A Biometria e suas Aplicações

Marco Antonio de Souza
Polícia Federal - Brasília/DF

RESUMO

Por meio da observação dos padrões biométricos, é possível individualizar uma pessoa. Durante muito tempo as impressões digitais foram a biometria mais empregada para este fim. Hoje, com o desenvolvimento tecnológico, várias outras formas de biometria podem ser usadas também para realizar a identificação de alguém, com destaque para a forma de caminhar, o reconhecimento facial, a íris, a retina, dentre outras. A importância da individualização de pessoas, hoje, é imprescindível. Em 2012, o Departamento de Justiça americano estimou que, aproximadamente 7% da população com 16 anos ou mais foi vítimas de ladrões de identidade, gerando um prejuízo de aproximadamente US$ 24,7 bilhões. Esse valor é maior do que o volume de perdas estimado para todos os outros tipos de crimes de propriedade (roubo e furto e roubo de veículos) – US$ 24 bilhões. Neste artigo serão apresentados conceitos e aplicações de identificação de indivíduos por meio da biometria (marcha, face, impressões digitais, íris e retina), assim como será iniciado um debate sobre a aplicaçao da biometria no combate a fraude e a relaçao entre biometria e privacidade.

Palavras chaves: Biometria. Identificação. Identificação biométrica. Marcha. Face. Papilas. Íris. Retina.

1. Introdução

Há milhares de anos a biometria tem sido utilizada para a identificação humana: Na Babilônia, há registros de transações comerciais que utilizaram impressões digitais, e na China, artesões assinavam suas obras com as suas impressões digitais datadas de 500 AC. No Egito antigo, os comerciantes eram identificados por meio de características físicas, como marcas ou cicatrizes, como forma de diferenciar aqueles de boa reputação (BLACKBURN et al., 2006).

Assim, desde a antiguidade, percebia-se que cada indivíduo possuía características singulares, físicas ou comportamentais, que poderia fazê-lo reconhecido por meio destas.

ISSN 2178-0013
ISSN Eletrônico 2318-6917

A necessidade de identificar criminosos era algo considerado fundamental pela sociedade e além das características físicas do indivíduo, os métodos antigos de identificação biométrica incluíam criar marcas, cicatrizes ou tatuagens nos criminosos, estratégia que deixou de ser utilizada na maioria dos países com o desenvolvimento de um sistema de lei criminal, na primeira metade do século XVIII (MAGUIRE, 2009).

Alphonse Bertillon, em 1879, propôs o primeiro método científico de identificação amplamente aceito. Esse método conhecido como antropometria ou Bertillonage consistia em uma combinação de medidas físicas coletadas por procedimentos prescritos. Era um sistema complexo de identificação humana, que também continha a descrição de sinais particulares, a fotografia do identificado de frente e de perfil. Esse método foi complementado em 1894, quando ele introduziu as impressões digitais como informação complementar (MAGUIRE, 2009).

Em 1880, Henry Faulds, médico missionário escocês, com residência em Tókio, publicou um artigo na revista Nature, sugerindo que as impressões digitais poderiam ser utilizadas para identificação científica de criminosos. Em seguida, o britânico William Herschel, Magistrado Principal na Índia, publicou outro artigo na Nature também abordando a possibilidade de identificação de indivíduos por meio da impressão digital (MAGUIRE, 2009).

Com isso, os primeiros passos para o desenvolvimento de um sistema de classificação das impressões digitais haviam sido dados, mas foi Francis Galton, no final do século XIX, quem comprovou cientificamente os pensamentos de Faulds e Herschel, estabelecendo uma classificação para os desenhos das digitais (FISHER et al., 2001).

Em 1891, Juan Vucetich, tornou-se chefe do Escritório de Identificação Antropométrica do Departamento Central de Polícia de La Plata e criou um sistema de classificação e um método para individualizar os prisioneiros usando as impressões digitais. Essa é considerada a primeira aplicação da datiloscopia pela lei. Um ano depois, foi solucionado o primeiro homicídio com as digitais como prova e desde então aprendeu-se a confiar nelas como prova forense (MAGUIRE, 2009).

Assim, a biometria, em especial o reconhecimento de um indivíduo por impressões digitais, passou a ser considerada como uma ferramenta poderosa para a identificação de criminosos ou mesmo civil. Muitos dos principais departamentos de polícia passaram a armazenar as impressões digitais de criminosos em um banco de dados (em cartões), o que possibilitaria a combinação de impressões digitais latentes encontradas na cena do crime com impressões digitais no banco de dados para determinar a identidade do criminosos (JAIN, A.K.; ROSS; PRABHAKAR, 2004). O uso das impressões digitais surgiu com um viés para a identificação científica de criminosos, estendendo sua aplicação posterirormente para a identificação civil.

O termo Biometria refere-se ao reconhecimento automatizado de indivíduos baseado em suas caraterísticas de comportamento ou biológicas, ou seja, consiste na associação de métodos estatísticos com as características físicas ou de comportamento para a identificação do indivíduo (LI; JAIN, 2015). Para tanto, são mensuradas características físicas, como a cor dos olhos, a voz, a textura da íris, o formato do rosto, as impressões digitais ou comportamentais, como a forma de andar ou de falar, entre outras. Essas características possuem como princípio serem únicas.

Os sistemas biométricos, desenvolvidos para possibilitar o reconhecimento automatizado, surgiram na segunda metade do século XX, juntamente com o desenvolvimento dos computadores. Houve um grande aumento de atividades ligadas à biometria durante a década de 1990. A partir dos anos 2000, os sistemas biométricos passaram a integrar o cotidiano das pessoas, como o uso de impressões digitais para autorizar operações bancárias, acessar os dados do celular ou entrar em edifícios ou residências (LI; JAIN, 2015).

Os sistemas biométricos são baseados na mensuração e armazenamento de um determinado padrão de medidas que são associadas a um usuário, pelo uso de inteligência artificial e de reconhecimento de padrões. Atualmente, as tecnologias biométricas mais utilizadas são: biometria de impressão digital, de geometria da mão e de dedos, da face, de íris e de voz. Melhorar as tecnologias de identificação e detecção é um desafio imposto pelo aumento das fraudes, de frutos e do desenvolvimento tecnológico, portanto é eminente a necessidade de evoluir a forma com a qual são protegidos as pessoas, os bens e os recursos pessoais, públicos ou privados (JAIN; NANDAKUMAR; ROSS, 2016).

