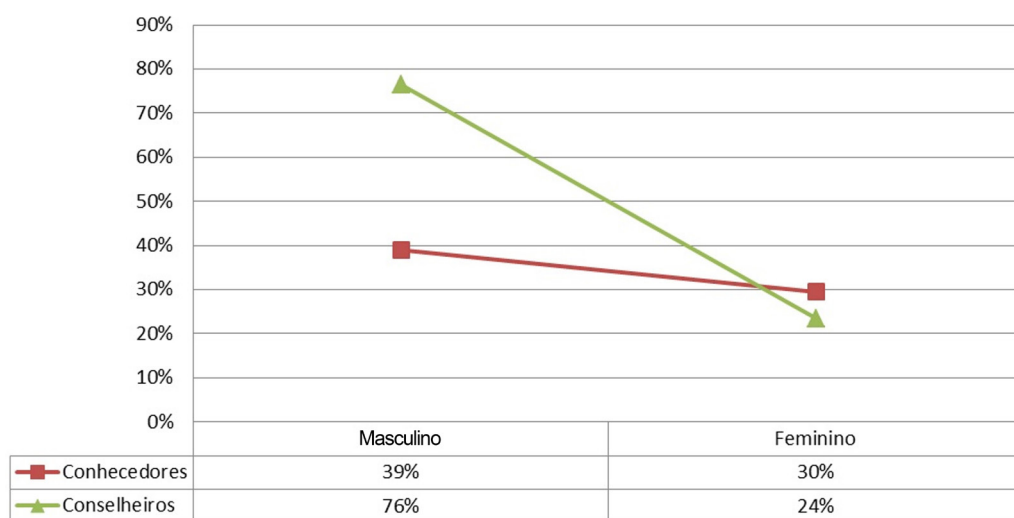


Figura 12.3 Não conselheiros conhecedores da Filosofia de Polícia Comunitária/Consegs e conselheiros agrupados por sexo.

Fonte: Elaboração do autor.

Por outro viés, resta claro que a capacidade de cooptar conselheiros dos Consegs está diretamente ligada à capacidade de difundir a Filosofia de Polícia Comunitária. Além disso, as redes sociais digitais apresentam-se como um campo fértil para difundir a filosofia e divulgar as ações dos Consegs, principalmente àqueles que são pouco ou nada representados nos conselhos: as mulheres e os jovens com menos de 25 anos.

A utilização das redes sociais digitais demonstra grande potencial para auxiliar na solução de quatro dos problemas dos Consegs: baixo número de conselheiros e representatividade, dificuldade de divulgar sua filosofia e ações, ausência de jovens e discrepância entre os gêneros.

Porém, a utilização das redes encontra severa resistência, inclusive figura entre os problemas inicialmente levantados. Para verificar suas possíveis causas, foram analisadas algumas questões: grau de instrução dos conselheiros, possibilidade de acesso à internet e adesão aos sites e aplicativos de redes sociais digitais pelos conselheiros.

Nenhuma das questões pesquisadas apresentou-se como causa para a não utilização das TIC pelos Consegs, especialmente dos sites e aplicativos de redes sociais digitais. O grau de instrução dos conselheiros é altíssimo para os padrões brasileiros (70% possuem nível superior, sendo que 41% possuem no mínimo

uma especialização, ou seja, os conselheiros provavelmente não possuem problemas em compreender e utilizar as TIC). Quanto ao acesso internet e a utilização de e-mail, os dados foram idênticos (94% possuem acesso à internet e e-mail pessoal e a participação nas de redes sociais em meio digital é praticada por 88% dos conselheiros).

Entende-se, pelos dados expostos, que os Consegs, por meio de seus conselheiros, estão plenamente aptos à utilização das redes sociais digitais. Contudo, os sites e os aplicativos destinados a este fim são inúmeros e não seria prático participar de todos eles simultaneamente, em especialmente para os Consegs, pois seus conselheiros são voluntários e nada recebem por seus serviços. Por esta razão, foram pesquisados quais são os sites e os aplicativos mais utilizados entres os grupos do estudo.

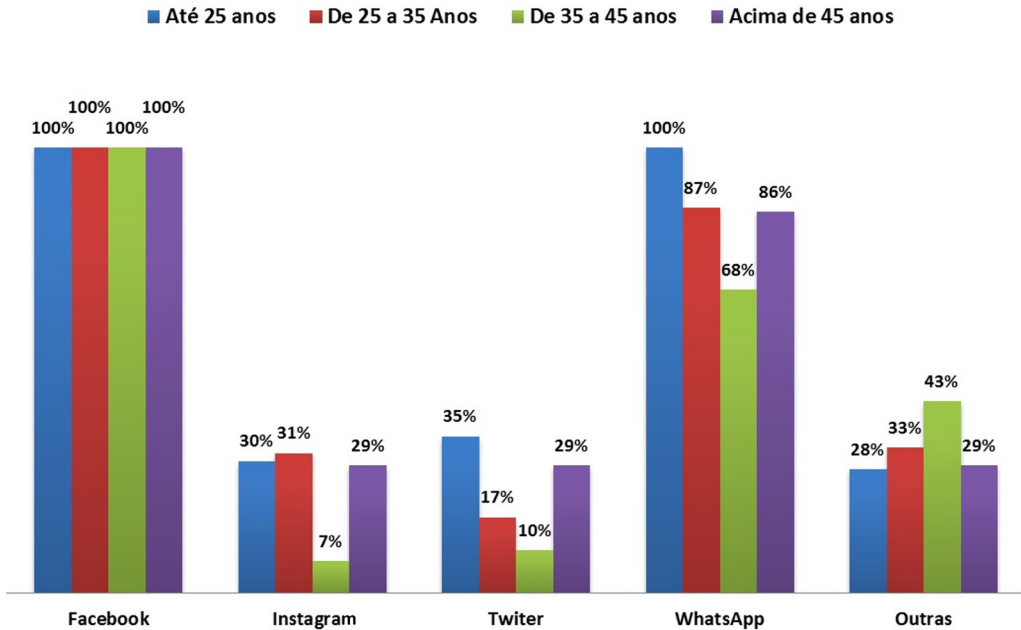


Figura 12.4 Principais sites e aplicativos de redes sociais acessados pelos grupos de não conselheiros por faixa etária.

Em todos os grupos, o Facebook e o WhatsApp são hegemônicos. Os jovens e as mulheres apresentam tendência a participar de mais de duas redes sociais digitais simultaneamente, mas, mesmo entre eles, a preferência permanece com o Facebook, com quase 100% de adesão, seguindo do WhatsApp, com quase 90% de adeptos.

3. CONSIDERAÇÕES FINAIS

Considerando o nível de instrução, possibilidade acesso à internet e participação em redes sociais dos conselheiros, pode-se afirmar que eles são plenamente aptos a utilizar as redes sociais digitais como ferramenta dos Consegs.

Tendo em vista que o Facebook e o Whatsapp são os sites/aplicativos de redes sociais digitais com maior número de adeptos na região do Vale do Araranguá, pode-se sugerir a utilização de ambos inicialmente. Considerando a dificuldade de manter os conselheiros ativos e participando das reuniões, sugere-se que as reuniões migrem para o meio digital ou, ao menos, partes delas.

Quanto ao problema do descrédito, de os conselheiros não verem os Consegs como um meio eficiente à Filosofia de Polícia Comunitária, deve-se deixar bem claro que tal descrédito não se estende à Filosofia, pois os entrevistados foram unânimes em afirmar que a Filosofia de Polícia Comunitária é um grande avanço rumo à democratização, eficiência e eficácia das polícias brasileiras.

Alguns pontos da pesquisa geraram dúvidas que suscitam maiores estudos, como a relação entre conhecer a Filosofia de Polícia Comunitária e participar dos Consegs, que se mostrou significativa; contudo, outros pontos necessitam de estudo. A diferença entre o número de participantes homens e mulheres não se explica, isoladamente, pelo fato dos homens terem o maior percentual de conhecedores da Filosofia de Polícia Comunitária. O reflexo de uma sociedade patriarcal, na qual o homem ainda é visto como o arrimo da família, poderia ser estudado como uma causa significativa da baixa representação feminina nos Consegs.

Por sua vez, os meios utilizados para difundir a Filosofia de Polícia Comunitária mostraram-se incapazes de alcançar os jovens com idades abaixo de 25 anos. Estudos da linguagem e meios usados pelos Consegs para divulgarem sua ideologia são imperiosos, pois a opinião dos jovens é importantíssima na construção democrática da segurança.

Sabe-se que a participação nos Consegs exige um mínimo de conhecimento. Um estudo sobre os impactos da formação dos conselheiros por EAD e MOOCs poderia sugerir melhorias consideráveis nesta área.

Outro ponto que merece um estudo mais aprofundado é a razão pela qual os Consegs mantiveram-se distantes das TIC, pois a presente pesquisa deixa claro que os conselhos, por meio dos seus conselheiros, são plenamente aptos a utilizarem as TIC, contudo não o fazem.

Ao final deste estudo, pode-se afirmar 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 dura-

douras. Estudos, para a utilização das TIC como ferramentas para sanar essas demandas são necessários e urgentes, caso contrário, viveremos um discurso de democracia participativa, maquiada com a oferta de ferramentas inválidas e inviáveis para real participação social na segurança pública.

