A SEGURANÇA ATRAVÉS DA BIOMETRIA

Clevertom Silva, Daiana de Miranda, Fabiana de Oliveira, Julio Cesar Ferreira, Leandro Falbo, Pedro Sérgio Silveira, Prof:Ernani
Associação Educacional Dom Bosco - AEDB

RESUMO

Há tempos que se faz necessário, por exemplo, o uso de mecanismos para restringir o acesso a determinados lugares ou serviços. Como nada é 100% eficiente, a busca pela solução perfeita é contínua. Este artigo trata de uma das idéias mais promissoras que surgiu, o uso da biometria. O objetivo desse estudo foi fazer uma revisão dos principais aspectos da biometria e sistemas biométricos existentes.

A premissa em que se fundamenta é a de que cada indivíduo é único e possui características físicas e de comportamento (a voz, a maneira de andar, etc.) distintas.

Palavras-chave: Biometria. Sistemas biométricos. Segurança. Tecnologia da Informação.

1 INTRODUÇÃO

Ao contrário do que se pensa, a biometria não é um conceito novo. Inédito é apenas sua aplicação em sistemas computacionais. Sabe-se por exemplo, que os faraós do Egito usavam características físicas de pessoas para distingui-las. No entanto, somente no século XIX a biometria ganhou atenção científica.

Atualmente o termo biometria esta na moda, principalmente relacionado à Tecnologia da Informação. Todo o mundo só fala nisso, porque do ponto de vista da segurança, biometria significa a verificação de identidade de uma pessoa através de uma característica inerente à mesma.

No presente ensaio optamos pela biometria, pois o constante avanço das tecnologias de comunicação faz com que haja cada vez mais interação entre as pessoas e, além disso, deve-se considerar que a biometria também pode representar uma comodidade ao usuário. Prova disso é que as tecnologias envolvidas ganham aprimoramentos constantes.

2. BIOMETRIA: O QUE É E O QUE FAZ?

Biometria [*bio* (vida) + *metria* (medida)] é o estudo estatístico das características físicas ou comportamentais dos seres vivos e pode ser utilizada numa grande variedade de aplicações, pelo que é difícil defini-la de forma exclusiva. No entanto, uma das definições que nos parece mais adequada refere que a biometria é a utilização automatizada de características fisiológicas ou comportamentais para determinar ou verificar entidades.

À medida que aumentam as quebras de segurança e as fraudes, aumenta também o recurso a soluções de elevada segurança. Atualmente podemos encontrar soluções biométricas em vários tipos de organizações, incluindo as de natureza governamental, militar, educacional ou comercial. Aeroportos, hospitais, hotéis, mercearias e até os parques temáticos da Disney usam cada vez mais a biometria para ter maior segurança.

A biometria e os laboratórios criminais tem muito em comum. A biometria usa as características físicas ou comportamentais para determinar ou confirmar uma identidade. O laboratório criminal usa o mesmo tipo de informação para estabelecer fatos em investigações civis ou criminais.

Goste-se ou não, a biometria tem vindo a mudar a forma como muitas atividades são realizadas pelos humanos. A utilização de características únicas de cada indivíduo e a possibilidade de comparação rápida fornecida pelos sistemas de informação atuais apresenta inegáveis vantagens no combate à fraude, ao crime e ao terrorismo, mas também levanta questões relativamente ao velho problema dos atentados à informação individual.

3. O QUE FAZEM AS SOLUÇÕES BIOMÉTRICAS

Em uma linguagem muito simples, as soluções de biometria não fazem mais do que ler ou medir características únicas dos indivíduos e compara-las com as mesmas que já tinham sido recolhidas e armazenadas anteriormente num sistema (normalmente uma base de dados). Quase todos nós já estamos habituados a identificarmo-nos regularmente nas mais diversas situações – apresentando o bilhete de identidade, o passaporte ou outro cartão, ou ainda introduzindo códigos as palavras de passe.

Com as soluções de biometria, o que muda é o rigor da informação utilizada para sermos autenticados e a verificação da mesma. As impressões digitais já são utilizadas atualmente em alguns documentos, mas ninguém costuma verificar, por exemplo, se as impressões digitais do bilhete de identidade correspondem realmente as da pessoa que o apresenta – a não ser que existam desconfianças de falsificação. O elemento identificador, neste caso, costuma ser uma rápida comparação entre a fotografia que consta de documento e a pessoa que o apresenta.

