

O uso de bancos de dados biométricos civis em investigações criminais: possíveis avanços à luz de direitos e garantias fundamentais

The use of civilian biometric databases in criminal investigations: possible advances in the light of fundamental rights and guarantees

El uso de bases de datos biométricos civiles en investigaciones criminales: posibles avances a la luz de los derechos y garantías fundamentales

Natalie Alves Lima

RESUMO

O Brasil não possui uma legislação que verse expressamente a respeito da possibilidade de utilização de bancos de dados biométricos civis, especialmente aqueles constituídos por órgãos públicos, como padrões no processo de investigação e identificação criminal. Entretanto, tal situação se tornou costumeira, mediante o acesso dos órgãos com função de polícia judiciária aos referidos bancos de dados, o que é legitimado por meio dos chamados “acordos de cooperação”. Mencionada temática gera repercussões na seara constitucional e infraconstitucional. O cenário que se revela é de um potencial questionamento da licitude quanto à

utilização desses bancos para fins criminais. Entende-se, contudo, que a ausência de uma legislação que disponha expressamente sobre a produção da prova pericial com base no confronto entre vestígios e padrões biométricos oriundos de bancos de dados civis não é capaz, por si só, de ocasionar a ilicitude e a ilegitimidade da prova pericial produzida. A despeito disso, a edição de lei específica para esse fim é capaz de conferir maior segurança jurídica e legitimidade incontroversa a exames periciais produzidos nessas circunstâncias.

Palavras-chave: banco de dados biométricos; acordos de cooperação; compartilhamento; identificação criminal; exame pericial.

ABSTRACT

Brazil does not have legislation that expressly relates to the possibility of using civil biometric databases, especially those constituted by public agencies, as a standard in the investigation and criminal identification process. However, this situation has become customary, through the access of the judicial police to these databases, which is legitimized through so-called "cooperation agreements". Mentioned theme generates repercussions in the constitutional and infra-constitutional area. The scenario that is revealed is a potential questioning of the lawfulness regarding the

use of these banks for criminal purposes. It is understood, however, that the absence of legislation that expressly deals with the production of expert evidence on the basis of the confrontation between traces and biometric patterns derived from civil databases is not capable, in itself, of causing the unlawfully and illegitimacy of the expert evidence produced. Despite this, the edition of a specific law for this purpose is capable of conferring greater legal certainty and uncontroversial legitimacy to expert examinations produced in these circumstances.

Keywords: *biometric database; cooperation agreements; sharing; criminal identification; expert examination.*

RESÚMEN

Brasil no tiene una legislación que expresamente trate acerca de la posibilidad de utilización de bancos de datos biométricos civiles, en especial aquellos constituidos por los órganos públicos, como un estándar en el proceso de investigación e identificación criminal. Sin embargo, tal situación se ha convertido en una costumbre, en que se permite el acceso de las policías judiciales a estos bancos de datos, legitimados a través de los “acuerdos de cooperación”. Dicha temática, tiene repercusiones en los temas constitucionales e infra constitucionales. El escenario que se crea es de un potencial

cuestionamiento de la licitud del uso de estas bases de datos con fines delictivos. Se entiende, sin embargo, que la ausencia de una legislación que se ocupa expresamente de la producción de pruebas periciales basadas en la confrontación entre los rastros y patrones biométricos procedentes del banco de datos civiles no sea capaz, por sí misma, de ocasionar la ilicitud y la ilegitimidad de la prueba pericial producida. A pesar de ello, la promulgación de una ley específica para este fin es capaz de conferir una mayor seguridad jurídica y una legitimidad incontrovertible a los exámenes periciales realizados en estas circunstancias.

Palabras claves: *banco de datos biométricos; acuerdo de cooperación, intercambio; identificación criminal; examen pericial.*

INTRODUÇÃO

A utilização da biometria envolve uma situação de determinação de origem ou fonte, em que a identificação ocorrerá por meio do cotejo entre materiais padrão, oriundos de suspeitos ou bancos dados, e materiais questionados, que são os vestígios que estão de alguma forma relacionados com o contexto do crime que está sendo investigado. Por consequência, será

permitido ao perito criminal oficial esclarecer se o material padrão é ou não a fonte do vestígio (VALENTE, 2012 *apud* GONÇALVES JUNIOR; PEDRINI, 2019).

Dentre as diversas áreas de estudo da biometria forense, vale considerar a papiloscopia forense, que objetiva identificar o indivíduo a partir de marcas únicas decorrentes das pontas dos dedos, palma das mãos e planta dos pés. A papiloscopia na biometria forense se revela como uma metodologia de identificação célere, prática e que demanda um menor empenho de recursos (YAMASHITA, 2011 & SENNA, 2014 *apud* SILVA, 2021).

Observa-se, portanto, que a papiloscopia forense é um dos principais meios de esclarecimento de identificação de determinado indivíduo em uma investigação criminal. Entretanto, esta área da biometria forense pode ter a sua importância reduzida, uma vez que os agentes públicos responsáveis pela investigação nem sempre dispõem de materiais padrão para lhes auxiliar na identificação do vestígio em análise.

Com o objetivo de afastar o comprometimento das investigações criminais, uma das propostas utilizadas foi a celebração dos chamados “acordos de cooperação”, em que entes públicos permitem o acesso dos órgãos com função de polícia judiciária aos seus bancos de dados biométricos civis, de maneira que passam a

ser utilizados como padrão no processo de identificação criminal.