Assim, uma vez que existem várias características biométricas, a escolha de qual deverá ser utilizada depende da sua aplicação, pois cada uma tem pontos fracos e fortes. Dificilmente um tipo de biometria irá efetivamente atender aos requisitos de todas as aplicações. Em outras palavras, nenhuma biometria é "ideal".

Neste trabalho serão apresentados os conceitos, vantagens, desvantagens e aplicações de cinco tipos de biometria: face, impressoes digitais, íris, marcha e retina, assim como será iniciado um debate sobre a aplicaçao da biometria no combate a fraude e a relaçao entre biometria e privacidade.

2. Metodologia

Este trabalho consistiu em uma revisão da literatura, de estudos que abordam o tema Biometria, de modo a ser possível a caracterização dos métodos biométricos selecionados, a saber: face, impressões digitais, íris, marcha e retina. Para tanto foram selecionados os artigos acadêmicos, livros de referência da área e alguns textos jornalísticos para exemplos reais. Os artigos acadêmico utilizados, assim como os livros foram buscados por meio da ferramenta *google scholar* utilizando as palavras chave: Biometrics, Biometrics review, Biometric aplications, fingerprint, iris recognition, gait recognition, retina recognition, face recognition. Dos resultados da busca, os que foram selecionados estavam no grupo dos mais recentes, com maior número de citações ou de revistas de maior impacto. Cabe destacar que não se busca aqui uma revisao extensiva da literatura e sim a apresentacao dos conceitos e aplicações.

3. Biometria: Características e aplicações

3.1 face

Nos últimos anos, o método biométrico de reconhecimento facial, tem ganhado atenção significativa, haja vista os bons resultados obtidos, seja em análises de imagens estáticas ou em vídeos, bidimensionais (2D) ou tridimensionais (3D) e utilizam-se de métodos estatísticos de análise de componentes principais (PCA), redes neurais artificiais, entre

outros para o reconhecimento das caraterísticas locais como olhos, nariz e boca, por meio de métodos de correspondência de gráficos e de métodos híbridos (combinando os dois últimos) para caracterizar um indivíduo, conforme a Figura 1 . Os bons resultados preliminares, conforme citado, não isentam o método de problemas (BOLLE et al., 2013).

O método 3D para o reconhecimento facial permite a exploração de recursos baseados no formato e na curvatura da face (o formato da testa, a linha da mandíbula, e bochechas) e não sofre influências da variações de iluminação, orientação e fundo que afetam os sistemas 2D (ZHANG; GAO, 2009).

Os algoritmos de reconhecimento facial podem ter duas aplicações distintas: verificação e identificação. A verificação consiste na comparação direta da imagem de uma pessoa desconhecida e uma imagem de referência de uma pessoa conhecida. Este é o processo utilizado para desbloquear o celular, computadores etc. O sistema compara as imagens e calcula o grau de semelhança entre elas. Se essa pontuação estiver acima de limite predeterminado, o sistema conclui que ambas as fotografias representam a mesma pessoa e libera o acesso e, se abaixo desse limite, recusa o acesso. A identificação consiste em uma comparação da imagem de uma pessoa desconhecida com todas as imagens de um banco de dados de indivíduos conhecidos. Nesse caso, o sistema classifica o banco de dados para encontrar os candidatos mais próximos. A identificação é muito utilizada para casos forenses (JACQUET; CHAMPOD, 2020).

O sistema de monitoramento biométrico por reconhecimento facial utilizado durante a *Champion 's League*, em 2017, apresentou 92% de falsos positivos, ou seja, das 2.470 pessoas identificadas como criminosas, apenas 173 foram confirmadas segundo dados divulgados pela polícia de Gales do Sul (SUMARES, 2018). Ainda assim, essa metodologia vem sendo acoplada a ferramentas tecnológicas para promover a segurança de um simples usuário de um dispositivo eletrônico, como um celular, e também a uma população de uma grande cidade. Diversos modelos de celulares já possuem sistemas de reconhecimento facial que permitem o acesso do usuário aos aplicativos do aparelho (MITRA; GOFMAN, 2016).

Também são encontrados drones capazes de identificar um indivíduo por meio do reconhecimento da face. Essa tecnologia vem sendo em-

pregada para promover a segurança de eventos envolvendo autoridades, incursões policiais e, ainda, para encontrar pessoas desaparecidas e criminosos no meio de uma multidão (KREUTZER; SIRRENBERG, 2020).

A biometria facial também encontra aplicação no combate à fraude no uso do cartão de acesso a transportes públicos em diversas cidades brasileiras como Brasília, Florianópolis, Porto Alegre, Rio de Janeiro, Fortaleza, Vitória e Caruaru (G1, 2018).

O *facebook* utiliza a biometria facial para prevenir que pessoas não se passem por outras (BUCKLEY; HUNTER, 2011). A polícia chinesa recentemente implantou o uso da biometria de reconhecimento facial para identificar indivíduos com uso de óculos dotados de inteligência artificial (MOZUR, 2018). Na Inglaterra foi adotado, de forma não-oficial pela comunidade, um sistema com o nome de *facewatch*, no qual pessoas comuns alimentem um banco de dados de imagens compartilhando informações com outros usuários do sistema (FACEWATCH, 2020).

A empresa aérea KLM vem fazendo testes para realizar o embarque de passageiros por meio da biometria facial. O Aeroporto de Brasília está utilizando equipamento de reconhecimento facial para voos internacionais. O investimento foi de 7,5 milhões em 32 equipamentos que serão instalados em outros aeroportos do território nacional (G1, 2016). A biometria facial encontra ainda aplicação para realizar pagamentos, pedir empréstimos e até mesmo para liberar o papel higiênico em banheiro público na China (MOZUR, 2018).

