Produção de Inteligência Forense com base em características das Impressões Digitais em Documentos Falsos

Carlos Magno Alves Girelli
Doutorando em Física na UFES
Polícia Federal - Brasil

RESUMO

Crimes de falsidade documental merecem atenção especial porque, dentre outros motivos, lesam sobremaneira os cofres públicos e oferecem risco à segurança nacional ao ocultarem a verdadeira identidade de terroristas e outros criminosos procurados pela justiça. A política de enfrentamento a esses crimes é geralmente reativa e focada na prova. Os exames periciais em documentos questionados geralmente se limitam a satisfazer as necessidades da investigação específica e produzir provas que serão utilizadas estritamente no caso em questão. Em geral, nenhum trabalho de inteligência adicional é feito no sentido de se obter uma visão mais ampla do problema que permita propor soluções mais abrangentes e eficazes. O presente estudo destaca a importância da atividade de inteligência no campo das ciências forenses e a necessidade de se assumir uma postura mais proativa no combate aos crimes envolvendo documentos falsos. O objetivo da inteligência forense é gerar informação útil em tempo hábil para assessorar tomadas de decisão em diferentes níveis por parte das autoridades gestoras. Algumas ferramentas potencialmente úteis no exame de documentos para fins de inteligência forense são apresentadas, dentre elas a análise de perfis, a representação geográfica e temporal de casos criminais e o exame de detalhes intrínsecos e extrínsecos das impressões digitais. Nesse sentido, ênfase é dada às impressões digitais presentes em documentos, cujas características podem indicar tendências de falsificação e *modus operandi* dos falsificadores, ajudando a polícia a identificar ligações entre crimes aparentemente desconexos e até mesmo chegar à fonte de falsificação. O estudo demonstra alguns benefícios provenientes da análise de impressões digitais em documentos falsos, utilizando como exemplo dados de casos reais. Por fim, é sugerida a implantação de um programa de perfilagem de documentos em âmbito nacional, integrando resultados obtidos a partir de exames papiloscópicos e documentoscópicos com as demais informações provenientes da investigação.

Palavras-Chave: Impressão Digital. Documento Falso. Inteligência Policial. Inteligência Forense. Ciências Forenses. *Profiling*.

Recebido em 1º de maio de de 2016.
Aceito em 30 de agosto de 2016.
Brasília, v. 7, n. 2, p. 73-96, jul/dez 2016.
ISSN 2178-0013
ISSN Eletrônico 2318-6917

1. Introdução

O exercício de direitos e deveres inerentes à cidadania requer muitas vezes que o indivíduo se identifique perante órgãos públicos e privados. A identificação civil pode ser realizada mediante apresentação de qualquer dos documentos previstos na Lei n° 12.037 de 2009 (BRASIL, 2009).

A pluralidade de instituições legitimadas a emitir documentos de identidade, a ausência de comunicabilidade entre seus sistemas e bancos de dados e a vulnerabilidade de itens de segurança presentes nos suportes adotados são alguns dos fatores que tornam os documentos de identificação civil utilizados no Brasil frágeis e bastante suscetíveis à falsificação.

De acordo com a base de dados do SINIC – Sistema Nacional de Informações Criminais da Polícia Federal, todos os anos são investigados por esta instituição mais de 7.000[1] casos envolvendo o uso ou a fabricação de documentos falsos (SINIC, 2016). Este número se torna muito maior se considerados os casos investigados pelas polícias civis dos Estados, e estima-se que a realidade seja ainda muito pior, considerando-se as cifras negras ou ocultas, isto é, o fato de que apenas parte dos crimes cometidos é registrada e apurada.

Em geral, os crimes de falsidade documental são meios para cometimento de outros crimes visando obtenção de vantagens ilícitas, desde pequenos golpes a fraudes que lesam sobremaneira os cofres públicos. Documentos falsos são também utilizados para ocultação de terroristas e outros criminosos procurados pela justiça, para auxiliar o cometimento de crimes como o tráfico de pessoas e tantos outros que extrapolam a esfera patrimonial.

A atuação da Polícia Judiciária e em especial da Polícia Técnico-Científica em relação aos crimes envolvendo documentos falsos é normalmente reativa, iniciando-se após a tentativa ou consumação do fato delituoso. Os exames periciais realizados em documentos questionados buscam verificar sua autenticidade, responder objetivamente aos quesitos formulados e prover informações estritamente destinadas ao caso em questão. Em geral, nenhum trabalho de inteligência adicional é feito no sentido de se obter uma visão macro do problema e propor soluções mais abrangentes.

1 Foram consideradas as incidências penais inseridas no SINIC referentes aos artigos 297, 298, 299 e 304 do Código Penal Brasileiro.

Este artigo sugere o uso de inteligência forense a partir da análise de impressões digitais em conjunto com as demais ferramentas de investigação ao lidar com crimes envolvendo documentos falsos. A justificativa reside no fato de que características das impressões digitais presentes em documentos falsos podem indicar tendências de falsificação e *modus operandi* dos falsificadores, levando a polícia a identificar ligações entre crimes aparentemente desconexos e até mesmo chegar à fonte de falsificação.

Serão apresentados alguns conceitos inerentes à atividade de inteligência forense, bem como discutidos possíveis modelos aplicáveis a documentos falsos, com ênfase na análise de impressões digitais. O objetivo é destacar a importância da inteligência forense para levar a uma melhor compreensão dos fenômenos criminológicos, dar suporte às tomadas de decisões por parte das autoridades competentes em diferentes níveis e estimular uma postura mais proativa no combate aos crimes de falsidade documental.

2. Inteligência Forense

O termo "inteligência" tem sido utilizado deliberadamente, e muitas vezes de forma inapropriada, por setores de diversas repartições públicas e privadas, que, em geral, não realizam atividades de inteligência em sua essência. Felipe Scarpelli de Andrade discute com maior profundidade efeitos dessas distorções no entendimento e na aplicação do termo. Segundo o autor, uma característica fundamental da atividade de inteligência é a sua natureza de assessoramento (ANDRADE, 2012). Nesse sentido, o produto da inteligência não precisa ser exato, nem mesmo provado. Baseia-se em probabilidades e tendências fundamentadas em metodologia própria que poderão ser utilizadas em caráter consultivo conforme melhor juízo da autoridade.

Inteligência é o resultado de um processo que visa transformar dados brutos (não tratados) em uma forma adequada para tomada de decisão (MORELATO et al., 2013). Este processo é contínuo, interativo e inclui coleta de dados, avaliação, confrontação, análise, interpretação, disseminação e reavaliação. O objetivo é agregar valor à informação coletada em tempo hábil (AEPLI, RIBAUX e SUMMERFIELD, 2011; RIBAUX et al., 2003; RATCLIFFE, 2003; PETERSON, 2005).