O referido caminho contribuiu para o andamento das investigações criminais, realizando, com mais verticalidade, o direito à segurança pública. Contudo, sob alguns aspectos, é possível suscitar uma situação de falta de segurança jurídica para as partes envolvidas no curso da ação criminal, visto que o Brasil não dispõe de uma legislação específica que trate ou regulamente a produção de provas periciais criminais com base em padrões biométricos de origem civil — pelo que se faz possível questionamento quanto à legalidade dessa situação, tendo em vista garantias dispostas no ordenamento jurídico brasileiro, tanto no âmbito constitucional quanto infraconstitucional.

Assim, tendo como base a área papiloscópica da biometria forense, o presente artigo possui o objetivo de analisar as possíveis implicações que a ausência de uma lei específica que disponha sobre os “acordos de cooperação” poderá acarretar, bem como busca propor soluções que objetivem proporcionar mais segurança jurídica para os sujeitos envolvidos na investigação criminal.

1 PRODUÇÃO DE PROVA PERICIAL NO BRASIL COM BASE EM INFORMAÇÕES BIOMÉTRICAS OBTIDAS DE BANCOS DE DADOS BIOMÉTRICOS CIVIS

CONSTITUÍDOS POR ÓRGÃOS PÚBLICOS

1.1 Constituição de banco de dados biométricos por órgãos públicos

Vale esclarecer e exemplificar que em uma situação na qual se solicita a expedição de um documento de identidade (Lei n.º 7.116/1983 e Decreto n.º 10.977/2022) (BRASIL, 1983, 2022), a expedição de um passaporte (Decreto n.º 1.983/1996), o acesso a uma plataforma para o usufruto de serviços públicos (Decreto n.º 8.936/2016 e Decreto n.º 10.977/2022) (BRASIL, 2016, 2022) e até mesmo a emissão e/ou renovação do título de eleitor (Resolução n.º 23.659/2021) (TSE, 2021), as condições normativas estabelecidas são a identificação e a coleta de dados biométricos do cidadão solicitante.

Para além do mencionado aspecto legal, é possível dizer que se tornou algo corriqueiro e até mesmo natural a coleta de impressões digitais como condição para acessar determinado serviço ou obter a expedição de um documento no âmbito público, que em um primeiro momento não tem gerado questionamentos ou discussões por parte daqueles que fornecem os seus dados biométricos.

A situação a ser considerada é que as impressões digitais coletadas pelos órgãos públicos não são descartadas após o fornecimento do produto ou serviço

ensejadores, mas permanecem armazenadas até que, em momento posterior, seja necessária a conferência ou verificação biométrica, considerando o contexto em que foram coletadas.

Portanto, observada a exigência de um órgão público de fornecimento de dados biométricos por parte do cidadão interessado para o alcance de finalidades civis, essa conduta de coletar, armazenar, organizar e manter dados de impressões digitais, com o intuito de serem acessados posteriormente quando necessário, é o que caracteriza a constituição dos bancos de dados biométricos civis no âmbito público.

1.2 Conduta de compartilhamento de bancos de dados biométricos civis geridos por órgãos públicos com o objetivo de se tornarem padrão para exames periciais criminais

Extrai-se, a partir disso, que os dados biométricos recolhidos pelos órgãos públicos representam uma fonte segura, única e precisa de identificação do cidadão, cuja reunião em um banco de dados se tornou mecanismo substancialmente completo de controle e aferição informacional nas finalidades civis que se pretende alcançar.

Um dos exemplos de completude e relevância de banco de dados biométricos civil é o constituído pela Justiça Eleitoral no Brasil. Desde o momento em que o Tribunal

Superior Eleitoral começou o cadastramento biométrico dos eleitores brasileiros em 2008, objetivando a modernização e a ampliação da segurança no processo eleitoral, formou-se o maior banco de dados biométricos das Américas, contemplando cerca de 120 milhões de registros (TSE, 2022).

Por sua vez, os órgãos com função de polícia judiciária enfrentam o contexto de não disporem de um banco de dados com padrões biométricos completos, muitas vezes com o número de registros substancialmente reduzidos em razão de sua circunscrição, no processo de identificação de pessoas com base em vestígios de impressões digitais coletados em cenas de crime, o que compromete as chances de êxito do trabalho pericial papiloscópico realizado para a identificação dos possíveis sujeitos envolvidos no crime.

Diante da necessidade de padrões de dados biométricos nos exames periciais e considerando as informações constantes nos bancos de dados civis, é que se observa a ascendência da celebração dos chamados “acordos de cooperação”. Uma de suas vertentes está representada no fato de um ente público permitir o acesso de órgãos com função de polícia judiciária ao seu banco de dados de registros biométricos oriundos da coleta para o alcance de finalidades civis (dados biométricos civis), a fim de que seja utilizado como padrão em exames periciais criminais.

Exemplificando, a impressão digital coletada de um cidadão para a expedição de um documento, com intuito estritamente civil, será armazenada no banco de dados biométricos do órgão expedidor. Posteriormente, tendo em vista a celebração do “acordo de cooperação”, será permitido que órgãos com função de polícia judiciária acessem a referida base de dados e utilizem as impressões digitais nela constantes como padrão de comparação para a aferição de eventual compatibilidade com vestígios biométricos encontrados em locais de crime, possibilitando ou não a identificação da pessoa no exame pericial criminal realizado.

