O IMPACTO DA BIOMETRIA NA ÁREA DE ABRANGÊNCIA DO CIOSP-MT E A BUSCA DE NOVAS TECNOLOGIAS

Cláudio Victor Freesz[1]
Oswaldo Marins Rabelo[2]

RESUMO

O presente artigo científico tem por objetivo demonstrar a importância da tecnologia, em especial, a implementação da biometria, sob suas diversas modalidades no trabalho policial diuturno, que por consequência lógica implicará na excelência e qualidade total em toda a cadeia da persecução penal. Foi utilizado uma metodologia hipotético-dedutivo com consulta documental por sites em tecnologia e referencial bibliográfica, além de mencionarmos as modalidades biométricas e suas especificidades, teceremos comentários sobre os problemas atuais da identificação no Estado, bem como a dificuldade entre os sistemas biométricos, a exemplo dos Tribunais Regionais Eleitorais e o projeto nacional do Registro de Identidade Civil (RIC). Proporemos a implementação da biometria de forma parcial e gradativa com sistemas compatíveis, tendo como ponto de partida a área delimitada pelo Centro Integrado de Operações de Segurança do Estado de Mato Grosso (CIOSP), e em segundo plano, o Estado em sua totalidade.

Palavras-chaves: Biometria - Identificação – Segurança - Sistema - AFIS - RPA – Drone – Digital - Face Recognition - Termografia.

ABSTRACT

This article aims to demonstrate the importance of technology, in particular, the implementation of biometrics, according its various modalities in the daily patrolling, which consequently logically imply excellence and total quality throughout the chain of criminal persecution, a hypothetical-deductive rule was used with documentary consultation by sites in technology and bibliographic reference, in addition to mentioning the biometric modalities and their specificities, we will comment on the current problems of identification in the State, as well as the difficulty between existing biometric systems, such as the Regional Electoral Courts and the national project of Civil Identity Registration, in a first moment, we will propose the implementation of biometrics in a partial and gradual way with compatible systems, starting from the area defined by the Integrated Center of Security Operations of the State of Mato Grosso, and in a second moment the State in total.

Keywords: Biometric - Identification – Security – System – AFIS – RPA – Digital – Face – Recognition - Termografy.

---

[1]Delegado da Polícia Judiciária Civil do Estado de Mato Grosso, Bacharel em Direito pela Universidade do Distrito Federal, Especialista em Direito Agroambiental pela UFMT, certificado pela IMASGAL Espanha PIX4D – Fotogrametria com RPAS, Pós-graduado no Curso Superior de Polícia com ênfase em Estudo de Comando e Estado Maior - APMCV/PMMT.

[2] Tenente Coronel da Polícia Militar do Estado de Mato Grosso. Graduado em Segurança Pública pela APMCV/PMMT, Bacharel em Direito pela Universidade de Cuiabá, Curso de Aperfeiçoamento de Oficiais pelo CBMRO e Pós-graduado no Curso Superior de Polícia com ênfase em Estudo de Comando e Estado Maior - APMCV/PMMT.

INTRODUÇÃO

O presente artigo científico partiu do momento em que se identificou uma problemática existente no âmbito de trabalho do Centro Integrado de Operações de Segurança Pública (CIOSP).

Foi utilizada uma metodologia hipotético-dedutiva com consulta documental por sites em tecnologia e referencial bibliográfico. Foi realizado consultas aos técnicos da área de tecnologia como servidores da Academia de Polícia Civil de Mato Grosso e POLITEC que serviram como norteadores ao tema, bem como entrevista a procurador da Seguradora Líder.

Verificou-se pontualmente certa dificuldade para a identificação de suspeitos e conduzidos, através do policiamento ostensivo, realizado na modalidade de rádio-patrulhamento da Polícia Militar.

Ressalte-se que a área de abrangência do CIOSP engloba toda a região metropolitana dos municípios de Cuiabá e Várzea. Temos a presença de dois plantões de ocorrências policiais (Polícia Judiciária Civil) para lavratura de autos de prisão em flagrante delito e termos circunstanciados de ocorrência, ambos de natureza criminal, sendo um para cada município.

A ERA DA INFORMAÇÃO OU ERA DIGITAL

São termos frequentemente utilizados para designar os avanços tecnológicos advindos da Terceira Revolução Industrial e que reverberaram na difusão de um ciberespaço, um meio de comunicação instrumentalizado pela informática e pela internet.

> Essa expressão também é uma forma de observar os avanços das técnicas atuais de transformação da sociedade em comparação a outras anteriores. Fala-se, por exemplo, que a era digital emerge como uma substituição à era industrial que, por sua vez, emergiu outrora em substituição à era da agricultura. Assim, ao menos em tese, estaríamos passando por um terceiro ciclo de renovações de ideias, ações e pensamentos que marcaram a história da humanidade (PENA, 2019, p. 02).

Com a era digital vem outro desafio, os crimes cibernéticos, todavia, não é o objeto deste artigo.

A IMPORTÂNCIA DA TECNOLOGIA DIGITAL NA BIOMETRIA

Quando se pensa no tema "justiça" somos obrigados a utilizar diferentes pontos de vista. De um modo geral, percebe-se a grandeza do Poder Judiciário em aplicar a lei a aqueles que a infringiram. O Ministério Público funciona como órgão acusador e, em seu oposto os advogados ou defensores públicos garantem aos acusados seu direito constitucional à ampla defesa e ao contraditório (OLIVEIRA, 2009).

Fora do triângulo que constitui a persecução criminal, a autoridade policial, imparcial, entra em cena, e busca no fato criminoso posto, a autoria e a materialidade do delito.

Não vem ao caso neste trabalho tecermos maiores considerações às instituições supracitadas, mas concentrarmos na importância da tecnologia digital na biometria, pois assim conferimos convicção praticamente absoluta na identificação acerca da autoria.

Questões importantes a serem debatidas quanto à implementação da biometria digital pelas polícias civil e militar no âmbito de atuação do CIOSP-MT:

a) Nosso sistema admite falhas quanto à duplicidade de identidades, falsas identidades, identidades indeterminadas, falsidades ideológicas, ausências de portes de documentos?

b) Nosso sistema admite falhas quanto à qualidade das prisões executadas?

c) Nosso sistema admite falhas no cumprimento de mandados de prisões?

d) Todos os processos e inquéritos policiais onde os respectivos réus e indiciados no curso do mesmo falecem, têm imediatamente os processos findos ou inquéritos arquivados?

e) Há algum critério de sondagem imediata do número de vezes e horários que determinado cidadão foi abordado ou encaminhado às delegacias?

f) Há transparência para com a sociedade sobre a legitimidade das prisões realizadas?

g) Há imagens de suspeitos arquivadas em vídeo que até o presente momento não teve sua autoria identificada ante a qualidade das imagens/vídeos?

Se a resposta às perguntas acima for "não" para a maioria dos questionamentos significa que devemos quebrar nossos paradigmas e procurar uma melhoria significativa, pois, qualquer pessoa poderá estar na condição de vítima ou acusado na "esfera da justiça". Só há uma solução para esta questão e ela passa pela mudança do atual quadro em que nos encontramos através da busca de uma implementação tecnológica pela biometria.

