CAPÍTULO 9

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

Fernando Henrique Borges Ferreira
Juarez Bento da Silva
Marta Adriana da Silva Cristiano
Priscila Cadorin Nicolete

1 INTRODUÇÃO

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

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

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

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

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

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

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

2 AUTO DE PRISÃO EM FLAGRANTE

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

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

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

> Considera-se em flagrante delito quem:
>
> I – está cometendo a infração penal;
>
> II – acaba de cometê-la;
>
> III – é perseguido, logo após, pela autoridade, pelo ofendido ou por qualquer pessoa, em situação que faça presumir ser autor da infração;
>
> IV – é encontrado, logo depois, com instrumentos, armas, objetos ou papéis que façam presumir ser ele autor da infração.

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

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

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

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

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

3 BIOMETRIA

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

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

Com a necessidade de se criar umaa tecnologia de desenvolvimento para escaneamento por impressão digital, o FBI contratou serviços da National Bureau of Sander (NBS), atualmente Institute of Standards and Technology (NIST), que veio a dar certo com a criação do escâner, 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. Essa técnica era utilizada para captar e coletar impressão digital (RATHA; BOLLE, 2007).

4 CONCEITO E FUNCIONAMENTO

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

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

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

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

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

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

5 IMPRESSÃO DIGITAL COMO IDENTIFICADOR BIOMÉTRICO

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

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

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

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

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

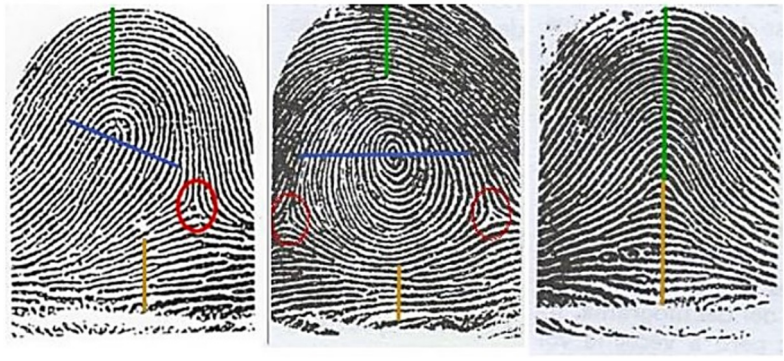

Figura 9.1 Exemplos de digitais do tipo monodelto, bidelto e adelto.

Fonte: Merysnow (2016).

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

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

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

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

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

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

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

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

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

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

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

6 SISTEMAS FORENSES DE IDENTIFICAÇÃO DIGITAL

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

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

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

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

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

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

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

7 EXTRAÇÃO DE CARACTERÍSTICAS, COMO É FEITO NO BRASIL?

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

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

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

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

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

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

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

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

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

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

8 CONCLUSÃO

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

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

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

REFERÊNCIAS

BASTOS, J. M. P. et al. **Biometria Impressões digitais**. Disponível em: <http://jpconsultoria.com.br/Seguranca/index.html>. Acesso em: 28 fev. 2016.

BORJA, C. T.; BUENO, A. G. **Sistemas biométricos**. [S.l.: s.n.], [20??]. Disponível em: <https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo Biometria.pdf>. Acesso em: 28 fev. 2016..

CHAMPOD, C.; LENNARD, C.; MARGOT, P.; STOILOVIC, M. **Fingerprints and Other Ridge Skin Impressions**. New York: CRC Press, 2004.

BRASIL. Constituição Federal. **Código Penal e Código de Processo Penal**. 16. ed. São Paulo: Atual, 2014.

COSTA, L. R.; OBELHEIRO, R. R.; FRAGA. Introdução à Biometria. **Minicursos do VI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'2006)**, Santos, ago. 2006, p. 103-151.

EKENEL, H.; SANKUR, B. Feature selection in the independent component subspace for face recognition. **Pattern Recognition Letters**, v. 25, n. 12, p. 1377-1388, 2004.

FINDLAW. **Fingerprints:** the first ID. 2016. Disponível em: <http://criminal.findlaw.com/criminal-procedure/fingerprints-the-first-id.html>. Acesso em: 29 fev. 2016.

FRÍAS, Z.; EDUARDO, X. **Diseño e implementación de un prototipo para autenticación, autorización y conteo (AAA) para el control de asistencia de los empleados de la Escuela Politécnica Nacional por medio de huellas dactilares**. 2004. Disponível em: <http://bibdigital.epn.edu.ec/bitstream/15000/5487/1/T2349.pdf>. Acesso em: 29 fev. 2016.

GALTON, F. **Finger Prints**. London: Macmillan, 1892. Disponível em: <http://www.clpex.com/Information/Pioneers/galton-1892-fingerprints-lowres.pdf>. Acesso em: 20 jun. 2016.

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

JIMENEZ, V. E. J. **Crestas papilares**. 2011. Disponível em: <http://pt.scribd.com/doc/64679879/CRESTAS-PAPILARES#scribd>. Acesso em: 1 mar. 2016.

LI, S. Z. **Encyclopedia of Biometrics**: I-Z. New York: Springer Science & Business Media, 2009.

LIMA, A. C. de. **Biometria**. Monografia. 2016. Disponível em: <http://superclickmonografias.com/blog/?p=48>. Acesso em: 28 fev. 2016.

LLORET, F. R. **Laboratorio Forense**. Espanha: Universidade de Alicate, 2013.

LÓPEZ GARCÍA, J. **Algoritmo para la identificación de personas basado en huellas dactilares**. 2009. Disponível em: <http://upcommons.upc.edu/handle/2099.1/8082>. Acesso em: 1 mar. 2016.

MACHADO, V. S.; ALMEIDA JUNIOR, J. R. **Sistemas de reconhecimento biométrico**

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

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

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

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

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

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

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

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

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

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

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