Inteligência é uma noção geral encontrada em diversos setores, dentre eles as ciências forenses. Neste caso, o processo é realizado dentro de estruturas organizacionais hierarquizadas como as instituições policiais. A inteligência forense consiste no processamento lógico dos dados oriundos de evidências de crimes, gerando informação precisa, útil e em tempo hábil para dar suporte às autoridades em suas tomadas de decisão (RIBAUX et al., 2003; RIBAUX et al., 2010). O tempo é um fator crítico quando se busca resolver um caso ou entender a criminalidade como um todo (MARGOT, 2000). Assim, por exemplo, a inteligência obtida através de evidências que leve à conexão entre diversos crimes pode impedir um criminoso de cometer novos crimes. Da mesma forma, um link entre diferentes apreensões perde seu potencial se detectado meses após a operação policial, pois os criminosos podem se livrar de provas incriminadoras, como por exemplo, drogas de um mesmo lote ou produtos roubados.

O princípio fundamental da inteligência forense é que, ao invés de tratar cada caso individualmente com o objetivo de auxiliar o julgamento (i.e. foco na prova), um foco mais amplo e uma abordagem holística baseada no fenômeno do crime dever ser seguido. (BAECHLER et al., 2015). A exploração sistemática e estruturada das evidências do crime é essencial para produzir conhecimento que irá guiar decisões em diferentes níveis. Ratcliffe (2007) distingue inteligência policial com base em três níveis de ação: inteligência tática, operacional e estratégica.

A Inteligência tática dá suporte aos policiais da linha de frente em ações orientadas a casos específicos e, por tal motivo, é relevante para determinadas investigações em particular (PETERSON, 2005; RATCLIFFE, 2012). O ambiente criminal de interesse é local ou pontual. O uso deste tipo de inteligência é caso a caso e dispensa um maior entendimento de longo prazo ou de problemas geográficos mais amplos (RATCLIFFE, 2012). Um exemplo de inteligência tática é a identificação de um suspeito com base em impressões digitais reveladas em local de crime.

A Inteligência operacional ajuda no planejamento de atividades de redução criminal, assessorando gestores responsáveis por determinadas regiões geográficas ou que comandam equipes. Permite a identificação de prioridades e, portanto, é relevante no combate a crimes em série (RATCLIFFE, 2012). Um exemplo de decisão operacional é a mudança na estratégia de intervenção em locais de crime durante um período de tempo definido, com relação a um contexto criminal específico, visando avaliar seu impacto.

Inteligência estratégica fornece uma compreensão de padrões e funcionamento de ambientes e comportamentos criminosos. Trata-se, portanto, de uma atividade proativa e voltada para o futuro (RATCLIFFE, 2012). A inteligência estratégica explora soluções de longo prazo e acomoda atrasos mais facilmente do que em uma perspectiva operacional (PETERSON, 2005). É utilizada por gestores em posições mais elevadas, cujas decisões afetam não apenas as atividades policiais, mas também outras áreas como saúde, seguridade social, política etc. Um exemplo consiste na detecção de mudança na forma de preparo ou na composição de determinada droga ilícita, o que poderia estimular um estudo sobre o motivo que levou a essa mudança (talvez mudança de precursor devido a restrições impostas aos outros). Isso poderia também ter um impacto sobre a política de combate às drogas.

Os limites entre esses tipos de inteligência não são claramente definidos. A análise de informações geradas em nível de inteligência tática ou operacional provenientes de diferentes casos pode contribuir também para uma visão estratégica global. Da mesma maneira, a inteligência estratégica pode também orientar esforços voltados para eventos específicos. Os resultados obtidos através da análise de perfis de drogas, por exemplo, podem ser integrados nesses diferentes tipos de inteligência. Em um nível operacional, amostras de drogas com perfis similares (físicos ou químicos) podem realçar conexões entre casos ou apreensões separados. Por outro lado, em um nível estratégico, links podem realçar tendências do tráfico, redes de distribuição ou processos de produção específicos em escala nacional ou internacional (WEYERMANN et al., 2008). A análise de perfis constitui um dos focos deste trabalho e será discutida em detalhes a seguir.

3. Análise de Perfis

A análise de perfis (do inglês *profiling*) é uma poderosa ferramenta utilizada na atividade de inteligência. Guilherme Damasceno Fonseca (2012) discute aspectos desta atividade em relação ao perfil de passageiros em aeroportos como ferramenta de prevenção ao terrorismo. Tratando-se de inteligência forense, os objetos de interesse são geralmente evidências de crime, como drogas ilícitas (MORELATO et al., 2013; WEYERMANN et al., 2008), documentos falsos (BAECHLER, RIBAUX e MARGOT, 2012; BAECHLER et al., 2013; AUBERSON et al., 2016), armas de fogo apreendidas (HANNAM, 2010), medicamentos contrafeitos (DÉGARDIN, ROGGO e MARGOT, 2015), dentre outras.

Uma vez definido o objeto de interesse, seu perfil é traçado com base em suas características relevantes que sejam adequadas ao propósito da atividade de inteligência em questão. Não há critério absoluto para escolha das características que devem compor o perfil. Em geral, as características devem ser representativas da fonte, de modo a se repetirem ou serem suficientemente semelhantes quando se tratarem de objetos provenientes de uma mesma fonte ou pertencentes a uma mesma classe. A variabilidade dessas características deve ser tal que, para objetos oriundos de fontes diversas ou pertencentes a classes distintas, essas características apresentem diferenças notáveis que possam ser detectadas. É interessante que as características que compõem o perfil possam ser facilmente observadas ou medidas, preferencialmente sem a necessidade de técnicas sofisticadas ou custosas. Em suma, há diversos critérios a serem levados em conta na definição das características que integrarão o perfil do objeto considerado. A natureza e os objetivos da atividade de inteligência pretendida e a relação de custo e benefício envolvidos serão preponderantes no processo de escolha.

Uma vez definido o rol de características que irão compor o perfil do objeto de interesse, inicia-se o exame dos objetos questionados, traçando-se o seu perfil e comparando-o com os perfis anteriores armazenados no sistema. De acordo com o grau de similitude encontrado entre pares de perfis comparados (perfil questionado versus perfil alvo), o sistema retorna um resultado que pode ser tanto um valor numérico (taxa de probabilidade) quanto uma resposta lógica do tipo "sim" ou "não" conforme limiar preestabelecido. Para retornar tais resultados, o sistema é previamente calibrado com base em perfis de objetos cujas fontes são conhecidas. A interpretação dos resultados poderá levar à identificação de links, correlações, padrões e tendências que possam nortear o trabalho de inteligência e consequentemente assessorar tomadas de decisões.

Baechler et al. (2013) apresentam um método original para análise de perfil de documentos de identidade falsos, onde explicam passo a passo toda a metodologia, desde os critérios na escolha das características que irão compor o perfil, os testes de calibração e validação utilizando diferentes métricas e fontes conhecidas, até o resultado das comparações entre perfis e a avaliação final do método.