A tecnologia desempenha um papel especialmente importante nesse desafio. O estado do Mato Grosso recentemente já deu o primeiro passo com a implantação do recadastramento biométrico junto ao TRE/MT.

Em segundo momento, aguarda-se implantação do RIC (Registro de Identidade Civil), a nível nacional, todavia, devendo observar a conexão entre os sistemas biométricos, pois nem sempre são compatíveis.

É um novo expediente de registro de identidade civil, que unifica todos os estados federados e o Distrito Federal, assegurando, mediante processos multibiométricos e da integração de bases de dados, a identificação segura do brasileiro nato ou naturalizado.

> O Registro de Identidade Civil - RIC surgiu com a Lei nº 9.454 de 07 de abril de 1997, tendo como finalidade precípua a institucionalização de um novo documento de identidade civil. Após 13 anos, a Lei foi regulamentada através do Decreto nº 7.166 de 05 de maio de 2010, que criou o Sistema Nacional de Registro de Identificação Civil – SINRIC e o Comitê Gestor, tendo como órgão central o Ministério da Justiça. O decreto também estabeleceu diretrizes e critérios para implantação, manutenção e controle do RIC, bem como regulamentou sua operacionalização (BRASIL, 2019, p. 03).

O Registro de Identidade Civil serve para identificar de forma absoluta o brasileiro nato ou naturalizado, com o objetivo de garantir sua segurança nas relações com a área pública e privada. É primordial no que diz respeito ao declínio de fraudes, minimizando os prejuízos em todas as esferas de governo e na iniciativa privada. Serve para inclusão social e digital de parcela significativa da população que ainda não tem

acesso a esse tipo de serviço. E, por fim, Inclui-se como instrumento para a melhoria da gestão da segurança pública no país e a modernização do Estado brasileiro.

No estado do Mato Grosso, com a implantação do GEIA (Conjunto de Sistemas da Polícia Judiciária Civil), há possibilidade de não só adicionarmos campo da fotografia dos suspeitos/conduzidos, bem como implementarmos os Sistemas biométricos, atualmente existentes à plataforma do GEIA, bastando haver compatibilidade entre os sistemas adotados. É lógico que tais medidas precisarão de uma pesquisa aprofundada, mas não é impossível.

Além dos plantões metropolitanos da Capital e Várzea Grande, Delegacias especializadas deverão ser prioridades, pois aqui temos a abrangência da área delimitada pelo CIOSP.

Esta tecnologia poderá, em curto espaço de tempo, ser implementada de forma móvel. Pode ser disposta em *tablets* ou celulares, bem como *escaners* digitais, palmares, de íris ou faciais para as viaturas, tanto das Polícias Civil como a Militar.

A BIOMETRIA

Biometria é a ciência que analisa as características físicas ou comportamentais dos seres vivos. Recentemente, este termo também foi associado à medida de características físicas ou comportamentais das pessoas como forma de identificá-las unicamente. Hoje, a biometria é usada na identificação criminal, controle de acesso, etc:

> A biometria é um método de autenticação tecnológica e científica baseado em biologia e usada na garantia de informação (IA). A identificação biométrica autêntica entrada segura, dados ou acesso através de informações biológicas humanas, como DNA ou impressões digitais. Os sistemas biométricos incluem vários componentes vinculados para funcionalidades efetivas. O sistema biométrico conecta um evento a uma única pessoa, enquanto outros formulários de identificação como um número de identificação pessoal (PIN), podem ser usados por qualquer pessoa. A biometria é usada para sistemas de segurança e sistemas de substituição para cartões de identificação, tokens ou PINs. Uma diferença fundamental entre a biometria e outros sistemas é que a verificação biométrica de informações físicas exige que uma pessoa esteja presente, o que adiciona uma camada de segurança porque outros tipos de ID podem ser roubados, perdidos ou falsificados (CRETO, 2019, p. 02).

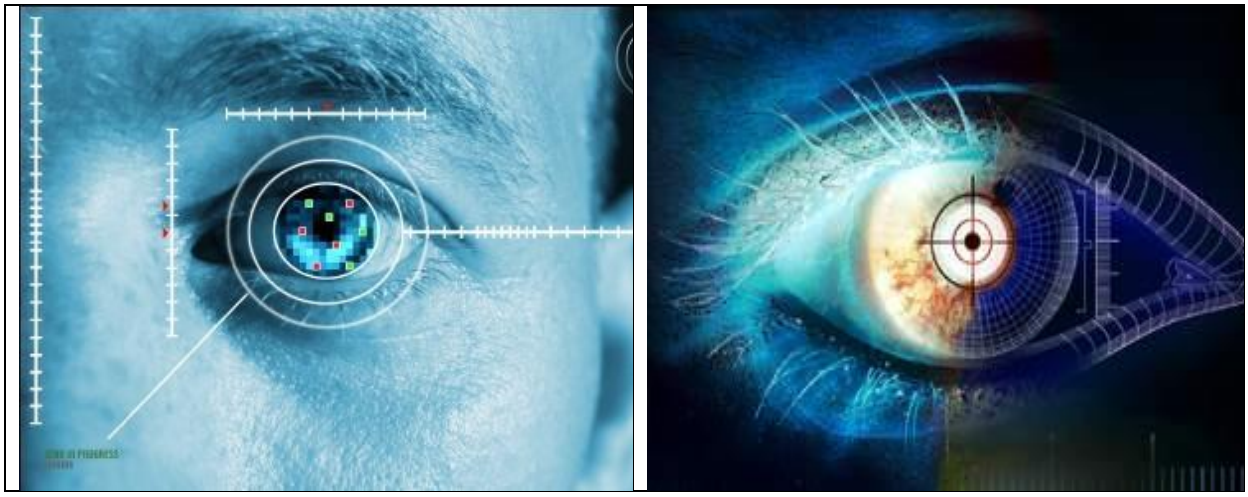
As tecnologias biométricas usam recursos biológicos como impressões digitais, veias, rostos e íris para identificar os indivíduos. Eles melhoram muito a

precisão e confiabilidade dos sistemas de identificação e verificação, eliminando elemento de erro humano.

A biometria também desempenhou um papel importante na garantia de segurança, tanto em termos de facilitar a prestação de serviços sociais em nível nacional, bem como proteger dispositivos pessoais.

No domínio da segurança pública, as tecnologias biométricas sob a forma de impressão digital, íris e reconhecimento facial fizeram uma significativa contribuição para o controle das fronteiras e para a aplicação da lei.

Figura 1. Identificação Biométrica pela íris ocular.



Fonte: Kant (2009).

Para que um sistema biométrico funcione sem problemas, alguns equipamentos são necessários: scanner ou sensor, um computador relativamente potente e um software para a análise das imagens captadas.

> Uma vez com as características extraídas, a última etapa consiste na comparação entre a imagem obtida e as fotos presentes no banco de dados. Esta verificação é feita com o auxílio de diversos algoritmos, cada um trabalhando da sua maneira. A identificação biométrica baseia-se no princípio de que cada indivíduo pode ter um conjunto de dados reconhecíveis e verificáveis, que são únicos e específicos para eles (MARTINS, 2009, p. 03).