As soluções de biometria aumentam a segurança porque comparam quase imediatamente as características únicas de um indivíduo com as mesmas que estão armazenadas numa base de dados. Além disso, como envolvem características biométricas (intrínsecas ao indivíduo), não existe o risco de perder os elementos identificadores ou de nos esquecermos deles (exceto nos casos de acidentes com conseqüências e/ou comportamentais). Isto que é realizado uma identificação mais completa das pessoas sempre que precisamos de nos autenticar diminuindo assim a substancialmente as possibilidades de fraude.

Além do rigor da identificação, podemos classificar as soluções de biometria em três categorias. Uma primeira categoria inclui as soluções que se baseiam em características comportamentais – coisas que fazemos de forma consistente (verificação da voz ou da escrita manual, por exemplo). Numa segunda categoria incluem-se as soluções que se baseiam em características fisiológicas que se mantém estáveis ao longo da vida de qualquer pessoa, nomeadamente as características faciais, a geometria da mão e a escrita manual. A terceira categoria inclui as soluções que se baseiam em características discretas, por exemplo, a estrutura vascular da retina.

4. EXEMPLOS DE INFORMAÇÃO BIOMÉTRICA

São muitos e variados os exemplos de informação biométrica. A lista que se segue inclui os mais comuns. No entanto, também convém sublinhar que alguns dos exemplos referidos podem envolver várias tecnologias. Por exemplo, no caso do reconhecimento da face, pode ser efetuado de forma óptica ou térmica.

- Impressões digitais
- Reconhecimento da face
- Reconhecimento da voz
- Reconhecimento da íris
- Geometria das mãos
- Verificação de assinatura

Além dos exemplos de informação biométrica referidos anteriormente, existem outros que não têm apresentado tanta viabilidade comercial. Entre eles podemos destacar:

- As análises de DNA

- A forma das orelhas
- O odor ou cheiro de cada indivíduo
- A leitura das veias das costas ou da palma da mão
- A geometria dos dedos
- A Identificação através das unhas
- O reconhecimento da forma de andar

5. COMO FUNCIONA A BIOMETRIA

Sistemas biométricos podem parecer complicados. Quando se utilizam características biométricas são realizadas normalmente três funções básicas:

- Registro: na primeira vez que se usa um sistema biométrico, ele registra informações básicas como o nome ou um número de identificação. Depois, captura uma imagem ou registro de uma característica específica do indivíduo.
- Armazenamento: a maioria dos sistemas não armazena a imagem ou o registro completo. Em vez disso, analisam determinada característica e a traduzem num código ou gráfico. Alguns sistemas também registram esses dados em um smart card.* que o indivíduo carrega com ele.
- Comparação: a próxima vez que o sistema for usado, ele irá comparar a característica apresentada com a informação no arquivo, para então aceitar ou rejeitar a pessoa que esta se identificando.

Os sistemas também usam os mesmos três componentes:

- Um sensor, que detecta a característica que esta sendo usada para a identificação;
- Um computador, que lê e armazena as informações e,
- Um software, que analisa as características e as traduz para um gráfico ou código, fazendo as comparações.

Um sistema biométrico pode tanto autenticar quanto identificar. A autenticação é uma comparação individual: ela compara uma característica com informações armazenadas da pessoa que se identificando. A identificação, por sua vez, é uma comparação com todas as informações arquivadas inclusive de outras pessoas.

Para alguns sistemas de segurança, um método de identificação não é suficiente. Sistemas em camadas combinam um método biométrico com um código ou PIN (número de identificação pessoal). Sistemas multimodais combinam múltiplos métodos biométricos, como um scanner de íris e um sistema de timbre de voz.

5.1 DETERMINANDO A PRECISÃO

Todos os sistemas biométricos usam características humanas que são, de alguma forma, únicas. Determinar qual é o melhor sistema depende do nível de segurança necessário do público que usará o sistema e de sua precisão. A maioria dos fabricantes usa medidas como estas para descrever a precisão:

- Taxa de falsa aceitação: quantos impostores o sistema aceita;
- Taxa de falsa rejeição: quantos usuários autorizados o sistema rejeita;
- Taxa de falha no registro: quantos registros de características são de qualidade insuficiente para serem usados pelo sistema e,
- Taxa de falha na obtenção: quantas vezes um usuário precisa apresentar a característica antes de o sistema aceitar ou rejeita-lo corretamente.