REFERÊNCIAS

- BOL NOTÍCIAS. Facebook tem 1,23 bilhão de usuários mundiais; 61,2 milhões são do Brasil. 3 fev. 2014. Disponível em: <<http://noticias.bol.uol.com.br/ultimas-noticias/tecnologia/2014/02/03/facebook-em-numeros.htm>>. Acesso em: 21 dez. 2014.
- BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 20 nov. 2014.
- _____. 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. Ano I. Brasília, 2009.
- CARVALHO, V. A.; SILVA, M. R. F. Política de segurança pública no Brasil: avanços, limites e desafios. *Revista Katálysis*, v. 14, n. 1, p. 59-67, jan. 2011.
- COUTINHO, C. P.; JUNIOR, J. B. B. Blog e wiki: os futuros professores e as ferramentas da web 2.0. *SIIE'2007*, 14-16 nov. 2007, p. 199-204. ISBN 978-972-8969-04-2.
- CRUZ, R. C. Redes sociais virtuais: premissas teóricas ao estudo em ciência da informação. *TransInformação*, Campinas, v. 22, n. 3, p. 255-272, set./dez. 2010.
- ESTADO DE S.PAULO, O. Facebook chega a 1,35 bilhão de usuários no mundo. *Link*. 28 out. 2014. Disponível em: <<http://blogs.estadao.com.br/link/facebook-chega-a-135-bilhao-de-usuarios-no-mundo/>>. Acesso em: 21 dez. 2014.
- FERNANDES, S. S. **O Conselho Comunitário de Segurança de Forquilha e a filosofia da polícia comunitária: um estudo de caso.** Florianópolis, 2011. 128 p. Dissertação (Mestrado) – Universidade Federal de Santa Catarina – Centro de Filosofia e Ciências Humanas – Programa de Pós-Graduação em Sociologia Política. Florianópolis, 2011.
- HIPÓLITO, M. M.; TASCA, J. E. **Superando o mito do espantinho: uma polícia orientada para a resolução dos problemas de segurança pública.** Florianópolis: Insular, 2012.
- MARCENEIRO, N. **Implantação do gerenciamento pela qualidade total na polícia militar de Santa Catarina: um estudo de caso.** 2001. 204 f. Dissertação (Mestrado em Engenharia de Produção) – Centro Tecnológico. Universidade Federal de Santa Catarina. Florianópolis, 2001.
- _____. **Introdução ao estudo da segurança pública: livro didático.** 3.ed. rev. e atual. Palhoça: Unisul Virtual, 2005.
- _____. **Polícia comunitária: construindo segurança nas comunidades.** Florianópolis: Insular, 2009.

MARCENEIRO, N.; PACHECO, G. C. **Polícia comunitária: evoluindo para a polícia do século XXI**. Florianópolis: Insular, 2005.

MARTINS, R. D.; LOTTA, G. S. Capital social e redes sociais como alternativa para análise de políticas públicas de educação: o caso de Icapuí-CE. **Aval. Pol. Públ. Educ.** [online], v. 18, n. 69, p. 843-860, 2010.

MARTELETO, R. M. Análise de redes sociais: aplicação nos estudos de transferência da informação. **Ci. Inf.** [online], v.30, n.1, p. 71-81, 2001.

MATOS, M. G. R. **Redes sociais e a polícia comunitária: estudo de caso dos CONSEGS do Vale do Araranguá**. Monografia (especialização) – Universidade Federal de Santa Catarina – Campus Araranguá. Pós-graduação em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos. Araranguá, 2015. 112 p.

RAUEN, F. J. **Roteiros de investigação científica**. Tubarão: Unisul, 2002.

RECUERO, R. **Redes sociais na internet**. Porto Alegre: Sulina, 2009.

SANTA CATARINA – SC. **Regulamento dos Conselhos Comunitários de Segurança**. 2001. Disponível em: <<http://notes1.pm.sc.gov.br/aplicacoes/policiacomunitaria.nsf>>. Acesso em: 10 jan. 2015.

_____. **Decreto nº 2.136**, de 12 de março de 2001. Autoriza criação de Conselhos Comunitários de Segurança e dá outras providências. Brasília, 2001.

SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA – SENASP. Curso Nacional de Promotor de Polícia Comunitária. Grupo de Trabalho. **Portaria SENASP nº 002/2007**. Brasília: Senasp, 2007.

SOUZA, M. V.; SIMON, R. M. Redes sociais e MOOCs: análise de mídias para uma educação em rede. **XI Congresso Brasileiro de Ensino a Distância**. 2014. Florianópolis: Unirede, 5-8 ago. 2014, p. 313-327.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação**. São Paulo: Atlas, 1987.

13

CAPÍTULO

TECNOLOGIAS DA INFORMAÇÃO APLICADAS NA PMSC E BPMA

Rosinei Freitas da Rosa

Rangel Machado Simon

Fernando Jose Spanhol

Marcio Vieira de Souza

1 INTRODUÇÃO

As dinâmicas colaborativas e em rede são a marca da sociedade da informação e do conhecimento. Em razão disso, é fundamental discutir a utilização das Tecnologias da Informação e Comunicação (TIC) como suporte à Segurança Pública, em especial na proteção do meio ambiente, bem como a otimização do trabalho técnico-profissional dos policiais militares lotados no Batalhão de Polícia Militar Ambiental (BPMA), objetivando a padronização dos conceitos de proteção ao meio ambiente.

A proteção ao meio ambiente é um dos ramos de atuação da Polícia Militar de Santa Catarina (PMSC), que exerce trabalho de preservação da ordem pública e exige, assim, profissionais capacitados para a garantia das liberdades individu-

ais e coletivas, bem como dos direitos humanos. Mas, além disso, é preciso que esses agentes públicos tenham à disposição aporte tecnológico, para facilitar e melhorar seu desempenho. Assim, o objetivo deste trabalho é expor como é feito esse suporte por meio de TIC.

Nosso ponto de partida está em identificar os sistemas utilizados no âmbito da Segurança Pública, para o desempenho técnico-profissional dos membros da BPMA, para a proteção do meio ambiente.

Para interpretar mais adequadamente os caminhos deste trabalho, partimos da premissa de que, embora a definição de o que pode ser meio ambiente seja elástica, segundo Silva e Figueiredo (1998, p. 139), trata-se aqui somente no que diz respeito ao meio ambiente natural.

Tomamos o conceito de meio ambiente apresentado por Silva (1995, p. 2, apud FIGUEIREDO; SILVA, 1998, p. 140), que o estabelece como “a interação do conjunto de elementos naturais, artificiais e culturais que propiciem o desenvolvimento equilibrado da vida em todas as suas formas”. Inclusive esse conceito foi utilizado na Resolução Conama nº 306/2002, como se pode ver a seguir:

ANEXO I

DEFINIÇÕES

XII – Meio ambiente: conjunto de condições, leis, influência e interações de ordem física, química, biológica, social, cultural e urbanística, que permite, abriga e rege a vida em todas as suas formas (BRASIL, 2002).

O Caderno Temático de TIC (ABDI, 2010), elenca o fato de as TIC estarem em todas as áreas de atividades, tornando-se o cerne da chamada Sociedade da Informação e, com isso, tem se tornado um segmento econômico valioso aos países desenvolvidos e em desenvolvimento, tomamos para o presente estudo o conceito apresento no mesmo.

Para efeito do presente estudo, Tecnologias de Informação e Comunicação (TIC) correspondem a todas as tecnologias que interferem e perpassam os processos informacionais e comunicativos dos seres. Ainda, podem ser entendidas como um conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação dos processos de negócios, dos serviços públicos, da pesquisa científica e de ensino e aprendizagem (ABDI, 2010, p. 16).

A ABDI (2010, p. 38-39), no desenvolvimento do Caderno Temático de TIC, formulou uma questão junto a seus colaboradores quanto aos condicionantes sociais, tecnológicos, econômicos, ambientais, políticos e éticos que mais influenciarão o fu-

turo do desenvolvimento das aplicações de TIC no Brasil, nos períodos 2008-2010, 2011-2015 e 2016-2025, sendo observado que, dentre este conjunto de condicionantes, é citado “a educação em todos os níveis”, que compreende uma formação educacional e tecnológica estruturada, demonstrando assim sua importância.

Quanto ao tema meio ambiente, o Caderno Temático em questão tem, em todas as menções, as aplicações mobilizadoras de maior impacto no Brasil, pois, como se depreende do texto, “vive-se um período no qual a preocupação com o meio ambiente tem sido forte demandador de soluções que o preservem”. Visando a esta ação, o mesmo texto apresenta a necessidades de “meios de controles mais eficientes e eficazes, onde sistemas aplicativos permitem à sociedade um maior controle”, no caso, o meio ambiente.

Como define a Constituição do Estado de Santa Catarina, em seu capítulo que trata do Meio Ambiente, a Polícia Militar deve possuir uma unidade especial de Polícia Florestal, orientada essencialmente para essa missão.

E desta feita, a atuação da PMSC na área ambiental é exercida por seu setor especializado de proteção ambiental, o Batalhão de Polícia Militar Ambiental (BPMA), que desenvolve atividades de educação ambiental, e quando constatados ilícitos ambientais, promove a lavratura dos procedimentos administrativos e judiciais cabíveis ao caso, sendo essa atuação relacionada à proteção dos interesses difusos e coletivos da sociedade.

Entendemos que a PMSC, como um ramo da Segurança Pública, que “compreende o conjunto de todas as esferas envolvidas na garantia de segurança do cidadão, incluindo a ordem social, a saúde, a integridade da pessoa e a integridade do patrimônio” (ABDI, 2010, p. 56).