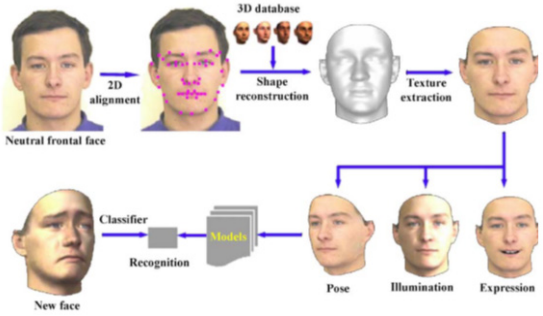

Figura 1 - Representação esquemática do processo de reconstrução 3D. Neste modelo a partir de uma imagem 2D, são projetadas camadas e reconstituídos em diferentes ângulos, de modo a diminuir a influência da posição, iluminação ou da expressão do indivíduo. Retirado de (ZHANG; GAO, 2009).

3.2 IMPRESSÕES DIGITAIS

Um dos principais métodos de identificação de um indivíduo é baseado na análise das impressões digitais, que são os desenhos formados nas poupas digitais pelas papilas dérmicas. Esses desenhos possuem configuração aleatória, ou seja, são únicos para cada indivíduo, de acordo com as condições encontradas no processo de desenvolvimento embrionário e genético. A base dos elementos formadores da convicção no processo de exame das impressões digitais está contida na anatomia e fisiologia da pele (U.S. DEPARTMENT OF JUSTICE, 2011).

A pele humana é constituída de duas camadas: a derme, camada mais profunda e a epiderme, uma camada superficial que recobre a derme. Na derme encontram-se elevações chamadas de papilas dérmicas, também conhecidas como linhas ou cristas, separadas por sulcos ou vales. As variações das cristas são uma característica que permite a identificação de um indivíduo e podem ser cristas interrompidas, bifurcadas, entre outras, conhecidas como minúcias ou pontos característicos. Além das minúcias, uma digital também é identificada pelo núcleo e pelo delta (GIROD; RAMOTOWSKI; WEYERMANN, 2012).

A impressão digital é composta por uma mistura de secreções (suor e gordura) com substâncias advindas do meio externo. A gordura encontrada com frequência nas impressões digitais é oriunda das glândulas sebáceas, espalhadas ao longo do corpo, com exceção das palmas das mãos e dos pés. O suor é expelido pelas glândulas apócrinas e écrinas e realiza importante função de refrigeração do corpo. As glândulas écrinas são as únicas encontradas no tecido tegumentar das impressões digitais. Água, substâncias inorgânicas e orgânicas estão contidas em concentrações variadas no suor (SOUZA et al., 2018).

A partir de 1960, houve uma quebra de paradigma, o estabelecimento da relação de uma identidade a um desenho digital, que até então era unicamente realizado por humano, passou a ser compartilhado com os computadores.

Em 1963, o FBI iniciou sua pesquisa para a completa automação de seu repositório criminal de impressões digitais, que passou por três diferentes fases durante o desenvolvimento do programa. A primeira fase tentou emular o sistema de classificação de Henry para a definições de padrões. No entanto, a metodologia era demorada e a classificação das impressões digitais foi substituída para a classificação do NCIC (JR.; ROBINSON; SLOWIKOWSKI, 2012).

No início dos anos 80, houve a terceira e última fase do processo de automatização que resultou no sistema chamado AFIS (*Automated Fingerprint Identification System*), que é baseado na aplicação de um algoritmo de correspondência, no qual o conjunto de minúcias de uma impressão digital questionada é comparado com minúcias de impressões digitais cadastradas no banco de dados do sistema conforme demonstrado na Figura 2 (JAIN; ROSS; PRABHAKAR, 2004).

O AFIS vem se aprimorando até os dias de hoje, acompanhando o desenvolvimento de hardwares e softwares para esse seguimento empregado pelas forças de segurança.

Além de sua utilização criminal, capaz de colocar um suspeito dentro da cena de um crime, também encontra utilidade civil na corroboração de informações ou de declarações e também na identificação de vítimas de desastres (HAWTHORNE, 2009).

A Polícia Federal do Brasil atualmente busca a modernização de seu sistema AFIS para um sistema automatizado de identificação biométrica (Automated Biometric Identification Systems - ABIS). A diferença entre estes sistemas é a ampliação do rol de biometrias utilizadas para a individualização de alguém. Assim, além de contar com as impressões digitais para identificar um suspeito, poderá contar ainda com o reconhecimento por meio de face, impressões palmares e íris (PF, 2019) .

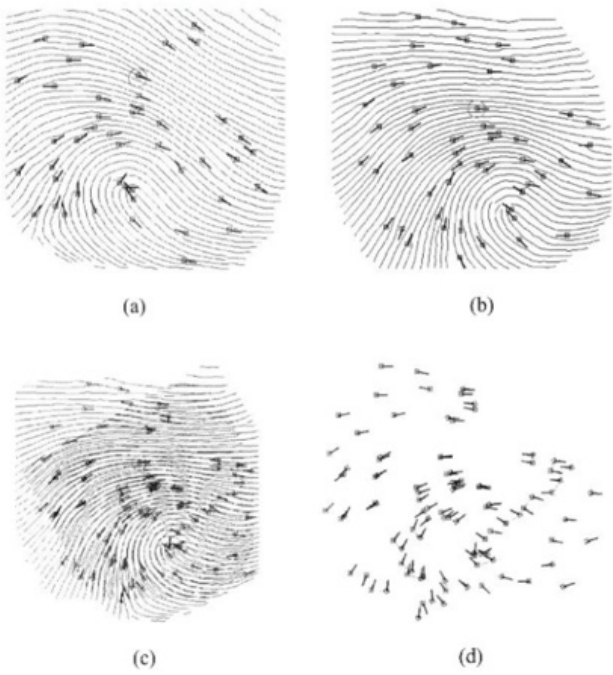

Figura 2 -. Representação da correspondência entre impressões digitais: a) conjunto de minúcias de uma impressão digital questionada; b) conjunto de minúcias de uma impressão digital do banco de dados do sistema; c) alinhamento das minúcias das impressões questionada e do banco de dados do sistema; d) checagem das correspondências somente com as minúcias alinhadas. Retirado de (BOLLE et al., 2013)

Dentre a gama de aplicações encontradas atualmente para essa biometria, destaca-se o investimento em torno de R$ 127.000.000,00 feito pelo Tribunal Superior Eleitoral para individualização do eleitorado brasileiro no momento da votação por meio das impressões digitais. Em 2018, ano da realização da última eleição no Brasil, havia 87.363.098 eleitores aptos a votar utilizando-se de sua biometria (59,31% do total de eleitores) (TSE, 2019). As autoridades brasileiras estudam o aproveitamento deste banco para auxiliar outras instâncias do poder público brasileiro no combate a fraudes.