Em teoria, o processo de análise biométrica é bem simples. Quando o scanner é acionado, a principal função dele é obter uma imagem nítida e de alta resolução do objeto em estudo: digitais e geometria da mão, íris, retina, expressões faciais.

O passo seguinte é colocar a imagem captada à disposição do software biométrico, o qual analisa e extrai as características mais relevantes da figura. Em uma foto da mão, por exemplo, o que interessa são as linhas que dão forma às digitais.

A INEFICIÊNCIA DO SISTEMA DE IDENTIFICAÇÃO DE SUSPEITOS ATUALMENTE ADOTADOS NO ESTADO DE MATO GROSSO

Ponto que merece destaque é a ineficiência do sistema atual de identificação de suspeitos quando em abordagens policiais de rotina. Embora seja exigível os documentos pessoais para verificação de qualquer cidadão, no âmbito dos alvos das polícias civil e militar, é fato comum a ausência destes documentos durante as abordagens pessoais e em veículos nas operações policiais.

Com a efetiva implementação de um sistema de tecnologia biométrico regionalizado para a coleta, armazenamento, busca e confrontação de impressões digitais latentes de suspeitos com um banco de dados doméstico a ser criado; haverá uma melhor otimização dos procedimentos policiais que envolvam identificação de suspeitos.

A adoção de um novo sistema de identificação por banco de dados doméstico, inicialmente por coleta digital de impressões de conduzidos nos plantões metropolitanos de Cuiabá (compreendida a área de atuação do CIOSP) evitará em pouco tempo que suspeitos e conduzidos não possam mais identificar-se falsamente, quer seja em nome de terceiros ou em nome de pessoa inexistente, fato este comum quando das abordagens policiais pelos executores da lei e da ordem.

Tem-se por meta também a identificação de adolescentes infratores para alimentação do banco de dados doméstico com finalidade de futura confrontação quando da maioridade penal, bem como para apreensões destes menores em casos de atos infracionais análogos a crimes.

A identificação exata de um suspeito ou autor de crime importa diretamente na certeza da punição de quem realmente infringiu a norma jurídica. Desta forma será indiciado, denunciado, processado e julgado na forma da lei, caracterizando desta feita

o princípio constitucional da individualização da pena de forma absoluta, o que hoje não se consegue na justiça brasileira.

SISTEMA INFORMATIZADO DE IDENTIFICAÇÃO (AFIS)

O sistema de identificação adotado pelos Institutos de Identificação dos Estados está em processo acelerado de mudança, haja vista a tecnologia implementada nessa área no início deste século XXI.

A metodologia até então aplicada, prestou grande contribuição para a Polícia quando as cidades eram menores e os criminosos conhecidos, o que possibilitava o confronto das impressões colhidas nos locais de crime com as de um suspeito ou até mesmo podiam ser encontradas nos arquivos monodactilares. Hoje a situação demográfica urbana é outra, as cidades cresceram sendo necessário um processo de identificação criminal mais dinâmico e com maior eficiência, que venha a substituir o método manual de pesquisa.

Nos países mais avançados, a informatização no reconhecimento de impressões digitais é uma realidade. Esta tecnologia é chamada de AFIS (*Automated Fingerprint Identificatio System)*Sistema de Identificação Automatizada de Impressões Digitais).

O AFIS é usado para comparar uma impressão digital com impressões previamente arquivadas no banco de dados do sistema. Nos países que já possuem este sistema, vários crimes do passado estão sendo solucionados com a identificação das impressões digitais arquivadas por falta de suspeitos com os quais pudessem ser confrontadas.

Figura 2. Identificação biométrica digital.

Fonte: Gemalto (2018).

A tecnologia de scanner de impressões digitais de hoje está substituindo a tradicional impressão digital baseada em tinta em muitos países.

> Os sistemas de identificação criminal surgiram originalmente no final do século XIX. Eles foram desencadeados pelo desenvolvimento histórico do Sistema Henrique de classificação de impressões digitais, no qual as impressões digitais são classificadas por características fisiológicas e antropométricas, também conhecidas como sistema Bertillon, nas quais as medidas são obtidas de suspeitos e arquivadas. No Reino Unido, a Polícia Metropolitana começou o uso de dados biométricos para identificação em 1901. Nos EUA, foi iniciada pela polícia de Nova York em 1902, com a polícia francesa iniciando o mesmo processo no final de 1902. Na década de 1920, o FBI criou seu primeiro Departamento de Identificação, estabelecendo um repositório central de dados de identificação criminal para as agências policiais dos EUA (GEMALTO, 2018, p. 02).

Todos precisavam ser classificados manualmente por uma equipe cada vez maior de funcionários. Procuras manuais, igualmente trabalhosas, tiveram que ser realizadas toda vez que uma possível correspondência foi buscada.

COMO O AFIS AJUDA A APLICAÇÃO DA LEI?

O AFIS em si pode traçar suas raízes até a revolução eletrônica da década de 60. A chegada dos computadores coincidiu com a preocupação generalizada com a crescente criminalidade no mundo desenvolvido. Nos EUA, um relatório compilado pela RAND Corporation se mostrou particularmente influente.

Significativamente, destacou as oportunidades para um uso muito mais efetivo das evidências físicas - principalmente impressões digitais - para melhorar o desempenho na solução de crimes.

> Reconhecendo o potencial da tecnologia emergente para ajudar a atingir esse objetivo, agências como o FBI, o Home Office do Reino Unido e autoridades policiais no Japão e na França realizaram iniciativas de pesquisa, juntos, este trabalho ajudou a impulsionar o desenvolvimento do AFIS, tal sistema trabalha tanto com as impressões digitais completas quanto com fragmentos encontrados em locais de crime (GEMALTO, 2018, p. 02).

Através de algoritmos poderosos, um AFIS compara uma impressão digital, ou até mesmo um fragmento de impressão, com milhões de outras impressões de um banco de dados, detectando uma ou mais impressões similares para serem confrontadas pelo perito.

NOVAS TENDÊNCIAS GLOBAIS DA BIOMETRIA

Entre as novas tendências tecnológicas, podemos apresentar a biometria que pode ser usada para melhorar a segurança pública, experimentar e proteger a privacidade pessoal. A combinação de múltiplos parâmetros biométricos tornam a tecnologia muito mais robusta contra os desafios lançados.

A biometria móvel e biometria em movimento são dois outros segmentos a serem observados. A integração de tecnologias biométricas com dispositivos móveis reduzirá os custos de infraestrutura, enquanto a facilidade e a conveniência da captura não invasiva possibilitada pela biometria stand off estimularão sua adoção generalizada. Abaixo elenca-se as diversas formas de aplicação da biometria, conforme as necessidades.

CONTROLE DE FRONTEIRA

As regiões de fronteira hoje constituem sem dúvida as áreas mais sensíveis para a Segurança Pública.