Os projetos que envolvem aplicações de Tecnologia da Informação (TI) não requerem dos profissionais de segurança, necessariamente, conhecimentos profundos de informática, contudo, faz-se necessária a difusão de seus conceitos básicos (FURTADO, 2002),

A constante necessidade do aperfeiçoamento do profissional da PMA elevava sobremaneira a qualidade do serviço prestado e, neste caso, como define Furtado (2002, p. 24), “ter um grande impacto no sucesso da empresa, beneficiando-a de diversas formas como: através da melhoria da qualidade dos serviços prestados, redução de erros e conseqüente redução de custos com maior eficiência das operações”.

A visão da necessidade de aprimorar a qualidade do profissional que executa a atividade de fiscalização do meio ambiente decorre da preocupação com este e suas inter-relações com o desenvolvimento humano e a qualidade de vida, sua evolução ao longo dos tempos, e as instituições que cumprem a garantia de tal preceito constitucional também devem evoluir, acompanhando a inúmeras leis preservacionistas que se adotou no Brasil.

Partindo desta premissa, temos o presente questionamento: quais TIC podem ser utilizadas para contribuir com a efetivação das atribuições da BPMA?

2 PROCEDIMENTOS METODOLÓGICOS

Para tal, foi realizada uma pesquisa descritiva, documental, bibliográfica e um estudo de caso, baseado em dados empíricos do Batalhão de Polícia Militar Ambiental (BPMA) do Estado de Santa Catarina.

Sendo a BPMA um órgão que integra o Sistema Nacional do Meio Ambiente, há a necessidade de se buscar novas tecnologias para alavancar a capacidade produtiva do efetivo dessa unidade de proteção ao meio ambiente.

Este autor, Rosinei Freitas da Rosa, faz parte do efetivo do 2º Pelotão da 3ª Companhia do Batalhão de Polícia Militar Ambiental, que possui um número reduzido de policiais (17) e cujo efetivo tem o compromisso de efetuar o policiamento de prevenção e fiscalização das atividades nocivas ao meio ambiente, nos 24 municípios que compreendem a Associação dos Municípios da Região Carbonífera (AMREC) e a Associação dos Municípios do Extremo Sul Catarinense (AMESC), sendo que tal dificuldade de efetivo se reproduz nas demais unidades da BPMA.

Ao se identificar e buscar orientar a necessidade de desenvolver novas tecnologias que possam auxiliar nas atividades do policiamento ambiental, poderemos assim ampliar e melhorar a capacidade de trabalho de todos.

Para o desenvolvimento deste trabalho, focou-se na atividade de proteção do meio ambiente por meio da BPMA, sendo que dentro do Caderno Temático de TIC (ABDI, 2010, p. 22), para a construção da visão de futuro, foram selecionadas sete aplicações considerando os objetivos dos cinco subprogramas do Programa Mobilizador em TIC da Política de Desenvolvimento Produtivo: (iii) sistemas aplicados à segurança pública: (v). sistemas aplicados à energia e ao meio ambiente.

Ao associarmos segurança pública e meio ambiente, em Santa Catarina temos, na PMSC, por meio da BPMA, a devida conjugação destes temas e, portanto, a necessidade de sua integralização e aperfeiçoamento.

3 TIC UTILIZADAS PELA PMSC

Antes de descrevermos as TIC utilizadas pela PMSC, faz-se necessário uma visita ao Plano Estratégico da PMSC 2005-2020 (SC, 2005) e ao Plano de Comando apresentado em 2011(SC, 2011).

Em junho de 2005, por meio da Portaria nº 020/PMSC, de 11 de janeiro de 2006, foi aprovado o Plano Estratégico, do então comandante geral Bruno Knih, que tinha o objetivo, segundo suas próprias palavras, de “manter a instituição

viva dentro do período em que se passa de grandes transformações no âmbito econômico-social, tecnológico e política” (SC, 2005).

Nesse Plano Estratégico, foram apresentadas algumas diretrizes, em que se definiu a importância na prática interna da instituição, traçando assim suas estratégias quanto a sua função pública e que tal planejamento é um processo contínuo e permanente, que considera os pontos fortes e fracos da organização.

Para o desenvolvimento deste trabalho, a Diretriz nº 8 (SC, 2005) mostra-se a mais adequada, pois trata do uso das tecnologias, prevendo, entre suas ações, a promoção da inovação e da modernização tecnológica da Polícia Militar, bem como se propõe a mapear os sistemas de informação existentes; projetar a integração desses sistemas, implantando banco de dados adequado à arquitetura *Data Ware House*; desenvolver novos sistemas de informação; e desenvolver o novo aplicativo de registro de atendimento e despacho de ações policiais (emergência 190).

Entendemos que foi um avanço o Plano Estratégico para a PMSC, pois se tem um arcabouço de ações e de definições para realizar sua missão. Segundo Senasp (2009, p. 2):

[...] para que no enfrentamento diário contra os sinistros e desastres, contra a violência e o crime, haja resultados positivos, há que estar atento a essas mudanças. Para atender com excelência à sociedade, o cliente, é preciso entender a razão da existência das corporações, saber claramente como realizar as missões e, vital, posicionar-se quanto ao futuro.

Segundo a divisão contida dentro da estrutura da PMSC, esta possui órgãos de direção, de apoio e de execução. Aos órgãos de direção, cabe o processo de gestão da instituição, objetivando a implantação das políticas necessárias para a realização de sua função no âmbito da segurança pública; aos órgãos de apoio fica o encargo das atividades nas áreas de Logística, Finanças, Instrução, Ensino, Saúde, Promoção Social, entre outros.

O Plano de Comando assim menciona quanto às Tecnologias da Informação e Comunicação:

2.2.8 TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

2.2.8.1 Sistemas informatizados de gestão operacional

2.2.8.1.1 Sistema de Atendimento e Despacho de Emergências

Implantar nas Centrais Regionais de Emergência (CRE) e Centrais de Operações Policiais Militares (Copom) o Sistema de Atendimento e Despacho de Emergências (Sade).

2.2.8.1.2 Sistema de BI (*Business Intelligence*)

Disseminar na corporação a utilização do BI (*Business Intelligence*) como suporte ao processo de tomada de decisão.

2.2.8.2 Inteligência embarcada

Ampliar a instalação de computadores ou tablets em viaturas, no sentido de ofertar informações qualificadas em tempo real e o registro dos atendimentos realizados.

2.2.8.3 Radiocomunicação (SC, 2013).

4 CONSIDERAÇÕES FINAIS

A PMSC, em decorrência de uma nova visão estratégica, tem buscado dispor de TIC como forma de melhorar suas atividades e assim prestar um melhor serviço ao cidadão, em especial no tocante ao meio ambiente, de modo que essas tecnologias passem a ser vistas como investimentos essenciais à gestão e não mais como despesa superficial, a ser incorporada ao plano plurianual da instituição.

A concepção em que devemos nos adaptar para assim termos uma reformulação de nossos pensamentos também ocorre com nossas instituições, em que estas devem ter como base a constante necessidade de mudar seus paradigmas e acompanhar esse turbilhão de mudanças que a globalização propicia e a velocidade com que ela chega, caracterizando o estado de necessidade de sobrevivência.

A PM como um todo tem a função de prestador de serviço à comunidade, sendo este serviço prestado de forma ininterrupta, 24 horas por dia. Seu desafio é acompanhar as constantes mudanças sociais e as exigências que se tem da criação de instrumentos que garantam sua finalidade para ter mais eficiência e eficácia em suas ações.

A base conceitual sobre o tema foram as TIC usadas pela PMSC, em particular aquelas que aderentes ao trabalho da BPMA. Devido a um dos autores ser membro do 2º Pelotão da 3ª Companhia do Batalhão de Polícia Militar Ambiental, tomamos por base as atividades exercidas neste local que, por ser uma unidade da BPMA, reproduz sua estrutura em nível de Estado.

Dentro de uma perspectiva, verifica-se que as TIC se tornaram uma força motriz dentro da PMSC, e este novo paradigma de transformação e desenvolvimento pode ser um novo modelo a se implantar, visando mudar as formas de interação da sociedade com a instituição, pois a excelência na execução de sua função pode elevar sobremaneira seu valor para a sociedade. Exemplo disto é o BO Online, documento que o cidadão pode retirar de qualquer lugar do Brasil pertinente a seu atendimento.

Entretanto, deve-se ampliar a ação de transformação, atingindo maior nível de interação com as TIC, fazendo com que as informações dispostas dentro da estrutura tornem-se conhecimento agregador.

Pode-se evidenciar que a PMSC levou algum tempo e ainda apresenta certa dificuldade para vislumbrar as possibilidades das TIC e suas vantagens de aplicação, embora este quadro possa vir a mudar gradativamente, como os últimos cinco anos demonstram.

Há diversos tipos de sistemas que foram desenvolvidos para atender as diversas atividades funcionais da PMSC, tanto corporativos, como estratégicos e específicos. Contudo, a adoção do SISP (antes, Sistema de Informática do Serviço Público, depois Sistema de Administração dos Recursos de Tecnologia da Informação), após este passar a ser administrado pela SSP, é uma ação que à época indicou um futuro a ser seguido, resultando no sistema SADE, criando assim um ambiente de futuro, em que, desta forma, criasse uma estrutura coordenada para a ação conjunta dos órgãos de segurança.

Silva et al. (2008), em seu artigo que trata da aplicabilidade do SISP, demonstra claramente a necessidade da integração dos sistemas públicos de segurança, fato que levou algum tempo a ocorrer.