Os leitores óticos coletores de impressões digitais podem ser utilizados também para controle de acesso de pessoas a determinados ambientes, garantir a segurança de transações bancárias, habilitar o uso de aparelhos celulares e até mesmo ligar um veículo (JAIN, A J; NANDAKUMAR; ROSS, 2016)

3.3 ÍRIS

A íris é um músculo do olho, responsável pela sua coloração. Suas características individualizadoras se mantém ao longo de toda a vida e são diferentes para cada indivíduo, ainda que quando bebê, a cor possa sofrer alguma variação. A proposta de se individualizar alguém por meio da íris foi idealizada pela primeira vez pelo oftalmologista Burch, em 1936. Somente em 1989, foram desenvolvidos algoritmos capazes de realizar tal feito, graças ao matemático Daugman. Esses algoritmos desenvolvidos por ele são usados até hoje como base de funcionamento dos scanners de íris, nos quais câmeras de vídeos sensíveis ao infravermelho, na faixa entre 700-900 nm, digitalizam a imagem do olho humano, que por sua vez são codificadas e armazenadas em um banco de dados para fins comparativos (LI; JAIN, 2015).

É possível o reconhecimento pela íris ainda que com uso de óculos ou lentes de contato. De todas as tecnologias de identificação biométricas, esta é a que o maior número de pessoas pode usar, pois tem como vantagem seu equilíbrio, ou robustez do modelo, uma vez que a íris é protegida contra danos e desgaste pela córnea (KALYANI, 2017).

Um dos maiores desafios dessa metodologia foi encontrar uma forma de diferenciar os olhos esquerdos e direitos. Algoritmos de comparação foram desenvolvidos para esta finalidade e realizados testes de comparação com o banco de dados NIST Iris Challenge Evaluation (ICE) 2005, sendo os observados na Tabela 1 demonstrando que ao analisar dados de segmentação usando algoritmo de classificação esquerda/direita as taxas de erro acerca da identificação são abaixo de 1% (LI; JAIN, 2015).

A biometria da íris também é imune, haja vista as tecnologias atuais, a subterfúgios capazes, em tese, de gerar falsos resultados, como por exemplo olhos de vidro, lentes de contato etc. Isso porque a íris responde a estímulos luminosos de forma muito característica e ainda possui suas ramificações arteriais capazes de absorver determinados comprimentos de onda no infravermelho próximo. Esse tipo de biometria vem sendo utilizado para controle de acesso a ambientes restritos, regiões de fronteiras, portos, aeroportos e até mesmo para ligar um veículo. (LI; JAIN, 2015).

Categoria	Imagens	Classificações incorretas	Indeciso	Percentual de identificação correta
Todas as imagens	2953	27	172	99.1%
Esquerdo	1528	15	78	99%
Direito	1425	12	94	99.02%

Tabela 1 Resultados experimentais para distinguir olhos esquerdos de direitos usando o banco de dados ICE 2005. Adaptado de (LI; JAIN, 2015)

3.4 MARCHA

Apresentada como uma técnica biométrica comportamental que permite reconhecer um indivíduo por meio de sua forma de caminhar. Uma das grandes vantagens desta metodologia é a possibilidade de reconhecer alguém a distância (10 metros ou mais), além de ser um método não intrusivo e não invasivo (LEE; BELKHATIR; SANEI, 2014).

Os bancos de dados de análise de marcha incluem o estudo do movimento humano, a cinesiologia. O movimento humano traz informações de origens diferentes, do esqueleto, que é resultado do movimento global de articulações do corpo humano e como se comportam durante a caminhada e da silhueta, que carrega informações do comportamento global do contorno do corpo humano. As fases da marcha humana obedecem a um padrão de comportamento e cada indivíduo produz um padrão diferente. O uso da marcha para reconhecimento pode ser feito por métodos baseados na silhueta ou no modelo (dinâmica). No primeiro, a forma da silhueta e seus atributos são a base do modelo, já no segundo, as medidas são baseadas no movimento do tronco e das pernas, concentrando- se na dinâmica do movimento e podem ser baseados no espaço ou espaço tempo (LV et al., 2015).

Sua base de funcionamento é a extração por meio de algoritmos das silhuetas de um indivíduo, conforme mostrado na Figura 3. Como fator limitante do método, pode ser apontada a dificuldade do reconhecimento a partir da caminhada sob uma superfície na qual o sistema não tenha sido treinado, ou seja, testes exitosos com a extração da silhueta em superfícies de concreto podem gerar resultados insatisfatórios usando a mesma silhueta na areia. Outros desafios a serem

superados por este método têm sido a variabilidade da forma de caminhar ao longo do tempo, devido a fatores como a alteração da massa corporal; doenças cerebrais que atingem a capacidade motora; conforme já apontado as alterações na forma de caminhar em diferentes superfícies como grama, areia, concreto; se carrega algum objeto enquanto caminha etc. (BOLLE et al., 2013).