Nesse sentido, para melhor elucidação, é relevante analisar alguns exemplos de condutas de compartilhamento de dados biométricos adotadas pelo Tribunal Superior Eleitoral nos últimos anos.

Em 2017, a Polícia Federal e o Tribunal Superior Eleitoral celebraram acordo de cooperação técnica, em que

o TSE poderá utilizar a base de dados da Polícia Federal no processo de identificar os eleitores por meio da impressão digital, enquanto a Polícia Federal poderá utilizar os dados do TSE para pesquisa de fragmentos de digitais, no caso de investigações criminais (TSE, 2017).

Outro exemplo ocorreu em novembro de 2021, quando o Governo do Estado de Minas Gerais, representando a Polícia Civil,

também celebrou acordo de cooperação técnica com o Tribunal Superior Eleitoral de compartilhamento de dados biográficos e biométricos:

O sistema irá viabilizar a pesquisa de latentes dactilares coletadas em cenas de crime pela Polícia Civil em confronto com os bancos de dados de impressões digitais decadaactilares de identificação civil e criminal, de latentes dactilares não resolvidas e, ainda, a pesquisa facial, auxiliando na identificação de autores de crimes (MINAS GERAIS, 2021).

Posteriormente, o Tribunal Superior Eleitoral também firmou acordo de cooperação técnica com o Instituto-Geral de Perícias do Rio Grande do Sul (IGP), em que ficou autorizado que a sua área papiloscópica poderia pesquisar a base de dados biométricas da corte eleitoral:

A perícia papiloscópica do IGP conta com mais uma ferramenta para auxiliar na resolução de crimes, em que seja necessário identificar o autor de vestígios por meio das impressões digitais. Um convênio firmado com o TSE permite que o IGP acesse o banco biométrico do tribunal para pesquisa de indivíduos (IGP, 2021).

Com efeito, os “acordos de cooperação” técnica, em um primeiro momento, atendem a interesses mútuos dos celebrantes, posto que haverá a integração,

transferência e aproveitamento de dados biométricos entre o órgão público cedente do banco de dados civis e o respectivo órgão responsável pela realização da perícia criminal, que poderá ter maiores chances de êxito em sua atividade investigativa.

1.3 Identificação criminal: ausência de previsão constitucional e legal expressas para o fornecimento e a utilização de dados biométricos integrantes de bancos civis como padrão em exames periciais criminais

Quando se observa o direito fundamental de não identificação criminal do civilmente identificado, salvo hipóteses legais (art. 5º, inc. LVIII, CF) (BRASIL, 1988), tem-se a ideia de que a identificação criminal pressupõe que a autoridade policial conheça o investigado e/ou autor de um crime e a faça de maneira direta/presencial, em que o agente público só prossiga com a coleta dos dados necessários à identificação criminal se estiver na presença do investigado ou autor, circunstância que pode ser definida como uma situação de identificação criminal direta.

Sucedem que a identificação criminal descrita no art. 5º, inc. LVIII, da CF/88, não se restringe à referida circunstância, pelo que se faz possível sua aplicação por outras formas, capazes de conferir plena eficácia ao processo de identificação criminal

(MENDES; BRANCO, 2021). Por conseguinte, é possível pontuar que a identificação criminal também ocorre por uma via indireta, em que mesmo sendo desconhecido o autor de determinado crime, são empregados os meios necessários para a identificação e atribuição de uma situação de autoria.

À vista disso, a identificação criminal deve ser encarada como o processo em que o Estado adota meios com o intuito de registrar a inserção direta ou indireta de determinada pessoa no contexto de uma prática criminosa investigada. E, para tanto, a autoridade investigadora deverá considerar e utilizar apenas os meios correlacionados ao âmbito da investigação criminal ou empregar aqueles alheios, desde que expressamente autorizados em lei (MENDES; BRANCO, 2021).

A necessidade de que os meios empregados na identificação criminal sejam inerentes ao contexto da investigação criminal, ou, ainda que diversos, sejam autorizados por lei, decorre da aplicação do princípio da não autoincriminação (*nemo tenetur se deterege*), em que se “assegura ao suposto autor de crime (investigado, denunciado, testemunha) o direito de não produzir prova contra si mesmo” (QUEIROZ, 2017). Logo, o fornecimento ou coleta de materiais que dependam de ação ou consentimento prévio do indivíduo recebe o amparo do referido princípio, a fim de que

posteriormente não se tornem provas contra si.

Nesse contexto, o Brasil já possui avanços com disposições legislativas referentes à identificação criminal mediante o emprego de procedimentos e técnicas, inicialmente não inseridos no âmbito da investigação criminal, qual seja, a obtenção de perfil genético e o armazenamento em banco de dados, a partir do advento da Lei n.º 12.654/2012 (BRASIL, 2012).

Para tanto, a mencionada legislação inseriu na Lei n.º 12.037/2009 a possibilidade de a identificação criminal ocorrer por meio da coleta de material biológico para a obtenção do perfil genético durante as investigações policiais, mediante autorização judicial (arts. 1º e 2º, Lei n.º 12.654/2012) (BRASIL, 2012). Além do mais, abriu-se espaço na Lei de Execução Penal (Lei n.º 7.210/1984) para ser obrigatória a coleta de material genético de condenados por crimes contra a vida, violência grave e sexuais (BRASIL, 2019).