> À medida que o número de pessoas que atravessam as fronteiras continua a aumentar, os funcionários de controle de fronteiras enfrentam o desafio de aumentar sua capacidade de processamento e velocidade sem comprometer o rigor de seus controles. Reconhecendo o papel que a tecnologia pode desempenhar para enfrentar esse desafio, países de todo o mundo começaram a adotar passaportes biométricos. Até o momento, mais de 60 países implementaram ou planejam implementar passaportes biométricos ou cartões de identidade, incluindo a União Europeia, os Estados Unidos, a China, a Índia, a Rússia e o Brasil (NEC, 2019, p. 03).

Implementar a biometria nas regiões de fronteira facilitaria a localização e identificação de suspeitos de crimes, com mandados de prisão, terroristas, bem como minimizaria diretamente o tráfico de drogas, armas e munições, tráfico de pessoas e crianças, principalmente voltadas para o tráfico de órgãos.

APLICAÇÃO DA LEI

Fora dos aeroportos, a biometria também tem sido oportuna para a aplicação da lei. A identificação criminal está cada vez mais sofisticada, utilizando-se de métodos precisos, movendo-se de marcas distintas, como tatuagens a impressão digital bancos de dados e agora análise facial. Seja qual for o método usado, o objetivo permanece o mesmo: identificar corretamente criminosos e excluir os inocentes.

Embora a identificação de impressões digitais tenha sido usada por mais de cem anos, a tecnologia melhorou muito esse processo, reduzindo drasticamente a quantidade de tempo gasto para pesquisar no banco de dados e liberar os investigadores para executar tarefas de nível superior.

> O reconhecimento facial é outra tecnologia que desempenha um papel significativo na aplicação da lei, impulsionada por duas grandes tendências. Devido à complexidade e tendo que levar em conta variações como mudanças na aparência, iluminação condições e ângulos de câmera, a identificação humana foi a única abordagem viável. No entanto, a tecnologia agora amadureceu para o ponto onde sistemas de reconhecimento facial informatizados superaram habilidades humanas. Eles são capazes de conectar vários tipos de informações, seja de gravações de CCTV, registros de banco de dados ou fotos da mídia social e vinculá-los a um único indivíduo. O que demandava uso de pessoal experiente e muitas horas de escrutínio agora pode ser automatizado e alcançado em questão de minutos (NEC, 2019, p. 05).

Em segundo lugar, a proliferação de mídias sociais significa que as fotografias são agora fáceis de encontrar, mudando a forma como o reconhecimento facial é usado

na aplicação da lei. Além disso, as redes sociais permitem que os investigadores não apenas encontrem fotos de suspeitos, mas podem vinculá-los ao perfil da pessoa.

O reconhecimento facial impulsionado por dados de mídia social tem sido usado para combater terrorismo, melhorar a vigilância e até localizar crianças desaparecidas. Nestes casos, a informação biométrica é muitas vezes o único link.

BIOMETRIA MÓVEL

Há pouca dúvida de que o campo da biometria continuará a crescer, estimulada por grandes projetos governamentais e adoção em larga escala por indivíduos. Destas duas forças, desempenho pessoal e mobilidade de tecnologias biométricas em particular, são susceptíveis de moldar a biometria do futuro.

Com a onipresença dos dispositivos móveis de hoje, é fácil dar como certo a tecnologia que impulsionou a revolução móvel. Cada smartphone tem poder de processamento que era inatingível por computadores de mesa na geração passada, sendo que hoje cabe em um bolso.

> Por meio de pesquisa realizada com 100.000 pessoas de 40 países diferentes concluídas em dezembro de 2013, a fabricante de redes móveis Ericsson descobriu que os consumidores estão dispostos a abraçar a tecnologia biométrica através de seus smartphones. Mais de 74% dos entrevistados acreditam que smartphones biométricos se tornaria mainstream em 2014, com os 52% e 48% dizendo que eles gostariam de ver impressões digitais e a varredura da íris substitui as senhas para desbloquear os telefones. A integração de tecnologias biométricas e móveis irá diminuir custos de infra-estrutura e ajudar a levar a biometria para onde as pessoas estão. A biometria com dispositivos móveis pode ser usada em locais remotos; qualquer lugar com uma conexão com a internet. A maior conveniência proporcionada por a biometria poderia contribuir muito para melhorar a segurança móvel. A digitação de senhas complexas foi recebida com resistência, uma série de problemas para as empresas que adotam políticas BYOD (traga seu próprio dispositivo) (NEC, 2019, p. 05).

Do ponto de vista biométrico, um smartphone é um sensor biométrico, com scanner e câmera embutidos de alta resolução, equipado com sofisticados dispositivos de medição giroscópicos e conectividade com a internet. Ser capaz de explorar esses recursos existentes de projetar e vender leitores biométricos independentes têm o potencial para revolucionar o uso da biometria.

BIOMETRIA EM MOVIMENTO

Antes de adentrarmos ao tema da biometria em movimento faremos uma breve explicação sobre aprendizado de máquina e inteligência artificial.

O aprendizado de máquina (em inglês: *machine learning*) é um subcampo da ciência da computação que evoluiu do estudo de reconhecimento de padrões e da teoria do aprendizado computacional em inteligência artificial. Em 1959, Arthur Samuel definiu aprendizado de máquina como o campo de estudo que dá aos computadores a habilidade de aprender sem serem explicitamente programados. O aprendizado automático explora o estudo e construção de algoritmos que podem aprender de seus erros e fazer previsões sobre dados. Tais algoritmos operam construindo um modelo a partir de inputs amostrais a fim de fazer previsões ou decisões guiadas pelos dados ao invés de simplesmente seguindo inflexíveis e estáticas instruções programadas.

Enquanto que na inteligência artificial existem dois tipos de raciocínio (o indutivo, que extrai regras e padrões de grandes conjuntos de dados, e o dedutivo), o aprendizado de máquina só se preocupa com o indutivo.

> O aprendizado de máquina (em inglês, machine learning) é um método de análise de dados que automatiza a construção de modelos analíticos. É um ramo da inteligência artificial baseado na ideia de que sistemas podem aprender com dados, identificar padrões e tomar decisões com o mínimo de intervenção humana. Graças às novas tecnologias computacionais, o machine learning de hoje não é como o machine learning do passado. Ele nasceu do reconhecimento de padrões e da teoria de que computadores podem aprender sem serem programados para realizar tarefas específicas; pesquisadores interessados em inteligência artificial queriam saber se as máquinas poderiam aprender com dados. O aspecto iterativo do aprendizado de máquina é importante porque, quando os modelos são expostos a novos dados, eles são capazes de se adaptar independentemente. Eles aprendem com computações anteriores para produzir decisões e resultados confiáveis, passíveis de repetição. Isso não é uma ciência nova – mas uma ciência que está ganhando um novo impulso (SAS, 2019, p. 02).

Embora diversos algoritmos de machine learning existam há muito tempo, a capacidade de aplicar cálculos matemáticos complexos ao big data automaticamente – de novo e de novo, mais rápida e mais rápida – é um desenvolvimento recente. Eis

alguns exemplos bem conhecidos de aplicações de machine learning, dos quais já deve ter ouvido falar:

- Os carros autônomos super esperados do Google - a essência do *machinelearning*;
- Ofertas recomendadas como as da Amazon e da Netflix - aplicações de *machine learning* para o dia-a-dia;
- Saber o que seus clientes estão falando de você no Twitter - *machine learning* combinado com criação de regras linguísticas;
- Detecção de fraudes - Um dos usos mais óbvios e importantes de *machine learning* no mundo de hoje.