Pode-se dizer que, em razão de certas dificuldades de se fazerem comunicar as estruturas de segurança, surgiu o conceito de que se faz necessária a integração dos sistemas de segurança. Cabe à SSP colocar um norte neste caminho e exercer seu poder de decisão para que ocorra tal fato.

É necessário que exista uma estrutura única de Segurança Pública. Se isso não ocorre fisicamente, que ocorra dentro da necessidade na integração das TIC, dos órgãos de segurança, fazendo com que se tenha mais conhecimento quanto aos fatos delituosos ocorridos, o que ajudará cada vez mais na tarefa de suplantá-los e buscar sua redução.

Estas concepções visam desburocratizar boa parte dos processos, gerando ganhos às instituições de segurança e, por conseguinte, para sociedade.

Devido à análise feita durante esta pesquisa, consegue-se chegar ao um resultado previamente estabelecido de que o problema da pesquisa era verificar quais ferramentas de TIC poderiam auxiliar na ação de policiamento da BPMA. Foi constatado que a BPMA não possui sistema garantidor de suas informações, pois não se encontra informatizado e, conseqüentemente, estão parametrizados, fazendo com que o planejamento estratégico seja executado com dificuldade.

A BPMA não dispõe de seus dados de modo informatizado e acessível via sistemas, nem de banco de dados centralizado, como os utilizados pela PMSC, no registro de ocorrências. Tendo esta possibilidade, ocorreria uma economia de recursos físicos e humanos, além de facilitar a busca por informações e dados, que seriam automatizados, bem como o armazenamento e a confiabilidade na geração de relatórios e análise estatísticas seriam melhores.

Os objetivos foram atingidos, pois foi possível verificar os sistemas existentes na PMSC que podem ser usados na BPMA para auxiliar sua atividade e, assim, otimizar os serviços realizados.

As possíveis ações para minimizar os efeitos gerados pelas ocorrências de danos ambientais são muitas, e pode-se dizer que, com a intensificação no uso das TIC, esta tarefa seria mais bem realizada.

Temos a percepção que o avanço tecnológico leva a grandes transformações nos campos econômico, social e político, e, para tanto, a BPMA tem que se especializar, alicerçada em um uso mais intensivo das TIC. Deve-se incorporar em sua estrutura eficientes sistemas de informações, pois os trabalhos pertinentes à proteção da natureza não podem estar desassociados das constantes mudanças e renovações pelas quais passam a sociedade e as instituições.

A utilização de informações nas áreas governamentais para subsidiar as tomadas de decisões pelos agentes públicos configura uma forte arma para combater a má utilização da máquina pública. É sabido que essas informações devem ser geradas de forma correta, confiável e com precisão, pois, do contrário, podem inviabilizar a sustentação necessária para estratégias fundamentais para a gestão.

As considerações finais deste trabalho estão estruturadas de acordo com os objetivos específicos localizados no primeiro capítulo:

- a) Desenvolver uma pesquisa bibliográfica sobre o uso de TICs na BPMA.
Dentro do levantamento feito, constitui-se uma única ferramenta de TIC, o GAIA, ferramenta usada na estrutura da BPMA para gerenciar as multas aplicadas por delitos ambientais em Santa Catarina. Essa ferramenta é gerida pela Fatma, com suporte do Centro de Informática e Automação do Estado de Santa Catarina (Ciasc) e compartilhada com a BPMA. Outras TIC utilizadas pela BPMA são aquelas empregadas na área administrativa, decorrente dos setores de Recursos Humanos, Patrimônio e Financeiro, que valem para toda a PMSC, sendo necessária a elaboração de uma plataforma de TIC para o registro de ocorrências ambientais como determina o Tribunal de Contas do Estado (TCE), em sua auditoria quanto às multas ambientais aplicadas.
- b) Identificar e descrever a natureza das TIC, presentes na PMSC, para policiamento ambiental.
Esta pesquisa identificou e descreveu as TIC presentes na PMSC, sendo constatado que a única TIC, usual do setor de policiamento da PMSC e aplicada na BPMA, é o CHIPSAT, usado para rastreamento da frota, em que este pode apresentar um roteiro do local da ocorrência e gerar um mapa para, nesse local, retornar em data futura e efetuar uma vistoria quanto à situação do mesmo, muito válido para situações de ocorrências em locais de difícil localização.
- c) Apresentar quais TIC que podem ser aderentes à função BPMA.
Durante a pesquisa, observou-se que todas as TIC de cunho administrativo são utilizadas pela BPMA. Contudo, a parte operacional tem sérias

dificuldades e o sistema SADE e SISP seriam de grande valia para a estrutura, bem como a nova TIC de Mobile SISP pode ser um grande ganho, desde que devidamente estruturada para a finalidade de fiscalização ambiental e produção de relatório.

Não tendo este trabalho o objetivo de esgotar a discussão sobre as TIC existentes na PMSC e que podem ser aderentes a BPMA, entendemos ser necessário um aprofundamento em trabalhos futuros quanto à falta de TIC que efetuem o controle de ocorrências ambientais dentro da BPMA, uma possibilidade de adequação de uma janela de uso para a BPMA dentro do SISP e de possíveis ganhos quanto à gestão do trabalho desenvolvido pela BPMA, com o auxílio de TIC para o desenvolvimento de um planejamento estratégico com vista à redução de determinados delitos ambientais.

REFERÊNCIAS

- AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL – ABDI. **Sistemas Aplicados à Segurança Pública**. Brasília: ABDI, 2010. 226 p. (Cadernos temáticos TICs – IBDI, 3).
- _____. Ministério do Meio Ambiente. Conselho Nacional de Meio Ambiente (CONAMA). Resolução Conama n° 302, de 5 de julho de 2002. Brasília, 2002. Disponível em: <<http://www.mma.gov.br/port/conama/res/res02/res30602.html>>. Acesso em: 28 abr. 2016.
- _____. **Resolução Conama n° 306**, de 5 de julho de 2002. Estabelece os requisitos mínimos e o termo de referência para realização de auditorias ambientais. Brasília, 2002. Disponível em: <<http://www.mma.gov.br/port/conama/legiabre.cfm?codlegi=306>>. Acesso em: 30 mar. 2016.
- FIGUEIREDO, G. J. P.; SILVA, S. T. Elementos balizadores da ação estatal na defesa dos bens ambientais para as presentes e futuras gerações. **Temas de Direito Ambiental e Urbanístico**. São Paulo: Max Limonad, 1998, ano II, n. 3, p. 136-153.
- FURTADO, V. **Tecnologia e gestão da informação na segurança pública**. Rio de Janeiro: Garamond, 2002.
- SANTA CATARINA – SC. **Plano de Comando da Polícia Militar de Santa Catarina de 2011**. Florianópolis: PMSC, 2011.
- _____. **Plano Estratégico 2005-2020**. Florianópolis: PMSC, 2005.
- SILVA, E. R. G.; OLIVEIRA, T. P. S.; BEDIN S. P. M.; ROVER, A. J.; KERN, V. M. Visão sistêmica na interoperabilidade dos sistemas para segurança pública estudo do caso de Santa Catarina. **Anais da Conferência Ibero-Americana WWW/internet**. Lisboa: IADIS Press, 2008, p. 377-384.

14

CAPÍTULO

EDUCAÇÃO A DISTÂNCIA, TECNOLOGIA E LEGISLAÇÃO PRISIONAL

*Leandro da Silva Reis
Rangel Machado Simon
Fernando José Spanhol
Marcio Vieira de Souza*

1 INTRODUÇÃO

Quando se fala de ressocializar aquele que cumpre pena no sistema carcerário brasileiro, em um primeiro momento, pensa-se em sua profissionalização. Para isso, a Lei de Execuções Penais (Lei nº 7.210, de 11 de julho de 1984) oferece aos apenados a possibilidade de estudar e trabalhar dentro do estabelecimento prisional, podendo reduzir o tempo de sua pena a cada a cada três dias de trabalho ou de estudo. Isso se tornou possível a partir de 2007, quando foi permitido, pelo Superior Tribunal de Justiça, o ensino formal dos apenados, sendo fixado com as alterações trazidas pela Lei nº 12.433, de 29 de junho de 2011.

Entretanto, essa profissionalização pode ser insuficiente para reinseri-lo na sociedade, que já não o verá com bons olhos no momento de contratá-lo. E é aí que o sistema educacional carcerário falha. Em razão disso, é preciso pensar em novas formas de ensino profissional dessa classe, de modo a superar o preconceito no momento do seu retorno ao mercado de trabalho, indo além de somente garantir o ensino fundamental e médio.

É nesse contexto que a educação a distância surge como uma solução que merece ser pensada e desenvolvida, diante de seu caráter inclusivo, capaz de diminuir as distâncias sociais para essas pessoas já privadas de tantos direitos.

As questões relativas à educação para os marginalizados sempre foram recorrentes no pensamento de muitos estudiosos, atrelada à emancipação humana. Thompson (2010), Martinho (2006), Beber (2007) e Claude (2006) foram expoentes desse pensamento, pautados na crença da possibilidade de se produzir um saber relacionado com o agir e com as condições marginais do ser.

Este estudo objetiva discutir aspectos pertinentes a processos educacionais direcionados à população carcerária. Para Vieira (2008, p. 87), “as políticas de segurança enfatizam o emprego em larga escala de instrumentos repressivos e ações mais severas sobre criminosos condenados”. Mas a maior preocupação tem sido a de assegurar o afastamento momentâneo de criminosos do convívio social e promover uma reinserção do detento após o fim de sua pena. Por meio das várias políticas implementadas, pergunta-se: qual a importância do EAD no sistema prisional?