Desse modo, os dados genéticos oriundos das supracitadas circunstâncias são armazenados em um banco de dados sigilosos, dentre eles o denominado Banco Nacional de Perfis Genéticos (BNPG) (Decreto n.º 7.950/2013) (BRASIL, 2013), de maneira que é possibilitado ao perito criminal autorizado acessá-lo com o objetivo de verificar a compatibilidade de vestígios e

a possível identificação do agente em determinada investigação criminal.

Quando uma impressão digital oriunda de um banco de dados civil é utilizada como padrão de confronto para se verificar a compatibilidade e identificação com o vestígio biométrico coletado no local de um crime, também se tem a consumação de uma forma de identificação criminal.

Entretanto, contrariando a referida tendência de regulamentação quanto à coleta, armazenamento e utilização de material genético nas investigações e identificações criminais, são singelas as previsões legais e regulamentares acerca da possibilidade de compartilhamento de impressões digitais de bancos civis com órgãos de segurança com o objetivo precípuo de identificação criminal. As poucas normatizações que aludem à integração e ao compartilhamento de base de dados biométricos são genéricas e omissas quanto à possibilidade específica de utilização como padrão em exames periciais criminais.

Para tanto, é possível exemplificar com o art. 9º, § 4º, da Resolução n.º 23.659/2021, do Tribunal Superior Eleitoral:

Art. 9º (...)
§ 4º O Tribunal Superior Eleitoral poderá firmar acordos de cooperação com entidades públicas ou privadas, visando à ampliação, transferência ou aproveitamento de dados biométricos, ouvida a Corregedoria-

Geral Eleitoral (TSE, 2021).

Além do mais, cumpre mencionar o art. 3º, § 2º, da Lei n.º 13.444/2017, a respeito das disposições que o Tribunal Superior Eleitoral poderá dar aos dados biométricos quanto aos órgãos com função de polícia judiciária:

Art. 3º O Tribunal Superior Eleitoral garantirá aos Poderes Executivo e Legislativo da União, dos Estados, do Distrito Federal e dos Municípios acesso à base de dados da ICN, de forma gratuita, exceto quanto às informações eleitorais.

§ 2º Ato do Tribunal Superior Eleitoral disporá sobre a integração dos registros biométricos pelas Polícias Federal e Civil, com exclusividade, às suas bases de dados (BRASIL, 2017).

O reconhecimento da necessidade de integração de banco de dados biométricos para se alcançar finalidades como ampliação, interoperabilidade e unificação de bancos de dados biométricos, com os “acordos de cooperação” celebrados, é o que justifica e concebe aspecto de legalidade ao compartilhamento de bancos de dados biométricos civis, por parte dos entes públicos detentores desses dados, com os órgãos com função de polícia judiciária.

Por outro lado, uma vez permitido o acesso a prontuários biométricos civis, tornou-se um “costume” a sua utilização

como padrão em investigações criminais, não obstante a ausência de uma expressa legislação que disponha sobre a identificação criminal nessa circunstância.

Portanto, quando há a utilização de dados biométricos constituídos em relações civis em investigações criminais, suscita-se uma possível e potencial violação da previsão constitucional do art. 5º, inc. LVIII, da Constituição Federal e do princípio da não autoincriminação, dado que a identificação criminal de determinado indivíduo decorre de uma circunstância alheia ao contexto criminal, sem que haja previsão legal expressa para tanto.

1.4 Tratamento de dados biométricos frutos de bancos civis para fins criminais: análise à luz da Lei Geral de Proteção de Dados Pessoais — Lei n.º 13.709/2018

Para além do plano constitucional, a ausência de uma legislação expressa que trate da possibilidade de emprego de dados biométricos de prontuários civis em investigações criminais também apresenta implicações que devem ser analisadas sob o plano infraconstitucional, sendo consideradas as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018).

A LGPD apresenta disposições que possuem como objetivo a proteção de direitos fundamentais relacionados às

liberdades, privacidade e desenvolvimento da personalidade decorrentes das informações inerentes à pessoa natural (MPF, 2022). A referida legislação reafirma que a titularidade dos dados é da pessoa que os fornece, de maneira que são asseguradas condições para que possa dispor deles.

O dado biométrico recebe a classificação de dado pessoal sensível (art. 5º, inc. II, LGPD), motivo pelo qual é empregada a regra de que as operações de tratamento aplicadas sobre ele devem atender a finalidades específicas e que dependem do consentimento do seu titular (art. 11, inc. I, LGPD) (BRASIL, 2018). De outra maneira, pelo fato de os dados biométricos possuírem uma natureza personalíssima, inerentes ao valor humano, a sua coleta deverá atender a destinações específicas que serão esclarecidas e consentidas pelo titular.

Considerando o contexto do presente artigo, vale observar que a referida regra do consentimento do titular é excetuada quando o tratamento de dados pessoais sensíveis ocorre: i) para cumprimento de obrigação legal ou regulatória; ii) para situações em que o compartilhamento seja necessário à execução de políticas públicas previstas em lei pela administração pública (art. 11, inc. II, *alíneas “a” e “b”*, LGPD) (BRASIL, 2018).

