UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ
ESPECIALIZAÇÃO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO APLICADA A SEGURANÇA PÚBLICA E DIREITOS HUMANOS

Fernando Henrique Borges Ferreira

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

Araranguá, 23 de maio de 2015

Fernando Henrique Borges Ferreira

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

Monografia submetida à Universidade Federal de Santa Catarina, como parte dos requisitos necessários para a obtenção do curso de pós graduação em Tecnologia da Informação e Comunicação Aplicada a Segurança Pública e Direitos Humanos Sob a orientação do Professor Juarez Bento da Silva.

Araranguá, 23 de maio de 2015

Fernando Henrique Borges Ferreira

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

Esta Monografia foi julgada aprovada para a obtenção do título de especialista, e aprovada em sua forma final pelo Curso tecnologia da informação e Comunicação aplicada a segurança pública e direitos humanos

Araranguá, 23 de maio de 2015.

Prof.
Coordenador do Curso

Banca Examinadora:

Prof. Juarez Bento da Silva, Dr.
Orientador
Universidade Federal de Santa Catarina

Profª.
Simone Meister Sommer Bilessimo
Universidade Federal de Santa Catarina

Profª.
Marta Adriana da Silva Cristiano
Universidade Federal de Santa Catarina

Dedico a minha estimada companheira e esposa Alexandra e minha mãe Elza pelo carinho, dedicação e atenção a minha pessoa.

AGRADECIMENTOS

Agradecemos à DEUS, aos mestres e todos orixás, minha esposa, mãe e irmãos pela dedicação e determinismo nessa nossa grandiosa caminhada em busca do saber e do ser**.**

.

.

“Ser invencível depende da própria pessoa, derrotar o inimigo depende dos erros do inimigo. Então, o perito pode tornar-se invencível, mas não pode garantir como certa a vulnerabilidade do inimigo”

Sun Tzu.

RESUMO

Busca-se analisar, conceituar e constatar se é possível aplicar a biometria por impressão digital da assinatura, quando da lavratura do auto de prisão em flagrante, tendo em vista que a legislação nada fala a respeito, mas com sua aplicabilidade tornará mais eficaz e ágil, bem como célere os trabalhos da polícia judiciária, uma vez que já encontra-se presente nos dias de hoje, o sistema SISP/SC (sistema integrado de segurança pública), que guarda e armazena em seus bancos de dados todos os procedimentos policiais que são feitos e encaminhados ao Poder Judiciário, bem como a biometria por impressão digital já é utilizada pelo I.G.P. (Instituto Geral de Perícia) por maioria dos Estados Brasileiro, incluindo o Estado de Santa Catarina no âmbito civil para identificação e confecção de registros civis.

Palavras Chave: Aplicação biométrica de Impressão digital.

ABSTRACT

Seeks to analyze, conceptualize and see if you can apply biometrics fingerprint signature when the arrest report of the drafting in the act, given that the legislation is silent about it, but its applicability become more effective and agile as well as quick work of the judicial police, as already is present today, the SISP / SC system (integrated system of public security), which stores and stores in its databases all police procedures are made and sent to the courts.

ÍNDICE DE FIGURAS

SUMÁRIO

1 - INTRODUÇÃO

As tecnologias biométricas tiveram seu uso em sua origem para fins legais, basicamente para investigação criminal, porém o avanço das TIC em todos os segmentos tem ampliado sua utilização para outras finalidades.

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

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

Um dos identificadores biométricos amplamente utilizado é a impressão digital, principalmente, nas áreas forense e policial, bem como no âmbito civil. Os fundamentos do reconhecimento de impressões digitais e sua adoção para o uso forense datam do final do século XIX. Seu uso se estendeu rapidamente e desde então vem sendo utilizando 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 AFIS (“Automatic Fingerprint Identification Systems”), cujo uso permitiu estender a utilização da impressão digital como meio de identificação para um grande número de aplicações, incluindo aplicações civis.

No início as técnicas de reconhecimento automático das impressões digitais tratavam de emular as técnicas que os especialistas utilizavam manualmente para analisar uma impressão digital. Estas técnicas se baseavam em encontrar os pontos singulares, denominados minúcias e sua posição relativa

dentro da impressão para poder compará-las. Este tipo de técnica, denominada técnica baseada em minúcias, ainda são as mais estudadas e utilizadas porém também apresentam uma série de problemas conhecidos.

Em primer lugar, a extração e comparação das minúcias não é uma tarefa trivial, já que é necessário um forte pré-processamento da imagem da impressão digital para poder extrair os pontos singulares. Neste processo, a imagem inicialmente capturada se modifica expressivamente e pode ser afetada pelo ruído introduzido nas sucessivas filtragens. Este processo produz um mapa de pontos singulares da impressão digital, que será comparado com outro mapa de pontos singulares de outra digital, e a partir do resultado pode-se tomar uma decisão sobre se as duas amostras pertencem ao mesmo dedo.

O ruído introduzido no pré-processamento influi na extração das minúcias, gerando falsas minúcias ou modificando sua posição relativa, dificultando com isso o processo de comparação. Em segundo lugar, as técnicas baseadas em minúcias se baseiam na extração dos pontos singulares para comparar sua posição e características, sem considerar o resto da informação contida na impressão digital. A impressão digital é uma textura que contém informação valiosa que pode ser utilizada no processo de comparação, e utilizar unicamente a posição de seus pontos singulares seria reduzir em grande parte o aproveitamento das informações contidas nela.

Atualmente os métodos de captura das impressões digitais tem evoluído consideravelmente, proporcionando imagens de alta qualidade e inclusive sem a necessidade de contato. (PARZIALE et Al., 2006) Esta evolução não tem encontrado todavia importantes consequências no campo das técnicas de comparação, já que até o momento se continua utilizando majoritariamente as técnicas baseadas em minúcias. Sem dúvida, as imagens que estes novos sensores podem produzir necessitam de novos métodos que sejam capazes de comparar toda a informação contida nelas e explorá-las, a fim de, realizar um reconhecimento mais robusto, sem a necessidade de reduzi-la a um subconjunto limitado de características como podem ser as minúcias.

Atualmente 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. Muitos governos utilizam a biometria para identificar as pessoas, autenticar sua identidade em sistemas informáticos, reforçar a segurança pública em aeroportos e cidades, restringir o acesso a locais seguros, tanto físicos como virtuais.

1.1 CONTEXTO DA PESQUISA E PROBLEMATIZAÇÃO

É de fundamental importância 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. Com o avanço da tecnologia a informática veio aprimorar e agilizar a lavratura da prisão em flagrante com surgimento de sistemas operacionais que desenvolvem e armazenam todos os procedimentos policias feitos pela polícia judiciária. Surge então a pergunta se pode ser aplicado na lavratura do auto de prisão em flagrante a biometria por impressão digital, o que tornaria o procedimento mais ágil e rápido.

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, dentre os métodos de reconhecimento biométricos podemos destacar, o reconhecimento pela impressão digital, reconhecimento pela voz, reconhecimento pela face e reconhecimento pela íris.

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

No caso, a captura da impressão digital na lavratura do auto de prisão em flagrante se fará por meio de leitor ótico que então, verificará e comparará as impressões armazenadas em banco de dados, que autenticará como sendo ou não a pessoa que se quer constatar.

Vale lembrar que esta tecnologia biométrica é fácil e muito bem aceita em comparação com outras tecnologias de identificação.

Também destaca-se o uso da biometria por impressão digital em setores privados e públicos. No privado usado atualmente em bancos principalmente em caixa eletrônicos. Com essa tecnologia a segurança e a confiabilidade do banco torna-se uma ferramenta aceitável e aprovada pelo cliente que vê com bons olhos. No setor público o mesmo critérios é aplicado, um exemplo seria nos Presídios. Em nosso Estado a biometria por impressão digital é aplicada como forma de autenticar e agilizar o cadastramento da população carcerária que ultimamente vem crescendo em longa escala. Com isso o sistema é implantado torna uma ferramenta útil, inclusive como forma de identificação e investigação. Não podemos esquecer de mencionar que no poder judiciário isso também já vem sendo aplicado, um exemplo claro é as urnas eletrônicas, onde o eleitor passa pelo sistema biométrico de impressão digital e somente após, sua confirmação é que pode exercer sua cidadania votando.

Também é bom ressaltar que o uso da biometria por impressão digital vem sendo utilizada pelo I.G.P (instituto Geral de Perícia) pela maioria dos Estados brasileiros, incluindo Estado de Santa Catarina, mas somente na identificação dos registro civis.

Portanto no contexto deste trabalho pretende-se buscar se a biometria na sua forma de impressão digital deve ou não ser aplicada no momento da lavratura do auto de prisão em flagrante como meio de autenticidade e viabilidade na sua conclusão, bem como se é legal o seu uso**.**

1.3 JUSTIFICATIVA

Com base no texto que será apresentado possibilitaremos tentar mostrar e elucidar que usando a biometria por impressão digital, após a lavratura do auto de prisão em flagrante, além de seguro e legal no ponto de vista jurídico, tornar-se-ão autenticas as assinaturas lançadas por impressão digital, além do que é uma nova tecnologia que vem crescendo e sendo usada cada vez mais

em estabelecimento comerciais, Tribunais, estabelecimentos públicos que requerem alto grau de segurança como por exemplo: bancos, TRE, Presídios.

1.4 MOTIVAÇÃO

A motivação está em demonstrar se o uso do sistema biométrico por impressão digital no momento da assinatura do auto de prisão em flagrante, além de seguro, ágil é também do ponto de vista jurídico brasileiro viável e legal**.**

Por outro lado é necessário analisar e discutir a possibilidade de sua aplicação como forma segura e rápida, além de sua autenticidade.

Dessa forma, busca-se tão somente analisar a viabilidade da aplicação biométrica por impressão digital na lavratura da prisão em flagrante.

Portanto, o objeto do presente texto é a biometria por impressão digital, cujas questões a serem pesquisadas serão, a viabilidade da aplicação da biometria por impressão digital quando da lavratura da prisão em flagrante e sua legalidade.

1.5 OBJETIVOS

Os objetivos deste trabalho estão divididos em objetivo geral e objetivos específicos.

1.5.1 Objetivo geral

Construir uma monografia que busque observar a viabilidade e legalidade da aplicação da biometria por impressão digital na prisão em flagrante, bem como demonstrar que é possível sua aplicação no âmbito penal no auxílio da polícia judiciária na identificação de criminosos.

1.5.2. Objetivos específicos

- Estudo bibliográfico sobre viabilidade e legalidade do uso de impressões digitais na atividade forense;
- Estudo bibliográfico dos avanços do tema biometria em impressões digitais;
- Apresentar de forma simplificada a aplicação biométrica por impressão digital na lavratura da prisão em flagrante.
- Demonstrar se é aplicado nos Estados brasileiros
- Sua legalidade

1.6 Opções metodológicas

A metodologia do trabalho seguirá os seguintes passos:

- Breve estudo da literatura sobre biometria;
- Estudo e revisão do estado da arte dos sistemas de reconhecimento de impressões digitais;

1.7 Estrutura do texto

Esta monografia é integrada por cinco capítulos e uma seção de apêndices. A seguir é realizada uma breve descrição dos capítulos que compõe o documento.

Capítulo 1. Introdução: descreve os objetivos, realiza a contextualização do problema e a justificativa para realização da monografia. Também é feita uma breve revisão e contextualização da técnica biométrica utilizando impressão digital.

Capítulo 2. Auto de prisão em flagrante: se faz uma revisão geral sobre o tema com conceitos, requisitos, tipos.

Capítulo 3. Biometria: histórico, conceito, funcionamento, tipos, características, classificação, falhas, controle de acesso, legalidade, estado da arte.

Capítulo 4. Discussão: far-se-á uma análise crítica buscando mostrar se é possível aplicar a biometria por impressão digital na lavratura do auto de prisão em flagrante, bem como se a nossa legislação brasileira permite a sua utilização. Capítulo 5. Conclusões e trabalhos futuros: neste capítulo se busca analisar as contribuições do trabalho e suas possíveis aplicações.

2. AUTO DE PRISÃO EM FLAGRANTE

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 estejam cometendo ou tenha acabado de cometer uma infração penal ou esteja em situação semelhante prevista nos incisos III e IV, do Art. 302, do 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 Mirabetti. A expressão **flagrante** vem da expressão *FLAGARE,* que significa queimar, arder. É o que está acontecendo ou acabou de acontecer. É o evidente, a certeza visual do crime.

Para elucidar, 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.”

No sentido jurídico é o delito no momento de seu cometimento no instante em que o sujeito percorre os elementos objetivos (descritivos e

normativos) e subjetivos do tipo penal. É o delito patente, visível, irrecusável do ponto de vista de sua ocorrência. Dar-se-á no momento e, que o indivíduo é surpreendido no cometimento da infração penal, sendo ela tentada ou consumada. Segundo Espínola Filho, “da certeza visual do crime”.

Portanto, a prisão em flagrante exige para sua consumação dois elementos imprescindíveis: a atualidade e 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 seu fundamento tem como base: evitar a fuga do autor do fato, resguardar a sociedade, dando lhe confiança na lei, e servir de exemplo para aqueles que desafiam a ordem jurídica, como também acautelar as provas que eventualmente serão colhidas no curso do inquérito policial ou na instrução criminal, quer quanto á materialidade, quer quanto à autoria.

Com relação a característica das medidas cautelares face a constitucionalização do processo penal tem-se, a jurisdicionalidade, acessoriedade, instrumentalidade hipotética, provisioriedade e homogeneidade. Jurisdicionalidade é a necessidade de que a restrição dos direitos e bens assegurados na Constituição e nas Convenções Internacionais somente possa ser feita por decisão judicial, a fim de evitar excessos ou abusos de poder. Quanto a acessoriedade, ou seja, a medida cautelar segue a sorte da medida principal dela sendo dependente, pois a medida em que há o resultado do processo principal, a medida perde a sua eficácia. A instrumentalidade hipotética, dá-se porque a medida cautelar serve de instrumento de modo e de meio para se atingir a medida principal. Assim dizemos que a medida cautelar serve hipoteticamente de instrumento para se atingir a medida principal. Na provisoriedade a medida cautelar dura enquanto não for proferida a medida principal e enquanto os requisitos que a autorizam estiverem presentes. Por fim, homogeneidade a ser adotada deve ser proporcional a eventual resultado favorável ao pedido do autor não sendo admissível que a restrição à liberdade

durante o curso do processo seja mais severa qual a sanção que será aplicada caso o pedido seja julgado procedente.