O método desenvolvido por aqueles autores (BAECHLER et al., 2013) foi aplicado a quatro diferentes tipos de documentos, dentre eles car-

teira de identidade portuguesa, semelhante à carteira de identidade brasileira no tocante a ser confeccionada utilizando-se suporte de papel e conter foto e impressão digital do titular. Dentre as 23 características utilizadas por aqueles pesquisadores para compor o perfil das carteiras de identidade de Portugal, nenhuma estava relacionada às impressões digitais (BAECHLER, 2016).

4. Identificação com Base em Impressões Digitais

Impressões papilares constituem um gênero do qual fazem parte as impressões digitais (dedos das mãos), impressões palmares (palmas das mãos) e impressões plantares (plantas dos pés). A forma como as papilas dérmicas se organizam nessas regiões é única (princípio da unicidade), de forma que uma mesma impressão papilar não se repete em pessoas distintas, nem mesmo em regiões distintas de uma mesma pessoa. Além disso, as impressões são formadas na derme e seu relevo reproduzido na epiderme desde a vida intrauterina e persistem por toda a vida até avançado estado de decomposição cadavérico (princípio da perenidade), sem que o desenho digital sofra modificações significativas ao longo do tempo (princípio da imutabilidade) (CHAMPOD et al., 2004).

A identificação humana por meio de impressões digitais oferece uma série de vantagens sobre outras biometrias devido à simplicidade, rapidez, baixo custo, confiabilidade dos resultados e método de coleta não invasivo. Por tal motivo, tem sido uma prática largamente utilizada em todo o mundo há mais de um século (CHAMPOD et al., 2004), com vasta aplicação nas áreas cível e criminal.

A presença de impressões digitais em documentos de identificação civil é muito importante, pois vincula os dados qualificativos constantes no documento à pessoa física que se apresentou como titular de tais informações. No Brasil, a grande maioria dos documentos válidos para fins de identificação civil elencados na Lei nº 12.037/09 (BRASIL, 2009) possuem impressão digital do titular, com exceção do passaporte, que é um documento pouco utilizado por brasileiros dentro de seu próprio país. A Carteira Nacional de Habilitação é outro documento sem impressão digital do titular que, embora não conste no rol específico da Lei nº 12.037/09 (BRASIL, 2009), equivale a documento de identidade em todo o território nacional por força do art. 159 do Código de Trânsito Brasileiro (BRASIL, 1997).

O exame de impressões digitais pode ser realizado com base em metodologia própria amplamente utilizada em nível internacional (SWGFAST, 2013), representada pela sigla em inglês ACE-V, que significa análise, comparação, avaliação e verificação. A fase de análise é um exame preliminar sobre as condições em que se encontra a impressão, concluindo a respeito de haver ou não condições técnicas suficientes para prosseguir com a comparação.

Na comparação a impressão questionada é posicionada lado a lado com a impressão padrão cuja fonte é geralmente conhecida, e o especialista busca características concordantes e discordantes. Uma ferramenta tecnológica bastante útil nesta etapa é o AFIS (Sistema Automatizado de Identificação de Impressões Digitais), que permite o armazenamento de milhões de impressões digitais e, com base em seu algoritmo e capacidade de processamento, otimiza sobremaneira a busca por impressões digitais suspeitas, apresentando ao usuário uma lista de candidatos mais prováveis. Feitas as comparações e assinaladas concordâncias e discordâncias, o examinador procede então à avaliação dos resultados, concluindo pela identificação (impressões originadas de uma mesma fonte), exclusão (impressões originadas de fontes distintas) ou inconclusivo (por exemplo, por comparar regiões distintas de duas impressões ou por não haver pontos característicos suficientes nas regiões visíveis de cada impressão).

Um segundo examinador realiza um trabalho de verificação quanto ao procedimento realizado pelo primeiro, preferencialmente sem conhecimento da decisão daquele (verificação cega). Havendo discordância entre eles, todo o procedimento deverá ser revisado em conjunto por ambos visando identificar o motivo e chegar a um consenso, inclusive podendo ser chamado um terceiro examinador para conferir maior segurança aos resultados.

O método ACE-V (SWGFAST, 2013) baseia-se em uma avaliação qualitativa e quantitativa de três níveis de detalhes das impressões. O Nível 1 se refere ao fluxo geral de linhas das cristas papilares. O Nível 2 corresponde aos caminhos individuais das linhas, aquelas regiões contendo minúcias como pontas de linhas, bifurcações, pontos e linhas contínuas. O Nível 3 se refere à estrutura da linha (formas das pontas e poros), e suas posições relativas.

Os níveis de detalhes citados constituem características intrínsecas das impressões digitais que obedecem aos princípios da papiloscopia da unicidade, perenidade e imutabilidade. Os exames papiloscópicos de rotina baseiam-se

nesses detalhes intrínsecos e seus resultados são, em geral, utilizados somente no conjunto probatório do caso em questão. Embora as conclusões convencionais restrinjam-se à busca pela autoria da impressão examinada, é possível ir além e extrair informações adicionais a partir dessas pequenas evidências (GIRELLI, 2015a). Na próxima seção serão exploradas algumas propriedades das impressões digitais que podem ser utilizadas para fins de inteligência forense.

5. Análise de Impressões Digitais para fins de Inteligência Forense

Além das características intrínsecas discutidas anteriormente, as impressões digitais também apresentam detalhes extrínsecos resultantes do método de coleta ou revelação, das características do substrato onde se encontram ou, ainda, devido a edições de imagem. Alguns exemplos são: contorno da região visível que varia conforme pressão, ângulo e rolagem do dedo; distorção, sobreposição, deslizamento, interrupção ou borrão nas linhas papilares; marcas resultantes de pressão excessiva ou excesso de suor durante a coleta das impressões; presença de ruídos ou artefatos como sujeiras, marcas d'água etc.

Essas características possuem natureza eventual e aleatória e não obedecem aos princípios da papiloscopia. Portanto, não são integralmente reproduzidas em impressões do mesmo dedo obtidas por coletas distintas (GIRELLI, 2015a; GIRELLI, 2016b). Assim, impressões digitais presentes em diferentes documentos de uma mesma pessoa devem possuir coincidência entre suas minúcias intrínsecas, mas razoável discordância entre suas características extrínsecas. A repetição sistemática de tais características extrínsecas em impressões digitais, presentes em documentos distintos, pode indicar que as impressões são cópias idênticas de uma mesma imagem, apontando possível falsidade documental (GIRELLI, 2015a; GIRELLI, 2016b).

A Figura 1 mostra dois documentos de identidade questionados Q1 e Q2, supostamente emitidos pelos Estados do Espírito Santo e de Minas Gerais. As fotografias sugerem tratar-se da mesma pessoa em ambos os documentos. O exame de confronto papiloscópico regular, baseado nas características intrínsecas das impressões, permitiu concluir que, de fato, as impressões digitais foram produzidas pela mesma pessoa. A princípio não há problema algum, afinal todo cidadão é livre para obter licitamente carteira de identidade (RG) em diferentes Unidades da Federação.

