NEXT GENERATION IDENTIFICATION (NGI): UM NOVO CONCEITO EM BIOMETRIA FORENSE

João Paulo Caldas Cardozo

Bacharel em Fisioterapia pelo Centro Universitário de Brasília (UniCEUB)
Especialista em Ciências Forenses IFAR/LS
E-mail: joaofisiocaldas@gmail.com

Palavras-chave: next generation identification, biometric systems, forensic identification.

INTRODUÇÃO

Uma das acepções do termo biometria remete à possibilidade de individualizar uma pessoa por meio de suas características físicas ou comportamentais (THOMPSON & BLACK, 2006). Os sistemas biométricos automatizados surgiram no início da década de 1960, sendo os sistemas para reconhecimento de voz e de impressões digitais os primeiros a serem explorados, principalmente nas áreas de segurança e controle de acesso (WAYMAN, 2007). As análises de retina, de assinaturas e de elementos da face surgiram na década de 1980 e com o constante evoluir tecnológico, foram desenvolvidos métodos capazes de integrar diferentes biometrias que partem de análises de características distintas para individualizar uma pessoa, dando origem aos sistemas integrados (WAYMAN, 2007; GUDAVALLI et al., 2012). Na última década o tema integração de biometrias esteve em voga com a divulgação do chamado Next Generation Identification (NGI), o banco de dados biométricos da Federal Bureau of Investigation (FBI) que conta com registros de aproximadamente um terço da população americana (FEDERAL BUREAU OF INVESTIGATION, 2016). O sistema NGI foi desenvolvido sobre a plataforma do banco de dados de impressões digitais do FBI, que foi totalmente reestruturado de modo a permitir a inclusão de outras biometrias, tais como impressões palmares, escaneamento de íris, padrão de voz e reconhecimento facial, além de implementar um novo algoritmo de correspondência de impressões digitais (FEDERAL BUREAU OF INVESTIGATION, 2016).

OBJETIVO

Apresentar o conceito de integração de biometrias com especial foco sobre o NGI, bem como suas aplicações em atividades investigativo-policiais e judiciárias.

METODOLOGIA

Trata-se de um estudo descritivo da modalidade resumo tendo como base a bibliografia pertinente ao tema. Para isso foi realizada uma pesquisa de artigos em periódicos de cunho forense, bem como na própria base de dados públicos disponível no sítio do FBI na internet, publicados entre 2005 e 2016, utilizando os termos “next generation identification”, “biometric systems” e “forensic identification”.

RESULTADOS E DISCUSSÃO

Atualmente o termo biometria não é limitado a impressões digitais, abarcando uma série de outras características como impressões palmares, reconhecimento facial, padrão de veias das mãos, formato do pavilhão auditivo e até mesmo a superfície lingual (UNAR et al., 2014). Com o surgimento de novos métodos de identificação biométrica, viu-se a possibilidade de criar um sistema que se valesse de diferentes características com o fim de identificar uma pessoa, de modo a conferir maior robustez e segurança no processo, sendo estes os denominados sistemas integrados de identificação (GUDAVALLI et al., 2012). Nesse sentido, a intenção do NGI é combinar todas essas informações no arquivo de cada pessoa, integrando-os com dados pessoais e biográficos (FEDERAL BUREAU OF INVESTIGATION, 2016). Outras ferramentas associadas ao sistema NGI chamam a atenção no que tange ao uso forense dos métodos de identificação das quais merecem destaque a Rap Back e o sistema de reconhecimento facial. A ferramenta denominada Rap Back permite que agências autorizadas recebam notificações em relação às atividades de indivíduos que ocupam cargos de confiança ou que estejam sob investigação ou supervisão da justiça criminal, eliminando dessa forma a necessidade de repetidas verificações sobre determinada pessoa requerida por uma mesma agência (FEDERAL BUREAU OF INVESTIGATION, 2016). Sabe-se que um dos motivos pelos quais os processos da justiça brasileira, por vezes relativos a causas simples, demoram anos para serem conclusos é a demora na comunicação entre diferentes órgãos