2 REFERENCIAL TEÓRICO

As penitenciárias foram criadas como alternativas mais humanas aos castigos corporais e à pena de morte. O Sistema Penal Brasileiro apresenta o aspecto da reprovação e a prevenção do crime. No entanto, a quase totalidade de presídios no Brasil apresenta uma realidade que põe em questionamento o alcance dessas duas finalidades da pena. Elas deveriam atender às necessidades sociais de punição enquanto se reeducassem os infratores. Infelizmente, as prisões têm servido a propósitos diferentes daqueles originalmente idealizados, privando o infrator de seu acesso à humanidade (MELGARÉ, 2010). “A educação é um direito social garantido pela Constituição e não um privilégio. Portanto, entende-se que a educação prisional não está excluída desse direito conforme o Art. 1º, inciso III, art 5º, § 2º” (BRASIL, 1988, art 6º e 205).

Para Beber (2007, p. 11), “o gerenciamento do Sistema Educacional Prisional Brasileiro tem sido nas últimas décadas, palco de expressivas reflexões e análises”. A autora ainda comenta que sua estrutura de gerenciamento e seu planejamento de ação, pois seres humanos encontram-se nestes espaços e necessitam

de ações eficientes, eficazes e efetivas que os auxiliem no processo de reeducação, reinserção e ressocialização.

Dentro dessa perspectiva e na tentativa de harmonizar os parâmetros de uma segurança cidadã com o contexto carcerário (cujo respeito à garantia dos direitos humanos é questionável), o Estado vem desenvolvendo ações com propostas humanizadoras no sistema penitenciário. Uma dessas iniciativas é o fomento à educação no processo de ressocialização do indivíduo privado da liberdade pelo o Decreto nº 1.093/94, que regulamentou os recursos do fundo que devem ser aplicados na formação cultural e educacional detento (MELGARÉ, 2010, p. 8). “Cometer um novo delito é o dilema que acompanha o ex-detento por toda a vida, e este medo chega também ao seu possível futuro padrão, inviabilizando o trabalho. A falta de oportunidades reserva uma única opção ao ex-presidiário: voltar a infringir a lei” (MARTINHO, 2006, p. 67).

É entendido pela sociedade que trabalhar ou estudar na prisão diminuem as chances de reincidência. Tratar o preso dignamente e oferecer a ele trabalho e educação, além de inseri-lo no mercado de trabalho, é uma maneira de combater o crime. A ressocialização é uma exigência. Para que isso ocorra, são necessários cursos profissionalizantes, atividades laborais e educação formal. Para Oliveira (2006, p. 11), “ações de ressocialização do indivíduo preso estão longe de ser uma realidade”. Shella (2007, p. 40) informa que “apenas 15% dos apenados estudam na prisão, participando de atividades educacionais de alfabetização, ensino fundamental, ensino médio e supletivo”. A sociedade precisa incentivar a criação de oportunidades de trabalho e de cursos de capacitação profissional para presos e egressos do sistema carcerário, de modo a concretizar ações de cidadania e promover a ressocialização.

A prisão existe para reabilitar o indivíduo, uma vez que o mundo externo à prisão não lhe deu esta condição (SOARES, 2002).

Devem-se buscar alternativas que possam reparar o problema relativo ao acesso à educação. Para isso, devemos admitir o fracasso da pena de prisão e a falácia do atual sistema (DALLARI, 2004).

O Decreto nº 5.622/97 determina em que a nível educacional a educação a distância poderá ser ofertada, dentre os quais se incluem a educação básica e a educação de jovens e adultos (BRASIL, 1998).

Nesta seara, a educação a distância representa uma proposta de ensino autônoma, em que o aluno deixa de ser um receptor passivo e torna-se responsável por sua aprendizagem, podendo estudar em ritmo individualizado (CLAUDE, 2006, p. 8).

O processo penal estigmatiza o indivíduo que já foi processado e condenado; ele ficará marcado, reiniciando o ciclo da discriminação na sociedade, aumentando as chances do apenado deixar a praticar crimes assim que posto em liberdade,

conforme Fonseca (2006). Nesse viés, critica Vieira (2008, p. 49): “[...] as pessoas presas como as ‘não lembradas’ pela Carta Magna de 1988: dentre todos os novos sujeitos de direitos emergentes da Constituição, um ficou esquecido: o preso. O sujeito privado da liberdade e que inclui tanto o adolescente, quanto a mulher e o homem adulto”.

No Brasil, a educação a distância tem valor estratégico por possibilitar a democratização do acesso à educação, ao propiciar inúmeras possibilidades de inclusão pelo acesso, conforme Coelho (2008, p. 82). Para Thompson (2010, p. 198), ela se mostra como uma modalidade de sucesso que, inclusive, vem sendo implantada em alguns estados como política de ressocialização de apenados do sistema prisional.

Beber (2007, p. 16) ressalta a necessidade de entendê-la como uma modalidade de ensino que possibilita gerir melhor a escolarização, uma vez que oferece recursos para redimensionar a dependência do ensino face a face, em razão de suas características principais serem a interatividade e a cooperação entre os envolvidos, bem como a autonomia estudantil (DALLARI, 2004).

Nesse contexto, Vieira (2008) registra inícios de projetos utilizando ensino a distância em penitenciárias, no Paraná e no interior de São Paulo, com o objetivo de difundir as atividades profissionalizantes. Essas iniciativas mostram a necessidade de apresentar novos modelos educacionais para essa classe, para garantir-lhes o acesso à educação, mesmo porque há ainda o risco de voltarem a cometer crimes caso saiam do presídio para estudar, como melhor expõe Carvalho (2008, p. 102): “Além do preconceito dos estudantes regulares à presença de detentos compartilhando o mesmo espaço e a possibilidade real de confrontos que ameaçaria a segurança de estudantes e professores”.

A Lei de Execução Penal, no § 1º do Art. 126, prevê que a remição da pena se dará com o abatimento de um dia de pena a cada 12 horas de frequência escolar, em atividade de ensino. Neste caso, a educação a distância pode se configurar de maneira estratégica para as pessoas que se encontram privadas de liberdade.

Carvalho (2008, p. 203) mostra que à medida que o ensino a distância é apresentado à penitenciária, transforma a realidade dos detentos que a ele tem acesso. O autor acompanhou o ensino de licenciatura em Pedagogia em uma penitenciária do interior de São Paulo. Segundo ele, depois que começam a estudar, eles não enxergam mais as grades e passam a projetar melhor o seu futuro.

Segundo Alves (2003, p. 78), é preciso “que o governo e a sociedade entendam que a pena e a prisão devem ser realizadas em função de objetivos e metas educacionais e não mais como meros instrumentos de controle social”.

Cada estado tem seu Plano Estadual de Educação nas Prisões, que contempla um projeto político-pedagógico, cuja estrutura é analisada a partir dos dispositi-

vos da Lei de Diretrizes e Bases da Educação (LDB – Lei nº 9.394/96) e da Lei de Execução Penal (LEP – Lei nº 7.210/84).

As ações educativas no sistema prisional e na perspectiva de afirmação de direitos das pessoas em privação de liberdade foi fundamental para dar operacionalidade à legislação. O Conselho Nacional de Política Criminal e Penitenciária, por meio da Resolução nº 14/94, editou as regras para o tratamento do preso. De acordo com Julião (2008, p. 92), esta redação aborda as instruções e assistência educacional:

Art. 8. A assistência educacional compreenderá a instrução escolar e a formação profissional do preso.

Art. 39. O ensino profissional será ministrado em nível de iniciação e de aperfeiçoamento técnico.

Art. 40. A instrução primária será obrigatoriamente ofertada a todos os presos que não a possuam.

Parágrafo único – Cursos de alfabetização serão obrigatórios e compulsórios para os analfabetos.

Art. 41. Os estabelecimentos prisionais contarão com biblioteca organizada com livros de conteúdo informativo, educativo e recreativo, adequado à formação cultural, profissional e espiritual do preso.

Art. 42. Deverá ser permitido ao preso participar de curso por correspondência, rádio ou televisão, sem prejuízo da disciplina e da segurança do estabelecimento.

A modalidade de ensino adotada nas escolas do sistema penitenciário, na maioria das unidades prisionais do Brasil, é a Educação de Jovens e Adultos (EJA), que, de acordo com a LDB nº 9394/96, “destina-se àqueles que não tiveram acesso ou continuidade de estudos no ensino fundamental e médio na idade própria”.

Para Alves (2003, p. 74), “a modalidade de ensino EAD vem ao encontro da necessidade do perfil dos reclusos no Sistema Prisional e sua inserção à ressocialização”. Assim, a EJA propõe articular esta modalidade com as diversidades do contexto social de uma população em privação de liberdade. “Sabemos da importância da presença física no decorrer do aprendizado. Para uma pessoa que se encontra privada de liberdade, entende-se que a EAD possa cumprir um papel importante em seu processo educativo” (MELGARÉ, 2010, p. 91).

A importância da EAD como elemento de integração e de aprendizagem do ensino inova nos parâmetros da limitação física em presídios ou qualquer outra unidade do sistema (MARTINHO, 2006).