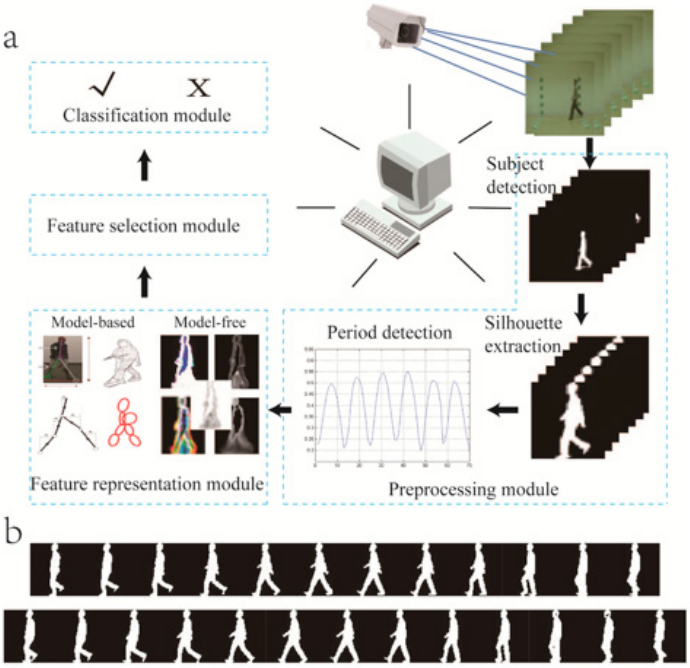

Figura 3 Estrutura geral de um sistema de reconhecimento de marcha baseado em sensor de vídeo. O sensor baseado na câmera captura informações da marcha e envia os dados para os computadores. O sistema inclui quatro módulos pré-processamento (isto é, detecção de assunto e extração de silhueta do vídeo original), de representação de recursos, de seleção de recursos e de classificação. Observe que o reconhecimento da marcha com base no modelo pode não precisar do módulo de pré-processamento; (b) As imagens de silhueta são os resultados da detecção do período correspondente ao módulo de pré-processamento na Figura 2ª. Retirado de (LV et al., 2015).

Em 2019, a polícia de províncias de Beijing, Shanghai e Chongqing na China, passou a identificar pessoas pela forma de caminhar com um índice de acerto de até 94%. Durante o registro da caminhada, o sistema observa pontos característicos da passada, dentre eles, o tamanho do passo, a velocidade e a postura. É possível a identificação a 50 metros de distância (WATRIZ, 2020).

Em artigo de revisão sobre reconhecimento humano por marcha, os autores relatam a acurácia de diferentes métodos baseados em marcha variando entre 86 e 99,6 %, as aplicações estudadas vão desde a utilização desta biometria para o sensor Kinect do console de jogos Xbox, roteadores WI-FI, até sensores para aeroportos, entre outros (PAVITHRA; MATH, 2019).

3.5 RETINA

Essa classe automatizada da biometria é conhecida com a mais segura forma de se identificar alguém e sua metodologia se baseia na observação do padrão vascular da retina, Figura 4. A possibilidade de identificação por meio da retina foi estudada, pela primeira vez, pelos oftalmologistas Carleton Simon e Isodoere Goldstein, ao estudarem doenças oculares. Eles publicaram um artigo apresentando fotografias de padrões de retina capazes de identificar os voluntários pela disposição dos vasos sanguíneos (LI; JAIN, 2015). Até mesmo entre gêmeos idênticos o método se mostrou eficiente, uma vez que a retina desses indivíduos apresentam padrões com pouquíssimas semelhanças, devido à rede de vasos sanguíneos (KALYANI, 2017).

Embora os estilos de retina possam ser alterados em casos de diabetes, glaucoma ou distúrbios degenerativos da retina, a retina normalmente permanece inalterada desde o nascimento até a morte. Devido à sua natureza única e imutável, a retina parece ser a biometria máxima precisa e confiável, com baixa prevalência de falsos positivos (BOLLE et al., 2013).

A retina está localizada na parte de trás do globo ocular e possui um conjunto de vasos sanguíneos denominado de vasculatura coroidal. Seus padrões possuem uma estabilidade que nenhum outro padrão biométrico possui. Isso porque o olho está localizado em um lugar bastante seguro e, devido a isso, a coroide apresenta pouca variação por exposição ao ambiente externo (LI; JAIN, 2015).

As imagens da retina são realizadas por meio de luz infravermelha. O primeiro dispositivo capaz de individualizar alguém por meio da retina foi apresentado em 1975, porém sem muita utilidade.

Em 1981, foi construído o primeiro protótipo funcional de um identificador de retina. Desde então, muitas empresas interessadas nessa tecnologia desenvolveram equipamentos com sua utilização focada em ambientes de alta segurança como locais de pesquisas nucleares, de instalações de armas e de controle de comunicação e para validar transações de altos valores (LI; JAIN, 2015)

Como setores com potencial de aplicação direta da tecnologia de reconhecimento por meio da retina, destaca-se o bancário, órgãos públicos ou empresas que demandam alto nível de segurança.

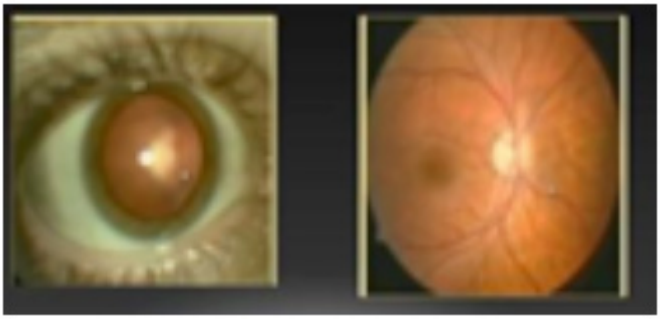

Figura 4 Figura 4. Imagem do padrão de veia da retina humana. Retirado de (KALYANI, 2017)

4. Algumas considerações

4.1 a biometria no combate à fraude

Além dos exemplos aqui citados, a tecnologia de individualização de alguém por meio da biometria vem se desenvolvendo de forma muito dinâmica. Cada vez mais entidades governamentais, privadas e financeiras buscam formas de identificar seus clientes proporcionando maior segurança em suas relações. O reconhecimento por meio da biometria se disseminou de tal forma, que hoje, abrange desde sofisticados equipamentos de monitoramento no controle de imigração e fronteiras, até os utilizados em um celular para liberar o acesso de uma criança ao aparelho.

Acerca da perspectiva de desenvolvimento nesta área, estima-se que o investimento no mercado de pesquisa em tecnologia biométrica chegará a US$ 45,96 bilhões em 2024, com uma taxa de crescimento de 19,6% ao ano, segundo Frost & Sullivan e alcançará US$ 55.5 bilhões, de acordo com o Biometrics Resarch Group (PASCU, 2020).