Uma das circunstâncias de aplicação das mencionadas exceções pode ser percebida nas motivações do Tribunal Superior Eleitoral para celebrar os “acordos

de cooperação” com os órgãos com função de polícia judiciária quanto a bancos de dados biométricos, que decorre da necessidade de constituir, integrar e gerir a Identificação Civil Nacional (ICN) instituída pela Lei n.º 13.444/2017 (arts. 2º e 3º) (BRASIL, 2017).

Entretanto, essa prescindibilidade do consentimento do titular em situações específicas de tratamento de dados pessoais sensíveis não parece ser autorizativa de disposição absoluta pelo Poder Público. O ente público deve ser amparado em preceito legal que autorize tal disposição, e, sobretudo, está adstrito àquelas finalidades públicas que se pretende alcançar com a legislação autorizadora, sem prejuízo da publicização da dispensa da autorização, dos procedimentos e das práticas aplicadas (art. 11, § 2º c/c art. 23, *caput* e inc. I, LGPD) (BRASIL, 2018).

Tem-se que o banco de dados biométricos de origem civil tratado por uma entidade pública deve primeiramente atender às finalidades que ensejaram a sua constituição (art. 6º, inc. I, LGPD) (BRASIL, 2018).

E, na excepcional situação de ser tratado ou operado em outra circunstância sem a autorização do titular, esse novo contexto deverá ocorrer para o atendimento daquela finalidade pública estabelecida na legislação autorizadora, de maneira que o agente público não poderia prosseguir com situações de compartilhamento de

prontuários biométricos civis para finalidades onde a legislação não prevê, sob pena de incorrer em potencial violação a direitos e garantias fundamentais.

Ainda com base no exemplo da Lei n.º 13.444/2017, se a legislação autoriza o compartilhamento de bancos de dados biométricos civis constituídos pelo Poder Público para o alcance de uma outra finalidade pública civil, constituir uma única base de dados biométricos para identificar o brasileiro nas relações sociais e organizacionais com entes governamentais e privados (BRASIL, 2017) significaria violar, no momento em que se destina outra finalidade, os dispositivos e objetivos da LGPD, notadamente na hipótese de utilização desses dados como padrão para identificação criminal nos exames periciais realizado.

É possível que se suscite o argumento de que dados biométricos de origem civil poderiam ser utilizados como padrão em exames periciais criminais independentemente da regra do consentimento, porquanto as disposições da LGPD não se aplicariam a situações de tratamento de dados pessoais praticados em “atividades de investigação e repressão de infrações penais” (art. 4º, inc. III, *alínea* “d”) (BRASIL, 2018).

Convém pontuar, entretanto, que a referida norma de exceção parece estar circunscrita apenas a dados pessoais já

inseridos no contexto penal. Isto é, as disposições de tratamento de dados pessoais previstos na LGPD não contemplam os dados pessoais coletados, obtidos e/ou constituídos no bojo da investigação criminal, por exemplo, no Banco Nacional de Perfis Genéticos (BNPC).

Contudo, se a obtenção e/ou utilização de um padrão biométrico para determinada investigação criminal depende do acesso ou emprego de um prontuário biométrico que não tenha a sua origem no âmbito criminal, valendo-se, por exemplo dos “acordos de cooperação” com bancos de dados biométricos civis, é possível interpretar-se que não está comportada a aplicação da exceção do art. 4º, inc. III, alínea “d”, da LGPD.

2 PERSPECTIVA INTERNACIONAL DE UTILIZAÇÃO DE INFORMAÇÕES BIOMÉTRICAS CIVIS EM INVESTIGAÇÕES CRIMINAIS

Em 2010, o *Federal Bureau of Investigation* (FBI) anunciou a implementação do chamado “*Next Generation Investigation*” (NGI), sendo uma versão avançada e melhorada de repositório de dados biométricos, em que uma única plataforma passou a permitir a utilização, a varredura e o cruzamento de dados como: impressões digitais, reconhecimento facial,

reconhecimento de íris e reconhecimento de voz, por exemplo (FBI, 2022a).

Para aumentar o número de dados biométricos, ter uma maior precisão no processo de identificação biométrica e compartilhamento de informações de histórico criminal, o FBI anunciou em 2014 que o NGI passaria a reter as informações de impressões digitais de origem civil que a ele fossem submetidas. Assim, o cidadão que estiver cadastrado nesse sistema será submetido à identificação para fins civis e/ou criminais, independentemente da origem de seus dados biométricos (NEGRON, 2015 *apud* CARRERO, 2018).

É esclarecido que a “*Public Law 92-544*” autoriza o FBI a receber dados biométricos civis para analisar e compartilhar os antecedentes criminais de um cidadão em razão de determinado processo de licenciamento, emprego ou outro benefício em que a ausência de infrações penais seja imprescindível (FBI, 2015). À vista disso, ao receber tais informações, o FBI utiliza o dispositivo “*28 U.S. Code § 534*” de maneira a legitimar a retenção de tais dados biométricos no NGI e utilizá-los, ainda que para fins criminais (DELILLO, 2015).

Sucedem que uma das principais críticas colocadas está no fato de os Estados Unidos, assim como o Brasil, não disporem de uma legislação específica que autorize referida modalidade de tratamento de dados. É observado que o FBI tenta atribuir aspecto

de legalidade às operações do NGI com base em uma interpretação ampliada da mencionada norma, transbordando a finalidade proposta pelo estatuto, da confiança pública e das liberdades individuais (DELILLO, 2015).