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 C.F., a prisão deverá ser comunicada imediatamente ao juiz, para que verifique a sua legalidade e caso não acontecendo deverá relaxar. Com a comunicação ao juiz, o ato irá se aperfeiçoar e observado seus requisitos será homologado.

Não obstante se trate de medida cautelar, o ato de prender em flagrante não passa de simples ato administrativo levado a efeito, pela polícia judiciária que é incumbida de zelar pela ordem pública, pouco importando a qualidade do sujeito que efetive a prisão. A prisão em flagrante talvez seja a mais natural e compreensível espécie de prisão cautelar, porque exsurge de plena aceitabilidade por todos que a pessoa que estejam cometendo um crime deverá ter sua atitude obstada, para o bom convívio social. Assim, as situações de flagrante previstas no art.302 do CPP, com alto grau de probabilidade autorizam a cessação daquela aparente ilegalidade pela prisão de seu agente.

Tratando-se de providência cautelar indispensável a coexistência dos dois pressupostos: fumus boni júris e periculum in mora, isto é, perigo na liberdade do acusado de justificar sua prisão e não o perigo na demora da prestação jurisdicional. A fumaça do bom direito é da prática do crime e não do bom direito.

Ensina Paulo Rangel que:

> “Periculum in mora traduz-se no fato de que a demora no curso do processo principal pode fazer com que a tutela jurídica que se pleiteia, ao ser dada, não tenha mais eficácia, pois o tempo fez com que a prestação jurisdicional se tornasse inócua. Fumus boni iuris, é a fumaça do bom direito, a probabilidade de uma sentença favorável no processo principal, ao requerente da medida. É a luz no final do túnel, demonstrando uma possível saída.”

Portanto, sua natureza jurídica é de uma medida cautelar de autodefesa social, porque como estabelece o artigo 301 do Código de Processo Penal:

> "Qualquer do povo poderá e as autoridades policiais e seus agentes deverão prender quem que seja encontrando em flagrante delito."

2.1. ESPÉCIES DE FLAGRANTE

A prisão em flagrante pode ser: **Próprio ou Real**: É o flagrante propriamente dito, aquele prescrito no artigo 302, incisos I e II do Código de Processo Penal, isto é, quem "está cometendo a infração penal" e quem "acaba de cometê-la". É aquele em que é surpreendido no ato de execução do crime e a de quem já esgotou os atos de execução.

Impróprio ou Quase Flagrante: Aquele em que havendo perseguição, logo após o crime em situação que faça presumir ser ele o autor da infração penal. A expressão logo após não significa 24 horas, mas sim um período de tempo. Segundo a jurisprudência entende que é até 6 a 8 horas, após o crime, isto é, perseguição contínua iniciada nesses horários, tempo esse razoável para haver a colheita de provas sobre quem é o autor e iniciar a perseguição. Por isso, se tem entendido que não importa se a perseguição seja iniciada por pessoas que se encontravam no local ou pela polícia diante de comunicação telefônica ou radiofônica. Tempo e lugar próximos da infração pena.

Por fim, **Flagrante Presumido**, quando o agente é encontrado **logo depois** com objetos, armas, que façam presumir ser ele o autor da infração penal. Nesse caso, o agente não é perseguido, mas encontrado logo depois, sendo que, segundo a jurisprudência, essa expressão significa o tempo de até 10 e 12 horas, após o crime, podendo haver um maior elastério de horas. A pessoa não é perseguida, mas encontrada pouco importando se por puro acaso, ou se foi procurado após investigações prévias. A lei exige estar o presumível

agente na posse de coisas que o indiquem como autor de um delito acabado de cometer. Por outro lado, a lei não permite que fora dessa situação se prenda, o agente meramente por ter confessado a prática do ilícito. Artigo 302, inciso IV do C.P.P.

2.2. SUJEITO ATIVO DA PRISÃO EM FLAGRANTE

No que tange o sujeito ativo, qualquer pessoa do povo poderá realizar a prisão em flagrante, estando, nesse caso, no exercício regular de um direito, tratando a hipótese de um flagrante facultativo. Já as autoridades policiais e seus agentes deverão realizar a prisão em flagrante, estando, nesse caso, no estrito cumprimento de um dever legal, quando ocorre um flagrante obrigatório ou compulsório**.** Há o dever legal de agir. O não-cumprimento desse dever dependendo do caso concreto poderá sujeitar a autoridade omissa á sanções de natureza administrativa e, ás vezes, às sanções de natureza penal, poderá configurar-se crime de prevaricação.

Quanto ao sujeito passivo pode ser qualquer pessoa, no entanto a exceções, que é o caso dos representantes diplomáticos que gozam de privilégio de não serem presos em flagrante.

Ademais, qualquer prisão que antecede a um decreto condenatório é medida odiosa e que se admite com um “mal necessário”. Dessa forma, é evidente que a prisão provisória somente poderá ser admitida dentro dos limites do inevitável dos indispensável do necessário.

2.3. NOTA DE CULPA

A nota de culpa é o instrumento pelo qual se dá ciência ao preso do motivo de sua prisão, bem como de quem o prendeu. É um requisito extrínseco do Auto de Prisão em Flagrante, sendo que a ausência da entrega ou omissão desse ato essencial irá ocasionar o relaxamento da prisão. Segundo o Art. 306

do CPP, o prazo será de 24 horas, sendo que a jurisprudência vem entendendo que aplica-se por analogia à hipótese prevista no Art. 5º, LXII, da CF, que diz que toda prisão deverá ser comunicada imediatamente ao Juiz.

É importante a observância da formalidade, sob pena de nulidade do Auto de Prisão em Flagrante. Havendo o relaxamento do Auto de Prisão em Flagrante perderá sua força coercitiva e servirá como peça de informação a possibilitar a *posteriori,* o ajuizamento da ação penal.

De outra parte, no caso da prisão em flagrante ter sido **legal** em tese, será cabível a "liberdade provisória" e caso o juiz não a conceda, a prisão tornará ilegal, ocorrendo o constrangimento por parte da autoridade cabendo no caso, o **"**Habeas Corpus"**,** o que não ocorre com a Prisão Preventiva, no qual será cabível o pedido de revogação com base no Art. 316 do CPP.

2.4. TIPOS DE FLAGRANTE

2.4.1. Flagrante Preparado ou Provocado

Flagrante preparado ou provocado é aquele em que o agente é induzido à prática de um crime por terceiros ou pela polícia, onde é chamado de agente provocador. Neste caso, o elemento subjetivo do tipo existe, mas sob o aspecto objetivo não há violação da norma penal, senão uma insciente cooperação para ardilosa averiguação de fatos. Segundo Damásio de Jesus, ocorre quando alguém de forma insidiosa provoca o agente a praticar o crime ao mesmo tempo em que adota providências para que, o mesmo não venha a se consumar.

Em relação a este tema, aplica-se a Súmula 145 do STF, que diz que "não há crime quando a preparação do flagrante pela autoridade policial torna impossível a sua consumação"**.** Segundo a jurisprudência, a Súmula 145 do STF, também se aplica no caso de o flagrante ter sido preparado pelo particular.

É importante observar que para ser aplicada a Súmula 145 do STF, deve haver a preparação e ao mesmo tempo a adoção de providências para que,

o crime não venha a se consumar, ocorrendo, no caso, um crime impossível ou putativo (imaginário), por obra do agente provocador.

Mirabete ressalta a hipótese em que apesar da preparação e das providências adotadas, caso o crime venha a se consumar irá ocorrer o crime.

Temos como exemplo clássico desta situação a hipótese em que o patrão desconfiado da sua secretária coloca alguns objetos sobre a cristaleira, ao mesmo tempo em que coloca policiais atrás da porta, para que no momento em que a secretária subtraia as joias ocorra a prisão. Nesse caso não haverá crime.

Nelson Hungria entende que no caso do flagrante preparado ocorre um crime de ensaio ou de experiência, onde os protagonistas participaram na verdade de uma comédia.

2.4.2. Flagrante Forjado

Ocorrerá no caso, por exemplo, em que um policial de forma leviana coloca drogas no carro de alguém, a fim de prendê-lo em flagrante. As provas de um crime inexistente são criadas tanto por policiais ou particulares. O flagrante forjado nesse caso não é válido.

2.4.3. Flagrante Esperado

É aquele em que a polícia tendo conhecimento de que irá ocorrer um crime espera que o mesmo aconteça e, logo em seguida realiza a prisão em flagrante do agente que o praticou. Não há preparação. Nesse caso o flagrante é válido

2.5. LAVRATURA DO AUTO DE PRISÃO EM FLAGRANTE

A lavratura do auto de prisão em flagrante nada mais é que um ato formal, onde capturado o agente da prática do crime é conduzido a Delegacia de Polícia, no qual presente a autoridade policial, este analisando o fato, no que tange aos seus requisitos, o formalizará. Preso o agente será comunicado de

sua prisão e mencionado seus direitos constitucionais, conforme artigo 5º, inciso da C.F., 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, que dispõe o artigo 306 do Código de Processo Penal, 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 tornar o ato ilegal, por ter decorrido vários dias depois da prisão.

3. BIOMETRIA

3.1. BREVE HISTÓRICO

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 onde eram identificados alguns dos pontos ou características das quais as impressões digitais podiam ser identificadas. A digital é uma característica biométrico 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 através das impressões digitais iniciou sua transição para a automatização, momento no qual foram criados os sistemas AFIS (Automatic Fingerprint Identification System). (RATHA, 1996) 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.

Em 1971 surgem os primeiros estudos acerca da identificação individual feitos por Francis Galton que definiu alguns pontos e características

que poderiam identificar as impressões digitais. Esses pontos foram chamados de “galton points” que são a base da ciência de identificação por impressão digital. Posteriormente nos finais dos anos 60 passou a ser automatizado, dando assim, surgimento a tecnologia de computadores.

Ressalta-se que as identificações individuais já veem desde os séculos passados com os chineses que começaram a utilizar a impressão digital para autenticar documentos. Na Roma antiga também eram utilizadas nos soldados como forma de ser reconhecer o indivíduo e como meio de evitar deserções.

O uso de minucias como meio de identificação tem sido utilizado para desenvolvimento da tecnologia de reconhecimento automatizado de impressões digitais. Estes sistemas são capazes de classificar bases de dados de milhões de digitais e realizar comparações em um espaço muito curto de tempo. Seu êxito tem sido muito expressivo sendo que atualmente a maioria dos países possuem um AFIS. (JAIN et Al., 2007)

Passando então, para os tempos modernos, com a necessidade de ser criar a 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 scaner, extraindo 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, o que permitiu a montagem de um protótipo de leito. Essa técnica era utilizada para captar e coletar impressão digital.

Em 1982, a polícia de Paris adaptou o sistema criado por Alphonse Bertillion, no qual media partes do corpo para a identificação de criminosos. É a partir daí que a tecnologia passou a ser aplicada nos processos criminais.

3.2. CONCEITO E FUNCIONAMENTO

Para conceituarmos a Biometria precisamos primeiramente observar 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.

Assim também podemos dizer que a biometria é uma característica física e única e medível de uma pessoa, ou seja, os seres humanos possuem algumas dessas características que podem ser unicamente identificadas, sendo elas, por exemplo, a impressão digital, a retina, a íris, formação da face, a geometria da mão e outras. Portanto, o ponto divergente em relação a outras formas de identificação como por exemplo, a senha ou cartão inteligente é que com a biometria não podemos perder ou esquecer as nossas características.

Do ponto de vista da tecnologia da informação podemos conceituar a, biometria dizendo que é a técnica utilizada para medir e se obter determinadas informações físicas sobre um indivíduo e, com base nessas informações, gerar uma identificação única para o mesmo de forma a tornar mais seguro e eficiente o seu processo de autenticação em sistemas computadorizados.

Quanto a sua utilização os sistemas biométricos são usados para a autenticação de pessoas, dos quais existem dois modos: a verificação e a identificação. A verificação é apresentada pelo usuário juntamente com uma identidade fornecida usualmente por meio da digitação de um código de identificação. Já na identificação o usuário fornece apenas suas características biométrica, tais como, a impressão digital, competindo então, ao sistema “identificar o usuário. Com todos esses dados, o sistema busca os registros existentes no banco de dados e retorna uma lista de registros com características suficientemente e similares à característica biométrica apresentada. Também é utilizada em aplicações conhecidas como aplicações de varredura (*screening*) que somente podem ser executadas como alguma forma de biometria.

Basicamente todos os sistemas biométricos trabalham da mesma forma, desde os mais simples aos mais complexos. Para melhor elucidação de sua aplicação mostraremos como ocorre: 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 biométricas são coletadas, transformadas em um código digital, numérico ou alfanumérico e depois armazenadas em um banco de dados. Após o armazenamento destas informações, o sistema já é capaz de reconhecer esta pessoa através de uma comparação dos dados recolhidos no instante da solicitação de reconhecimento e dados armazenados no banco de dados.

A figura abaixo mostra como funciona o reconhecimento de padrões que podem ser utilizados em vários métodos biométricos:

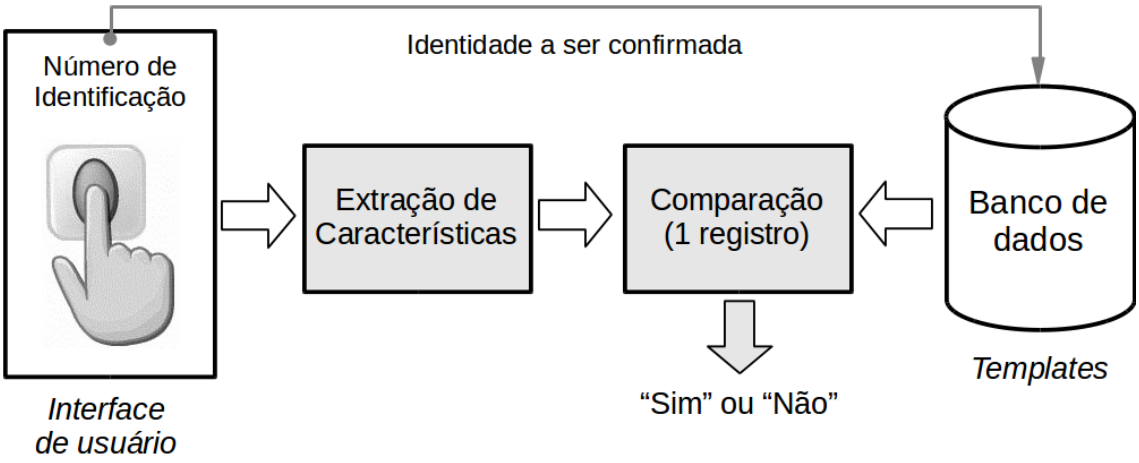


Figura 01: Funcionamento biometria impressão digital

Tem como requisitos básicos o seguinte:

a) A característica biométrica deve conter diferenças significativas entre indivíduos distintos;
b) As características devem ser estáveis durante o período de vida do indivíduo;
c) O sistema deve ser robusto e oferecer segurança contra tentativas de fraudes.