Figura 1 - Documentos de identidade questionados Q1 e Q2 contendo imagens de impressões digitais idênticas.

Um exame minucioso das impressões digitais apresentadas na Figura 1 mostrou haver concordância exacerbada entre suas características extrínsecas, algo incompatível com o que seria obtido se para cada documento confeccionado fosse realizada uma coleta própria. As impressões digitais são, na verdade, reproduções de uma mesma imagem. A Figura 2 mostra as referidas impressões digitais presentes nos documentos Q1 e Q2, com o assinalamento de alguns detalhes extrínsecos coincidentes que dificilmente se repetiriam caso fossem feitas coletas distintas (GIRELLI, 2016b).

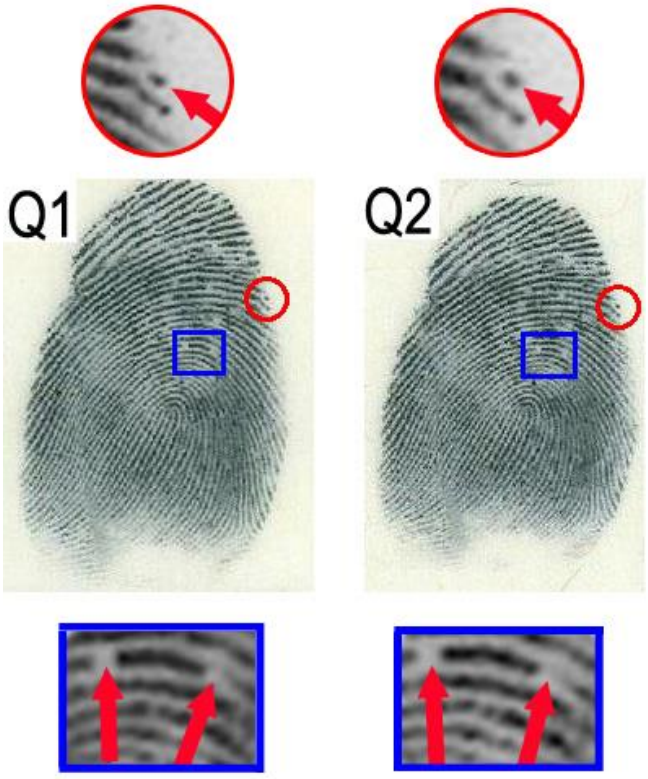

Figura 2 - Impressões digitais presentes nos documentos questionados Q1 e Q2 mostrados na Figura 1, com indicação de alguns detalhes extrínsecos coincidentes. A repetição sistemática dos mesmos detalhes extrínsecos em ambas as impressões levou à conclusão de que elas são reproduções de uma mesma imagem.

Nas regiões demarcadas por círculos vermelhos, reproduzidas em destaque no topo da Figura 2, uma seta indica um ponto que se encontra sobre o contorno da região visível da impressão digital. Aquele ponto corresponde a uma linha papilar que foi interrompida no ato da rolagem do dedo quando da deposição da impressão. Pequenas variações durante a rolagem ou aplicação de pressão ligeiramente diferente entre o dedo e a superfície fariam o ponto tornar-se uma linha ou desaparecer. As regiões destacadas por um retângulo azul reproduzidas em detalhes abaixo das impressões mostram duas falhas na linha papilar, característica imprevisível que geralmente também não se repete em coletas distintas. Em uma impressão padrão referente ao mesmo dedo que se encontra armazenada no AFIS (não mostrada neste artigo) tais falhas não existem.

Além do exemplo citado acima sobre reprodução de uma mesma imagem de impressão digital em diferentes documentos, outras conclusões interessantes também já foram obtidas a partir da análise de detalhes extrínsecos de impressões digitais em documentos falsos (GIRELLI, 2015b; GIRELLI, 2014; GIRELLI, 2016a).

Em um caso analisado por papiloscopistas do Grupo de Identificação da Polícia Federal no Espírito Santo (GID/ES), uma mesma impressão digital foi utilizada em diversos documentos falsos, sendo que em alguns dos documentos ela aparecia de forma revertida, como se vista através de um espelho. A detecção desse tipo de fraude é muito difícil, mesmo com a utilização regular do AFIS e aplicação do método ACE-V (GIRELLI, 2015b; GIRELLI, 2014). A primeira detecção contou com a perspicácia do examinador e com uma série de coincidências favoráveis. A partir de então, o GID/ES estabeleceu um procedimento operacional padrão e novos casos de reversões já foram descobertos (GIRELLI, 2014; GIRELLI, 2016a).

Em outra ocasião, examinadores foram além das buscas convencionais na base de dados do AFIS e pesquisaram por imagens de impressões digitais em fontes abertas disponíveis na *internet*. Obtiveram resultados positivos (GIRELLI, 2016a), o que motivou uma pesquisa mais aprofundada acerca da frequência com que impressões digitais oriundas da *internet* são utilizadas para forjar documentos de identidade no Brasil (GIRELLI, 2016c).

Os resultados da referida pesquisa foram surpreendentes. De 100 imagens de impressões digitais obtidas na *internet*, 34 já foram utilizadas em documentos de identidade falsos, conforme pesquisa realizada no AFIS da Polícia Federal (GIRELLI, 2016c). Novamente, acredita-se que este número seja muito maior, considerando a enorme quantidade de casos apurados em que as impressões digitais não foram incluídas naquele sistema, bem como a imensidão de crimes não investigados.

O fato de que falsificadores utilizam imagens de impressões digitais retiradas da *internet* para confeccionar documentos falsos é uma informação relevante que pode ser explorada para fins de inteligência forense. Antes de tudo, é preciso ter cautela com relação a documentos que apresentem impressões digitais coincidentes, especialmente quando se tem conhecimento de que tal impressão encontra-se disponível na *internet*.

Em um procedimento normal, quando um examinador confronta duas impressões e conclui que foram originadas de uma mesma fonte (mesmo dedo), ele conclui positivamente pela identificação entre elas, o que no AFIS representa assinalar a opção "HIT". Fazendo isso, um link é estabelecido entre os casos, que passam a ficar atrelados no sistema. Ora, se a referida impressão encontra-se livremente disponível para qualquer usuário na *internet*, não se deve assumir que dois documentos apreendidos em ocasiões distintas contendo essa mesma impressão estejam necessariamente correlacionados. Por outro lado, dentro de uma infinidade de imagens de impressões digitais disponíveis na *internet*, seria coincidência a mesma imagem ser utilizada por dois falsificadores independentes. Como proceder, então?