Um dos riscos apontados pelo FBI, por meio de um *Privacy Impact Assessment* (PIA), está no fato de que o indivíduo desconhece com quem suas impressões digitais serão compartilhadas e em quais finalidades serão utilizadas. Por outro lado, a mitigação do risco é assegurada com base na apresentação do “*Privacy Act*” ao cidadão solicitante, que esclarecerá que as impressões digitais civis serão retidas e que só poderão ser utilizadas como padrão biométrico em investigações civis e criminais (FBI, 2015).

Convém observar que a supracitada mitigação de risco, em verdade, se revela como uma imposição ao cidadão americano para que autorize o armazenamento e o compartilhamento/utilização de seus dados biométricos nas finalidades civis e criminais. Isso pelo fato de que o formulário de impressão digital do solicitante, do qual consta o “*Privacy Act*”, traz a seguinte mensagem: “*providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application*” (FBI, 2022b).

Ou seja, o aspecto de voluntariedade e consentimento do cidadão requerente é de

alguma maneira afastado na medida em que o fornecimento de suas impressões digitais se torna condição para que obtenha licenças, autorizações, acesse empregos ou outros serviços em que haja a exigência de fornecimento do dado biométrico.

Ainda, vale observar que, em um primeiro momento, as informações constantes no NGI estarão disponíveis somente para os órgãos integrantes do “*Department of Justice (DOJ)*”. Entretanto, é permitido o amplo compartilhamento dos dados de impressões digitais civis a outras agências federais, estaduais ou locais dos Estados Unidos, desde que haja disposições normativas autorizadoras para tanto (FBI, 2015).

O contexto norte-americano para a utilização de impressões digitais civis como padrão em investigações criminais está baseado em um singelo amparo legal que não observa plenamente a autonomia e a privacidade do cidadão quanto a seus dados pessoais. Isso porque, para além do caráter impositivo/condicionante do fornecimento das impressões digitais, não são possibilitados meios para que o indivíduo requeira administrativamente e por espontânea vontade a remoção de seus dados do NGI, considerando a regra de que os cartões com impressões digitais sejam mantidos por 110 (cento e dez) anos ou por 7 (sete) anos, após a morte do indivíduo (FBI, 2015).

3 SOLUÇÕES PARA A CONTROVÉRSIA JURÍDICA NO CONTEXTO BRASILEIRO

O emprego da técnica de interoperabilidade e unificação de bancos de dados para atividades de investigações criminais e de segurança pública se tornou tendência no contexto brasileiro por meio dos “acordos de cooperação”, ou ainda, exemplificando de maneira concreta, pela adoção de medidas para a implementação do novo ABIS (Solução Automatizada de Identificação Biométrica) (GOV.BR, 2021).

Em que pese os inequívocos avanços proporcionados com o aumento da eficiência e da segurança, além da redução de gastos no processo de identificação criminal por meio da utilização de bancos de dados biométricos, de certa forma integrados e unificados (GOV.BR, 2021), referida perspectiva, por si só, não é capaz de suprir a lacuna legislativa a respeito da autorização para a utilização de dados biométricos civis como padrão em investigações criminais.

O Supremo Tribunal Federal já reconheceu que a proteção de dados pessoais se trata de um direito fundamental do titular, visto que se relaciona a direitos fundamentais quanto à liberdade individual, à privacidade e ao livre desenvolvimento da personalidade (art. 5º, X e XII, CF/88) (BRASIL, 2020). E, em 10 de fevereiro de 2022, o entendimento

do STF adquiriu *status* constitucional com a promulgação da Emenda Constitucional n.º 115, em que o direito à proteção dos dados pessoais foi elevada ao patamar de garantia fundamental (art. 5º, inc. LXXIX, CF/88), além de estabelecer que a competência para legislar sobre proteção e tratamento de dados pessoais é da União (art. 22, inc. XXX, CF/88) (BRASIL, 2022).

À vista disso, a sanção de um estatuto legal que preveja e autorize o acesso e utilização de dados biométricos de origem civil como padrão em exames periciais criminais é a medida que deve ser adotada, tendo em vista que se trata de dados sensíveis e em virtude da especial condição que recebem do ordenamento jurídico, de modo que o tratamento deverá ter finalidade expressa, lícita e delimitada.

Por outro lado, é relevante pontuar que as provas periciais até aqui produzidas ou que serão produzidas com a identificação criminal baseada em padrões biométricos de origem civil não detêm caráter ilícito, tampouco são ilegítimas. Cumpre observar que prova ilícita é aquela obtida mediante violação de normas de direito material, enquanto provas ilegítimas são aquelas decorrentes de violação de normas de direito processual (BRASIL, 2001 *apud* MORAES, 2021)

Sob o aspecto legal, não há qualquer vedação legislativa expressa quanto à impossibilidade de utilização de dados

biométricos advindos de formulários civis como padrão em investigações criminais. Pelo contrário, ainda que as disposições normativas atualmente existentes sejam singelas quanto a disposições de tratamento e compartilhamento de dados nos “acordos de cooperação”, ainda assim, para todos os efeitos, representam amparo legal suficiente para que os órgãos com função de polícia judiciária acessem prontuários biométricos civis constituídos por órgãos públicos, e, assim, alcancem a finalidade de seu trabalho na investigação criminal.