Além disso há outras três características importantes no que tange ao seu funcionamento que merecem serem mencionados, que são:

a) Precisão e Desempenho;
b) Aceitabilidade características esta que indica nível de aceitação do sistema de reconhecimento biométrico por parte de seus usuários;
c) Proteção.

Vale lembrar que a identificação biométrica por meio de impressão digital é feita por algoritmos especializados que consiste na identificação de sinais característicos nas digitais, as minúcias e no estabelecimento de relações entre as localizações destas em termos de ângulos e distancias. Para isso é preciso utilizar um leitor digital e posterior codificação preparando-o para o processo de comparação.

Existem três partes principais em um sistema de identificação biométrica utilizando impressão digital que são:

a) Interface com usuário, que refere-se ao conjunto de elementos que permitem ao usuário utilizar o equipamento, tais como: tela de exibição, teclado, bem como área de captura biométrica;
b) Cérebro, cuja função é de processar e manusear as caraterísticas biométrica obtidas e armazenadas na base de dados;
c) Comunicações; interface com os outros elementos do sistema seja para enviar resultados ou para complementar a própria operação de liberação de acesso.

Assim, 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.

Salienta-se que no caso de controle de acesso todas as tentativas de entrada são registradas em históricos e podem ser auditadas para diversos fins.

Por fim, para que o sistema biométrico possa ser utilizado todos os usuários devem ser registrados. O registro envolve o indivíduo que fornece uma amostra de sua característica biométrica que será usada pelo sistema para gerar um modelo biométrico e o próprio sistema biométrico, isto é, primeiramente se inicia com o reconhecimento do ambiente e das características biométricas selecionadas. Após, será armazenado no sistema, para ser utilizado em um ciclo e comparação posterior.

Assim, dentre os métodos de reconhecimento biométricos podemos destacar, o reconhecimento pela impressão digital, o reconhecimento pela voz, o reconhecimento pela face e o reconhecimento pela íris.

3.3 - CARACTERÍSTICAS BIOMÉTRICAS

Os traços biométricos são definidos como aquelas características intrínsecas a uma pessoa que a tornam única e a diferenciam das demais. Podem ser de dois tipos:

- Anatômicas: são aquelas que proveem da biologia do ser humano, genéticas e herdadas.
- Comportamentais: são aquelas que vem serem adquiridas ou aprendidas com o tempo através da repetição de um mesmo comportamento de maneira rotineira.

Para que uma determinada característica de uma pessoa possa ser considerada como um traço biométrico, deverá cumprir as seguintes premissas:

- Universalidade: todas as pessoas deverão possuir a característica biométrica a ser verificada;
- Unicidade ou singularidade: pessoas diferentes devem possuir características diferenciadas, ou seja, a característica a ser verificada não pode ser igual em pessoas diferentes;
- Permanência: a característica biométrica não pode variar no tempo, em curto prazo;
- Perenidade: indica que o traço biométrico deva durar por muitos anos, ou seja, invariante com o tempo em longo prazo;
- Mensurabilidade: o traço biométrico deve permitir sua caracterização qualitativa.

É claro que nem todas as características biométricas cumprem da mesma maneira todos os requisitos apresentados. Por exemplo, a escrita não é

um traço universal, uma vez que, nem todas as pessoas sabem escrever, o rosto não é um traço permanente, pois, ao longo da vida de uma pessoa ele pode variar significativamente. Por isso, na hora de escolher uma característica biométrica para sua utilização no reconhecimento de pessoas, deve-se avaliar se a mesma cumpre as características requeridas em função da finalidade para a qual se deseja utilizar o sistema biométrico.

Adicionalmente a estas premissas, existem outras opcionais que podem ser consideradas:

- Aceitabilidade: nível de invasão de privacidade na qual o indivíduo é submetido para extração do traço biométrico. Deve ser muito baixa, para que apresente a máxima colaboração possível por parte do indivíduo;
- Rendimento: precisão, confiabilidade, eficácia e velocidade de aquisição e avaliação dos traços;
- Fraude ou ataques: vulnerabilidade relacionada a falsificação. Deve ser mínima ou deve oferecer um método de comprovação de veracidade.

3.4 - CLASSIFICAÇÃO DOS TRAÇOS BIOMÉTRICOS

Conforme mencionado anteriormente, as características biométricas são diferenciadas em dois subgrupos: os traços fisiológicos e os comportamentais. A seguir serão apresentados de forma breve os traços biométricos mais conhecidos e suas principais características. São exemplos de traços biométricos fisiológicos: impressão digital, rosto e íris.

Impressão digital: as cristas digitais dos dedos, das palmas das mãos e pés são formadas no sétimo 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 se trata de identificar 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.

Figura 02: Exemplo de traço biométrico – Impressão digital

Rosto: é um dos traços biométricos mais aceitos, já que é o mais empregado pelas pessoas para reconhecimento entre si de maneira visual. Além disso, o método empregado na aquisição de imagens do rosto é um método não intrusivo, o que lhe permite ser uma técnica com boa aceitação entre os usuários. O desafio para este tipo de aplicação é conseguir o desenvolvimento de técnicas de reconhecimento capazes de tolerar alterações proporcionadas pelos efeitos da idade, das expressões faciais, das variações nas condições de iluminação do ambiente e variações na posição do rosto em relação à câmera que estiver captando a imagem.

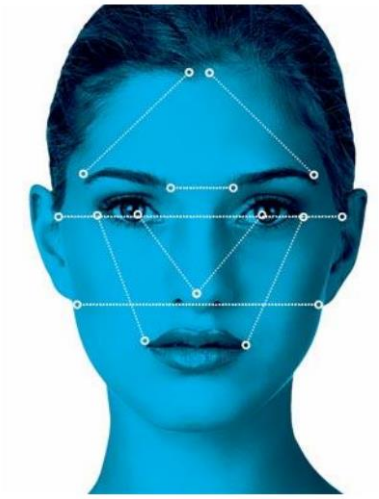


Figura 03: Exemplo de traço biométrico – Rosto

Iris: o padrão de textura de cada íris é único para o indivíduo e se forma durante o desenvolvimento embrionário, mantendo-se invariante ao longo de toda a vida. Sua captura é realizada mediante imagens, onde a iluminação e a cooperação do usuário são determinantes, pelo que é bastante sensível às condições ambientais. Por tudo isso é considerado um método intrusivo, porém com um alto potencial devido à rapidez dos sistemas e ao alto poder de discriminação que oferece.

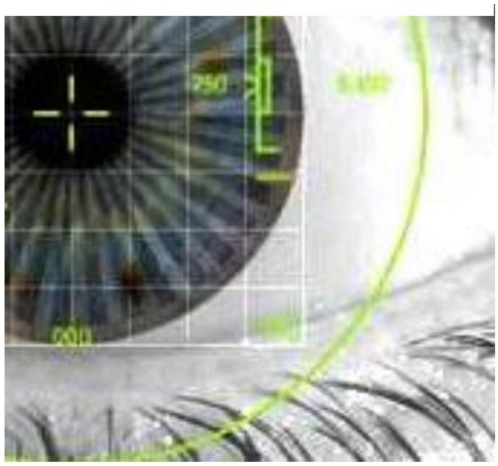


Figura 04: Exemplo de traço biométrico – Íris

Entre as características biométricas comportamentais. São exemplos deste tipo de traço biométrico a assinatura manuscrita, a forma de caminhar e a voz.

Assinatura manuscrita: o modo pelo qual uma pessoa assina um documento é um traço de comportamento característico de cada indivíduo. Ao largo da história, a assinatura tem sido o meio de identificação mais comum. Sem dúvida, este traço biométrico apresenta uma grande variabilidade a curto e longo prazo, e um alto risco de falsificação por parte de outros indivíduos, o qual o converte em uma característica difícil para um reconhecimento automático confiável. Por outro lado, por tratar-se de um processo de aquisição não intrusivo tem um alto grau de aceitação.

Forma de caminhar: este não é um traço biométrico especialmente distintivo, porém sim o suficientemente característico como para permitir a verificação em algumas aplicações de baixa segurança. Por ser um traço comportamental pode não ser invariante, especialmente a longo prazo, por culpa de flutuações importantes no peso, ou lesões nas articulações ou no cérebro. A aquisição deste traço biométrico é similar a das fotografias faciais, pelo que pode ser considerado um traço biométrico aceitável. Não obstante, devido ao fato que os sistemas biométricos baseados nesta característica utilizam sequências de vídeo da pessoa caminhado para medir os diferentes movimentos de cada ponto de articulação, sua carga computacional é bem alta.

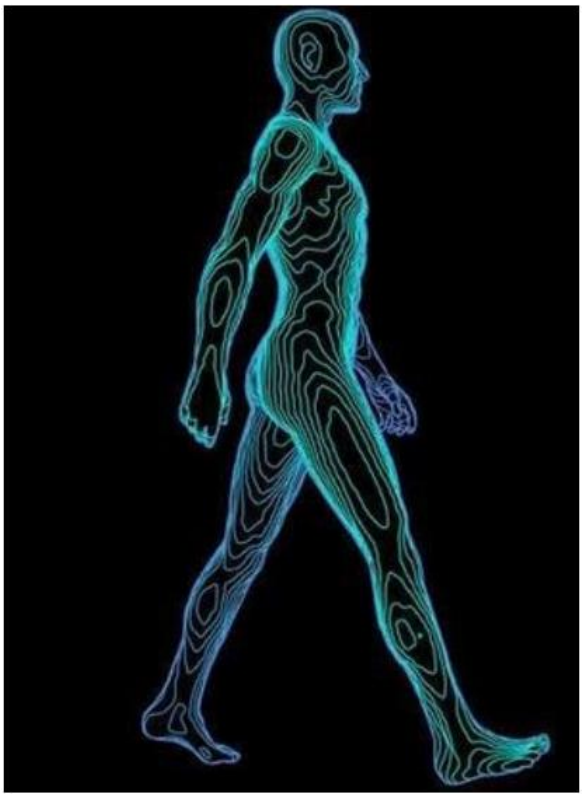


Figura 05: Exemplo de traço biométrico – Maneira de caminhar

Voz: o poder de diferenciação da voz é uma característica amplamente reconhecida. Sua captura é realizada mediante um processo não invasivo, o que a converte em um traço biométrico muito atrativo. Não se considera, sem dúvida, que seja o suficientemente diferenciada para permitir a identificação de um indivíduo em uma grande base de dados. Por outro lado, o sinal de voz que está disponível para o reconhecimento de um indivíduo tenha sofrido degradação de qualidade pelo microfone, pelo canal de comunicação e pela digitalização. A voz se vê afetada, além disso, pela saúde da pessoa, seu estado de ânimo e emoções. Este traço é na verdade uma combinação de características físicas (fisionomia do trato vocal) e de comportamento (ritmo, entonação). Estas últimas não são invariantes ao longo do tempo.

Figura 06: Exemplo de traço biométrico – Voz

Além dos mencionados, existem outros estudados em menor escala como podem ser: a retina, as orelhas, o termograma, a distribuição das veias na mão e, inclusive, traços que podem ser considerados menos distintivos como o odor, a forma de teclar, etc. São denominados de “soft biometrics”. Unicamente podem proporcionar informação adicional a outros traços e não pode ser discriminativos.

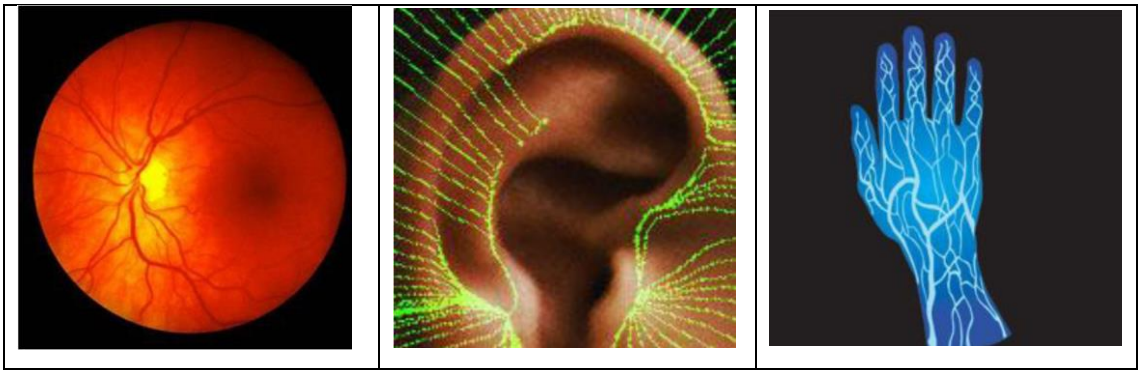


Figura 07: Outros exemplos de características biométricas

3.5. A IMPRESSÃO DIGITAL COMO IDENTIFICADOR BIOMÉTRICO

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

Já faz mais de cem anos que a ideia, de utilizar características individuais com o objetivo de resolver crimes, foi concebida por Alphonse Bertillon. (MALTONI Et Al., 2009) Em 1893 foi aceita no Reino Unido a ideia de que não existem dois indivíduos que tenham impressões digitais iguais. Assim, iniciou-se então a coleta e armazenamento das impressões digitais dos criminosos detidos, para utilizá-las em sua identificação e para auxiliar na solução do problema das mudanças de identidade que estes realizavam continuamente com seus nomes. Além disso, com a comparação destes registros com impressões digitais anônimas encontradas em casos de delitos, as forças de segurança podiam identificar algum culpado, caso este tivesse sido detido previamente. Assim foi o início do uso das impressões digitais como uma aplicação forense.