A educação deveria ser prioritária no processo do tratamento penal, durante todo o período de cumprimento da pena. É evidente que o apenado tem preserva-

do seus direitos constitucionais de acesso a programas educacionais, mas o que se coloca como desafio é de que forma tornar realidade aquilo que a lei lhe assegura. Geralmente, as unidades penais, em sua grande maioria, não têm acesso aos avanços tecnológicos e benefícios sociais para prestar este serviço, razões pelas quais acabam ficando à margem do processo educacional (OLIVEIRA, 2006).

Segundo Siqueira (2001, p. 93), a modalidade EAD tende aumentar seu valor social à medida que as tecnologias se aperfeiçoam e princípios pedagógicos compatíveis são construídos. Novos dispositivos computacionais têm alterado o conceito da distância a partir da internet. Nas instituições prisionais, o EAD surge como possibilidade de difusão da educação e como uma opção para a inclusão social face à limitação do sistema educativo convencional e da problemática em adotá-lo no sistema prisional.

Já Carvalho (2008, p. 159) entende que “o primeiro passo para reduzir ou até evitar o fosso digital entre o contexto prisional é definir o que é essencial no aprendizado EAD”. Ao conhecer as instituições do sistema prisional, qualquer um entenderia que perante as condições atuais dos estabelecimentos prisionais é imperativo equipar os espaços de aula de modo a que os reclusos possam ter acesso às tecnologias de informação e comunicação que povoam o dia a dia das pessoas e das sociedades.

3 CONSIDERAÇÕES FINAIS

Retomando a pergunta de pesquisa, a importância do EAD no sistema prisional é fundamental para os apenados oportunizarem uma qualidade de vida melhor. Por meio do pensamento de que o estudo abre a mente e muda a vida, passa a ser importante um amparo educacional do porte que o EAD oferece. É direito dos apenados serem tratados com dignidade e respeito. Assim, a importância cresce de políticas que promovam a recuperação do preso no convívio social e tendo por ferramenta básica a Lei de Execução Penal e seus dois eixos: punir e ressocializar.

A maneira como se conduz a educação dentro do sistema penitenciário não tem até o momento representado efetiva contribuição para que o preso possa, de fato, ser reinserido na sociedade. Em 1984, o Congresso aprovou uma reforma para o sistema prisional por meio da Lei de Execução Penal, que reconhece o direito do preso à assistência educacional. O Brasil tem uma das legislações mais avançadas do mundo para o setor penitenciário. Mas creio que o problema é de infraestrutura e de iniciativa financeira dos governos. Essa inovação não foi, ainda, suficiente para resolver o caos em que se encontra o sistema penitenciário do país.

É necessário conceber as ações educacionais para o desenvolvimento da cognitividade, da percepção crítica dos interesses presentes na cena social e da pro-

dução, sob diversos modos, de ações (e a questão do EAD proporciona isso aos presos) sem discriminar perversamente a massa carcerária. Ações educacionais devem ressaltar a condição dos presos e buscar dotá-los de instrumentos capazes de empreender o repensar crítico, expressas sob estereótipos, legitimando mecanismos de dominação social e de discriminação, obstaculizando a democratização da sociedade na medida em que esses apenados são os que mais sofrem as incidências das desigualdades sociais.

Alguns experimentos em educação a distância revelaram a possibilidade de concretizar o oferecimento de atividades educacionais aos presos. Algumas políticas públicas vislumbram projetos desenvolvidos que tornam possível a sensação de pertencimento destes apenados, oferecendo-lhes oportunidade de conviver no ambiente acadêmico. Trata-se de iniciativas tímidas, em confronto com a ampla população carcerária. Mas creio ser uma iniciativa que sinaliza para a promoção de um modelo penitenciário mais moderno, mas não se apresenta como solução para os problemas que atravessa o sistema prisional.

O impacto do ensino na vida e na autoestima dos presos é evidente. A receptividade do EAD em penitenciárias que disponibilizam um projeto educacional como meio de ressocializar indica que os resultados podem ser bastante promissores.

Assim, o educação a distância mostra-se como uma ferramenta essencial deste processo, valorizando o trabalho da educação democrática, sem discriminação, diminuindo a criminalidade e formando cidadãos conscientes e praticantes de boas ações.

Como trabalhos futuros, sugere-se um estudo de caso com a aplicação de um projeto-piloto de educação a distancia profissionalizante em uma penitenciária, bem como uma análise qualitativa por meio de questionários semi-estruturado com os reeducandos participantes do projeto, com vista a observar o grau de desempenho e aprendizado em relação ao método tradicional hoje aplicado nos presídios brasileiros, buscando melhorias na metodologia de ensino à distancia e no conteúdo a ser abordado.

REFERÊNCIAS

ALVES, J. D. *Do tratamento penal à reinserção social do criminoso*. Universidade Federal do Paraná. Pós-Graduação em Modalidades de Tratamento Penal e Gestão Prisional. Curitiba, 2003.

BEBER, B. *Reeducar, reinserir e ressocializar*. 2007. 146 f. Tese (Doutorado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2007. Disponível em: <<http://btd.egc.ufsc.br/wp-content/uploads/2007/08/bernadette-beber.pdf>>. Acesso em: 9 mar. 2016.

- BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <<http://www.planalto.gov.br/constituicao>>. Acesso em: 9 mar. 2016.
- CARVALHO, S. **Pena e garantias**. Rio de Janeiro: Juris, 2008.
- CHAVES, E. **Tecnologia na educação: conceitos básicos**. 2004. Disponível em: <<http://www.feg.unesp.br/eadconceitos.htm>>. Acesso em: 9 mar. 2016.
- CLAUDE, R. P. **Direito à educação e educação para os direitos humanos**. *Revista Internacional de Direitos Humanos*, n.2, 2006.
- COELHO, E. C. **A criminalização da marginalidade e a marginalização da criminalidade**. *Revista de Administração Pública*, v.15, 2008.
- DALLARI, D. A. **Direitos humanos e cidadania**. São Paulo: Moderna, 2004.
- FONSECA, R. V. **A profissionalização dos apenados, por meio da educação a distancia, como contribuição à inserção ao mercado de trabalho: o caso da Penitenciária de Florianópolis/SC. Pós-Graduação**. Universidade Federal de Santa Catarina. Florianópolis, 2011. Acesso em: 10 mar. 2016.
- JULIÃO, E. F. **Educação e trabalho como propostas políticas de execução penal. Alfabetização e cidadania, revista de educação de jovens e adultos**. Brasília: Unesco, 2008.
- MARTINHO, A. **A educação no sistema prisional**. 2006. Disponível em: <<http://www.artigonal.com/educacao-no-sistema-prisional>>. Acesso em: 10 de mar. 2016.
- MELGARÉ, P. **Dignidade da pessoa humana**. São Paulo: Malheiros, 2010.
- OLIVEIRA, E. G. **Educação à distância na transição pragmática**. 3. ed. São Paulo: Papirus, 2006.
- SHELLA, F. **Prisão e reabilitação: a visão das assistentes sociais do departamento penitenciário**. Dissertação de mestrado. Universidade Federal do Paraná. Curitiba, 2007.
- SIQUEIRA, J. R. **O trabalho e a assistência social na reintegração do preso à sociedade**. *Periódicos*, v. 22, n. 67, ex. 1. São Paulo: Cortez, 2001.
- SOARES, R. **Direitos do presidiário**. São Paulo: Método, 2002.
- THOMPSON, A. **A questão penitenciária**. 8.ed. Rio de Janeiro: Forense, 2010.
- VIEIRA, O. **Direitos fundamentais**. São Paulo: Malheiros, 2008.

15

CAPÍTULO

O USO DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NA MEDIAÇÃO DA ESPECIALIZAÇÃO EM TIC APLICADAS À SEGURANÇA PÚBLICA E DIREITOS HUMANOS

*Natana Lopes Pereira
Fernando José Spanhol
Thabata Clezar de Almeida*

1 INTRODUÇÃO

O desenvolvimento das tecnologias impulsionou o surgimento da cultura digital, tendo como principal característica o uso das Tecnologias da Informação e Comunicação (TIC) e propondo maior acesso ao processo de ensino aprendizagem e na construção competência virtual individual.

Nesse contexto, destaca-se o estudo de caso realizado no curso de especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos (Pós TIC Senasp), da Universidade Federal de Santa Catarina, *campus* de Araranguá.

O referido curso é destinado a profissionais de segurança pública em atividade: policiais civis, policiais militares, bombeiros militares, profissionais de perícia forense, guardas municipais, policiais federais, policiais rodoviários federais, agentes penitenciários federais e estaduais, disponibilizando-se 40 vagas para os mesmos, assim como dez vagas para representantes da sociedade civil.

Pereira (2015) apud Lunardi (2013) destaca como objetivo geral do curso a capacitação de profissionais de Segurança Pública e membros da sociedade civil, na utilização de Tecnologias da Informação e Comunicação para prevenção, combate e diminuição da violência e criminalidade, bem como na defesa e na promoção dos direitos humanos no extremo sul catarinense.

Seus objetivos específicos, segundo Pereira (2015) apud Lunardi (2013), são os seguintes: capacitar 40 profissionais de Segurança Pública e dez membros da sociedade civil, e consolidar grupos interinstitucionais e de movimentos sociais com projetos de ensino, pesquisa, extensão e inovação na área de TIC aplicada à Segurança Pública e Direitos Humanos na região do extremo sul catarinense.

O curso, realizado de forma presencial, utilizou alguns sistemas computacionais disponibilizados pela Universidade Federal de Santa Catarina (UFSC) em sua execução. Visando observar a importância desses sistemas, aplicou-se um instrumento de coleta de dados, com o objetivo principal de analisar a aplicabilidade dos sistemas computacionais utilizados no decorrer do curso, além de obter uma avaliação global do curso envolvendo professores, infraestrutura, apoio extraclasse, desenvolvimento próprio, curso, biblioteca (BSARA) e restaurante universitário (RU).