De tal maneira que o próprio Código de Processo Penal prevê a imprescindibilidade do exame de corpo de delito, seja direto ou indireto, quando a infração penal deixar vestígios (BRASIL, 1941).

Os exames periciais produzidos sob a mencionada perspectiva também não violaram as garantias constitucionais. Em que pese a discussão a respeito da não identificação criminal do civil e da aplicação do princípio da não autoincriminação, cânones dos interesses individuais do investigado, a Constituição também disciplina interesses sociais coletivos quanto às acepções de segurança, de maneira que não devem ser arbitrariamente amenizados.

A utilização de dados biométricos advindos de fontes civis como padrão no exame pericial criminal representa justamente um dos meios em que o Estado

pode cumprir com alto grau de certeza o seu dever constitucional de prevenir, identificar e reprimir ilícitos criminais, de maneira a evitar a ofensa a direitos e interesses dos indivíduos, justificando a sua legitimidade constitucional.

Os laudos periciais baseados em padrões biométricos de origem civil valem-se de conhecimento científico, de maneira que as conclusões obtidas foram, são e serão baseadas em valores como a verdade, probidade, qualidade, isenção e a imparcialidade, de maneira a assegurar a Justiça e a preservação de direitos humanos individuais e coletivos (APCF, 2022).

Nesses termos, a ausência de previsão legal específica quanto à possibilidade de utilização de informações biométricas civis como padrão em investigações criminais, por si só, não é capaz de macular com ilicitude ou ilegitimidade os exames periciais criminais realizados nas mencionadas circunstâncias, na medida em que são meio de preservação de disposições constitucionais de interesses individuais e coletivos, entre eles, o direito à prova, um direito de estatura constitucional, corolário do devido processo legal (art. 5º, inc. LIV, CF/88).

De todo modo, a proposta de previsão legal não deve ser encarada como um mecanismo para burocratizar e dificultar o trabalho dos peritos criminais; em verdade, será mais uma garantia de conformidade, legalidade e segurança jurídica das

conclusões que obtiverem. Isso pelo fato de que poderá ser aferido o cumprimento das garantias fundamentais de proteção de dados e demais garantias processuais dos sujeitos envolvidos, de maneira a evitar questionamentos quanto à legalidade das conclusões produzidas pelo perito, mitigando as possibilidades da declaração da ilegalidade/nulidade da prova pericial gerada.

CONCLUSÃO

A partir do exposto, verifica-se que medidas legais e efetivas podem e devem ser adotadas disciplinando princípios, diretrizes e linhas da proteção e tratamento de dados nas atividades periciais, especialmente a obtenção e utilização de dados biométricos de origem civil como padrão em investigações criminais, em que haveria a harmonização entre os deveres do Estado no enfrentamento de atividades criminais, além de assegurar a observância das garantias processuais e as prerrogativas fundamentais dos cidadãos brasileiros no que tange ao tratamento de dados pessoais para tais fins (CÂMARA DOS DEPUTADOS, 2020).

Para isso, a propositura legislativa que busque alcançar tal objetivo deverá ser norteadada por disposições como: i) quais bancos de dados biométricos civis os órgãos com função de polícia judiciária estão autorizados a acessar; ii) uma vez acessados,

para quais finalidades estritas deverão ser utilizados, bem como a possibilidade de serem retidos; iii) quais agentes públicos dos órgãos com função de polícia judiciária poderão acessar e utilizar os dados biométricos de origem civil nas investigações criminais; iv) como o cidadão será cientificado a respeito do compartilhamento de seus dados biométricos; v) se será imprescindível o seu consentimento para o compartilhamento; e vi) que a utilização de dados biométricos civis representa uma hipótese legal de exceção do direito de não identificação criminal do civil, previsto no art. 5º, inc. LVIII, CF/88.

E, assim, para além da prática costumeira de compartilhamento de dados biométricos civis constituídos por órgãos públicos por meio dos chamados “acordos de cooperação”, com o intuito de contribuir para a consolidação de políticas de segurança pública, a aprovação da mencionada norma conferirá mais segurança jurídica e consolidará a legalidade à conduta de acesso aos bancos de dados biométricos civis e utilização como padrão em exames periciais criminais pelos órgãos com função de polícia judiciária.

REFERÊNCIAS

ASSOCIAÇÃO NACIONAL DOS PERITOS CRIMINAIS FEDERAIS (APCF). **Áreas de atuação da perícia federal**. Disponível em:

<<https://apcf.org.br/pericia-criminal/areas-de-atuacao-da-pericia-federal/>>. Acesso em: 22 mai. 2022.

CÂMARA DOS DEPUTADOS.

Anteprojeto de Lei de Proteção de dados

para segurança pública e perseguição

penal. 5 nov. 2020. Disponível em:

<<https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf>>. Acesso em: 25 mai. 2022.

BRASIL. Constituição da República

Federativa do Brasil de 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 26 abr. 2022.

BRASIL. Decreto-Lei n.º 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em:

<http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm>. Acesso em: 21 de mai. 2022.

BRASIL. Decreto n.º 7.950, de 12 de março de 2013. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/112037.htm>. Acesso em: 26 abr. 2022.