Um recurso potencialmente útil para verificar possíveis *links* entre casos criminais distintos e assim auxiliar a atividade de inteligência forense é a análise espaço-temporal. A título de ilustração, consideremos a situação real citada acima (GIRELLI, 2016c), em que impressões digitais obtidas na *internet* foram utilizadas em documentos falsos. A Figura 3 (GIRELLI, 2016c) indica a distribuição espacial dos 34 casos criminais nos quais documentos falsos contendo impressões da *internet* foram apreendidos. Cada caso criminal é representado por um símbolo. Símbolos iguais repetidos no mapa indicam casos distintos nos quais os documentos apreendidos continham impressões digitais coincidentes. Portanto, a premissa utilizada na análise geográfica da Figura 3 é a existência de link entre casos distintos com base na coincidência de suas impressões digitais. O que se busca, então, é verificar se esse critério é válido, e em que medida.

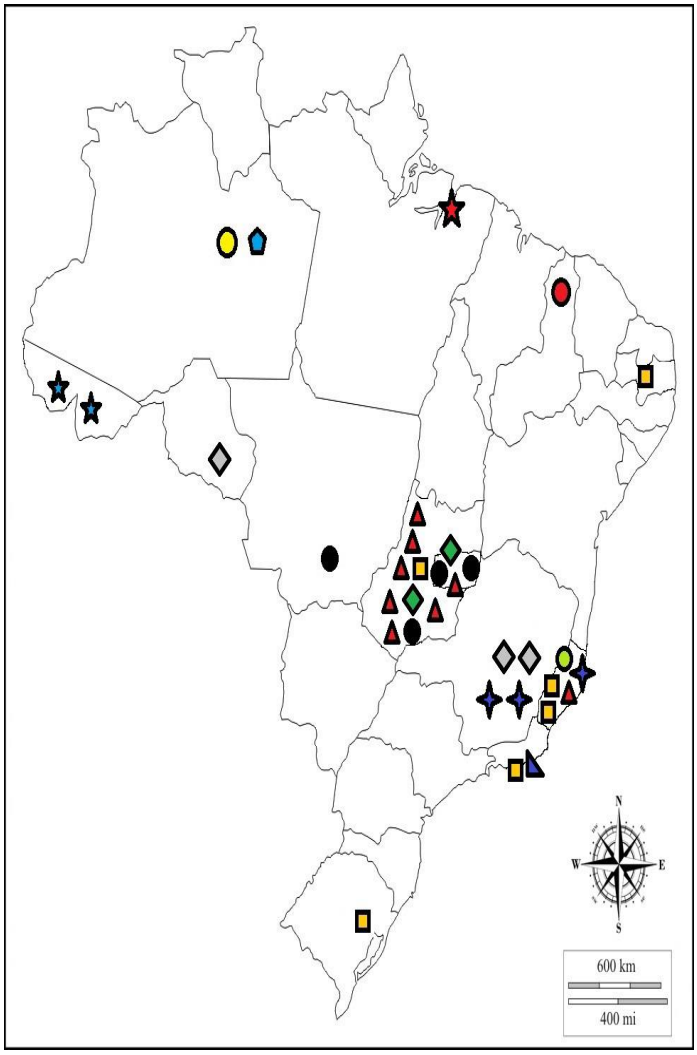

Figura 3 - Representação geográfica da ocorrência de casos criminais onde documentos falsos foram apreendidos. Símbolos iguais indicam casos criminais distintos nos quais documentos apresentavam impressões digitais coincidentes. Em todos os casos mostrados, as impressões digitais presentes nos documentos foram localizadas em páginas da *internet* de livre acesso (GIRELLI, 2016c).

Uma rápida leitura do mapa na Figura 3 permite identificar uma concentração de casos criminais na Região Centro-Oeste e na Região Sudeste, o que em princípio poderia sugerir uma maior tendência de falsificação de documentos nessas regiões. Inferências desse tipo, baseadas na interpretação visual do mapa, devem ser utilizadas em conjunto com informações provenientes de outras fontes.

Nesse sentido, o presente estudo obteve acesso a alguns termos de declaração de pessoas autuadas nos casos em questão. Algumas declarações apontaram a existência de dois pontos de distribuição de documentos falsos, um em cada uma das regiões supracitadas, em conformidade com os resultados obtidos a partir da análise gráfica. Concordâncias dessa natureza fortalecem o produto final da atividade de inteligência, transmitindo maior segurança à autoridade gestora em suas tomadas de decisão.

Ainda no mapa mostrado na Figura 3, é possível notar a estranha ausência de casos criminais no Estado de São Paulo, o mais populoso e não menos afetado pela criminalidade que os demais. Talvez o referido estado não faça inclusões regulares no sistema AFIS, ou a amostragem utilizada neste trabalho tenha sido insuficiente. Uma análise mais profunda dessa ausência de ocorrências em São Paulo e em outros grandes estados brasileiros é necessária, registrando-se aqui essa limitação do presente estudo.

Além da distribuição geográfica, é conveniente apresentar também a distribuição temporal dos referidos casos criminais em que foram utilizadas impressões digitais da *internet*. A Figura 4 (GIRELLI, 2016c) mostra uma linha do tempo, no qual é possível ver a distribuição temporal dos 34 casos criminais mostrados na Figura 3, sendo que os mesmos símbolos utilizados anteriormente foram mantidos para facilitar a análise.

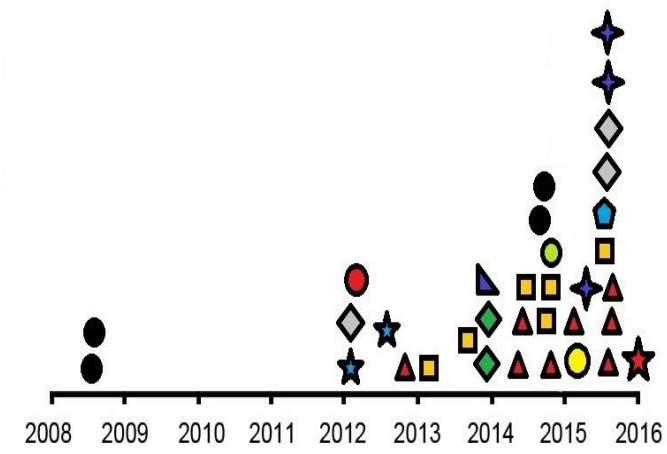

Figura 4 - Distribuição temporal dos casos criminais envolvendo documentos falsos que continham impressões digitais obtidas da *internet*. Símbolos iguais representam casos contendo impressões digitais coincidentes (GIRELLI, 2016c).

Com base na repetição dos símbolos representados em ambos os gráficos das Figuras 3 e 4, é possível notar que algumas impressões digitais aparecem mais vezes do que outras nos documentos falsos considerados neste trabalho. Visando demonstrar o potencial da análise de impressões digitais no contexto da atividade de inteligência forense, tomaremos como exemplo uma categoria de casos com grande representatividade. Consideremos os casos representados por triângulos equiláteros na cor vermelha nas Figuras 3 e 4.