Desta forma, o presente estudo objetiva apresentar, além do desempenho e aplicabilidade do curso, os sistemas e os aspectos referentes à tecnologia disponibilizados aos alunos no mesmo.

2 FUNDAMENTAÇÃO

O uso de novas TIC está cada vez mais presente no cotidiano das pessoas. A sociedade as utiliza para vários fins, como lazer, educação, trabalho, entre outros. Podem ser utilizadas por distintas faixas etárias e por diferentes classes sociais, proporcionando, segundo Andrade e Silva (2008), uma sociedade globalizada, o conhecimento de diversas culturas, a melhoria dos meios de comunicação e aumento da rapidez.

Para Silva et al. (2011), a tecnologia está tão presente em nosso cotidiano que não notamos mais que são artificiais. O avanço tecnológico garantiu novas

maneiras de usar as TIC para a produção e propagação de informações, a interação e a comunicação em tempo real, contribuindo, assim, para o surgimento das Tecnologias de Informação e Comunicação.

A cada instante surge um novo recurso tecnológico, para um ou diversos fins, visando facilitar ou auxiliar em diversas ou determinada atividade.

Nesse contexto, Rosseti e Morales (2007) destacam que essas novas informações, comunicação e tecnologias computacionais estão mudando a organização e o conteúdo de trabalho; enfatizando, em certa escala, que carreiras de trabalho de longa vida estão se transformando em um mosaico, no qual o trabalho produtivo, o aprendizado e o desenvolvimento de competência são inseparáveis. Os autores consideram, ainda, que elas favorecem a renovação em redes informais de aquisição e de troca de conhecimento, além de facilitar o compartilhamento de problemas, perspectivas, ideias e soluções em seu dia a dia profissional.

Este avanço tecnológico molda a sociedade, em constante busca por informação e conhecimento. Desta forma, é de extrema importância o investimento das organizações em capacitações nas mais diversas áreas. Nesse contexto, visando principalmente qualificar profissionais de segurança pública, instituiu-se a Rede Nacional de Estudos em Segurança Pública, a ser implementada pela Secretaria Nacional de Segurança Pública (Senasp), por meio do Departamento de Pesquisa, Análise de Informação e Desenvolvimento de Pessoal em Segurança Pública (Depaid).

A Renaesp é um projeto de educação permanente, voltado aos profissionais de segurança pública, e também aos interessados e atuantes nesta área. A rede constitui-se a partir da parceria com Instituições de Ensino Superior (IES), que promovem cursos de pós-graduação *lato sensu*, na modalidade presencial, sobre diferentes temas relacionados à Segurança Pública (BRASIL, 2015 apud MIKI, 2015)

A proposta do curso de especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos foi aprovada pelo Ministério da Justiça, por meio do Edital de Chamada Pública nº 6, de 21 de junho de 2012. Este edital selecionou propostas referentes a projetos de curso de pós-graduação *lato sensu*, especialização em segurança pública, com o escopo de estabelecer parceria que se efetivasse por meio de Termo de Cooperação. O objetivo de edital proposto foi a oferta por instituições federais de ensino superior de cursos de pós-graduação *lato sensu* (especialização), na modalidade presencial, destinados a profissionais da segurança pública da ativa, tendo por referência a Matriz Curricular Nacional nas áreas temáticas informadas no edital. A proposta conteve-se nas temáticas de gestão de conhecimento, informações sobre violência e criminalidade, e Segurança Pública e Direitos Humanos.

3 PROCEDIMENTOS METODOLÓGICOS

Com o objetivo de analisar a importância dos sistemas computacionais utilizados no curso, o procedimento metodológico adotado nesta pesquisa caracteriza-se como descritivo, predominantemente qualitativo, documental e bibliográfico.

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. Permite ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que poderia pesquisar diretamente.

Para poder identificar os benefícios e as dificuldades encontradas na execução do projeto foi adotada a pesquisa descritiva que, de acordo com Lakatos e Marconi (2010, p.170) “apresenta como principal finalidade o delineamento ou análise das características de fatos ou fenômenos, a avaliação de programas, ou o isolamento de variáveis principais ou chave”.

Como a pesquisa abrangia dados de difícil mensuração, utilizou-se da pesquisa quantitativa, que, segundo Dalvofo, Lana e Silveira (2008) apud Richardson (1989), é uma forma adequada para entender e analisar dados de difícil mensuração como motivações e dificuldades pessoais.

Em relação aos meios, caracteriza-se, segundo Lakatos e Marconi (2010, p.157), como pesquisa documental pela fonte de coleta de dados constituída de fontes primárias como documentos internos, arquivos virtuais e físicos com dados sobre o curso, website institucional, relatórios e outros documentos.

3.1 Coleta de Dados

Quanto à coleta de dados, realizou-se pesquisa aplicada aos alunos do curso de especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos.

A pesquisa, composta por 61 questões, abrangia avaliação sobre: **docentes, infraestrutura, apoio extraclasse, desenvolvimento próprio, o curso, Moodle, CAPG, ID UFSC–SETIC, biblioteca e restaurante universitário.**

O instrumento para coleta de dados utilizado foi o Formulário Google Drive. Ele organiza, de forma automática em Planilhas Google as informações dos dados coletados, possibilitando a visualização dos dados por meio de gráficos.

Segundo Pereira (2015, p. 35), o “software utilizado para elaboração e aplicação da pesquisa possibilita o armazenamento de arquivos na nuvem, podendo estes ser compartilhados com quem o usuário disponibilizar o acesso”.

Para a análise dos dados, utilizou-se itens de múltipla escolha, sendo disponibilizada a seguinte escala de satisfação: **Ótimo**, **Bom**, **Regular**, **Ruim** ou **Péssimo**, correspondendo aos valores 5, 4, 3, 2, 1, respectivamente.

Além dos temas de múltipla escolha, foi aplicada uma questão descritiva, com predominância da análise qualitativa.

4 AMBIENTES COMPUTACIONAIS DA UFSC

A Universidade Federal de Santa Catarina utiliza diversos ambientes computacionais, visando à melhoria na gestão administrativa e acadêmica, refletindo em um sistema organizado, eficiente e consistente.

Nesse sentido, Pereira (2015) lista como sistemas de gestão acadêmica:

Quadro 15.1 Sistemas de gestão acadêmica

Gestão Acadêmica	<p>CAPG – Controle Acadêmico de Pós-Graduação</p> <p>CAGR – Controle Acadêmico de Graduação</p> <p>MOODLE – <i>Modular Object Oriented Distance Learning</i></p> <p>BSARA – Biblioteca Universitária da Universidade Federal de Santa Catarina</p> <p>IdUFSC – Sistema de Gestão de Identidade da UFSC</p>
-------------------------	---

Os sistemas de gestão administrativa, criados para servir de suporte técnico ao propósito de reduzir o uso de papel nas rotinas administrativas da instituição, são os seguintes (PEREIRA, 2015):

Quadro 15.2 Sistemas de gestão administrativa

Gestão Administrativa	<p>ALX – Sistema de Gestão de Materiais</p> <p>SCL – Sistema de Gestão de Compras e Licitações</p> <p>SIP – Sistema de Gestão Patrimonial</p> <p>SPA – Sistema de Processos Administrativos</p> <p>SCL – Sistema de Gestão de Compras e Licitações</p>
------------------------------	---

5 AMBIENTES UTILIZADOS

Além da avaliação sobre docentes, infraestrutura, apoio extraclasse, desenvolvimento próprio e avaliação do curso, a pesquisa também analisou os seguin-

tes sistemas computacionais da área de gestão acadêmica utilizados no decorrer do curso:

- a) CAPG (Controle Acadêmico de Pós-Graduação).
- b) MOODLE (*Modular Object Oriented Distance Learning*).
- c) IdUFSC (Sistema de Gestão de Identidade da UFSC) e serviços SETIC.
- d) BSARA (Biblioteca Universitária da Universidade Federal de Santa Catarina – *Campus Araranguá*).

6 RESULTADO DA PESQUISA APLICADA

Visando à análise sobre os elementos que regem o curso, em especial sobre os sistemas computacionais utilizados, aplicou-se instrumento de coleta de dados aos alunos do curso de especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos para avaliar o índice de satisfação sobre os itens analisados.

A pesquisa foi enviada aos 33 alunos do curso, obtendo retorno de 20 acadêmicos. Constatou-se que todos os itens pesquisados obtiveram maior porcentagem nos índices: Ótimo e Bom, sendo interpretado como um indicativo da positiva execução do curso.

A partir da análise dos dados coletados, referente a professores, infraestrutura, apoio extraclasse, desenvolvimento próprio e curso, pode-se constatar que:

- a) aulas planejadas de forma clara e objetiva, com dinâmicas predominantemente expositivas, sendo estas realizadas por professores qualificados, com alto nível de conhecimento;
- b) o incentivo pelos docentes aos discentes na publicação de artigos;
- c) infraestrutura com espaço, iluminação e equipamentos adequados;
- d) avaliação positiva ao desempenho da coordenação do curso;
- e) predominância da escala de satisfação Ótima referente à avaliação do curso, sendo de extrema importância ao desempenho profissional dos alunos;
- f) ótimo desempenho dos professores, apresentando proposta curricular equilibrada;
- g) material didático mais utilizado: livros, artigos e periódicos;
- h) dificuldades no curso em relação ao conteúdo, mas não em relação à condução do mesmo pelo docente.