Podemos encontrar atualmente no mercado um grande número de tecnologias biométricas com provas dadas, e cada característica biométrica pode ser utilizada para

confirmar a exatidão da identidade pessoal. No entanto, algumas características biométricas são mais adequadas para determinar aplicações do que outras.

5.2 A LONGEVIDADE DE CARACTERÍSTICAS BIOMÉTRICAS E A UTILIZAÇÃO DE VÁRIOS MÉTODOS DE AUTENTICAÇÃO

De uma forma geral, as características biométricas mais utilizadas atualmente têm um período de vida bastante longo, mas algumas são mais persistentes e estáveis do que outras. Por exemplo, as impressões digitais são normalmente estáveis, mas podem ser danificadas ou obscurecidas por danos na pele ao envelhecimento da pessoa ou a desgastes ocupacionais.

Os padrões de íris são formados muito cedo na nossa vida e permanecem estáveis até a morte, a não ser que sejam obscurecidos por cataratas ou por outras doenças oftalmológicas. A geometria da face e da mão é menos estável e persistente, devido ao envelhecimento dos indivíduos, as variações do seu peso, e a outros fatores. No entanto, estes problemas podem ser ultrapassados através de recapturas periódicas das características biométricas.

Pode-se confirmar diferentes biométricas para se conseguirem níveis de segurança mais elevados em aplicações de alta segurança. No entanto, é mais comum combinar características biométricas com outros mecanismos de autenticação, por exemplo, cartão inteligente, ou número de identificação pessoal (PIN). Este conceito de autenticação múltipla permite uma abordagem por níveis que pode aumentar a privacidade e a segurança.

Um sistema de identidade que utilize cartões e características biométricas pode reforçar significativamente a relação de confiança entre o portador de um cartão e o emissor desse cartão, bem como reduzir o risco e o custo de fraude e roubo de identidade. Neste tipo de sistemas, a característica biométrica é utilizada como chave de segurança que desbloqueia a informação sensível armazenada no cartão inteligente e ativa a utilização do cartão. Desta forma, se o cartão for roubado ou perdido, não terá qualquer utilidade sem a chave biométrica única do sue portador original.

6. TIPOS DE IDENTIFICAÇÃO BIOMÉTRICA

Figura 01. Impressão Digital

As impressões digitais são as características biométrica mais utilizada, uma vez que esta tecnologia é fácil de utilizar, muito exata e relativamente barata. Esta característica biométrica funciona bem nas identificações um para um e um para muitos.

Figura 02. Reconhecimento Facial

A face humana é outra característica biométrica que pode ser utilizada. Tem características e medições de distâncias e de ângulos que podem ser processadas a duas ou três dimensões para determinar a identidade de uma pessoa. Apesar desta tecnologia não ser tão exata como a de impressões digitais, o reconhecimento facial tem várias vantagens na verificação automatizada e como ferramenta de identificação. O processo de fotografia digital que utiliza é algo a que as pessoas estão habituadas, não se sentido, portanto, desconfortáveis com esta forma de identificação. Por outro lado, o reconhecimento facial pode ser realizado à distância, sema necessidade da pessoa tocar num dispositivo de captura biométrico.

Figura 03. Reconhecimento da Íris

O reconhecimento da íris mede os padrões da íris, ou seja, da área colorida em torno da pupila do olho. A íris é normalmente considerada como a característica biométrica mais exata, uma vez que pode ser medido em volume de informação mais significativo. O reconhecimento da íris pode ser realizado a curtas distâncias do leitor e utiliza uma fonte de luz de infravermelhos de baixa intensidade, similar ao que é utilizado no controle remoto de um televisor. O reconhecimento da íris tem vindo a ganhar popularidade naquelas áreas em que as pessoas têm de utilizar luvas ou outra roupa protetora na sua atividade normal, uma vez que a recolha de impressões digitais não é muita prática. O reconhecimento da íris também esta a ser utilizado para o acesso a instalações e em aplicações de controle fronteiriço.