Desde então, a identificação digital forense tem sofrido mudanças muito significativas e evoluído constantemente. Sem dúvida, graças aos avanços da tecnologia, a datiloscopia, é atualmente uma das principais técnicas de identificação forense e de grande ajuda na resolução de casos reais.

3.5.1 - A impressão digital: forma e classificação

A impressão digital pode ser considerada como formada e com capacidade de diferenciação a partir de sexto mês fetal. O padrão de vales e cristas que se forma permanece invariável até o falecimento da pessoa. As exceções são os cortes, queimaduras, etc. A figura formada pelas cristas e vales

é única e apresenta o traço característico de cada indivíduo. O padrão da impressão digital, ou datilograma, pode ser analisado a partir de três níveis:

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. (HENRY, 1900) 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.

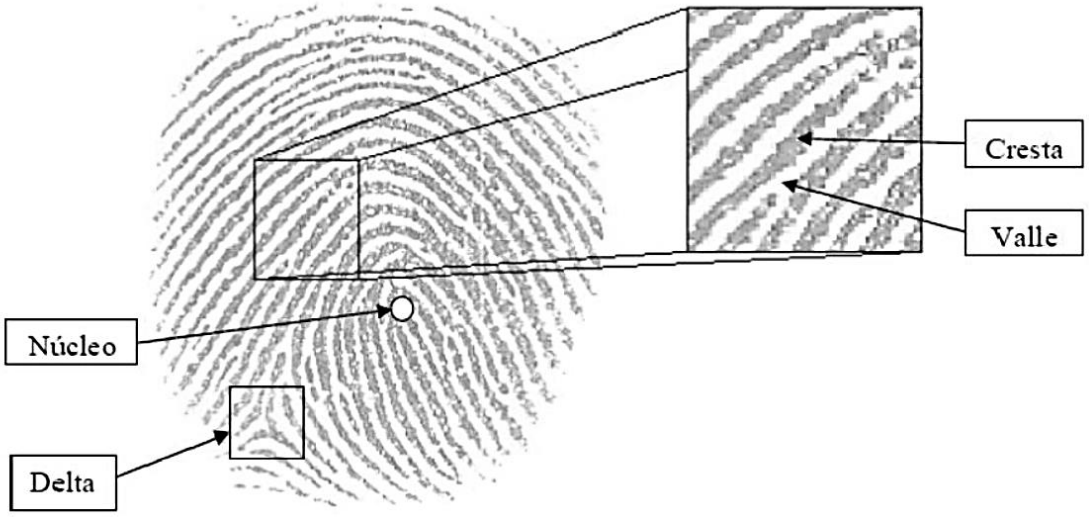


Figura 08 – Padrão da impressão digital

Segundo a presença e distribuição de núcleo e deltas, são obtidos diferentes tipos de datilogramas: monodeltos (um único delta), bideltos (dois deltas) e adeltos (não contém deltas), etc.

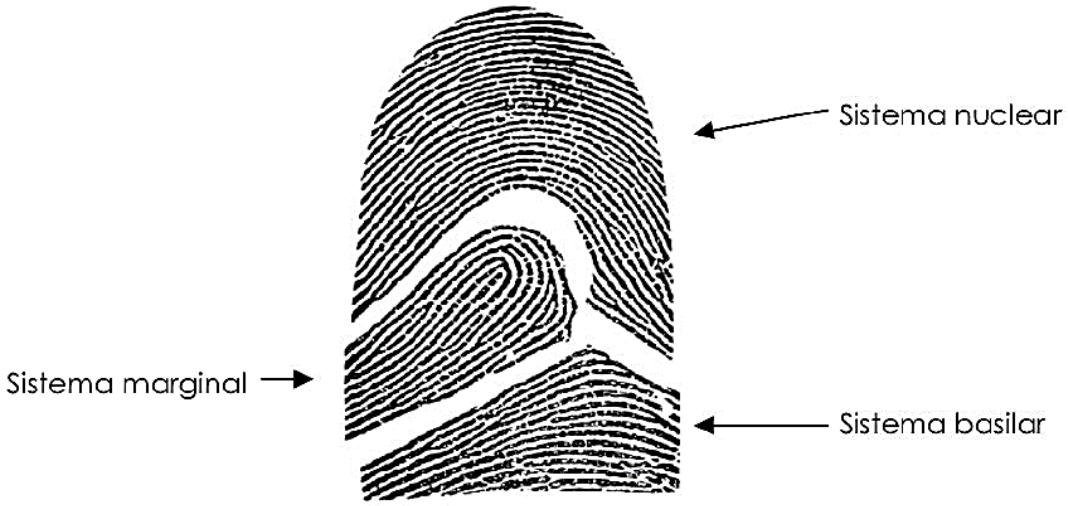


Figura 09 – Padrão de impressão digital NÍVEL 1

O tamanho e forma da impressão digital e a orientação do fluxo de cristas são incluídos também como características pertencentes a este nível.

Figura 10 – Exemplos de digitais do tipo monodelto, bidelto e adelto

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

Figura 11 – Minucia do tipo terminação abrupta

Figura 12 – Minucia do tipo convergência/bifurcação

Cada minucia é caracterizada por suas coordenadas x e y, seu ângulo θ que forma a reta tangente à crista com o eixo horizontal, e o tipo de minucia.

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

Figura 13 – Detalhe das características internas das cristas

Também existem outras formas diferentes de analisar o datilograma dependendo do formato e da situação em 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 intencionada para marcar a digital (impressões digitais) ou de forma menos visível e normalmente acidental em um cena que esteja sendo analisada (latente).

3.5.2 - 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. (CHAMPOD et Al., 2004) A identificação da referida amostra é realizada mediante a análise das características extraídas. Uma vez que, que o processo de identificação é posterior ao de extração das características da amostra da impressão digital.

Para poder confirmar a identificação de uma impressão digital é necessário estabelecer alguns critérios prévios que definem o protocolo de atuação. Este protocolo deve recolher um convenio 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.

O criminalista Edmond Locard enunciou a primeira regra que estabelecia um número mínimo de minucias 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 deste debate foram propostas as seguintes regras:

1. Se forem encontradas mais de doze 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 doze 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 a marca e a impressão quanto a largura das cristas e 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 dactiloscópica forense, ainda que, infelizmente, a terceira regra tenha sido constantemente ignorada (CHAMPOD et Al., 2004). Atualmente o processo de identificação das impressões digitais tem evoluído muito e geralmente, podendo variar entre países ou continentes, em um processo de quatro passos, conhecido no Brasil como “confronto papiloscópico”, onde 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. Em geral, o passo de avaliação pode seguir duas vertentes: limiar qualitativo ou de limiar quantitativo.

O limiar qualitativo é mais utilizado nos USA. É uma abordagem que defende a postura de que cada processo de identificação representa um conjunto único de circunstancias e não pode-se 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.

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 assim existem variações entre o número de minúcias fixado em

cada país, variando entre as sete da Rússia e as dezesseis da Itália, sendo doze o número na maioria dos países.

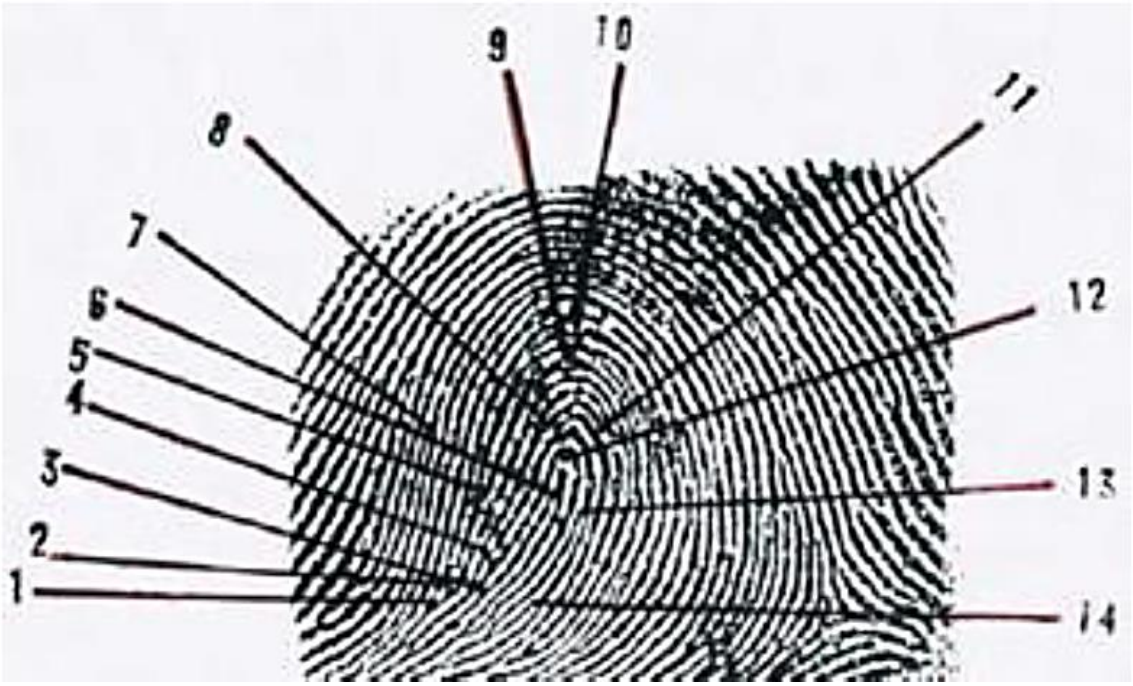


Figura 14 – Localização de minúcias em uma digital

3.6 – SISTEMAS BIOMÉTRICOS

Os sistemas biométricos são procedimentos que são utilizados para a identificação automática de pessoas mediante o uso de características físicas do indivíduo ou de seu comportamento. (JAIN et al.,2007)

Em geral, um sistema biométrico deverá incluir as seguintes fases:

- **Aquisição de dados**: é o processo pelo qual são recolhidas as amostras com a informação e são digitalizadas. Este passo é de especial importância, uma vez que, a maneira em for realizado definirá a qualidade da informação e portanto o rendimento posterior do sistema;
- **Pré-processamento**: é a fase de armazenamento do sinal digital obtido como amostra. Se seleciona a parte importante (dependendo do tipo de

amostra que seja, uma imagem, uma gravação de voz, de vídeo, etc.) e se busca são eliminados os ruídos e outros fatores não desejados;

- **Extração de características**: de acordo com o traço biométrico que se está utilizando se extrai a informação que será caracterizada na amostra para representar o indivíduo e diferenciá-lo dos demais;
- **Cálculo da similaridade:** com a extração da planilha de características do usuário compara-se os modelos armazenados na base de dados e se calcula um escore que quantifica a semelhança entre as duas amostras;
- **Tomada de decisão**: a partir do valor de score obtido a respeito de um limiar previamente fixado. Classifica-se a amostra como coincidente ou não coincidente (em sistemas de verificação), o que seria o mesmo de declarar se um indivíduo é impostor ou genuíno.

3.6.1 -Tipos de sistemas biométricos

Os sistemas biométricos podem ser de dois tipos segundo seu modo de funcionamento: de verificação ou de identificação. Além destes, existe outro modo de operação que é complementar e comum a ambos, chamado modo de registro. A seguir serão explicados brevemente cada um deles.

- **Modo de registro**: é o modo de funcionamento focado no usuário e seus dados no sistema. Para isso é necessário que seja introduzida a sua identidade e sua característica biométrica. Em seguida são extraídas as características que serão associadas a esta identidade e serão armazenadas na base de dados do sistema. Em certas situações pode-se solicitar ao usuário o aporte de sua característica biométrica mais de uma vez para levar em conta a variabilidade, o que torna o sistema mais robusto frente aos possíveis ataques.

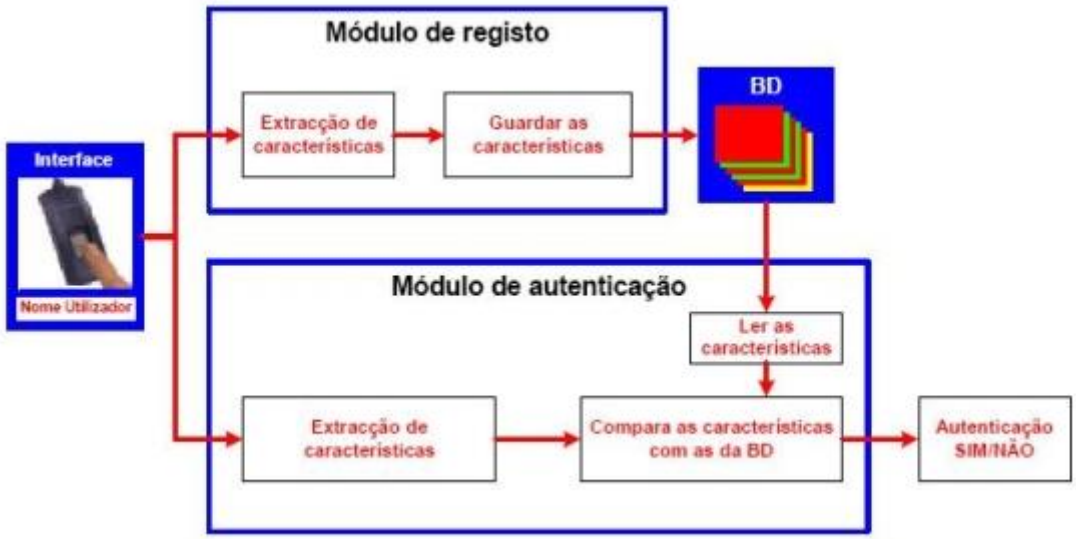


Figura 15 – Funcionamento de um sistema biométrico em modo Registro. (www.gta.ufrj.br)

- **Modo verificação**: neste modo de funcionamento o usuário introduz seu nome (ou identificação no sistema) através de um cartão de identificação ou similar. Após isso os traços biométricos são comparados unicamente com os de um padrão previamente armazenado. Este processo implica em conhecer previamente a identidade do indivíduo a ser identificado, portanto, caso este indivíduo apresente algum tipo de credencial, que depois do processo de autenticação biométrica seja validada ou não. Ou seja, um sistema biométrico de verificação se encarrega de confirmar a partir de uma característica biométrica se um usuário é realmente quem diz ser. Em geral, esta decisão se baseia no resultado quantitativo da comparação se ele supera ou não um fator de decisão. Como o comparador do sistema realiza uma única comparação, diz-se que é uma comparação “um a um”.