haja vista a burocracia envolvida nesse processo aparentemente simples. O desenvolvimento ou a implementação em território brasileiro de sistemas de notificação automática semelhantes ao Rap Back contribuiria sobremaneira na redução de tais prazos, entretanto, percebe-se que não existem incentivos por parte do Estado ou das Instituições policiais para o desenvolvimento desse tipo de tecnologia. Já a ferramenta de reconhecimento facial permite, a partir da inserção de uma imagem no módulo de busca, pesquisar em um acervo que conta com milhões de fotografias relacionadas a fatos criminosos ocorridos nos Estados Unidos da América ao longo de décadas (FEDERAL BUREAU OF INVESTIGATION, 2016). Como resultado, é gerada uma lista de candidatos classificados como potenciais identificados, sendo essa uma outra maneira de como a biometria pode ser utilizada como instrumento de investigação. Essa tecnologia tem sido aplicada no aeroporto de Brasília desde julho de 2016 que, em virtude dos jogos olímpicos, teve o número de voos internacionais significativamente aumentado. A princípio, a ferramenta está sendo utilizada apenas no desembarque internacional, mas a ideia é expandi-la para os itinerários domésticos. Cabe ressaltar que um software de reconhecimento facial não é baseado nos aspectos morfológicos das imagens faciais, e sim em informações estatísticas e matemáticas obtidas a partir delas (WAYMAN, 2007). Diante de um sistema novo e inovador como o NGI, dúvidas por parte da população surgiram e receios vieram à tona, haja vista a quantidade de informações pessoais – em regra, sigilosas – que estariam agora em poder de autoridades policiais e judiciárias do Estado sob o argumento de garantia da segurança dos cidadãos (ELETRONIC FRONTIER FOUNDATION). O FBI não informou, pelo menos publicamente, acerca de restrições quanto ao tipo de dados que poderão ser adicionados ao sistema, quem são as pessoas que terão acesso a ele e ainda como esses dados serão efetivamente utilizados. Segundo o FBI (2016), em publicação no seu sítio oficial na internet, o sistema é capaz de impedir resultados falsos-positivos, algo que, sob uma perspectiva científica, é impossível de se garantir. Fica claro que faltam informações concretas acerca de como tal sistema trabalha e como será efetivamente utilizado, mas fato é que, se utilizado com lisura e para fins legítimos, tem um enorme potencial para auxiliar na execução de atividades policiais e judiciárias.

CONCLUSÃO

A aplicação da biometria por meio do sistema NGI tem sido extremamente útil para o FBI e para os seus parceiros no que tange à aplicação da lei e ao desenvolvimento de ações de inteligência, representando o que há de mais novo em relação à tecnologia aplicada na identificação humana forense. Sistemas desse tipo representam o futuro dos métodos de identificação humana para fins civis e criminais e influenciam os departamentos policiais de outros países a continuar em constante desenvolvimento.

REFERÊNCIAS

ELETRONIC FRONTIER FOUNDATION. Transparency Project. Disponível em: <https://www.eff.org/foia/fbis-next-generation-identification-biometrics-database>. Acesso em: 12 de outubro de 2016.

FEDERAL BUREAU OF INVESTIGATION. Next Generation Identification. Disponível em: <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>. Acesso em: 18 de agosto de 2016.

GUDAVALLI, M.; BABU, A.V.; RAJU, S.V.; KUMAR, D.S. Multimodal biometrics – sources, architecture and fusion techniques: na overview. In: Preceedings of the 2012 International Symposium on Biometrics and Security Technologies. Institute of Electrical and Electronic Engineers, p. 27-34, 2012.

THOMPSON, T. & BLACK, S. Forensic human identification: an introduction. CRC press, 550 p., 2006.

UNAR, J.A.; SENG, W.C.; ABBASI, A.A. A review of biometric technology along with trends and prospects. Pattern Recognition, 47: 2673 - 2688, 2014.

WAYMAN, J.L.; JAIN, A.; MALTONI, D.; MAIO, D. Biometric systems: technology, design and performance evaluation. Springer, 379 p., 2005.

WAYMAN, J.L. The scientific development of biometrics over the last 40 years. In: LEEUK, K.D.; BERGSTRA, J. The history of information security: a comprehensive handbook. Elsevier, p. 263 – 274, 2007.

AGRADECIMENTOS

Ao professor especialista Petterson Vitorino de Morais pela brilhante orientação durante o desenvolver deste trabalho.

Não foram declarados conflitos de interesse associados à publicação deste artigo.