Na Figura 3, nota-se uma concentração dos referidos casos em Goiás e no Distrito Federal, restando apenas um caso isolado no Espírito Santo. A distribuição espacial sugere, então, que a fonte de falsificação esteja localizada provavelmente na Região Centro-Oeste. O caso do Espírito Santo, afastado dos demais, pode ser interpretado de duas maneiras: 1) está correlacionado aos demais (mesma fonte de falsificação), tendo o portador adquirido o documento falso na Região Centro-Oeste e o utilizado no Espírito Santo; ou 2) não está correlacionado aos demais (fontes diferentes); foi produzido por falsificador independente.

Analisando os mesmos crimes na Figura 4, representados por triângulos equiláteros na cor vermelha, é possível ver que um caso ocorreu em 2012 e todos os outros a partir de 2014. Embora os casos não estejam individualmente identificados nas Figuras 3 e 4, cumpre afirmar que o caso cronologicamente afastado dos demais é, de fato, o caso do Espírito Santo. Portanto, a análise cronológica corrobora a análise geográfica no sentido de que o caso do Espírito Santo, apesar de conter impressão digital coincidente com as dos demais casos da Região Centro-Oeste, aparentemente não está vinculado a eles.

A análise dos detalhes extrínsecos das impressões digitais também é pertinente à discussão em tela. A Figura 5 mostra quatro impressões digitais: a primeira (esq.) obtida em página da *internet* (Google Imagens, 2016), e as demais obtidas, respectivamente, em documentos falsos apreendidos em Goiás, Distrito Federal e Espírito Santo. Todas apresentam detalhes intrínsecos suficientes para se afirmar que foram produzidas pela mesma pessoa, sendo sua demonstração desnecessária. As três primeiras apresentam detalhes extrínsecos suficientes para se afirmar que são reproduções de uma mesma imagem, assim como todas as outras da Região Centro-Oeste (não mostradas aqui). Por outro lado, a última impressão mostrada na Figura 5, referente ao documento apreendido no Espírito Santo, é diferente das demais, não se trata

de cópia da mesma imagem utilizada em todos os outros documentos. Com isso, a hipótese de que o documento apreendido no Espírito Santo originou-se de fonte de falsificação diversa dos demais é altamente provável, tendo em vista a convergência apontada pelos resultados da análise geográfica, análise temporal e exame de detalhes extrínsecos das impressões digitais.

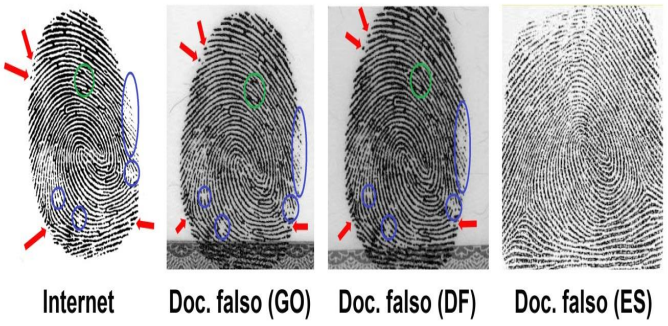

Figura 5 - Impressões digitais obtidas na *internet* (Google Imagens, 2016) e em documentos falsos apreendidos em Goiás, Distrito Federal e Espírito Santo (GIRELLI, 2016c). As quatro impressões apresentam detalhes intrínsecos coincidentes o suficiente para concluir que foram produzidas pela mesma pessoa (dedo). No entanto, apenas as três primeiras possuem detalhes extrínsecos coincidentes o suficiente para concluir que são cópias de uma mesma imagem, diferentes da última impressão digital (ES). Alguns detalhes extrínsecos presentes nas três impressões idênticas e ausentes na última são indicados nas primeiras imagens.

Outro resultado interessante que pode ser deduzido a partir da Figura 5 é com relação à origem das impressões digitais presentes nos documentos falsos apreendidos em Goiás e no Distrito Federal e a imagem equivalente disponível na *internet*. As imagens são idênticas, mas aquelas impressas nos documentos encontram-se sobre a moldura, de modo que a parte inferior da impressão digital se sobrepõe à moldura presente no fundo do suporte. Como a imagem disponível na *internet* não está contaminada com essa sobreposição, conclui-se que as impressões presentes nos documentos foram obtidas da *internet* e não o contrário. Também é curioso notar que o fato de as impressões digitais terem sido impressas sobre a moldura nos documentos apreendidos na região Centro-Oeste pode indicar uma "assinatura" do modus operandi daquela fonte de falsificação.

Através da pesquisa por impressões digitais na *internet* (GIRELLI, 2016c) foi possível também verificar que diversos sites acrescentam marcas d'água com suas logomarcas nas imagens que disponibilizam. Muitas vezes a

marca d'água não é removida da impressão digital pelo falsificador, seja por incapacidade de fazê-lo, por ignorância quanto à presença da marca ou por acreditar que isso não será percebido pelo destinatário a quem o documento será apresentado. A Figura 6 (GIRELLI, 2016c) mostra uma carteira de identidade falsa contendo marca d'água sobre a impressão digital, com indicação de página da *web* (*Google Imagens*, 2016b) onde a imagem foi possivelmente adquirida.

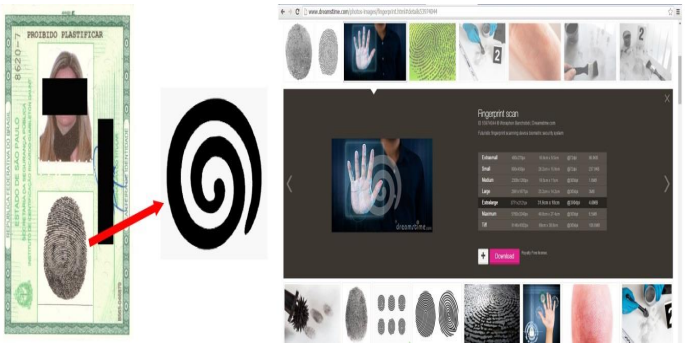

Figura 6 - Documento de identidade falso contendo marca d'água (destacada) sobre a impressão digital, com indicação de página da web (Google Imagens, 2016b) de onde a imagem de impressão digital foi provavelmente baixada. (GIRELLI, 2016c)

A identificação de artefatos na imagem como a marca d'água mostrada na Figura 6 é uma informação digna de registro. Configura objeto de inteligência tática, eis que indica, de pronto, provável falsificação e com isso permite tomada de decisão no âmbito do caso específico. Além disso, tal informação pode também ser utilizada em nível de inteligência operacional ou até estratégica, pois é possível que um mesmo falsificador faça uso de imagens de impressões digitais diferentes, mas obtidas a partir da mesma fonte (mesmo site, por exemplo).