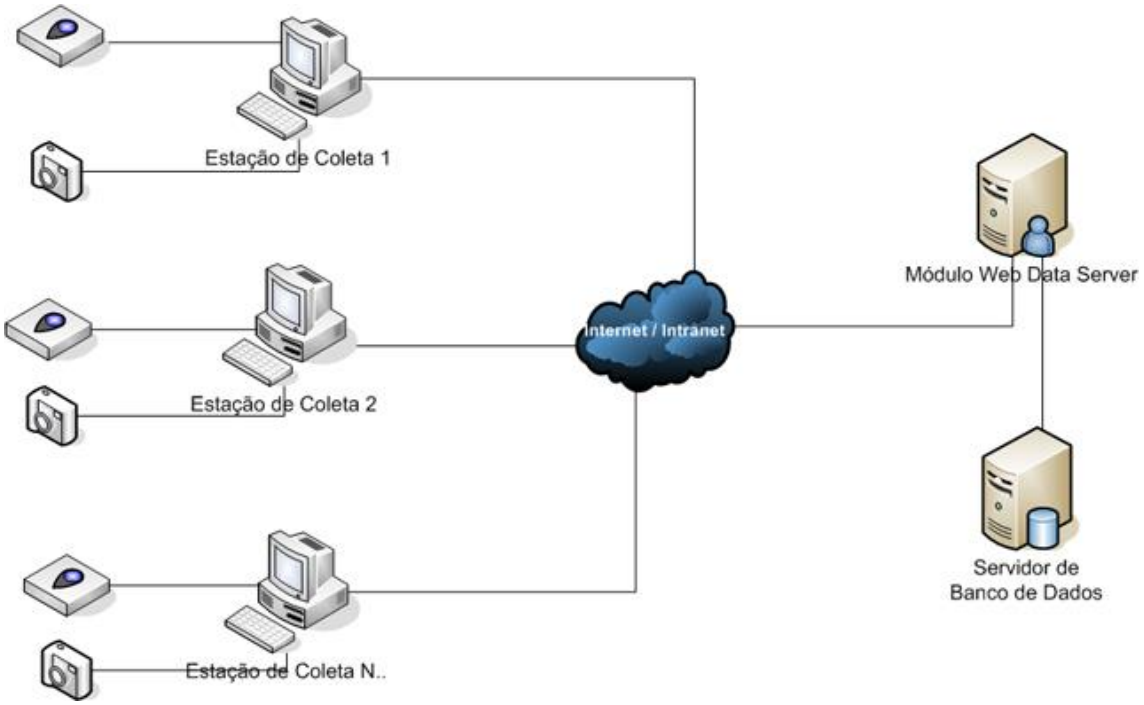


Figura 16 – Funcionamento de um sistema biométrico em modo Verificação. (www.vsoft.com.br

Modo identificação: neste modo de operação, o usuário não reclama nenhuma identidade, e sim trata de averiguar se o indivíduo que solicita o acesso se encontra ou não em uma base de dados previamente armazenada no sistema. A diferença no modo verificação, no qual somente realizava uma comparação, neste caso são realizadas múltiplas comparações, já que se deve encontrar o usuário dentro da base de dados. Isto leva a um grande custo computacional, sem dúvida, este modo é necessário em sistemas nos quais o usuário cuja identidade se busca não vá a aportar informação sobre sua identidade, porque seu objetivo precisamente é não ser identificado. Este é o caso mais habitual dos sistemas forenses de reconhecimento biométrico. Este modo de trabalho é denominado “um para muitos”. A saída de um sistema de identificação pode ser muito determinista (o usuário se encontra ou não na base de dados) ou pode ser uma lista de candidatos ordenados do maior para o menor escore (pontuação de similaridade).

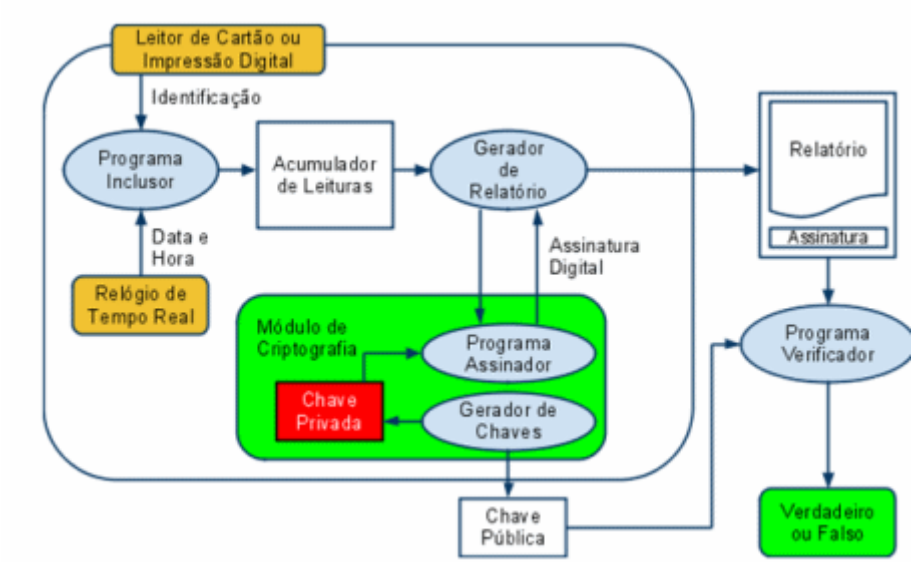


Figura 17 – Funcionamento de um sistema biométrico em modo Identificação. (www.ambito-juridico.com.br)

3.6.2 - Sistemas forenses de identificação digital

Como foi mencionado anteriormente, os sistemas biométricos utilizados no âmbito forense são em sua grande maioria sistemas de identificação. A diferencia que tem 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 a 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 sistemas se obtém um resultado de confirmação ou de negação. Porém no caso dos sistemas de identificação é diferente, são realizadas tantas comparações como amostras das que se disponha na base de dados. O resultado será uma lista ordenada com o valor do escore entre a digital da qual se deseja obter a identidade e o resto das amostras da base de dados. Ou seja, esta lista mostrará do maior para o menor,

quais são as identidades as quais mais se parece a nossa digital, as que tem maior probabilidade de acerto.

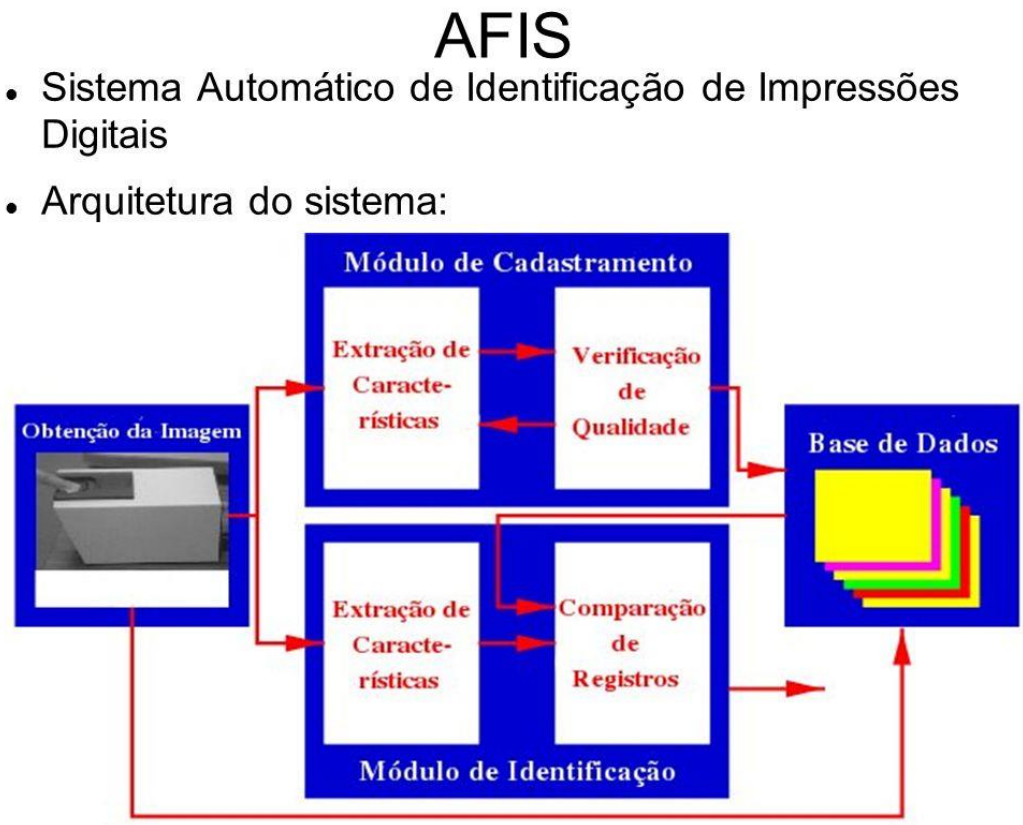


Figura 18 – Diagrama de funcionamento de um sistema de identificação biométrico. (www.slydeplayer.com.br)

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.

Extração de características

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 através de um exame das características das cristas e dos vales para decidir se pertencem ou não à mesma fonte. (RATHA; BOLLE, 2003) A extração das minucias pode ser realizada da seguinte maneira:

1. **Segmentação**: consiste em diferenciar dentro da imagem o fundo da região de interesse (área da imagem que inclui as cresta e vale da impressão). Existem diferentes técnicas de segmentação, por exemplo algumas delas baseadas na grande diferença de nível de cinza que existe entre o fundo da imagem e a impressão digital;
2. **Estimativa da orientação das cristas**: a orientação é calculada para cada pixel da imagem como a direção do fluxo das cristas em torno deste pixel. Esta orientação é então determinada pelo angulo que formam as cristas em relação a horizontal e calcula-se em blocos, fazendo uso de janelas deslizantes;
3. **Extração das cristas**: melhora e binarização. Nesta fase pretende-se melhorar a qualidade da imagem para ressaltar as cristas de maneira que seja mais fácil a extração posterior das minucias. Se for melhorada a definição das cristas e vales e finalmente se for binarizada a imagem para determinar os dois tipos de valores: cresta (preto) e vale (branco).
4. **Afinamento**: se reduz a largura das cristas para um só pixel na imagem, ajudando a eliminar o ruído e outros artefatos não desejados;
5. **Extração de minucias**: finalmente são selecionados automaticamente todos os pontos nos quais existir uma terminação ou bifurcação das crista. São comprovados os pixels pretos (cristas) de forma que se existir somente outro pixel preto em seu entorno será uma terminação abrupta, e forem três, será uma bifurcação.

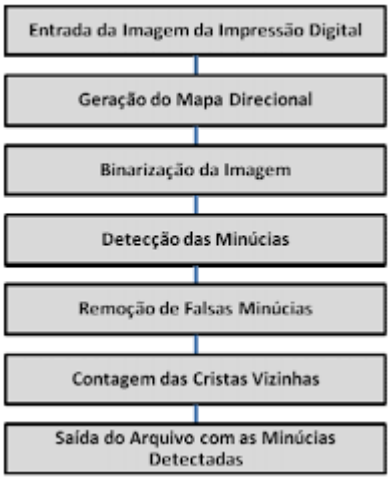


Figura 19 – Diagrama do processo de extração de minucias. (www.cec.catalao.ufg.br)

Na realidade, as características a serem extraídas nesta fase do processo não tem porque ser necessariamente minucias já que existem numerosos tipos de características que podem ser utilizadas no processo de identificação.

Comparador

Após a extração das características vem a etapa de comparação ou matching. Esta 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 que tem é a grande variabilidade que reside na captura da amostra. A característica biométrica em si permanece invariante (tal e como indica sua definição) porém a forma de capturá-la interfere nas características de cada amostra. Em especial nas imagens das digitais se pode variar a espessura das cristas, já que se vê alterada pela pressão exercida sobre a superfície, a orientação, o deslocamento, curvatura da superfície, estado da pele e muitos outros fatores.

Apesar disto, as técnicas de comparação dos sistemas automáticos no estado da arte tem um alto rendimento, dando lugar a algumas taxas de erro

muito baixas. Sem dúvida, em geral dependem bastante da qualidade das digitais. Por isso, a identificação automática com digitais latentes segue sendo um tema que requer muita pesquisa. Em geral, os sistemas de impressão digital podem ser divididos em três tipos de comparadores:

I. **Comparador baseado em minucias**: consiste na comparação de padrões de minucias que tenham sido armazenados para a posterior extração. Ao fazer a comparação entre digitais, são estes padrões os que representam cada uma das digitais com as quais realmente se realiza a comparação, dando lugar a uma medida quantitativa de similaridade conhecida como escore. Antes da fase de comparação, podem ser alinhados os padrões de minucias a partir de uma minucia em comum para tomar um ponto de referência em ambas as digitais a partir da qual será iniciada a comparação. Existem vários métodos de comparação de padrões de minucias como por exemplo passar as minucias para coordenadas polares, tomando uma minucia como ponto de referência para posteriormente, segundo um critério fixado previamente, ordená-las em cadeias que vão sendo comparadas entre os dois padrões. (RATHA et al., 1996)

II. **Comparador baseado em textura**: neste método é utilizado o padrão do campo de orientação e da frequência espacial da imagem da digital. A principal vantagem deste método é sua robustez frente ao ruído existente nas imagens de baixa qualidade, nas quais a extração de minucias pode resultar mais complicada. Sem dúvida, para imagens de boa qualidade, este processo apresenta uma maior taxa de erro. (RATHA;BOLLE, 2003)

III. **Comparador baseado em correlação**: calcula-se a correlação entre as imagens de duas digitais. Para isso se superpõem as duas imagens e se faz a comparação de cada par de pixels correspondentes. Quando a correlação supera um limiar, considera-se que ambas digitais comparadas pertencem à mesma fonte. Também existem outras técnicas para o cálculo da correlação entre ambas as imagens como a multiplicação no domínio da frequência, ainda que seu custo computacional seja muito maior devido à necessidade de conversão para

> o domínio espectral. Outra opção é dividir a imagem em partes e calcular a correlação por setores. Em geral são técnicas que apresentam muitos problemas quando as digitais não estejam alinhadas ou quando existe deformação não linear. (RATHA; BOLLE, 2003)

Atualmente os sistemas usam combinações de várias destas técnicas para mostrar uma maior robustez frente aos possíveis ataques. 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. Estes sistemas são conhecidos como AFIS (Automated Fingerprint Identification System).