Em relação aos sistemas acadêmicos utilizados pelos alunos (MOODLE e CAPG), a pesquisa apontou os seguintes índices:

- a) utilização do ambiente virtual de aprendizagem Moodle, sendo constatado baixo grau de dificuldade em utilizar os recursos disponibilizados;

- b) frequência de acesso ao Moodle, pelos acadêmicos, duas a três vezes por semana;
- c) prática frequente de exercícios, por meio de recursos disponibilizados do Moodle;
- d) dificuldade de acesso ao CAPG relacionado à falta de informação sobre sua funcionalidade;
- e) frequência de acesso ao CAPG com predominância mensal e quinzenalmente.

O instrumento de avaliação aplicado apresentou um positivo índice de aprovação ao curso e todos seus fatores relacionados. Destaca-se, entre vários itens, a avaliação dos acadêmicos em relação ao nível de conhecimento e qualificação didática do corpo docente.

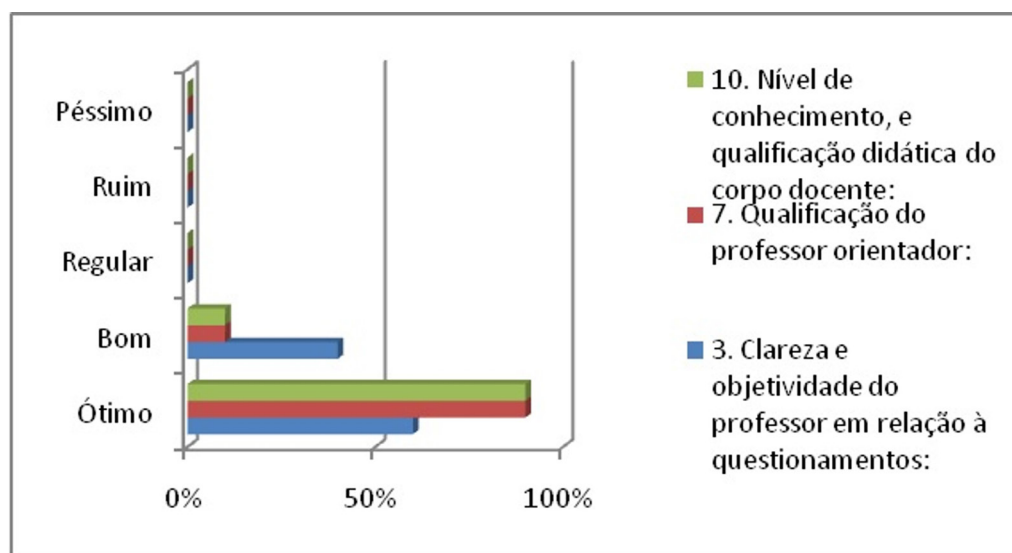


Figura 15.1 Resultado da pesquisa – professores.

7 CONCLUSÃO

O curso de especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos proporcionou aos alunos, por meio de formação acadêmica, o aprimoramento do conhecimento sobre TIC.

As temáticas abrangidas pela proposta do curso são de extrema importância, refletindo maior eficiência e eficácia, maior interatividade e o compartilhamento de informações nas atividades profissionais desenvolvidas pelos alunos.

Com esta pesquisa, pode-se perceber a importância dos sistemas computacionais utilizados na execução do curso, tanto na área de gestão acadêmica, quanto na área de gestão administrativa, que proporcionaram mais qualidade ao ensino dos alunos, destacando-se principalmente o uso do Ambiente Virtual de Ensino e Aprendizagem (AVEA) MOODLE customizado para o curso.

De acordo com os dados coletados, o acesso frequente ao AVEA e a prática constante na utilização de seus recursos interferiram de forma positiva no processo de ensino aprendizagem. Esse ambiente virtual permitiu a integração de distintas mídias, recursos, além das informações apresentadas de maneira organizada, com o intuito de facilitar a interação entre o aluno e o conhecimento proposto pelo curso.

Por fim, evidencia-se, além da importância da proposta do curso de especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos, a relevância de cada item analisado e suas atribuições para resultados satisfatórios do mesmo possam ser repetidos para registro de futuras pesquisas.

REFERÊNCIAS

- ALVES, R. M. Gestão educacional e novas tecnologias da informação comunicação: atualizações necessárias disponíveis para a cultura educacional. **Revista PUC-SP**, São Paulo, v. 12, n. 2, 2014.
- ANDRADE, L. M.; SILVA, F. C. Tecnologias de Informação e Comunicação: as influências das novas tecnologias perante a sociedade. **Associação de Leitura do Brasil**, São Paulo, 2008. Disponível em: <http://alb.com.br/arquivo-morto/anais-jornal/jornal4/comunicacoesPDF/62_tecnologiasFABIANO.pdf>. Acesso em: 15 ago. 2015.
- BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. **MJ oferece vagas para pós-graduações em segurança pública**. Brasília, DF, 2015. Disponível em: <<http://www.justica.gov.br/noticias/mj-oferece-vagas-para-pos-graduacoes-em-seguranca-publica-oferecem-250-vagas-em-cinco-estados/>>. Acesso em: 9 ago. 2015.
- CORREIA, R. L.; SANTOS, J. G. A importância da Tecnologia da Informação e Comunicação (TIC) na Educação a Distância (EAD) do Ensino Superior (IES). **Revista Aprendizagem em EAD**, Distrito Federal, v. 2, n. 1, 2013. Disponível em: <<http://portalrevistas.ucb.br/index.php/raead/article/viewFile/4399/2899>>. Acesso em: 30 jun. 2015.
- DALFOVO, M. S.; LANA, R. A.; SILVEIRA, A. Métodos quantitativos e qualitativos: um resgate teórico. **Revista Interdisciplinar Científica Aplicada**. Blumenau, v. 2, n. 4, p. 1-13, 2008. Disponível em: <http://www.unisc.br/portal/upload/com_arquivo/metodos_quantitativos_e_qualitativos_um_resgate_teorico.pdf>. Acesso em: 02 jul. 2015.
- GIL, A.C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.
- LAKATOS, E. M.; MARCONI, M. A. **Fundamentos da metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

- LUNARDI, G. M. **Processo 23080.003511/2013-69**. Araranguá: Universidade Federal de Santa Catarina, 2013.
- NAKAYAMA, M. K. et al. **A atuação da Universidade Federal de Santa Catarina no Programa Aluno Integrado: um projeto de extensão**. Florianópolis: UFSC, 2010. Disponível em: <<https://repositorio.ufsc.br/bitstream/handle/123456789/96862/A%20ATUA%C3%87%C3%83O%20DA%20UNIVERSIDADE%20FEDERAL%20DE%20SANTA%20CATARINA%20NO%20PROGR.pdf?sequence=1>>. Acesso em: 28 jun. 2015.
- PACHECO, A. S. V. et al. **Ambientes computacionais e Tecnologias da Informação para a gestão do conhecimento na Universidade Federal de Santa Catarina**. Florianópolis, 2009.
- PEREIRA, D. M.; SILVA, G. S. As Tecnologias de Informação e Comunicação (TICs) como aliadas para o desenvolvimento. **Caderno de Ciências Sociais Aplicadas**. Bahia, n. 10, 2010. Disponível em: <<http://periodicos.uesb.br/index.php/cadernosdeciencias/article/viewFile/884/891>>. Acesso em: 03 jul. 2015.
- PEREIRA, N. L. Avaliação dos sistemas computacionais utilizados no curso Pós TIC SENASP- UFSC. Araranguá. 2015. 55 p. (Relatório de Estágio II - UFSC)
- ROSSETI, A.; MORALES, A. B. O papel da tecnologia da informação e na gestão do conhecimento. **Revista Ciência da Informação**, Brasília, DF, v. 36, n. 1, p. 124-135, jan.-abr., 2007. Disponível em: <<http://revista.ibict.br/ciinf/article/view/1191/1363>>. Acesso em: 18 jun. 2015.
- SILVA, E. R. G.; OLIVEIRA, T. P. S.; ARAÚJO, T. S.; ROVER, A. J. Sistema integrado de gestão da informação para segurança pública. **3ª Conferência Ibérica de Sistemas e Tecnologias de Informação**. Vigo, Espanha, 2008. Disponível em: <<http://revistapos.cruzeirosul.edu.br/index.php/epd/article/viewFile/511/436>>. Acesso em: 20 jun. 2015.
- SILVA, J. F.; SCHIMIGUEL, J. O uso das TICs no ensino superior: a integração de diferentes tecnologias à educação estatística. **Encontro de Produção Discente PUCSP/Cruzeiro do Sul**, São Paulo, v.1, n.1, 2012. Disponível em <<http://revistapos.cruzeirosul.edu.br/index.php/epd/article/viewFile/511/436>>. Acesso em: 20 abr. 2015.
- SILVA, R. P. Educação e segurança pública: uma perspectiva de cidadania e Direitos Humanos. **Revista Espaço Acadêmico**. v.11, n.125, 2011. Disponível em: <<http://www.periodicos.uem.br/>>. Acesso em: 20 abr. 2015.
- UNIVERSIDADE FEDERAL DE SANTA CATARINA. **Sistemas de Gestão Administrativa**. Florianópolis, 2015. Disponível em: <<http://egestao.ufsc.br/>>. Acesso em: 16 maio. 2016.