Nesse sentido, a repetição da mesma marca em documentos apreendidos em casos distintos, contendo impressões digitais diferentes, pode indicar um possível link entre os casos, que não seria descoberto pelo processamento convencional da impressão digital através do AFIS nem tampouco pela aplicação do método ACE-V. Links com base em marcas iguais presentes em impressões distintas podem ser testados combinando-se os resultados da análise espacial, análise temporal, exame de detalhes extrínsecos, comparação de perfis e demais informações provenientes da investigação.

6. Conclusão

Conforme demonstrado, as impressões digitais presentes em documentos de identidade possuem características que podem ser exploradas visando produzir inteligência forense em diferentes níveis. A análise espacial e temporal e o exame dos detalhes extrínsecos são alguns exemplos nos quais informações potencialmente relevantes podem ser obtidas.

A análise de perfis é uma ferramenta poderosa na atividade de inteligência policial que encontra aplicação também no âmbito da inteligência forense. No caso de documentos falsos, o perfil pode ser traçado com base em características das impressões digitais e do suporte do documento em conjunto com informações provenientes da própria investigação criminal. A incorporação dos perfis em um banco de dados apropriado e a análise sistemática dessas informações podem realçar links entre casos criminais distintos, ajudando a identificar crimes em série e a localizar fontes de falsificação.

Uma parcela considerável das investigações realizadas pela Polícia Federal está direcionada a fraudes contra instituições públicas federais como o INSS e a Caixa Econômica Federal. Muitos desses crimes são cometidos mediante uso de documentos falsos. Além disso, na maioria dos casos a suposta fraude só é percebida tempos depois do comparecimento do estelionatário ao local, de modo a restar no dossiê arquivado na agência apenas cópia do documento de identidade por ele apresentado. Essa ausência do documento original inviabiliza o exame documentoscópico, mas ainda assim é possível analisar as impressões digitais. Este fato se soma a outros tantos motivos que fundamentam a inclusão de características das impressões digitais na composição do perfil de documentos falsos.

Com base nos argumentos apresentados, este trabalho sugere a implantação de um programa de perfilagem de documentos falsos em âmbito nacional. A Polícia Federal reúne condições para isso, haja vista sua competência estender-se ao longo de todo o território nacional e também pelo fato de possuir, em seu quadro de pessoal, profissionais habilitados para o desempenho das funções requeridas. Tal atividade poderia ser realizada regularmente em suas unidades, em trabalho conjunto entre peritos criminais, papiloscopistas e analistas. O produto da atividade de inteligência forense obtido a partir da análise

dos perfis de documentos falsos apreendidos em todo o país poderia ser usado pela Polícia Federal não apenas para resolver casos isolados, mas para propor soluções abrangentes no combate à criminalidade associada a esses crimes.

Carlos Magno Alves Girelli

Papiloscopista Policial Federal há 12 anos, lotado no Grupo de Identificação da Superintendência Regional no Espírito Santo. Possui graduação em Física (1998) e Direito (2007), mestrado em Física (2001) e pós-graduação em Política e Gestão em Segurança Pública (2009), todos na Universidade Federal do Espírito Santo (UFES). Atualmente é doutorando em Física na UFES, onde também atuou como professor substituto no Departamento de Física em 2002-2003 e 2011-2013.

E-mail: girelli.cmag@dpf.gov.br

Application of Fingerprint Analysis in False Documents in the Field of Police Intelligence: case Study

ABSTRACT

Crimes involving false documents deserve special attention because, among other reasons, cause great harm to the public coffers and put at risk national security by concealing the true identity of terrorists and other wanted criminals. The confrontation policy to these crimes is usually reactive and focused on the evidence. The expert examinations in questioned documents are generally limited to support the specific investigation and produce evidence that will be used strictly in the particular case. No additional intelligence work is done aiming to get a broader view of the problem and a greater understanding of the phenomenon of crime associated enabling propose more comprehensive and effective solutions. This study highlights the importance of intelligence activity in the field of forensic sciences and the need to take a more proactive stance in combating crimes involving false documents. The objective of forensic intelligence is to generate useful information in a timely manner to assist decision making at different levels by the managing authorities. Some potentially useful tools in the examination of documents for forensic intelligence purposes are presented, among them the documents profiling, geographical and temporal distribution analysis of criminal cases and examination of intrinsic and extrinsic details of fingerprints. In this regard, emphasis is given to fingerprints present on documents whose characteristics may indicate counterfeiting trends and modus operandi of the counterfeiters, helping police to identify links between seemingly unrelated crimes and even get to the source of forgery. The study shows some benefits from the analysis of fingerprints on false documents, taking information from actual case basis. Finally, the implementation of a profiling program at national scale, integrating results from fingerprints and documents examination with other information from investigation is suggested.

Keywords: Fingerprint. False Document. Police Intelligence. Forensic Intelligence. Forensic Sciences. Profiling.

La Producción de Inteligencia Forense basada en las Características de las Huellas Dactilares en Documentos Falsos

RESUMEN

Los crímenes de falsedad documental merecen especial atención pues, entre otras razones, perjudican grandemente el patrimonio público y ofrecen riesgo para la seguridad nacional mediante la ocultación de la verdadera identidad de terroristas y otros criminales buscados. La política de confrontación con estos delitos suele ser reactiva y se centra en la prueba. Los exámenes de expertos en documentos generalmente se limitan a satisfacer las necesidades de la investigación específica y producir indicios que serán utilizados estrictamente en este caso. En general, no se realiza un trabajo de inteligencia adicional con el fin de obtener una visión más amplia del problema que permita proponer soluciones más completas y eficaces. Este estudio pone en relieve la importancia de la actividad de inteligencia en el campo de la ciencia forense y la necesidad de adoptar una postura más activa en la lucha contra los delitos relacionados con documentos falsos. El objetivo de la inteligencia forense es generar información útil en el momento oportuno para ayudar en la toma de decisiones, en diferentes niveles, por las autoridades de gestión. Se presentan algunas herramientas potencialmente útiles en el examen de los documentos para fines de inteligencia forense, entre ellos los perfiles de análisis, la representación geográfica y temporal de los casos criminales y los exámenes de los detalles intrínsecos y extrínsecos de las huellas dactilares. En este sentido, se enfatiza las huellas dactilares presentes en los documentos, cuyas características pueden indicar tendencias de falsificación y el modus operandi de los falsificadores, ayudar a la policía a identificar los vínculos entre los crímenes aparentemente no relacionados e, incluso, llegar a la fuente de falsificación. El estudio muestra algunos beneficios a partir del análisis de las huellas dactilares en documentos falsos, usando como ejemplo datos de casos reales. Por último, se sugiere la implementación de un programa de registro de documentos en el ámbito nacional, la integración de los resultados de los exámenes documentoscópicos con otros datos de la investigación.

Palabras Clave: Impresión digital. Documento falso. Inteligencia de la Policía. Información de inteligencia. Ciencias Forenses. Perfilado.