3.6.3 - Extração de Características, como é feito no Brasil?

Atualmente as impressões digitais são utilizadas extensamente tanto em aplicações civis como forenses/policiais. Esta ampla utilização e aceitação da impressão digital como identificador biométrico se deve em grande parte ao seu estudo científico como meio de identificação unívoco das pessoas. Ao final do século XIX apareceram dois estudos científicos relevantes neste contexto: Galton, com a análise das impressões digitais e o surgimento das minúcias para sua comparação, e o de Henry, com a classificação das impressões digitais em função da forma macroscópica formada por suas cristas.

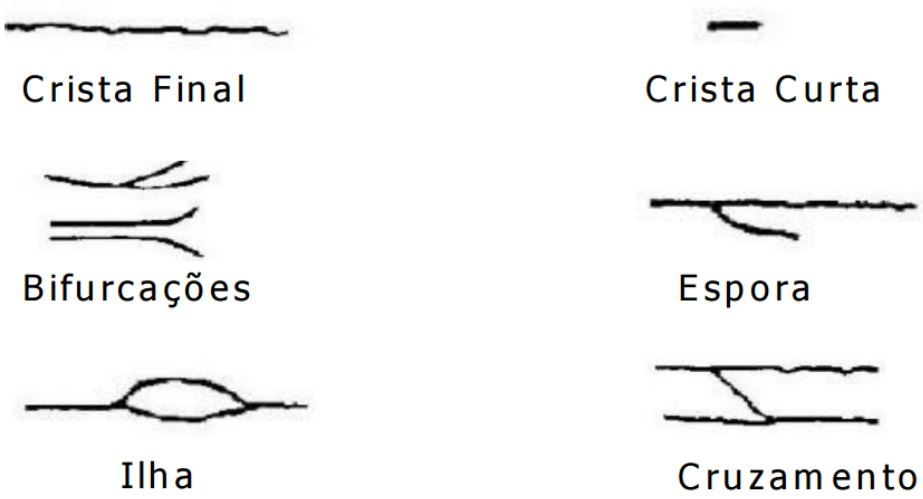


Figura 20 - Alguns tipos de minúcias encontradas nas imagens de impressão digital

No início do século XX as impressões digitais começam a ser utilizadas profusamente na ciência forense, facilitando por sua vez a ação policial na identificação de criminal. Isto leva a 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: “Automatic Fingerprint Identification System”) e assim diversas pesquisas neste âmbito são iniciadas em meados do século XX.

Este conhecimento científico gerado desde cedo, unido a ampla utilização da impressão digital no âmbito forense e policial, proporcionou impulsionou o estudo e desenvolvimento dos AFIS. Este 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 inclusive preço. Este 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.

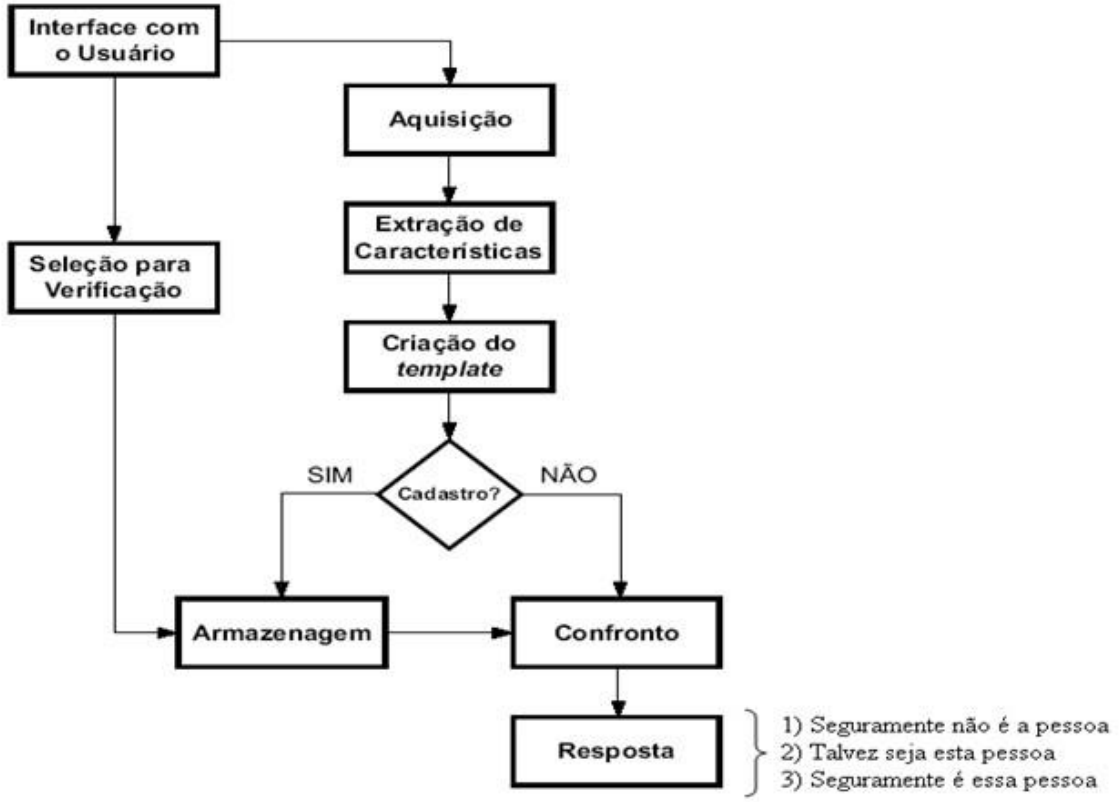
As impressões digitais são a reprodução da epiderme da parte posterior dos dedos da mão. Como se observa na figura 15, uma impressão

digital é formada por um conjunto de linhas que são denominadas cristas (linhas escuras) e vales (linhas claras). Este conjunto de linhas que formam as impressões digitais podem assemelhar-se a padrões ou texturas que podem ser analisar de diferentes maneiras dependendo do grau de detalhes.

As características mais utilizadas para a análise e comparação das impressões digitais são as minúcias, que são os pontos singulares que apresentam as cristas. Dentro das minúcias existem diferentes tipos entre os quais se destacam as bifurcações e as terminações por sua facilidade para a extração automática (figura 21). As minúcias eram utilizadas no reconhecimento manual que realizavam os especialistas antes de existir os AFIS e foi por isso que ao desenhar os primeiros sistemas automáticos grande parte dos algoritmos se basearam nelas. Esta tendência segue existindo com o passar do tempo e as técnicas baseadas em minúcias ainda são as mais estudadas e sobre as quais existe uma maior quantidade de algoritmos de identificação.

Figura 21 - Impressão Digital. (www.jpconsultoria.com.br)

A figura 22- abaixo, ilustra um esquema típico de um sistema de comparação automática de impressões digitais (AFIS). (www.slideplayer.com.br)



As etapas apresentadas na Figura 22 são descritas a seguir:

- **Aquisição**: nesta etapa coleta-se uma amostra da impressão digital de um sujeito. Existem atualmente diferentes tipos de sensores (ópticos, capacitivos, térmicos, ultrassônicos, etc.). Dependendo do sensor utilizado, a qualidade e a resolução da imagem obtida podem variar enormemente. Os parâmetros mais relevantes que são utilizados para caracterizar os sensores são a resolução, a área de captura, o número de pixels, a precisão geométrica, o contraste e a distorção geométrica.
- **Pré-processamento**: a imagem coletada na etapa de aquisição é tratada em função das necessidades dos algoritmos de extração e comparação que serão utilizados. Normalmente sempre é necessário algum ajuste da imagem para aumentar a qualidade da mesma, como podem ser o ajuste de contraste, equalização do histograma e alguma eliminação de partes

da imagem que não contém a impressão digital, o que é denominado segmentação. Em muitos algoritmos é necessário o cálculo do campo de orientação que determina a orientação das cristas em cada zona da impressão digital. (BAZEN; GEREZ, 2002) Normalmente o pré-processamento requerido para os algoritmos de comparação de impressões digitais é bastante complexo e requer uma alta capacidade computacional. A comparação de minúcias requer um forte pré-processamento já que é necessário afinar as cristas até formar um fluxo de linhas da espessura de um pixel (thinning) para depois extrair a localização dos pontos singulares.

- **Extração das características**: nesta etapa é extraída a informação relevante das impressões digitais para sua posterior comparação. A maior parte dos algoritmos de comparação de impressões digitais utilizam como característica as minúcias. Um dos algoritmos de extração de minúcias mais destacados é o algoritmo de acompanhamento de cristas de Maio (1997), que consiste em traçar todas as cristas da impressão digital, determinando como minúcias as bifurcações (desdobramento de uma crista em duas cristas) e terminações (fim de uma crista). Cabe destacar que os algoritmos de extração de minúcias extraem geralmente grande quantidade de minúcias falsas que é necessário eliminar antes de passar à fase de comparação para evitar erros na decisão.
- **Comparação:** nesta etapa são comparadas as características extraídas para determinar se as duas amostras pertencem ao mesmo indivíduo. Existem algoritmos que não necessitam extração de características e por tanto realizam diretamente a comparação.

Figura 23 - Filtro de Suavização

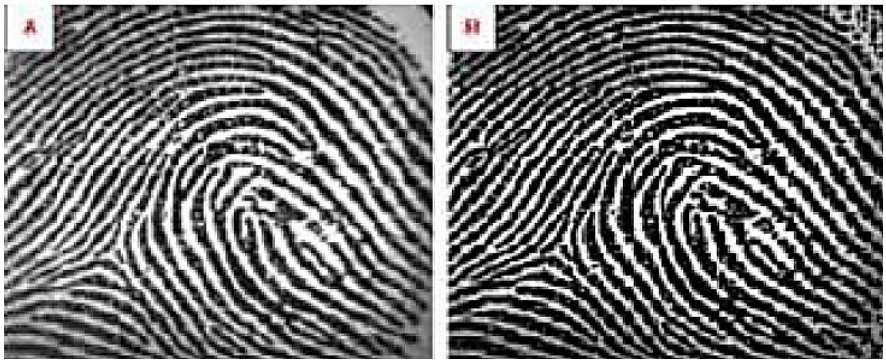


Figura 24 - Filtro de Contraste

Original	Imagem Filtrada
	
Imagem binarizada	Esqueletização

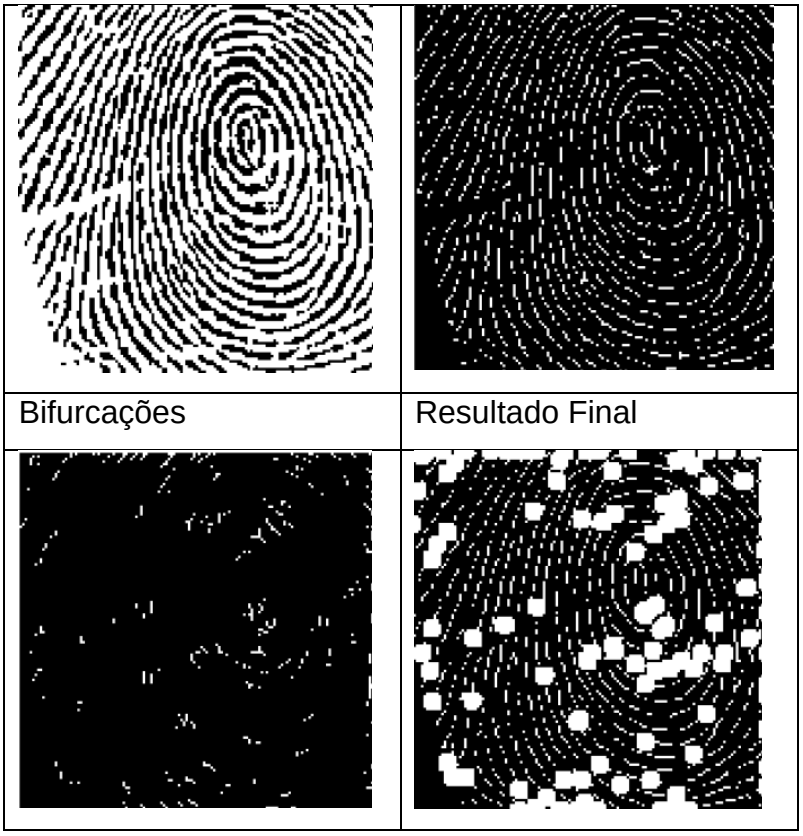


Figura 25 – comparação

A imagem é obtida por dispositivos eletrônicos especiais, a qual está baseada em quatro tecnologias: ótica, capacitiva, térmica e ultrassônica.

Na ótica, FTIR (*Frustrated Total Internal Reflection)* a superfície da aquisição de 1” x 1” é convertida em imagens de cerca de 500 dpi. Assim a luz refletida vai depender da pele e das imagens saturadas ou difusas que podem sdr 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

Na capacitiva, as cristas e 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 num valor de intensidade de um pixel. A superfície de aquisição de 0,5” x 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 que o ar. O contato com as cristas da pele causa uma alteração observável na temperatura da superfície do sensor. É melhor 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 num feixe ultrassônico dirigido a superfície do dedo para medir diretamente a profundidade dos sulcos com base no sinal refletido. A oleosidade da pele não afetam a imagem obtida, que reflete bastante bem a topologia dos sulcos. Mas, estas unidades tendem a ser grandes e requerem um tempo de leitura maior que os leitores óticos.

O processamento de aquisição se dá na ponta (cliente da aplicação) ou pode ser transmitida ao servidor para processamento. No processo de extração que é o ponto central dos sistemas de autenticação baseiam-se em impressões digitais com implicações para o projeto do restante do sistema. Classificam-se em três níveis: global, local e fina.

Na global se descreve a formação geral das linhas. Podem ser observados um núcleo e mais de dois deltas. Estas formações singulares são usadas como pontos de controle, em volta dos quais as linhas são organizadas.

Na abordagem local que está relacionada com detalhes marcantes das próprias linhas conhecidas por minúcias, os mais utilizados em sistemas automatizados são a terminação de linha e a bifurcação de linha. A extração destas características locais depende fortemente da qualidade da amostra adquirida.

Ademais a abordagem fina está baseada nos detalhes intra-linhas que nada mais é que a posição e formação geral dos poros de suor que medem cerca de 60 mícron. Sua extração somente é viável e imagens de alta resolução (cerca de 1.000 dpi) obtidas de impressões digitais de boa qualidade.