Figura 04. Reconhecimento das mãos

O reconhecimento das mãos mede o comprimento, a espessura e a forma dos dedos da mão. Os leitores da geometria da mão já são utilizados há vários anos para proteger o acesso a áreas de grande segurança em edifícios. Esta tecnologia pode ser implementada de forma eficaz em ambientes internos e externos. È utilizada normalmente para a verificação (comparação um para um), em conjunto com um cartão ou com um número de identificação pessoal (PIN).

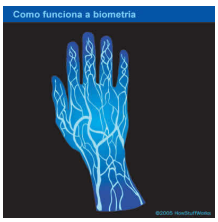

Figura 05. Reconhecimento das veias

Quanto ao reconhecimento do padrão das veias, é uma tecnologia biométrica nova que utiliza luz projetada para a pele de uma pessoa para permitir uma comparação de alto contraste dos padrões de veias nos dedos ou na área da mão. O padrão das veias de sangue é único para cada indivíduo e este padrão não varia ao longo da vida das pessoas. A medição de características que estão por baixo da pele faz com que sejam mais difíceis de observar pelos outros, tornando assim a característica biométrica do padrão das veias, um método de verificação especialmente seguro.

6.1 CALIGRAFIA

Figura 06:.Identificador de caligrafia

A primeira vista, usar a caligrafia para identificar pessoas pode não parecer uma boa idéia, pois qualquer um pode aprender a copiar caligrafias em pouco tempo. Seria fácil conseguir uma cópia da assinatura de alguém e falsifica-la.

Mas os sistemas biométricos não prestam atenção somente ao formato que se dá a cada letra. Eles analisam o ato de escrever, a pressão, a velocidade e o ritmo com os quais escreve. Eles também registram a seqüência que se usa para formar as letras, como se adicionam pontos e traços ao escrever ou depois de escrever cada palavra.

Ao contrário da forma das letras, essas características são mais difíceis de falsificar. Mesmo que alguém consiga uma cópia de sua assinatura e a reproduza, o sistema provavelmente não aceitará a falsificação.

Sensores do sistema de reconhecimento de caligrafia podem incluir uma superfície sensível ao toque ou uma caneta que contenha sensores que detectam ângulo, pressão e direção. O software traduz a caligrafia para um gráfico e reconhece as pequenas mudanças na caligrafia de uma pessoa no dia-a-dia e durante determinado tempo.

6.2 GEOMETRIA DE MÃOS E DEDOS

Figura 07. Identificador de mãos e dedos

As mãos e os dedos das pessoas são características únicas, mas não tão únicos quanto às impressões digitais ou a íris. É por isso que empresas e escolas, em vez de aparelhos de alta segurança, usam leitores de geometria das mãos e dos dedos para autenticar os usuários e não para identificá-los. Os parques temáticos da Disney, por exemplo, usam leitores de geometria dos dedos para garantir a entrada de pessoas que tenham o bilhete em todos os lugares do parque. Algumas empresas usam os leitores de geometria das mãos em vez de cartão de ponto.

Os sistemas que medem a geometria das mãos e dos dedos usam uma câmera digital e luz. Para usar um, você simplesmente coloca sua mão em uma superfície plana, alinhando seus dedos com as várias lingüetas para ter uma leitura precisa. Uma câmera tira uma ou mais fotos de sua mão e da sombra que ela produz. O sistema usa essas informações para determinar comprimento, largura, grossura e curvatura da mão e dos dedos e traduz essas informações para um padrão numérico.

Esses tipos de sistema têm prós e contras. Uma vez que as mãos são menos específicas do que as impressões digitais ou a íris, algumas pessoas sentem que esses sistemas invadem menos sua privacidade. De qualquer maneira, as mãos das pessoas mudam com o tempo em razão de machucados, mudanças de peso ou artrite. Alguns sistemas atualizam os dados para refletir as mudanças do dia-a-dia.

6.3 IMPRESSÃO DIGITAL

Figura 08. Identificador de Impressão Digital

Por décadas, os leitores de impressões digitais computadorizados apareciam somente nos filmes de espionagem. Nos últimos anos, no entanto, eles começaram a surgir por toda à parte: em delegacias, distritos policiais, edifícios em elevado grau de segurança e até mesmo em teclados de computador.