Para o setor bancário, a segurança em suas operações é ponto crucial no estabelecimento da confiança entre clientes e instituições. Assim, segundo relatório publicado pela *Biometrics Research Group Inc*. há uma previsão de redução de 20% no risco sobre as operações neste setor até o final desta década com os investimentos a serem realizados neste ramo. Ainda segundo a *Biometrics Research Group Inc*, o desenvolvimento desta tecnologia ficará concentrada nos países desenvolvidos sendo os países em desenvolvimento a principal fonte de receita das empresas deste segmento (MITRA; GOFMAN, 2016)

Num mundo cada vez mais globalizado, a biometria como instrumento garantidor da segurança da tramitação de dados se faz cada vez mais necessária. Nos EUA, de acordo com o Departamento de Justiça americano, em 2012, cerca de 7% da população com 16 anos ou mais foram vítimas de ladrões de identidade. Naquele ano, essas vítimas, juntas, arcaram com um prejuízo direto e indireto de US$ 24,7 bilhões. Esse valor é maior do que o volume de perdas estimado para todos os outros tipos de crimes de propriedade (roubo e furto e roubo de veículos) – US$ 24 bilhões (MITRA; GOFMAN, 2016).

Dentro de uma contextualização de risco, seguem o setor bancário o setor governamental e o de saúde. Assim, países em desenvolvimento já utilizam tecnologias biométricas para verificar os destinatários dos pagamentos do governo. Como exemplo, o governo das Filipinas autentica os recebimentos dos subsídios em dinheiro para as famílias de baixa renda por meio da tecnologia biométrica. No Paquistão, são emitidos cartões biométricos pelo governo aos pensionistas, que podem utilizar-se desta ferramenta para retirar pensões dos bancos e dos correios (MITRA; GOFMAN, 2016) (KING, 2012). O governo indiano de Aadhaar fornece cartões de identidade aos cidadãos, bem como contas bancárias para todas as famílias indianas utilizando de tecnologia biométrica (TOTAPALLY et al., 2019).

No Brasil, recentemente, foram apontadas irregularidades em 5,7 milhões de recebimentos de benefícios para pessoas com baixa renda, gerando uma economia de cerca de R$ 10 bilhões (WIZIACK; PRADO, 2018). No futuro, o aprimoramento da segurança do recebimento desses benefícios por meio da tecnologia de reconhecimento pela biometria pode auxiliar essa logística de controle da distribuição pelo governo brasileiro.

Outro exemplo disso é a fraude em assistência médica. Em 2008, entre 3% e 10% do total gasto em assistência médica nos Estados Unidos (US$ 2,4 trilhões) foi perdido por fraudes (MITRA; GOFMAN, 2016). Boa parte dessas deficiências podem ser superadas com o emprego da biometria (KING, 2012).

Neste contexto, os dados de trabalhadores também apresentam vulnerabilidade, uma vez que as empresas são possuem uma grande quantidade de informação, sendo um incentivo aos que pretendem ter acesso a dados alheios. Em 2014, mais de 1.500 grandes violações de dados foram realizadas, resultando em mais de 1 bilhão de registros comprometidos globalmente. A Sony Pictures Entertainment e a provedora de seguros de saúde Anthem Inc. sofreram graves violações de dados, recentemente, comprometendo amplamente os dados de identidade de seus funcionários. Há ainda aquelas empresas que estimulam o furto de informações em detrimento da competitividade de mercado. Jornalistas do "News of the World", de Rupert Murdoch, foram encorajados a invadir ilegalmente contas de telefones celulares para obter informações particulares e informações sensacionalistas, o que fez o tabloide interromper sua publicação por indignação pública, após o episódio (CARPENTER et al., 2018). Assim, as ferramentas biométricas prometem um caminho em direção à maior segurança da informação.

4.2 A BIOMETRIA E A PRIVACIDADE

Outro ponto que merece destaque é a necessidade de um amplo debate para redefinir o conceito de privacidade que conhecemos hoje. As leis brasileiras de proteção de dados fornecem o modelo adequado para regular esta tecnologia? Para tanto devem ter uma abordagem orientada, flexível e tecnologicamente neutra de modo

a permitir o desenvolvimento de novas aplicações, mas reduzindo os usos excessivos e intrusivos.

O tipo, a forma de obtenção e o propósito de uso são fatores que influenciam o julgamento acerca da privacidade de uma informação.

Há uma controvérsia entre o motivo da implementação de sistemas biométricos em utilitários para a proteção da identidade de seus usuários e a segurança dos dados biométricos armazenados, uma vez que ameaças à segurança das informações tornam esses sistemas vulneráveis. Assim, a depender dessa vulnerabilidade, podem ocorrer intercorrências indesejáveis na rotina do indivíduo, como impossibilidade de solicitar serviços, furto de informações, privacidade exposta etc (JAIN, A J; NANDAKUMAR; ROSS, 2016).

Apesar de estudos buscarem de forma exaustiva medidas corretivas para essa falha na segurança de sistemas biométricos, a desconfiança sobre essa novidade acolhida, inclusive, pelas redes sociais, ainda é grande. Após a implementação de sistemas biométricos de reconhecimento facial no facebook, por exemplo, foi constatada uma diminuição da utilização desta rede social (BUCKLEY; HUNTER, 2011).

Corrobora com esse contexto a legislação brasileira, que não define com uniformidade e clareza os conceitos de dados restritos, sigilosos e protegidos. Observa-se também uma dificuldade na identificação do que está abrangido no direito à privacidade e à publicidade da informação (GONÇALVES; VARELLA, 2018). Esse cenário de ausência de uniformidade conta ainda com uma quarta nomenclatura: "dados sensíveis". O conceito de dados sensíveis abarca, dentre outros tipos de informações, os dados biométricos, segundo Lei 13.709/2018, mas que, apesar da data de sanção, passa a vigorar somente em 2020. Essa lei regula os dados pessoais e sensíveis (BRASIL, 2018).

Outra discussão que merece destaque é o limite de vigilância do estado por sistemas biométricos, uma vez que é crescente a implementação de sistemas de monitoramento em ambientes públicos (drones, câmeras de vigilância etc.) (MITRA; GOFMAN, 2016).

Assim, o uso da tecnologia moderna que se utiliza de informações biométricas com o propósito de oferecer maior segurança a seus usuários merece cautela, uma vez que, geralmente, esse tipo de tecnologia evolui mais rápido do que o legislativo pode responder e que o nível de segurança desses sistemas precisam sempre estar um passo à frente de fraudadores.