No que pertine ao processo de comparação esse 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, a concordância qualitativa, cujos detalhes de minúcias devem ser idênticos e a Suficiência quantitativa que especifica que ao menos um certo número de detalhes de minúcias devem ser encontrados (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.

Ressalta-se que as técnicas feitas por imagens inclui técnicas de correlação de imagem tanto ótica quanto numéricas. Já nas técnicas baseadas em características, esta comparação que é feita por minúcias é um dos métodos mais conhecidos e mais largamente usados, pois se refere a analogia feita pelos especialistas que comparam impressões digitais em aplicações forenses, que é aceita como prova legal em maioria dos países.

Os pontos forte usados na tecnologia de autenticação biométrica por impressão digital são a precisão, 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: a não aceitação da técnica por questões de higiene e outros, a qualidade das impressões digitais varia enormemente dentro de uma população e os sensores mais baratos poder ser comprovadamente falsificados e fraudados.

3.7 - FALHAS

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 e outros parâmetros. Os sistemas biométricos não estão totalmente imunes contra 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 sistema

biométrico foi projetado e é utilizado. O modulo de aquisição são considerados os menos vulneráveis do sistema de identificação.

Por outro lado existe meios para enganar sistemas comercias de reconhecimento apresentando amostras biométricas artificiais tais como uma impressão digital falsificada, uma íris artificial ou uma máscara facial. Assim, para poder elaborar uma impressão digital enganosa, o atacante deve conseguir uma representação da característica biométrica original.

Ultimamente há diversas pesquisas onde a reversibilidade de alguns modelos biométricos, como a impressão digital, por exemplo é possível. Basta usar uma imagem da impressão digital reconstruída a partir do modelo reduzido da característica armazenada no bando de dados, conhecida como minutiae, com o objetivo de invadir os sistemas computacionais. A cópia da impressão digital obtida dessa forma, embora provavelmente seja incapaz de enganar um perito humano demonstra a possibilidade de iludir sistemas comerciais do reconhecimento da impressão digital.

Assim, o grau de precisão de cada sistema normalmente pode ser definido pelo método biométrico usado e pelo padrão codificado. A tolerância para aceitar ou não um indivíduo deve ser configurado de forma que a taxa na identificação seja minimizada, ao mesmo tempo em que ninguém seja reconhecido com identidade de outro que tenha características semelhantes.

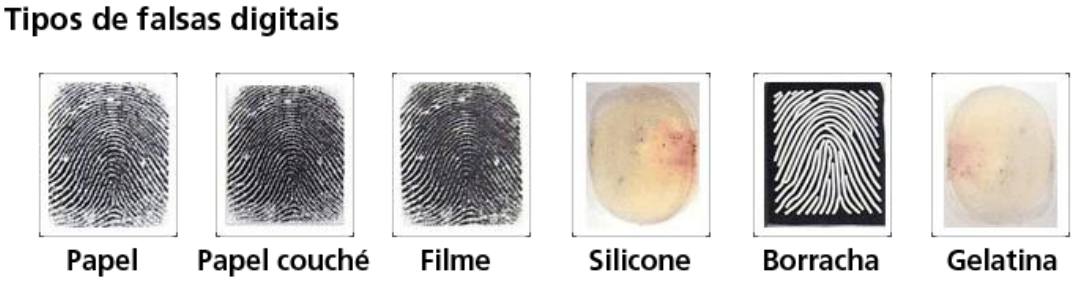


Figura 26. Tipos de falsas digitais. (www.vird.com.br)

3.8 – CONTROLE DE ACESSO

Quanto ao controle de acesso esse deve ser rigorosamente aplicado no sistema biométrico por impressão digital, como forma segura na autenticidade e aplicação. Portanto podemos dizer que o controle de acesso são recursos importante utilizados para garantir que as redes, computadores e informações estejam acessíveis somente por pessoas autorizadas.

No caso do auto de prisão em flagrante a autorização seria concedida ao policial responsável pela lavratura que seria, o Delegado de Polícia e Escrivão de Polícia, que 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, feita a lavratura do auto de prisão em flagrante. Também o acesso poderia ser feito de outra forma que não por pessoas, e sim, por exemplo por um programa acessando um arquivo. Para isso dever-se-á ser concedido, a integridade, confidencialidade e disponibilidade da informação, cuja função é de garantir que os dados sejam corrompidos e que somente as pessoas autorizadas acessem esses dados e que eles estejam disponíveis as pessoas competentes sempre que necessário, respectivamente. Com a integridade garante-se a exatidão dos dados.

A disponibilidade tem por fim garantir o funcionamento pleno do sistema computacional e dos seu recursos aos usuários autorizados.

Já confidencialidade é o que prevê que somente pessoas autorizadas tenham acesso a um determinado local ou informação. Por isso a figura 18 a baixo mostra quatro fazes que levam a concessão do acesso requerido, sendo eles: identificação, autenticação, autorização e responsabilidade.

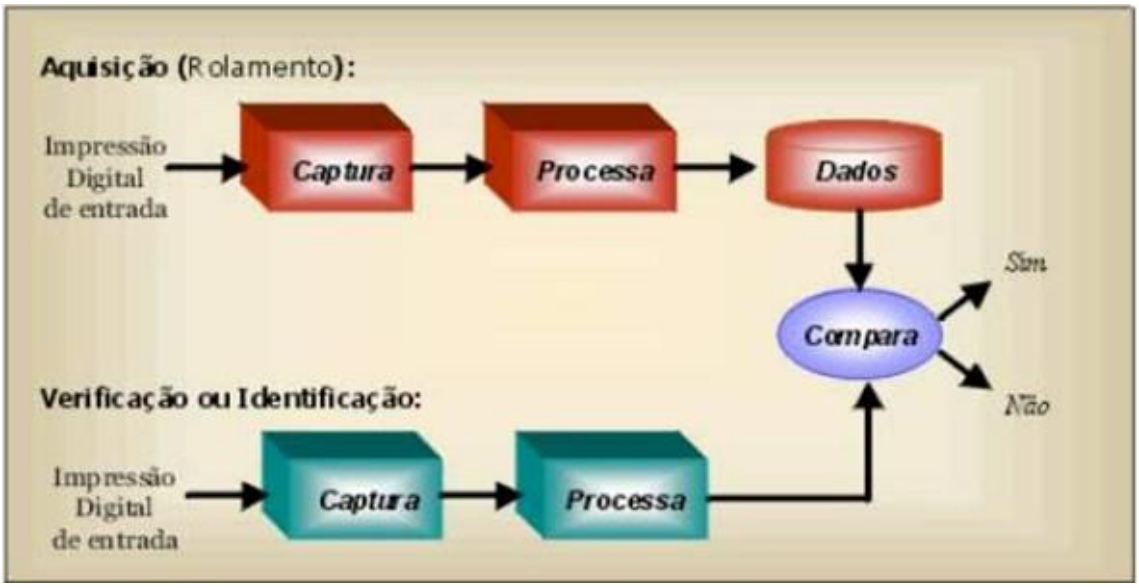


Figura 27 - Controle de Acesso. (www.slideplayer.com.br)

3.9 – LEGALIDADE

O sistema biométrico na forma de impressão digital como meio identificador vem sendo utilizado com frequência como forma segura na aplicação da identidade da pessoa que está usando. Por isso as aplicações de identificação biométrica já encontram algum respaldo no nosso ordenamento jurídico. Isto é visto em órgão públicos e organizações privadas. No nosso sistema carcerário, por exemplo, já se aplica o uso de identificação biométrico com o uso da impressão digital. Cada detento é cadastrado e identificado com o uso da biometria de impressão digital. Até o momento não houve discussão e um questionamento acerca de sua legalidade, uma vez que o sistema apresenta ser seguro e certo. O uso da biometria como forma de identificação deve ser sempre utilizado respeitando os princípios da proporcionalidade e adequação sem ferir sua finalidade. Dessa forma, os dados contidos e armazenados devem ser adequados pertinentes e não excessivos em relação à finalidade e proporcionais aos objetivos propostos pelo sistema, isto é, as características biométricas não podem ser utilizadas com finalidade diversa da determinante da coleta.

Pergunta-se se os sistema biométrico por impressão digital não estaria violando a integridade física do indivíduo do seu direito de privacidade ou intimidade. Não, o sistema biométrico não deve ser encarado como uma violação desses direitos, pois a peculiaridade deste método de controle resulta da necessidade do usuário cooperar e aceitar que elementos da sua identidade física, morfológica ou comportamental seja capturados e armazenados numa base de dados e apresentados perante um sistema de reconhecimento para garantir a conformidade com a política de segurança da corporação contra ameaças, ataques e tentativas de acessos indevidos ao sistema computacional. No entanto, o indivíduo pode recusar a fornecer seus dados para identificação, alegando razões legitimas relacionadas com uma situação em particular e que se apresentem com relevância para fazer prevalecer o seu direito sobre os interesses do sistema. Mas, isso só ocorrera desde que os responsável pela aplicação do sistema biométrico assegure junto ao indivíduo o esclarecimento prévio em relação as finalidades determinantes da coleta, destinatários e condições de utilização dos dados, bem como o esclarecimento de dúvidas e receios que a tecnologia posse suscitar.

Ocorrendo invasão de privacidade pode-se identificar quem a violou observando primeiramente o registro das características biométricas com o subsequente armazenamento no sistema e a identificação, com objetivo de assegurar o registro dos acessos do usuário ao sistema computacional.

Denota-se que a captura das características biométricas implica na cooperação, anuência do usuário por meio de exposição da respectiva parte do seu corpo para obtenção das características físicas ou morfológicas de sua identidade pessoal não podendo ser realizada com violação da sua identidade pessoal, lesão da sua integridade física ou com intromissão da intimidade. Dessa forma, na coleta de características biométricas como a impressão digital, geometria da mão ou da face, padrão da íris ou reconhecimento da retina, a captura não tem qualquer implicação com a integridade física do indivíduo na medida em que a finalidade visada ou a forma como os elementos da identidade são capturados não tem implicações pessoais.

Fica então, a preocupação quanto a utilização de características biométricas quando a sua ponderação no caso concreto da idoneidade da necessidade da conformidade dos motivos apresentados para utilizar a tecnologia. O que afeta diretamente a privacidade é a finalidade com que é utilizada e os riscos que apresenta para a própria pessoa e as consequências produzidas em razão da sua falta de confiabilidade e os efeitos no caso de falsificação ou usurpação da característica biométrica e não a característica biométrica. Para sua prevenção basta utiliza-la com eficiência se as características biométricas não se encontrarem centralizadas numa base de dados, razão pela qual se defende sempre que possível o registro das características biométricas em um meio físico que o indivíduo possa carregar consigo, um cartão do tipo Smart Card, por exemplo.

Por fim é de se considerar que pode ocorrer extravio, roubo ou falha por mau estado de conservação a inserção das características biométricas, não estando afastados riscos efetivos de falsificação ou apropriação das características por terceiros, o que pode trazer sérias consequências para o sistema. Se isso ocorrer, o tratamento das características físicas intrínsecas do indivíduo contribui para violar os princípios da política de segurança da corporação.

Portanto, impõe-se a necessidade de que os responsáveis pelo sistema biométrico não encarem a sua introdução como ferramentas definitivas e infalíveis em termo de segurança, mas que devem abordar com realismo os diversos envolvidos na sua aplicação.

Juridicamente não há uma legislação específica que venha disciplinar o uso e aplicação da biometria no Brasil. Mesmo assim, a informação biométrica goza de proteção específica, pois está relacionada diretamente aos conceitos de intimidade, privacidade e imagem do usuário.

Portanto, analogicamente se aplica o princípio constitucional previsto no artigo 5º, inciso X, da Constituição Federal:

> “Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, a liberdade, à igualdade, à segurança e à propriedade nos termos seguintes:

> X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”

Dessa forma, se uma pessoa cadastrar sua digital ou íris no processo não há que aventar invasão de privacidade ou que outra pessoa esteve naquele local, porque apenas o dono da própria digital ou íris tem tal prerrogativa. Será um caso em que se configura a impossibilidade de transferência de responsabilidade.

Ressalta-se que as empresas de plano de saúde e odontológico pelo crescente número de usuários ao implantarem em seus sistemas a solução biométrica para coleta de dados devem deixar claro para o consumidor preferencialmente por escrito, as condições de uso e a forma de armazenagem destas informações. Também, isto é visto nas academias, onde se coloca o uso de biometria na catraca de entrada e saída. Deve a empresa antes de tudo ter em seu contrato de adesão do serviço prestado uma cláusula específica informando a coleta do dado biométrico, e que após a rescisão do contrato os dados serão guardados ainda por três anos. Essa precaução é válida também para os bancos, plano de saúde em especial e demais estabelecimentos comerciais.

Por outro lado, uma maneira de garantir a inviolabilidade do sistema é por meio de chaves de segurança, onde a informação eletrônica deve ser preservada em ambiente seguro, isolado. Recomenda-se o uso de um servidor que gera certificação que prove que qualquer alteração fica também documentada. Qualquer visita àquela informação está registrada e é conhecida a origem daquele que consultou a informação. Há regras internacionais que regulam a forma como deve ser feita a armazenagem segura de informações para evitar o vazamento desses dados.

Assim sendo, o melhor procedimento legal para o uso da biometria na relação de empresas com indivíduos é a definição de uma política de segurança com avaliação do risco para os templates biométricos, a adoção de controles de segurança que minimizem os riscos com controle e registro do uso dos dados

biométricos somente por pessoas e sistemas autorizados, além de um documento que será apresentado ao indivíduo para a anuência da coleta de suas características biométricas. Também, é bom lembrar que nunca sob hipótese alguma guardem as imagens das características biométricas tomadas dos indivíduos, somente dos templates gerados por algoritmos biométricos a partir destas imagens que deverão ser descartadas imediatamente após esse processamento.

Ao final pergunta-se se no nosso País tem condições de conviver com tal aparato tecnológico sem oferecer risco à integridade física do detentor do acesso. Responda-se que dependerá da divulgação dos cadastros e da possibilidade do crime organizado em descobrir quem são os protagonistas das empresas que detém o acesso tão almejado. Se houver uma proteção adequada será viável e possível.

3.10 – ESTADO DA ARTE

Vemos ultimamente que o uso da biometria por impressão digital vem sendo usada com frequência nos estabelecimentos comerciais tais como, bancos e também em alguns órgãos públicos.