O uso de impressão digital é uma das formas de identificação mais usadas. Consiste na captura da formação de sulcos na pele dos dedos e das palmas das mãos de uma pessoa. Esses sulcos possuem determinadas terminações e divisões que diferem de pessoa para pessoa. Para esse tipo de identificação existem, basicamente, três tipos de tecnologia: óptica, que faz uso de um feixe de luz para ler a impressão digital; capacitiva, que mede a temperatura que sai da impressão, e ultra-sônica, que mapeia a impressão digital através de sinais sonoros. Um exemplo de aplicação de identificação por impressão digital é seu uso em catracas, onde o usuário deve colocar seu dedo em um leitor que ao confirmar a identificação, liberará seu acesso.

6.4 TIMBRES DE VOZ

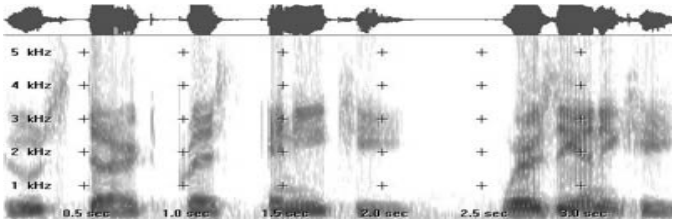

Figura 09. Espectrograma de timbre de voz

A voz é uma característica única me razão do formato das cavidades vocais e da forma que se movimenta a boca ao falar. Para se registrar em um sistema de timbre de voz, você diz exatamente as palavras ou frases solicitadas ou dá amostra de seu discurso, para que o computador possa identificá-lo, não importando as palavras que foram ditas.

Quando as pessoas pensam no timbre de voz, normalmente pensam na onda que variam em um osciloscópio. Mas os dados usados no timbre de voz são um espectrograma de som e não o formato de uma onda. Um espectrograma é basicamente um gráfico que exibe a freqüência do som no eixo vertical e o tempo no eixo horizontal. Diferentes sons de falas criam diferentes formatos dentro do gráfico. Os espectrogramas também usam cores ou tons de cinza para representar as qualidades acústicas do som.

Algumas empresas usam o reconhecimento do timbre de voz para que as pessoas tenham acesso à informação ou possam passar informações sem estar fisicamente presentes. Em vez de aproximar-se de um scanner de íris ou de um leitor de geometria das mãos, alguém pode fazer uma autorização dando um simples telefonema. Infelizmente, as pessoas conseguem enganar alguns sistemas, principalmente os que funcionam por telefone, com uma simples gravação de voz de uma pessoa autorizada.

Esse é um dos motivos pelos quais os sistemas usam várias senhas de voz escolhidas aleatoriamente ou usam timbres de voz gerais em vez de timbres de palavras específicas. Outros usam tecnologia que detecta os artefatos criados em gravações e playbacks.

6.5 ESCANEAMENTO DA ÍRIS

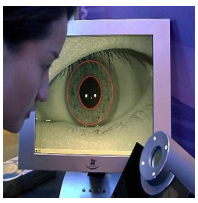

Figura 10. Identificador da íris

O scanner da íris pode parecer futurístico, mas o centro do sistema é uma simples câmera digital CCD. O escaneamento usa tanto a luz quanto à luz infravermelha para ter uma foto clara e de alto contraste da íris. Próximo à luz infravermelha, a pupila de uma pessoa fica bem escura, facilitando a separação, pelo computador, da pupila e da íris.

Quando você olha para um scanner de íris, ou a câmera focaliza automaticamente ou você usa um espelho ou um feedback* sonoro do sistema para ter certeza de que seu posicionamento está correto. Normalmente seu olho fica de 7,5 cm a 25 cm da câmera. Quando ela tira uma foto, o computador localiza:

- O centro da pupila
- A beirada da pupila
- A beirada da íris
- As pálpebras e os olhos

Em seguida o scanner analisa os modelos da íris e os traduz para um código.

Os scanners de íris estão se tornando mais comuns nos aplicativos de alta segurança, porque os olhos das pessoas são únicos (a possibilidade de trocar o código de uma íris pelo de outra é de 1 em 10 elevado à 78ª potência). Os olhos também permitem mais de 200 pontos de referência para comparação, diferente dos 60 ou 70 pontos das impressões digitais.