Referências

AEPLI, P.; RIBAUX, O.; SUMMERFIELD, E. **Decision Making in Policing**. Lausanne: EPFL Press, 2011.

ANDRADE, F. S. "Inteligência policial: efeitos das distorções no entendimento e na aplicação". **Revista Brasileira de Ciências Policiais**, vol. 3 (2): 37-54, 2012.

AUBERSON, M.; BAECHLER, S.; ZASSO, M.; GENESSAY, T.;

PATINY, L.; ESSEIVA, P. "Development of a systematic computer vision-based method to analyse and compare images of false identity documents for forensic intelligence purposes-Part I: Acquisition, calibration and validation issues". **Forensic Science International**, vol. 260: 74-84, 2016.

BAECHLER, S. **Comunicação pessoal de Simon Baechler em 20.01.2016**.

BAECHLER, S.; MORELATO, M.; RIBAUX, O.; BEAVIS, A.; TAHTOUH, M.; KIRKBRIDE, P.; ESSEIVA, P.; MARGOT, P.; ROUX, C. "Forensic intelligence framework. Part II: Study of the main generic building blocks and challenges through the examples of illicit drugs and false identity documents monitoring, **Forensic Science International**, vol. 250: 44-52, 2015.

BAECHLER, S.; RIBAUX, O.; MARGOT, P. "Toward a novel forensic intelligence model: systematic profiling of false identity documents". **Forensic Science Policy & Management: An International Journal**, vol. 3 (2): 70-84, 2012.

BAECHLER, S.; TERRASSE, V.; PUJOL, J. –P.; FRITZ, T.; RIBAUX, O.; MARGOT, P. "The systematic profiling of false identity documents: Method validation and performance evaluation using seizures known to originate from common and diferente sources". **Forensic Science International,** vol. 232: 180-190, 2013.

BRASIL. **Lei n° 12.037, de 1° de outubro de 2009.** Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm. Acesso em: 30.04.2016.

BRASIL. **Lei n° 9.503, de 23 de setembro de 1997**. Institui o Código de Trânsito Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9503.htm. Acesso em: 30.04.2016.

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

DÉGARDIN, K.; ROGGO, Y.; MARGOT, P. "Forensic intelligence for medicine anti-counterfeiting". **Forensic Science International**, vol. 248: 15-32, 2015.

FONSECA, G. D. "O Profiling nos aeroportos como ferramenta de prevenção ao terrorismo". **Revista Brasileira de Ciências Policiais**, vol. 3 (2): 107-128, 2012.

GIRELLI, C. M. A. "Application of a Standard Procedure to Avoid Errors When Comparing Fingerprints with Their Reversals in Fake Documents". **Journal of Forensic Science and Medicine**, vol. 2: 60-64, 2016a.

GIRELLI, C. M. A. "Detecção de Impressões Digitais Revertidas em Documentos Falsos". **Revista Brasileira de Ciências Policiais**, vol. 5 (2): 11-29, 2014.

GIRELLI, C. M. A. "Fingerprints: Beyond the source". **Journal of Forensic Identification**, vol. 66 (3): 187-195, 2016b.

GIRELLI, C. M. A. "Impressões papilares podem revelar mais do que a identidade de seus autores". **Brazilian Journal of Forensic Sciences**, Medical Law and Bioethics, vol. 5 (1): 28-41, 2015a.

GIRELLI, C. M. A. "Laterally Reversed Fingerprints Detected in Fake Documents". **Journal of Forensic Identification**, vol. 65 (1): 1-17, 2015b.

GIRELLI, C. M. A. "The use of fingerprints available on the web in false identity documents: Analysis from a forensic intelligence perspective". **Forensic Science International**, vol. 262: 84-96, 2016c.

Google Imagens. Disponível em https://www.google.com.br/search?q=fingerprint&biw=1600&bih=795&site=webhp&source=lnms&tbm=isch&sa=X&sqi=2&ved=0ahUKEwixjvfNnafKAhWKFZAKHYzlAFYQ_AUIBigB#imgrc=iG6zoNFkG8_wZM%3A. Acesso em: 13.01.16. (a)

Google Imagens. Fingerprint Stock Photos, Images, & Pictures. Disponível em: www.dreamstime.com/photos-images/fingerprint.html#details53974044. Acesso em: 20.01.16. (b)

HANNAM, A. G. "Trends in converted firearms in England & Wales as identified by the National Firearms Forensic Intelligence Database (NFFID) between September 2003 and September 2008". **Journal of Forensic Sciences**, vol. 55 (3): 757-766, 2010.

MARGOT, P. "A question of time". **Science & Justice**, vol. 40 (2): 64-71, 2000.

MORELATO, M.; BEAVIS, A.; TAHTOUH, M.; RIBAUX, O.; KIRKBRIDE, P.; ROUX, C. "The use of forensic case data in intelligence-led policing: The example of drug profiling". **Forensic Science International**, vol. 226: 1-9, 2013.

PETERSON, M. **Intelligence-led policing: The new intelligence architecture**. Washington: U.S. Department of Justice (Ed.), 2005.

RATCLIFFE, J. H. **Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders**. Washington: U.S. Department of Justice (Ed.), 2007.

RATCLIFFE, J. H. **Intelligence-led Policing, Trends & Issues in Crime and Criminal Justice**. Camberra: Australian Institute of Criminology, 2003.

RIBAUX, O.; BAYLON, A.; ROUX, C.; DELÉMONT, O.; LOCK, E.; ZINGG, C.; MARGOT, P. "Intelligence-led crime scene processing. Part I: Forensic intelligence". **Forensic Science International**, vol. 195 (1-3): 10-16, 2010.

RIBAUX, O.; GIROD, A.; WALSH, S. J.; MARGOT, P.; MIZRAHI, S.; CLIVAZ, V. "Forensic intelligence and crime analysis". **Law, Probability & Risk**, vol. 2: 47-60, 2003.

SINIC. **Sistema Nacional de Informações Criminais.** Ministério da Justiça – Polícia Federal, BRASIL (Acesso em: 06.01.16).

SWGFAST. **Scientific Working Group on Friction Ridge Analysis, Study and Technology.** Document #10 Standards for Examining Friction Ridge Impressions and Resulting Conclusions (Latent/ Tenprint). Ver. 2.0. September 13, 2013. Disponível em: http:// swgfast.org/documents/examinations-conclusions/130427_ Examinations-Conclusions_2.0.pdf. Acesso em: 22.04.2015.

WEYERMANN, C.; MARQUIS, R.; DELAPORTE, C.; ESSEIVA, P.; LOCK, E.; AALBERG, L.; BOZENKO Jr., J. S.; DIECKMANN, S.; DUJOURDY, L.; ZRCEK, F. "Drug intelligence based on MDMA tablets data: I. Organic impurities profiling". **Forensic Science International**, vol.177 (1): 11-16, 2008.