Como visto acima, por meio de aprendizado de máquina podemos comparar padrões pré-existentes, como de uma filmagem que determinado criminoso cobrindo o rosto ou com capacete apresenta um determinado comportamento ao andar, correr ou se movimentar, e pode ser confrontada a outra cena de crime também filmada. Esses comportamentos são processados pelo software e transformados em algoritmos, onde será feito a correspondência e saberemos com alto grau de porcentagem se os dois suspeitos nos vídeos seriam ou não a mesma pessoa.

Permitido pelos mais recentes avanços na tecnologia de captura, a biometria em movimento permite que os recursos sejam tomados sem intervenção manual e mesmo quando o assunto está em movimento. Também conhecido como stand off biometrics, esta tecnologia permite a captura de impressões digitais sem contato, bem como a íris ou face por detecção baseada em vigilância por vídeo.

Em contraste, as tecnologias mais antigas são trabalhosas e demoradas, exigindo contato direto com um scanner de impressões digitais ou para o sujeito se apresentar ao dispositivo de captura, mantendo-se imóvel para garantir uma digitalização de alta qualidade.

Figura 3. Identificação biométrica multifuncional.

Fonte: NEC, (2019).

Figura 4. Identificação biométrica multifuncional.

Fonte: NEC, (2019).

Pode-se verificar na figura acima a biometria auricular, por movimento ou marcha, palmar e de reconhecimento pela voz. A biometria em movimento poderia revolucionar a aplicação da lei, permitindo a detecção em tempo real e monitoramento de pessoas em movimento através de áreas sensíveis, como centrais nucleares e segurança de instalações.

Na segurança pública, a biometria em movimento poderia ajudar na multidão controle e gerenciamento de fluxo, prevenindo automaticamente gargalos que poderia ser potencialmente perigoso ou, pelo menos, perda de tempo.

> A biometria em movimento também encontra muitas aplicações no fornecimento de inteligência de negócios. Monitoramento em tempo real anônimo e não intrusivo pode capturar características biométricas "suaves" como idade, gênero e etnia, permitindo que os varejistas forneçam serviços direcionados em características demográficas. Informações sobre as pessoas que atravessam um shopping center, por exemplo, poderia ajudar os varejistas a tomar decisões sobre como para projetar e estocar suas lojas. Acima de tudo, a biometria em movimento faz com que a adoção de dados biométricos tecnologia conveniente para os usuários. Por exemplo, pode ser usado para capturar informações dos passageiros assim que entram no aeroporto, reduzindo a quantidade de tempo despendida na imigração. Biometria embutida no ambiente vão além das soluções móveis, sem problemas integrando tecnologia na vida cotidiana (NEC, 2019, p. 05).

Poderemos muito em breve identificar suspeitos que utilizam máscaras, coberturas ou capacetes por confrontação pela biometria por movimento de marcha, e até distinguir o gênero das pessoas.[3]

TECNOLOGIA DA EMPRESA NIPON ELETRIC COMPANY (NEC).

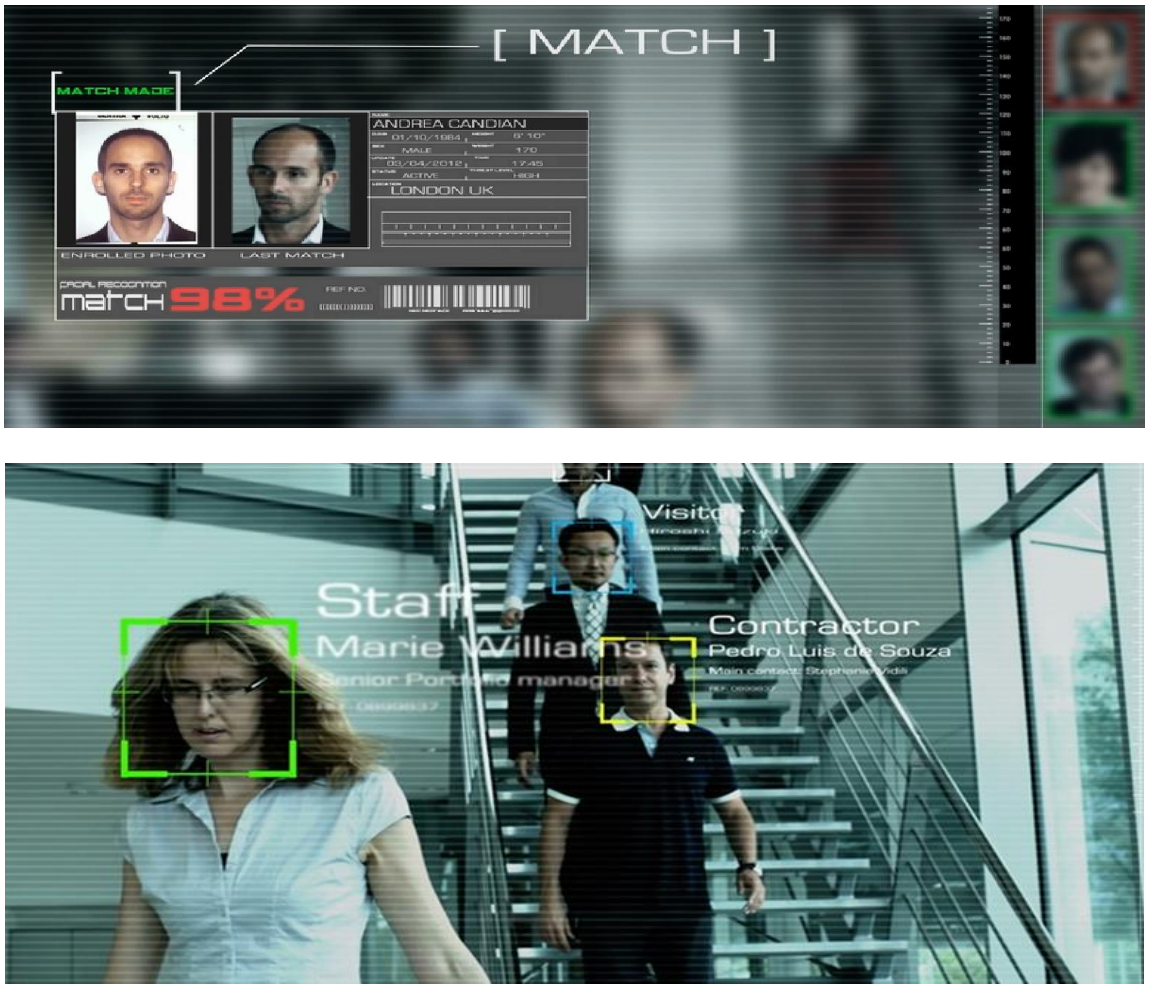
A força da tecnologia da *NEC NeoFace* reside na sua tolerância à má qualidade. Vídeos e imagens de vigilância altamente compactados, antes considerados de pouco ou nenhum valor, são agora evidências utilizáveis e levam a taxas mais altas de identificação positiva.