A íris é uma estrutura visível, mas protegida, e não se modifica com o tempo, tornando-se ideal para a identificação biométrica. Na maioria das vezes, os olhos das pessoas

permanecem ilesos após uma cirurgia ocular e mesmo se pessoas cegas podem usar scanner de íris, desde que seus olhos tenham íris. Os óculos e as lentes de contato normalmente não interferem nem causam inexatas.

6.6 ESCANEAMENTO DA RETINA

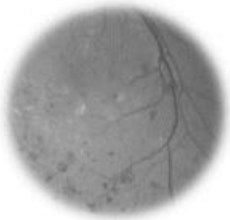

Figura 11.Análise da Retina

Algumas pessoas confundem o escaneamento de íris com o escaneamento da retina. O escaneamento da retina é uma tecnologia mais antiga, que precisava de uma luz brilhante iluminando a retina da pessoa para que o sensor pudesse tirar uma foto da estrutura dos vasos sanguíneo da parte escura dos olhos. Algumas pessoas achavam o sistema desconfortável e invasivo. Além disso, as retinas mudam conforme a idade, o que pode levar a leitura inexata.

6.7 GEOMETRIA DAS VEIAS

Figura 12. Identificador das veias da mão

Assim como a íris e as impressões digitais, as veias de uma pessoa também são características exclusivas. Gêmeos não têm veias idênticas e as veias de uma pessoa são bem diferentes nos lados esquerdo e direito. Muitas não são visíveis através da pele, tornando-se extremamente difíceis de serem falsificadas ou manipuladas. Suas formas também se modificam muito pouco com a idade.

Para usar um sistema de reconhecimento de veias, você simplesmente coloca seu dedo, pulso, palma ou as costas das mãos no scanner ou bem próximas a ele. Uma câmera tira uma foto digital usando luz infravermelha. A hemoglobina presente no sangue absorve a luz, de forma que as veias aparecem escuras na foto. Assim como com todos os outros tipos biométricos, o software cria um padrão de referência baseado no formato e na localização da estrutura das veias.

Os scanners que analisam a geometria das veias são totalmente diferentes dos usados nos testes hospitalares. Os scanners com finalidades médicas normalmente usam partículas radioativas. Já os scanners da segurança biométrica apenas usam uma luz parecida com a luz que vem de um controle remoto.

6.8 RECONHECIMENTO FACIAL

Figura 13. Reconhecimento facial

O reconhecimento facial refere-se a um processo automatizado ou semi-automatizado de confrontação de imagens faciais. A imagem é obtida através de um scanner e depois analisada com o objetivo de se obter uma assinatura biométrica.

Para a aquisição das imagens utilizam-se diferentes temas sendo mais comum às imagens 2D. O reconhecimento facial a 2D é mais fácil de implementar e é mais barata, mas os desafios técnicos são maiores (os sistemas funcionam mal quando existem variações na orientação da face e nas condições de iluminação) originando baixas taxas de precisão.

Têm sido realizados estudos utilizando imagens à 3D que causam uma redução na sensibilidade a fatores como a variação de iluminação, mas com a desvantagem de os scanners serem mais caros e destas não serem compatíveis com as atuais imagens a 2D. Uma alternativa é utilizar radiação infravermelha para examinar padrões de calor na face, embora esta não seja uma área preferencial de estudo.

Um sensor, ou uma câmera digital registra a imagem facial. Para evitar que um rosto falso, ou mesmo um molde seja apresentado diante do sensor, alguns sistemas requerem que o indivíduo sorria, pisque ou se mova, de tal maneira que fica patente que a face apresentada realmente pertence a um ser humano. Em seguida, é gerado um algoritmo que representa a assinatura biométrica normalizada ou padronizada, da tal forma que ela fique no mesmo padrão, tamanho, resolução e posição das outras assinaturas existentes na base de dados.