5. Considerações Finais

Assim, a biometria, de modo geral, refere-se à identificação automática de uma pessoa com base em suas características fisiológicas ou comportamentais e se propõe a fornecer maior segurança da informação, com contribuições também no campo da segurança pública. Com a popularização de sensores biométricos, que tem se tornado menores e mais baratos e com percepção do público de que a biometria é uma estratégia eficaz para proteção dos seus dados, é provável que se observe um aumento dos investimentos desse tipo de tecnologia por parte das empresas e, consequentemente, a preferência do usuário em utilizar-se da biometria como ferramenta de segurança.

Com a expansão dos investimentos nesse tipo de tecnologia, espera-se o desenvolvimento e a utilização de novos métodos, como por exemplo, métodos baseados em DNA, unhas, dentes, formatos de orelhas, características da pele e pulsação sanguínea. Além disso, há uma perspectiva de maior precisão dos sistemas de uso domésticos como acesso a celulares, computadores, residências etc.

O futuro da biometria também está relacionado à discussão sobre a privacidade dos dados, uma vez que diferentes empresas e órgãos governamentais vêm adotando esse tipo de tecnologia como forma de proteção de indivíduos e dados.

Nas escolas, a tecnologia biométrica pode ser capaz de promover uma melhor integração entre a criança e as áreas acessíveis do estabelecimento escolar que venha a exigir alguma identificação.

Cartões podem ser perdidos, PINs esquecidos, mas os dados biométricos podem sempre proporcionar uma identidade, quando for

exigida. Desta forma, os alunos poderão usufruir de maior segurança dentro da escola, comprar um lanche com maior facilidade, acessar o conteúdo das aulas, ingressar no ônibus que os conduzirá no trajeto para casa ou para a escola de forma mais segura etc (MITRA; GOFMAN, 2016)

Na segurança, destaca-se o projeto chinês em andamento que vem dando resultados e que prevê a identificação de 1,4 bilhão de pessoas utilizando reconhecimento facial e inteligência artificial. É especulado um número de 200 milhões de câmeras de vigilância espalhadas pelo território chinês (MOZUR, 2019).

Em Zhengzhou, um contrabandista de drogas foi identificado numa estação de trem por um policial que usava um óculos capaz de realizar o reconhecimento facial. Na cidade de Quingdao, câmeras controladas por meio de inteligência policial auxiliaram a polícia local a capturar 24 criminosos durante um festival de cervejas (MOZUR, 2019).

Marco Antônio de Souza

Papiloscopista Policial Federal. Instituto Nacional de Identificação - Polícia Federal

Biometrics and its Applications

ABSTRACT

By observing biometric patterns, it is possible to individualize a person. For a long time, fingerprints were the most used biometrics for this purpose. Today, with technological development, several other forms of biometrics can also be used to perform person identification, with emphasis on the gait recognition, facial recognition, iris recognition, retina recognition, among others. The importance of individualizing people today is essential. In 2012, the US Department of Justice estimated that, nearly 7% of the population aged 16 and over were victims of identity thieves, causing a damage of ca. US $ 24.7 billion. This amount is bigger than the estimated volume loss for all other types of

property crimes (robbery and theft and vehicle theft) - US $ 24 billion. In this article, will be presented the concepts and applications of biometric tools (gait, face, fingermarks, iris, retina). Also, will begin a discussion about the application of biometrics against fraud crimes and the relationship between biometrics and privacy.

Keywords: Biometry. Identification. Biometric identification. Gait. Face. Fingermarks. Iris. Retina.

Biometría y sus Aplicaciones

RESUMEN

Al observar patrones biométricos, es posible individualizar a una persona. Durante mucho tiempo, las huellas digitales fueron los datos biométricos más utilizados para este propósito. Hoy, con el desarrollo tecnológico, se pueden usar otras formas de biometría para identificar a alguien, con énfasis en la forma de caminar, reconocimiento facial, iris, retina, entre otros. La importancia de individualizar a las personas hoy es esencial. En 2012, el Departamento de Justicia de los Estados Unidos estimó que aproximadamente el 7% de la población de 16 años o más eran víctimas de ladrones de identidad, lo que generó una pérdida de aproximadamente $ 24.7 mil millones. Esa cifra es mayor que el volumen de pérdida estimado para todos los demás tipos de delitos contra la propiedad (robô, hurto y robo de vehículos): $ 24 mil millones. En este artículo, se presentarán conceptos y aplicaciones para identificar individuos a través de la biometría (marcha, rostro, huellas dactilares, iris y retina), así como comenzará um debate sobre la aplicación de la biometría para combatir la fraude y la relación entre la biometría y la privacidad.

Palabras-clave: Biometría. Identificación. Identificación biométrica. Marzo. Cara. Papilas Iris. Retina

Referências

BLACKBURN, D.; MILES, C.; WING, B.; SHEPARD, K. Biometrics History, 2006. Available at: https://www.hsdl.org/?view&did=463907.

BOLLE, R. M.; CONNELL, J. H.; PANKANTI, S.; RATHA, N. K.; SENIOR, A. W. Guide to Biometrics. 1st ed. New York, NY: Springer New York.

BRASIL. Lei no 13.709 de 14 de agosto de 2018. 2018. Available at:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BUCKLEY, B.; HUNTER, M. Say cheese! Privacy and facial recognition. Computer Law and Security Review, vol. 27, no. 6, p. 637–640, 2011.

CARPENTER, D.; MCLEOD, A.; HICKS, C.; MAASBERG, M. Privacy and biometrics: An empirical examination of employee concerns. Information Systems Frontiers, vol. 20, no. 1, p. 91–110, 2018.

FACEWATCH. The UK's leading facial recognition security system. 2020. Available at: https://www.facewatch.co.uk/. Accessed on: 19 Apr. 2020.

FISHER, B. A. J.; HILTON, O.; LEE, H. C.; GAENSSLEN, R. E.; TERRY MILLS, I.; ROBERSON, J. C.; MCCURDY, H. H.; WALL, W. H.; LOTHRIDGE, K. L.; MCDOUGALL, W. D.; GILBERT, M. W. Advances in Fingerprint Technology. Segunda ed., Boca Raton, FL: CRC Press, 2001.