Com a capacidade comprovada do NeoFace de combinar imagens faciais de baixa resolução, incluindo imagens com baixas resoluções até 24 pixels entre os olhos, existe uma grande separação entre a tecnologia NeoFace da NEC e todos os outros sistemas de reconhecimento facial que correspondem à precisão do mercado. Enquanto a busca de impressões digitais latentes (cena do crime) é a norma, a

[3] Para melhorar o desempenho do sistema de identificação humana baseado na marcha, o gênero pode desempenhar um papel importante no campo das aplicações de vigilância e monitoramento. O algoritmo proposto consiste em quatro etapas. Na etapa inicial, a detecção de objeto de silhueta é realizada usando subtração de plano de fundo e operação morfológica. Na etapa de segmentação, o corpo da silhueta é dividido em seis regiões. Em seguida, seus recursos de marcha são extraídos usando transformada wavelet discreta 2D e, por fim, o classificador K-Nearest Neighbor (KNN) é empregado para classificar o gênero para identificação da pessoa. Para avaliar o desempenho do algoritmo proposto, os experimentos são conduzidos no banco de dados CASIA Gait. Um resultado experimental mostra que o método proposto é mais efetivo para identificação de gênero usando a biometria da marcha. Publicado em: 2015 Quinta Conferência Internacional sobre Computação Avançada e Tecnologias de Comunicação.

tecnologia de reconhecimento facial NeoFace da NEC agora pode identificar positivamente fotos latentes com alto grau de precisão.

Figura 5. NEC excelência em leitura de face biométrica



Fonte: NEC, (2019).

Para continuar a conduzir tecnologia e soluções de reconhecimento facial de classe mundial, a NEC lançou o NeoFace® Face Recognition Suite. O NeoFace® Watch é o primeiro da série a ser lançado, e em breve será seguido pelo NeoFace® Smart ID, NeoFace® Reveal e NeoFace® Match - todas as soluções de ponta que revolucionarão o uso de reconhecimento facial para fins comerciais e de segurança.

INOVAÇÃO E TECNOLOGIA NA SEGURANÇA PÚBLICA

Com a farta tecnologia à disposição, é nossa obrigação como servidores policiais pertencentes à Secretaria de Segurança Pública no estado de Mato Grosso buscar novas tendências em implementação de tecnologias que visem a manutenção da lei e da ordem.

O crime organizado ultimamente é pedra no sapato de toda as instituições policiais, bem como o que gera a sensação de insegurança nas metrópoles e até no campo.

Até outrora nunca ouvimos falar em agroterrorismo ou agrosabotagem. Hoje temos que buscar meios de vencer o crime organizado transnacional que a cada dia procura novas formas de produzir riquezas não importando a quem doer.

Em caso de identificação de integrantes de grupos criminosos como o PCC, a identificação biométrica de suspeitos que compõe uma mesma rede do crime organizado poderá estar vinculada a outros sistemas conhecidos como o GEIA (no Estado de Mato Grosso) ou o INFOSEG (a nível nacional).

A própria plataforma do Sistema GEIA no Estado de Mato Grosso também foi pensada em absorver a plataforma biométrica existente.

Vale ressaltar, segundo informações de especialistas neste assunto, que os vários sistemas disponíveis nem sempre são compatíveis. Por exemplo, o banco de dados biométricos dos atuais TRE`s não são compatíveis com um banco de dados biométricos do Sistema AFIS, adotados por alguns estados da Federação.

Neste ponto, não basta simplesmente colhermos a biometria de uma determinada população sem base metodológica e sistêmica, pois dificilmente teremos conexão entre sistemas, a não ser que foram inicialmente projetados para isso.

O ideal é que, se formos utilizar um banco de dados biométricos de um Instituto de Identificação de determinado estado da Federação, que os dados já coletados sejam compatíveis com o sistema biométrico futuro a ser adotado pela respectiva Secretaria de Segurança Pública Estadual. Podemos comparar analogicamente como tentarmos fazer a migração de dados de um Sistema Android para um Apple ou de um Sistema Windows para MacOS.

Hoje, além dos tablets, dispomos de tecnologia relativamente barata, como câmeras presas ao uniforme, capacetes ou para-brisa das viaturas para que filmem a ação policial. Desta forma, os procedimentos de autos flagranciais ou apreensões de materiais ilícitos ganham maior valoração quando submetidos ao contraditório judicial. Essa mesma filmagem também poderá ser utilizada para reconhecimento facial.

Como vimos acima, por meio do aprendizado de máquina, biometria em movimento e biometria facial, podemos, mesmo em vídeos de baixa resolução, obtermos êxito na identificação por comparação entre um determinado suspeito e um indivíduo constante em banco de dados de integrantes de uma determinada organização criminosa.

Câmeras de vídeo de alta resolução (4k) poderão estar embarcadas em drones de longo alcance (a exemplo do Hibrix.2.0, da marca Quaternum, que é um drone que voa duas horas sem parar e pode carregar 20 kg de produto).

Por meio de softwares de reconhecimento facial, a exemplo do Innovatrix, podemos de pronto fazer o reconhecimento dos suspeitos comparando ao banco de dados previamente existente, com alto grau de precisão.

Figura 6. Tecnologia que voa.

Fonte: Quaternium (2019).

O modelo do drone na imagem acima é ideal para a atividade ligada à Segurança Pública, pois além da velocidade de cruzeiro (50 km/h, podendo chegar a 80 km/h) possui longo alcance e autonomia (de 2 a 4 horas de vôo, conforme o

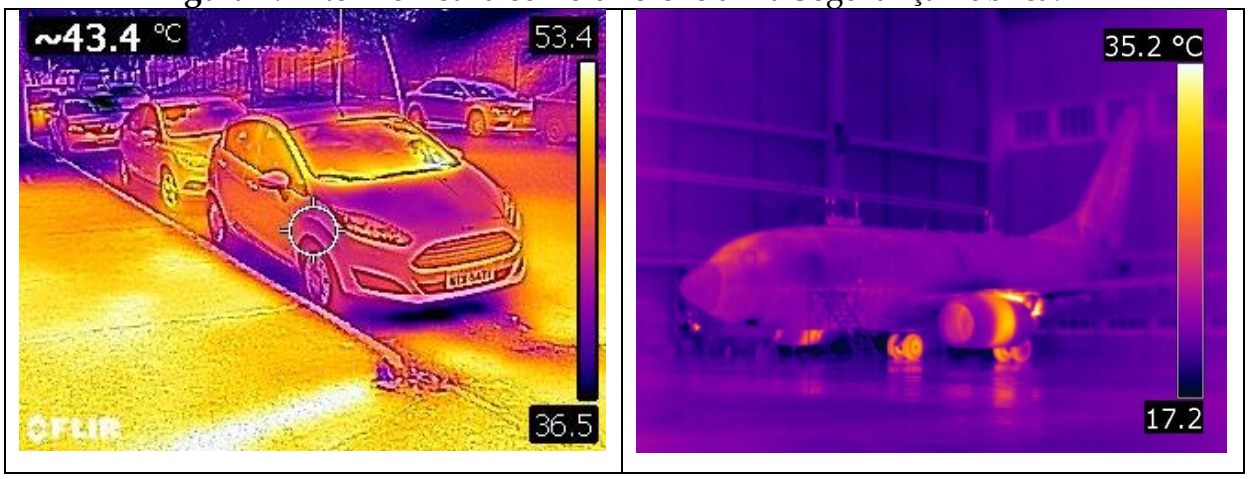
modelo), sendo que o reservatório de 20 kg pode ser perfeitamente adaptado para que o drone possa lançar tinta com luminescência a fim de identificar posteriormente suspeitos e veículos que tenham participado de determinado teatro criminoso, como os crimes na modalidade novo cangaço (assaltos a bancos com várias vítimas como reféns, principalmente em cidades pequenas no interior do Estado de Mato Grosso) ou quando furtam ou roubam gado (abigeato) principalmente em áreas de fronteira.