7. O FUTURO DA BIOMETRIA

A biometria pode fazer muito mais do que apenas determinar se alguém tem autorização para entrar em determinado local. Alguns hospitais usam sistemas biométricos para garantir que as mães levam o recém-nascido certo para casa. Os especialistas também têm aconselhado as pessoas que escaneiem documentos como certidão de nascimento, e CPF e os guardem em uma memória com segurança biométrica no caso de uma emergência. Seguem algumas tecnologias biométricas que você poderá ver no futuro:

- Novos métodos que usam o DNA, unhas, dentes, formato das orelhas, cheiro do corpo, características da pele e da pulsação sanguínea;
- Sistemas de uso doméstico mais precisos;
- Clubes preferenciais, programas de compradores freqüentes e sistemas rápidos de verificação com segurança biométrica e,
- Mais sistemas biométricos presentes em passaportes para serem usados em fronteiras e aeroportos.

8. COMO FUNCIONAM AS EVIDÊNCIAS DE DNA

Nos últimos anos, a evidência de DNA passou a desempenhar um papel importante nos sistemas de justiça criminal de muitas nações. É utilizada para provar que os suspeitos estiveram envolvidos em crimes e para libertar pessoas condenadas erroneamente.

- A chave para a evidência de DNA está na comparação do DNA encontrado na cena do crime com o DNA do suspeito. Para isso, os investigadores devem fazer três coisas:
- Coletar o DNA na cena do crime e também do suspeito;
- Analisar o DNA para criar um perfil de DNA e,
- Comparar os perfis entre si.

As autoridades podem extrair o DNA de quase todos os tecidos, incluindo cabelos, unhas, ossos, dentes e fluídos sanguíneos. Às vezes os investigadores possuem a evidência de DNA, mas não têm suspeitos. Nesse caso, os oficiais da lei podem comparar DNAs da cena do crime com perfis armazenados em um banco de dados. O banco de dados mais utilizado mos Estados Unidos chama-se CODIS, que significa Sistema de DNA Índice Combinado e é mantido pelo FBI. Pela lei, autoridades de todos os 50 Estados devem coletar amostras de DNA de estupradores para inclusão no CODIS. Alguns Estados americanos também obrigam todos os criminosos condenados a fornecerem uma amostra de DNA.

9. PRIVACIDADE E OUTRAS PREOCUPAÇÕES

Algumas pessoas fazem objeções culturais ou religiosas à biometria. Outras imaginam um mundo no qual câmeras as identificam e as rastreiam enquanto andam pelas ruas, seguindo suas atividades e padrões de consumo sem sua permissão. Elas se perguntam se as empresas venderão dados biométricos da mesma forma que vendem endereços de e-mail e números de telefone. Pessoas se preocupam também com a possibilidade de existir uma enorme base de dados com informações vitais de cada um e se isso seria seguro.

Os sistemas biométricos não têm a capacidade de armazenar e catalogar informações sobre todas as pessoas do mundo. A maioria deles armazena uma quantidade mínima de informações sobre um número relativamente pequeno de usuários. A maioria dos sistemas também trabalha apenas no lugar em que estão, como num prédio comercial ou num hospital. As informações de um sistema não são necessariamente compatíveis com as de outros, embora várias organizações estejam tentando padronizar os dados biométricos.

Além do potencial quanto à invasão de privacidade, surgiram outras preocupações sobre a biometria:

- Confiança em demasia: a idéia de que os sistemas biométricos são perfeitos e podem fazer as pessoas esquecerem de procedimentos básicos de proteção aos dados do sistema;
- Acessibilidade: alguns sistemas não podem ser adaptados para certas pessoas como idosos ou deficientes físicos e,
- Interoperabilidade: em situações emergenciais, agências que usam sistemas diferentes podem precisar compartilhar dados e atrasos podem ocorrer se os sistemas não conseguirem comunicar entre si.

10. REFERÊNCIAS

MIRANDA, Leonel. Biometria: O que é e o que faz?. Disponível em: <http://www.sinfic.pt/SinficNewsletter/index.html>. Acessado em maio 2007.

HARRIS, Tom. Como funcionam os leitores de impressões digitais. Disponível em: <http://www.uol.com.br/leitores-de-impressoes-digitais.htm >. Acessado em maio 2007.

BRASIL, HowStuffWords. Como funciona a biometria. Disponível em <http://ciencia.hsw.uol.com.br/bometrica1.htm>. Acessado em maio 2007.

O'CONNELL, Ann Meeker. Como funcionam as evidências de DNA. Disponível em: <http://ciencia.hsw.uol.com.br/evidencias-de-dna.htm >. Acessado em maio 2007.