Nos bancos o uso da biometria por impressão digital são usados nos caixas eletrônicos, onde o correntista só precisa aproximar o dedo do leitor e aguardar a identificação. Em alguns bancos não é necessário o uso do cartão.

Também visível o uso da biometria por impressão digital em alguns órgãos públicos tais como em presídios. O primeiro passo é cadastrar todo o preso que dá entrada e coletar sua impressão digital, que ficará armazenada em banco de dados daquele órgão, podendo posteriormente identifica-lo quando necessário. Em nosso sistema prisional catarinense isso já existe e funciona normalmente. Basta haver um leitor que fará a coleta da impressão digital e sua leitura. Assim torna-se mais eficiente a identificação dos presos e inclusive como fonte de pesquisa por parte de peritos criminalísticos quando num eventual delito cometido.

Dessa forma, o uso da biometria por impressão digital em bancos tem como objetivo aumentar a segurança dos correntistas, a confiabilidade das transações e conferir mais agilidade e conveniência de acordo com o banco. Além disso o cliente o leitor verifica o padrão da circulação sanguínea para autenticar a operação. Para que o leitor faça a leitura é necessário que antes o correntista se cadastre.

De outra parte vê-se também o uso da biometria por impressão digital no processo eleitoral. Desde o ano de 2008, a justiça eleitoral vem usando essa ferramenta como forma de segurança do eleitor e agilização na forma de votar. Isso já acontece por enquanto nas capitais brasileiras.

A justiça eleitoral tem como objetivo no que tange a biometria por impressão digital de é tornar o processo democrático ainda mais seguro excluindo qualquer possibilidade de uma pessoa votar em lugar de outra. Por outro lado pensa-se que o procedimento possa contribuir significadamente para a redução da revisões eleitorais que passam gradativamente gerar custos elevados no orçamento público. Esse custo chega em torno de dois milhões anuais.

Procedimento se faz quando o eleitor é convocado para recadastramento, onde é recebido por um funcionário da justiça eleitoral munido de uma série de equipamentos chamados de Kit Bio, onde são armazenados todos os dados necessários do eleitor como se fosse um computador portátil. Assim, autorizada a convocação do eleitor ele é chamado e no cartório da justiça eleitoral é tirada uma fotografia desse eleitor que é armazenada nos servidores do TSE (Tribunal Superior Eleitoral) e incorporada aos dados recém colhidos ou atualizados. Depois um programa de computador corrige os erros de posicionamento, foco e iluminação da fotos, fazendo com que passem a serem capturadas de maneira rápida prática evitando que o serventuário passe por treinamento específico. Posteriormente é feita a coleta de impressão digital com auxílio de um scanner com os padrões de todos os dedos, onde são digitalizados e armazenados.

Na hora do voto o eleitor somente pressiona seu dedo indicador no aparelho scanner acoplado a urna que faz a coleta da impressão digital, leitura e compara os padrões datiloscópicos com aqueles armazenados no servidor.

Dessa forma com a identificação positiva o eleitor é reconhecido e habilitado a votar.

4. DISCUSSÃO

O presente texto se baseia na análise da possibilidade de se utilizar e aplicar a biometria por impressão digital quando da lavratura da prisão em flagrante no que pertine ao momento da assinatura, tornando-o ágil e válido.

Logo se faz necessário discutir se é viável utilizar a biometria por impressão digital no caso e, uma vez possível se é legal, quanto a sua aplicação.

A biometria como tecnologia aplicada a dados corporais, tais como a impressão digital e não a informações biográficas pode sim ser usada para identificação do indivíduo após a lavratura do auto de prisão em flagrante.

É por meio do sistema biométrico conhecido por AFIS que se vai buscar identificar e autenticar pessoas. A autenticação se faz de dois modos: a verificação e identificação.

A verificação é feita com a captura da impressão digital da pessoa por meio de um leitor optico ou scaner que vai coletar as minucias ou os pontos característicos (linhas da digital como bifurcações e outros) por meio de algoritimos matemáticos que vai fazer análise para depois comparar e identificar.

Na identificação, a impressão digital coletada, analisada e comparada com as demais contidas em um banco de dados vai verificar se aquela é a que está armazenada neste banco de dados para então, no final identificar ou não a pessoa pretendida.

Para isso faz-se necessário cruzar informações de outros bancos de dados junto aos governos, ao sistema bancário e de crédito, redes sociais na internet e a partir daí construir um perfil.

Portanto, partindo do princípio de que os Estados devem investir nessa tecnologia , uma vez implantado o sistema biométrico na segurança pública ficar-se-á fácil, ágil e célere identificar qualquer cidadão, desde é claro que haja cruzamento de informações entre os órgãos governamentais. Basta trazer informações dos bancos de dados das identificações civis coletadas dos

registros civis, junto com outras informações de registros obtidos juntos aos presídios e armazena-los em um outro banco de dados criados especificamente para a identificação do suposto autor do crime no uso policial.

Vale lembrar que na época do governo Lula, o Brasil importou da França por US$ 36 milhões, o sistema biométrico AFIS, quando a empresa brasileira Griaule á desenvolvia essa tecnologia pelo custo mais baixo. Dessa forma, os Estados do Tocantis, Goias, Rondônia, Mato Grosso, Pernambuco e Sergipe já vinham utilizando essa tecnologia para identificação civil. Ressalta-se que o EUA já utiliza o sistema biométrico AFIS há muito tempo, inclusive para fins de identificação de criminosos no âmbito penal.

O Brasil atualmente está aplicando o sistema biométrico AFIS não só no campo de identificação civil, mas também no campo penal. O Estado de Santa Catarina por exemplo utiliza o AFIS no âmbito da identificação civil inclusive em presídios, mas não aplica ainda no âmbito penal. Observa-se o quadro abaixo a utilização da biometria na identificação civil apenas, pois a penal ainda não é usada por maioria dos Estados, somente o Estado de São Paulo é que começou a utilizar o AFIS para identificação de criminosos;

Acre	Uso de biometria identificação **civil** por impressão digital	Não uso de biometria identificação **civil** por impressão digital
Amazonas		Não
Amapá		Não
Bahia	Sim	
Ceará		Não
Distrito Federal	Sim	
Goias	Sim	
Maranhão		Não
Mato Grosso		Não
Mato Grosso do Sul	Sim	
Piaui		Não
Pernambuco	Sim	
Paraiba		Não
Rondonia		Não
Rio Grande do Norte		Não

Rio de Janeiro	Sim	
Rio Grande do Sul	Sim	
Sergipe		Não
Santa Catarina	Sim	
Tocantins		Não
Espirito do Santo		Não
Paraná	Sim	
São Paulo	Sim	
Pará		Não
Minas Gerais	Sim	

Sendo assim, não resta dúvida de que havendo de fato o sistema AFIS na segurança pública fica demonstrado que é possível aplicar a biometria por impressão digital para identificação da pessoa no âmbito penal, quando da lavratura do auto de prisão em flagrante, tornando-o ágil, célere e legal no ponto de vista jurídico, logo viável a sua aplicação, até porque a biometria por impressão digital apresenta ser um instrumento de identificação tecnológico que pode ser usado tanto na iniciativa privada quanto na pública, proporcionando um aparato seguro em sentido amplo, sem deixar de lado que poder ocorreu falhas, uma vez que computadores são máquinas falíveis.

5. CONCLUSÕES E TRABALHOS FUTUROS

Como visto e discutido neste contexto, desde há tempos a humanidade vive em grupos sociais e desse grupos formam-se outros grupos guiados e orientados por norma regida e estabelecida por eles próprios. As normas que via de regra eram penais, não visavam limitar a liberdade do indivíduo, isto é, determinando prisão para aqueles que o infringiam. No entanto, com o surgimento do Estado, essa privação de liberdade passou a ser imposta e servida de exemplo para todos àqueles que tentavam desafiar o poder Estatal.

A partir daí surge prisão como meio de privação da liberdade do indivíduo e também como forma exemplificativa e como meio de correção para todo o indivíduo que viesse a violá-la. A palavra flagrante que no latim significa flagrans, flagrantis (do verbo flagare, queimar) significa ardente que está em

chamas, que arde, que está crepitando. Por isso a expressão flagrante delito, para significar o delito no instante mesmo da sua perpetração, o delito que está sendo cometido, que ainda está ardendo.

Dessa forma prisão em flagrante delito é assim, a prisão daquele que é surpreendido no instante mesmo da consumação da infração penal. Também não podemos deixar de observar que a prisão em flagrante é espécie de prisão cautelar e ocorre conforme determinação legal nas hipóteses o artigo 302 do CPP, denominadas situações de flagrância. Assim, verificado um fato em tese delituoso, e sendo o agente encontrado cometendo a infração ou acabado de cometê-la, pode ser preso em situação denominada pela doutrina como de “flagrante real” “flagrante próprio”, ou ainda “flagrante perfeito”. Pode também, ser perseguido, logo após, pela autoridade ou qualquer outra pessoa em situação que faça presumir que tenha cometido a infração poderá ser preso em situação flagrância denominada “flagrante”, perfeito, imperfeito ou ainda impróprio. Por fim, se encontrado, logo depois, com instrumentos, armas, objetos ou papéis que façam presumir ser ele o autor da infração, também poderá ser preso por estar na denominada situação de “flagrante ficto” ou “flagrante presumido”.

Ademais, a prisão em flagrante pela própria relação de imediatidade que se estabelece entre situação fática aparentemente criminosa, é dever da autoridade policial proceder à prisão, e é a única modalidade de prisão cautelar que não se inicia por ordem escrita e fundamentada de juiz competente.

Por essa ordem, capturado o autor do fato, presente testemunhas, e a situação de flagrância, a autoridade policial observando que há fundada suspeita contra o conduzido deverá lavrar o auto de prisão em flagrante e encaminhar o autor para o presídio. Mas aí, pergunta-se, se é possível aplicar a biometria por impressão digital quando da assinatura nos depoimentos?

Buscando conceitos científicos e doutrinários chega-se a uma breve conclusão de que é possível aplicar a biometria por impressão digital, pois além de tornar o procedimento ágil e célere no seu termino e no momento do seu encaminhamento da comunicação ao poder judiciário, é legal na ótica de nosso ordenamento jurídico e legislativo, bem como seguro na sua aplicabilidade.

O uso da biometria por impressão digital na identificação civil está sendo usada no Brasil por cause todos os Estados, incluindo aí o Estado de Santa Catarina. No entanto, quanto a aplicação na identificação penal, o mesmo não se aplica ainda, pois falta recursos tecnológicos para seu uso, embora exista um banco de dados com muitas informações, mas o sistema não se comunica com os demais órgãos, o que torna dessa forma, prejudicada a aplicação da biometria por impressão digital na identificação penal por enquanto. É bom lembrar que os EUA, por exemplo já aplicam o sistema AFIS na identificação de criminosos elucidando com mais agilidade os delitos que ocorrem.

Assim sendo, a aplicação da biometria por impressão digital após a lavratura do auto de prisão em flagrante é possível e legal no ponto de vista legislativo brasileiro, além de seguro e ágil.

REFERÊNCIAS

_____. Código de Processo Penal Interpretado. Ed Atlas, São Paulo. 2001.

_____. **A Busca Pessoal e Suas Classificações**. WWW.jusnavegandi.com.br.

ABREU FILHO. N.P. Porto Alegre, **Verbo Jurídico**, 2009. 840p. (série Noronha, Magalhães. Curso de Direito Processual Penal. Ed. Saraiva. São Paulo. 2000.

BAZEN, A.M.; GEREZ, S.H.: **Systematic methods for the computation of the directional fields and singular points of fingerprints**, IEEE Transactions on Pattern Analysis and Machine Intelligence, July 2002, vol. 24, Issue 7, pp: 905–919.

BRICHETTI G. **La evidencia en el derecho procesal penal** – trad. Esp. Buenos Aires, 1973

CHAMPOD, C., LENNARD, C., MARGOT, P., AND STOILOVIC, M. **Fingerprints and Other Ridge Skin Impressions**. CRC Press, 2004.

CHAVES, L.G. **Prisão Em Flagrante**. (WWW.adpesp.org.br Práxis).

CONSTITUIÇÃO FEDERAL, **Código Penal e Código de Processo Penal**. 10ª.Edição,

EKENEL, H; SANKUR,B. **Feature selection in the independent component subspace for face recognition**, Pattern Recognition Letters, vol. 25, no. 12, pp. 1377-1388. 2004.

FRANCO, A.L.N. **A Voz de Prisão em Flagrante**. WWW.jusnavegandi.com.br.

FRANCO, R.S. **Código de Processo Penal e sua Interpretação Jurisprudencial** – 2. ed. Ver., atual e ampliada. Vol 02 – São Paulo: Editora Revista dos Tribunais, 2004. p.2135

GALTON, F. **Finger Prints**. Macmillan, London. 1892.

GOMES CANOTILHO, J.J. **Estado de Direito, Cadernos Democráticos**, nº 07, Ed. Gradiva.

HENRY, E. **Classification an Uses of Finger Prints**. Routledge, London, 1900.

JAIN, A.K., FLYNN, P.J., ROSS, A. **Handbook of biometrics**. Springer, New York, 2007.

MAIO, D., MALTONI, D.: **Direct gray-scale minutiae detection in fingerprints.** IEEE Transactions on Pattern Analysis and Machine Intelligence, 1997, vol. 19, Issue 1, pp: 27–40.

MALTONI, D., MAIO, D., JAIN, A.K.,PRABHAKAR, S. Handbook of fingerprint Recognition. Springer, 2009.

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

NUCCI, G.S. **Código de Processo Penal Comentado** – 6º edição revista, atualizada e ampliada. 2. tir. São Paulo: Editora Revista dos Tribunais, 2007.p.502 e 576

PAGLIONE, E.A. **Prisão Em Flagrante**. WWW.adpesp.org.br

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 in Computer Science, LNCS, vol. 3832, 2006, pp: 244-250. 2006.

PINHEIRO, J.M. **Biometria nos Sistemas Computacionais – Você é Senha –** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

RANGEL, P. **Direito Processual Penal -**. 12ª Ed. Rio de Janeiro, Lummen Júris, 2007.

RATHA, N. AND BOLLE, R. **Automatic Fingerprint Recognition Systems**. Springer, 2003.

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

TOURINHO FILHO, F.C. **Processo Penal**. 3º volume. 28ª Ed. São Paulo, Saraiva.