Outra aplicação indispensável para a biometria seria nas fraudes. É possível minimizar praticamente 100% das fraudes bancárias e contratuais. Podemos também implementar a biometria no seguro obrigatório DPVAT do Governo Federal por meio de escaneamento de indicador e polegar da pessoa acidentada, vinculando o ressarcimento do seguro a futura confrontação da digital aposta pelo segurado no dia do acidente, ou ao seu sucessor elencado pela legislação civil. O receptor digital da biometria poderá ser operado pelo próprio socorrista do SAMU, se o leitor biométrico e sua CPU estiverem nessa ambulância.

Em entrevista realizada com o advogado Dr. Luís Jesus da Gerência Jurídica Criminal da Seguradora Líder em 11/02/2019 disse que houve nos três últimos anos cerca de meio bilhão de reais em prejuízo ao Governo Federal com fraudes do DPVAT e que a Seguradora tem interesse em encontrar caminhos para minimizar prejuízos desta monta.

Dentro do tema inovação e busca de novas tecnologias não podemos deixar de citar o uso da termografia como ferramenta de investigação e auxílio no ambiente Segurança Pública, como por exemplo a utilização da imagem térmica para localização de pessoas escondidas em uma mata fechada, detecção de calor irradiado por veículos em movimento ou que acabaram de estacionar, recenticidade de disparo de arma de fogo, áreas de pastagens ou florestas suscetíveis a combustão espontânea ou classificação das qualidades de uma plantação conforme refração da planta pelo nível de fotossíntese.

Figura 7: A termometria como diferencial na Segurança Pública.



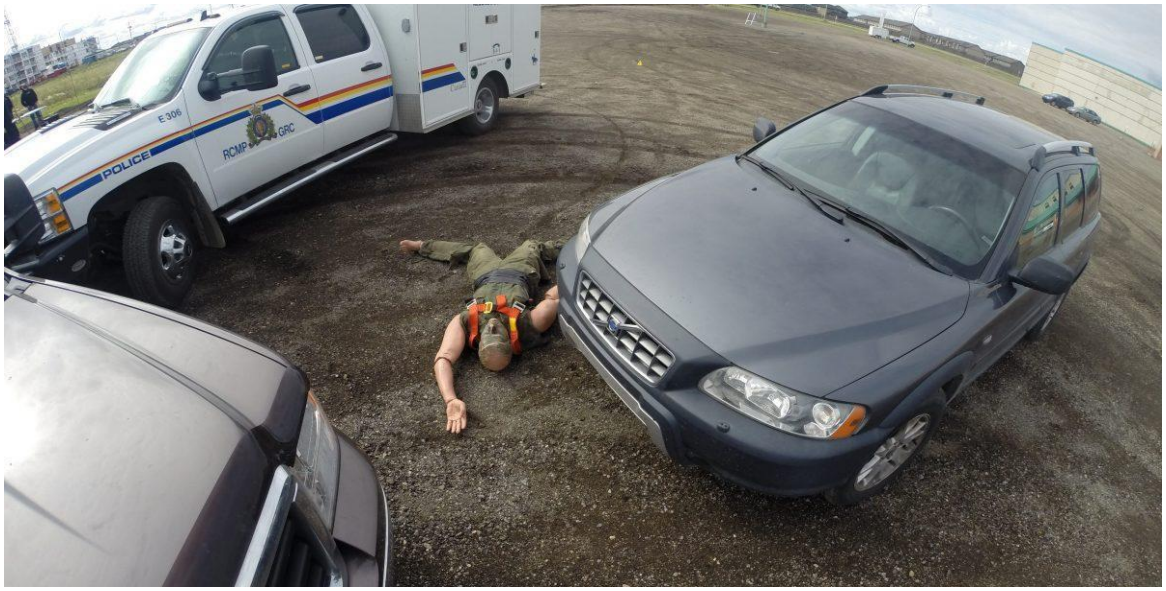
Fonte: FLIR C3-Internet

Na imagem da esquerda capturada com câmera FLIR C3 vimos que o veículo a frente está mais tempo estacionado que o veículo atrás – capô e rodas. Na imagem da direita podemos observar que esta aeronave pousou e foi rebocada para o hangar.

Um outro campo que abre as portas e que servirá de apoio iminente para as Secretarias de Segurança Pública é a modelagem 3D por processamento de imagens capturadas por drones em circuito pré-definido, como o Software Suíço Pix4D. Neste é possível, após a captura de fotografias bidimensionais, criar um modelo tridimensional 3D que pode ser girado 360 graus e, com esta ferramenta, criarmos simulações de locais de entrada, locais de crime ou sinistro, inclusive medindo distâncias entre pontos, áreas ou volumes, desde que os objetos visados sejam inanimados. Aqui, quando as fotografias são processadas pelo software é criado uma nuvem de pontos que vai dar forma ao objeto tridimensional.

A Real Polícia Montada do Canadá usa este projeto desde 2014 para documentar colisões e cenas de crime. O mapeamento por drones permite que as investigações sejam conduzidas sob todas as condições climáticas e fornece visões mais amplas do que os procedimentos tradicionais.

Figura 8. Uma visão além do alcance.



Fonte: Software Suíço Pix4D-Internet

Acima segue fotografia do projeto supracitado, cuja demonstração compara os drones aos métodos tradicionais de levantamento (fita métrica, scanner a laser). As medições foram feitas com drones e métodos tradicionais para demonstrar a precisão e a confiabilidade dos resultados de reconstrução alcançados, de modo que eles possam eventualmente ser usados como evidência admitida no tribunal.

O uso de drones e do Pix4Dmapper para reconstruir cenas de acidentes e crimes fornece uma resposta imediata, economiza tempo e despesas e oferece resultados altamente precisos. Os resultados gerados estão disponíveis permanentemente e os usuários podem acessar arquivos de arquivos e fazer medições a qualquer momento, quando necessário. As cenas reais são preservadas em 3D e com informações detalhadas dentro da precisão do centímetro.

PONTOS CRÍTICOS E POSITIVOS DA BIOMETRIA

Toda mudança de comportamento ou adoção de novas metodologias implicam em novos paradigmas. Para muitas pessoas esta adaptação pode ser sentida como um ponto negativo, mas não há como evoluir sem que os obstáculos sejam superados. A formação de profissionais com habilitação para a aplicação da biometria também será necessária.