G1. Aeroporto de Brasília passa a adotar reconhecimento facial de viajantes. 2016. Available at: http://g1.globo.com/distrito-federal/noticia/2016/08/aeroporto-de-brasilia-passa-adotar-reconhecimento-facial-de-viajantes.html. Accessed on: 19 Apr. 2020.

G1. Biometria facial flagra mais de 33 mil ocorrências de uso irregular de benefício no transporte de Porto Alegre. 2018. Available at: https://g1.globo.com/rs/rio-grande-do-sul/noticia/biometria-facial-flagra-mais-de-33-mil-ocorrencias-de-uso-irregular-de-beneficio-no-transporte-de-porto-alegre.ghtml. Accessed on: 19 Apr. 2020.

GIROD, A.; RAMOTOWSKI, R.; WEYERMANN, C. Composition of fingermark residue: A qualitative and quantitative review. Forensic Science International, vol. 223, no. 1–3, p. 10–24, 2012.

GONÇALVES, T. C. N. M.; VARELLA, M. D. Os desafios da Administração Pública na disponibilização de dados sensíveis. Revista Direito GV, vol. 14, no. 2, p. 513–536, 2018.

HAWTHORNE, M. R. Fingerprints Analysis and Understanding. Boca Raton, FL:, 2009.

JACQUET, M.; CHAMPOD, C. Automated face recognition in forensic science: Review and perspectives. Forensic Science International, vol. 307, 2020.

JAIN, A. J.; NANDAKUMAR, K.; ROSS, A. 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, vol. 79, p. 80–105, 2016.

JAIN, A. K.; ROSS, A.; PRABHAKAR, S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, p. 4–20, Jan. 2004.

JR., H. H.; ROBINSON, L. O.; SLOWIKOWSKI, J. The fingerprint sourcebook. US Department of Justice Office of Justice Programs, 2012.

KALYANI, C. Various Biometric Authentication Techniques: A Review. Journal of Biometrics & Biostatistics, vol. 08, no. 05, 2017..

KING, R. Emerging economies embracing biometric banking technologies. 2012. Available at: https://www.biometricupdate.com/201212/emerging-economies-embracing-biometric-banking-technologies.

KREUTZER, R.; SIRRENBERG, M. Fields of Application of Artificial Intelligence—Security Sector and Military Sector. Understanding Artificial Intelligence. Springer,. p. 225–233, 2020.

LEE, T. K. M.; BELKHATIR, M.; SANEI, S. A comprehensive review of past and present vision-based techniques for gait recognition. Multimedia Tools and Applications, vol. 72, no. 3, p. 2833–2869, 2014.

LI, S. S.; JAIN, A. K. (Eds.). Encyclopedia of Biometrics. 2nd ed. Springer US, 2015.

LV, Z.; XING, X.; WANG, K.; GUAN, D. Class energy image analysis for video sensor-based gait recognition: A review.

Sensors (Switzerland), vol. 15, no. 1, p. 932–964, 2015.

MAGUIRE, M. The birth of biometric security. Anthropology Today, vol. 25, no. 2, p. 9–14, 2009.

MITRA, S.; GOFMAN, M. (Eds.). Biometrics in a data driven world. CRC Press, 2016.

MOZUR, P. Looking Through the Eyes of China's Surveillance State. 2018. Available at: https://www.nytimes.com/2018/07/16/technology/china-surveillance-state.html. Accessed on: 19 Apr. 2020.

MOZUR, P. One month, 500,000 face scans: how chine is using A.I. to profile minority. 2019. Available at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html. Accessed on: 19 Apr. 2020.

PASCU, L. Global biometrics market to surpass $45B by 2024, reports Frost & Sullivan. 2020. Available at: biometricupdate.com/202003/global-biometrics-market-to-surpass-45b-by-2024-reports-frost-sullivan.

PAVITHRA, D. S.; MATH, S. A Review on Human Gait Detection. Global Journal of Computer Science and Technology Articles, vol. 19, no. 1, 2019. .

PF. Licitação ABIS. 2019. Available at: http://www.pf.gov.br/servicos-pf/licitacoes/2019/distrito-federal/orgaos-centrais/dti/audiencias-publicas/equipamentos-abis.

SOUZA, M. A.; DE OLIVEIRA, K. V.; OLIVEIRA, F. C. C.; SILVA, L. P.; RUBIM, J. C. The adsorption of methamphetamine on Ag nanoparticles dispersed in agarose gel – Detection of methamphetamine in fingerprints by SERS. Vibrational Spectroscopy, vol. 98, no. August, p. 152–157, 2018.

SUMARES, G. Reconhecimento facial policial da Champion's League errou 92% das vezes. 2018. Available at: https://olhardigital.com.br/fique_seguro/noticia/reconhecimento-facial-policial-confundiu-2300-pessoas-com-potenciais-criminosos/75918. Accessed on: 19 Apr. 2020.

TOTAPALLY; SONDEREGGER; RAO; GOSSELT; GUPTA. State of Aadhaar 2019. 2019. Available at: https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf?utm_source=download_report&utm_medium=button_dr_2019.

TSE. Estatísticas eleitorais 2018. 2019. Available at: http://www.tse.jus.br/eleicoes/estatisticas/estatisticas-eleitorais. Accessed on: 19 Apr. 2020.

U.S. DEPARTMENT OF JUSTICE. The Fingerprint - Sourcebook. Washington, D.C.: National Institute of Justice, 2011.

WATRIZ. Gait recognition. 2020. Available at: http://www.watrix.ai/en/gait-recognition/. Accessed on: 19 Apr. 2020.

WIZIACK, J.; PRADO, M. Pente-fino corta R$ 10 bi em gastos irregulares com Bolsa Família, aposentadoria e auxílio-doença. 2018. Available at: https://www1.folha.uol.com.br/mercado/2018/07/pente-fino-corta-r-10-bi-em-gasto-irregular-com-57-mi-de-beneficiarios.shtml.

ZHANG, X.; GAO, Y. Face recognition across pose: A review. Pattern Recognition, vol. 42, no. 11, p. 2876–2896, 2009.