O custo da implementação da biometria por certo será por muitos considerado empecilho. Todavia se verificarmos, a médio e longo prazo, o retorno e segurança que dará em primeiro plano aos operadores e beneficiários da Segurança Pública, por certo este valor será irrisório.

Um efeito reflexo e não menos importantes é o da estabilidade econômica e segurança jurídica, pois com uma Secretaria de Segurança Pública Estadual mais efetiva implicará em diminuição dos índices de criminalidade e aumento da sensação de segurança, trazendo para o Estado novos investimentos, pois, além da infraestrutura, o critério segurança pode ser considerado um dos principais fatores para o investimento.

O ex-prefeito de Nova York, Rudolph Giuliani, disse em entrevista à revista Exame que o combate a criminalidade é a melhor forma de tornar as cidades brasileiras mais atraentes para os bons negócios. Embora tenha deixado o cargo há mais de uma década, não passa um dia sequer sem falar de sua experiência à frente da metrópole. Durante seus dois mandatos, de 1994 a 2001, o republicano criou uma série de medidas duras para o combate ao crime, apelidadas de políticas de tolerância zero (STEFANO, 2015).

Com a queda da criminalidade que se seguiu e uma política de isenções fiscais, Nova York tornou-se um polo de atração de novas empresas, sobretudo de tecnologia.

CONSIDERAÇÕES FINAIS

Não há dúvidas que a aplicação da biometria na área de atuação da Secretaria de Segurança Pública do Estado de Mato Grosso, com especial atenção na área de atuação do CIOSP-MT trará aos trabalhos policiais um enorme salto quanto à eficiência e qualidade total nas identificações de conduzidos e suspeitos.

A certeza nessas identificações implicará diretamente uma melhoria considerável na qualidade dos inquéritos policiais e respectivos processos criminais, com a baixa imediata em caso de morte do agente.

Esta tecnologia aumentará a eficiência e eficácia para o desenvolvimento do inquérito policial digital, que já se encontra em fase de desenvolvimento e

implementação pela Polícia Judiciária Civil do estado de Mato Grosso para o calendário de 2019, conforme já anunciou o novo Diretor da Polícia Judiciária Civil do Estado de Mato Grosso Dr. Mário Demerval Aravéchia de Resende na gestão 2019/2020.

Como visto, um Estado com menor criminalidade implica diretamente em investimentos externos, tanto nacionais, como internacionais, ligados não só ao agronegócio (principal fonte de recursos do Mato Grosso) como propiciará novos campos de exploração, como a implementação de novas indústrias e exploração das riquezas minerais do Estado de Mato Grosso.

Vale ressaltar que no campo da biometria, o reconhecimento facial e a biometria em movimento (ou em marcha) têm despertado destaque nos últimos tempos, pois em vários crimes onde, mesmo com máscara, bandidos roubam e ameaçam vítimas poderemos com a aplicação desta modalidade biométrica restringir o campo de suspeitos. Nem sempre as imagens apresentam qualidade para identificação e o rol de suspeitos muitas vezes é extenso demais para que investigadores permaneçam por horas a fio à frente de um computador tentando uma identificação positiva ou ainda que vítimas tentem o reconhecimento fotográfico.

Com o cadastramento biométrico realizado a nível Estadual e até Nacional, criminosos de outros Estados previamente cadastrados poderão ser reconhecidos e crimes até hoje sem solução passariam a estar praticamente solucionados com a implementação da biometria.

O campo da biometria não tem limites. Vimos pelo estudo da marcha que já é possível o reconhecimento do gênero e a detecção de traços biométricos por análises comportamentais como *modus operandi,* modo de caminhar ou correr, já que traços como altura e tipo físico são facilmente adotados na biometria. Hoje já é conhecido dentro da tecnologia moderna o deep learning ou machine learning (aprendizado de máquina), base para a inteligência artificial, onde a própria interface digital aprende com suas pesquisas, como por exemplo, no momento em que fazemos pesquisas sobre hotéis ou passagens aéreas, mesmo não solicitando, nosso computador pessoal nos apresenta uma variedade de sugestões de pesquisas passadas.

Vemos, sem medo de errar, que o aprendizado de máquina, a inteligência artificial, a utilização da termografia como ferramenta de investigação e a biometria são imprescindíveis à evolução e eficiência da nossa Polícia e de todo o sistema processual penal. Com a farta tecnologia à disposição temos que urgentemente quebrar os paradigmas que nos atingem e buscar uma mudança imediata em prol da verdadeira justiça. A busca de novos elementos já tarda, visto que a ordem pública a cada dia que passa está mais aterrorizada com os recentes acontecimentos. Os vândalos mascarados de hoje se escondem por trás dos trapos visando seu não reconhecimento. Todavia, métodos científicos e matemáticos podem ser capazes de reconhecer por algoritmos comportamentais, *modus operandi,* e até a íris dos algozes.

Busca - se uma sociedade mais segura e com melhor qualidade de vida para todos, a ferramenta *biometria* é imprescindível, pois o seu próprio corpo é a senha. A biometria é hoje a esperança de ontem.

REFERÊNCIAS

BRASIL, República Federativa do. **O que é o RIC?** Disponível em: http://www.justica.gov.br/Acesso/governanca/ric. Acesso em: 10 fev. 2019.

CRETO, Alexandre. **O corpo é a senha.** Disponível em: http://revistapesquisa.fapesp.br/2017/05/23/o-corpo-e-a-senha/. Acesso em 12 fev. 2019.

GEMALTO. **Automated Fingerprint Identification System (AFIS) – a short history.** Disponivel em: https://www.gemalto.com/govt/biometrics/afis-history. Acesso em: 24 jan. 2019.

KANT, C. N. Systems, Man, and Cybernetics. **International Journals of Biometric and Bioinformatics,** 2009.

MARTINS, Elaine. **O que é biometria.** Disponível em: www.tecmundo.com.br/o-que-e/3121-o-que-e-biometria-.htm. Acesso em: 09 fev. 2019.

NEC – The State Of The Art In Public Safety. **Biometrics**. Disponível em: https://www.nec.com/en/global/solutions/safety/pdf/NEC_Biometrics_Final.pdf . Acesso em: 24 jan. 2019.

OLIVEIRA, Eugênio Pacelli de. **Curso de Processo Penal**. Rio de Janeiro: Lumen Juris, 2009.

PENA, Rodolfo F. Alves. **Era da Informação.** Disponível em: https://mundoeducacao.bol.uol.com.br/geografia/era-informacao.htm. Acesso em: 12 fev. 2019.

QUATERNIUM.**Hybrix.20.** The first hybrid drone. Disponível em: http://www.quaternium.com/. Acesso em: 20 fev. 2019.

SAS. **Machine Learning.** O que é e qual a sua importância. Disponível em: https://www.sas.com/pt_br/insights/analytics/machine-learning.html. Acesso em: 14 fev. 2019.

STEFANO, Fabiane. Cidade segura atrai bons negócios, diz ex-prefeito de NY. **Revista Exame.** Disponível em: https://exame.abril.com.br/revista-exame/cidade-segura-atrai-bons-negocios-diz-ex-prefeito-de-ny/. Acesso em: 12 fev. 2019.