BRASIL. Decreto n.º 8.936, de 19 de dezembro de 2016. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8936.htm>. Acesso em: 25 mai. 2022.

BRASIL. Decreto n.º 10.977, de 23 de fevereiro de 2022. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D10977.htm>. Acesso em: 25 mai. 2022.

BRASIL. Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em: 25 mai. 2022.

BRASIL. Lei n.º 7.116, de 29 de agosto de 1983. Disponível em:

<http://www.planalto.gov.br/ccivil_03/leis/1980-1988/17116.htm>. Acesso em: 24 mai. 2022.

BRASIL. Lei n.º 12.654, de 28 de maio de 2012. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112654.htm>. Acesso em: 25 mai. 2022.

BRASIL. Lei n.º 13.444, de 11 de maio de 2017. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13444.htm>. Acesso em: 16 abr. 2022.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 26 abr. 2022.

BRASIL. Lei n.º 13.964, de 24 de dezembro de 2019. Disponível em: <

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm#art4>. Acesso em: 21 mai. 2022.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). ADI 6387. Diário de Justiça Eletrônico, 11 nov. 2020.

Disponível em:

<<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>>. Acesso em: 25 mai. 2022.

CARRERO, Angelica. Biometrics and Federal Databases: Could You Be In It?

UIC Law Review, [S. l.], v. 51, n. 589, p. 589–612, 2018. Disponível em:

<<https://repository.law.uic.edu/lawreview/vol51/iss3/4/>>. Acesso em: 21 abr. 2022.

DELILLO, Christopher. Open Face: Striking the Balance Between Privacy and Security With The FBI's Next Generation Identification System. **Notre Dame Journal of Legislation**. [S. l.], v. 41, n. 2, p. 264–290, 21 jun. 2015. Disponível em: <<https://scholarship.law.nd.edu/jleg/vol41/iss2/4/>>. Acesso em: 21 abr. 2022.

FEDERAL BUREAU OF INVESTIGATION (FBI). **Next Generation Identification (NGI)**. 2022a. Disponível em: <<https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>>. Acesso em: 21 abr. 2022.

FEDERAL BUREAU OF INVESTIGATION (FBI). **Applicant Fingerprint Form (FD-258)**. 2022b. Disponível em: <<https://www.fbi.gov/file-repository/identity-history-summary-request-fd-258-110120/view>>. Acesso em: 21 mai. 2022.

FEDERAL BUREAU OF INVESTIGATION (FBI). **Next Generation Identification (NGI) – Retention and Searching of Noncriminal Justice Fingerprint Submission**. 20 fev. 2015. Disponível em: <<https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions>> Acesso em: 21 abr. 2022.

GONÇALVES JUNIOR, Admilson; PEDRINI, Helio. A Estatura como Traço Biométrico Auxiliar na Identificação de Autores de Delito –Aplicação de Metodologia Forense de Estimativa de Altura Humana em Vídeos de Sistema de Vigilância. **Revista Brasileira de Criminalística**, Brasília, v. 8, n. 2, p. 7-21, 17 fev. 2020. DOI: <https://doi.org/10.15260/rbc.v8i2.282>. Disponível em: <<https://revista.rbc.org.br/index.php/rbc/arti>

<cle/view/282/pdf>>. Acesso em: 25 abr. 2022.

GOV.BR. **Polícia Federal implementa nova Solução Automatizada de Identificação Biométrica**. 06 jul. 2021. Disponível em: <<https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica>>. Acesso em: 23 abr. 2022.

IGP – Instituto-Geral de Perícias do Rio Grande do Sul. **Dados biométricos do TSE serão usados pelo IGP**. 03 dez. 2021. Disponível em: <<https://igp.rs.gov.br/dados-biometricos-do-tse-serao-usados-pelo-igp>>. Acesso em: 16 abr. 2022.

MENDES, Gilmar F.; BRANCO, Paulo Gustavo G. **SÉRIE IDP - Curso de Direito Constitucional**. São Paulo: Editora Saraiva, 2021. ISBN 9786555593952. *E-book*.

MINAS GERAIS. **Minas assina acordo de cooperação com o TSE para compartilhamento de dados biográficos e biométricos**. nov. 2021. Disponível em: <<https://www.mg.gov.br/probrumadinho/noticias/minas-assina-acordo-de-cooperacao-com-o-tse-para-compartilhamento-de-dados>>. Acesso em: 16 abr. 2022.

MORAES, Alexandre de. **Direito Constitucional**. São Paulo: Grupo GEN, 2021. ISBN 9788597027648. *E-book*.

MINISTÉRIO PÚBLICO FEDERAL (MPF). **Lei Geral de Proteção de Dados**. Disponível em: <<http://www.mpf.mp.br/servicos/lcpd/oque-e-a-lcpd#:~:text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o,da%20personalidade%20da%20pessoa%20natural.>>. Acesso em: 19 abr. 2022.

QUEIROZ, Paulo. **Princípio da não autoincriminação**. 17 mar. 2017.

Disponível em:
<[identificacao-do-eleitor-no-momento-da-votacao>. Acesso em: 16 abr. 2022.](https://www.pauloqueiroz.net/principio-da-nao-autoincriminacao/#:~:text=O%20princ%C3%A9pio%20da%20n%C3%A3o%20autoincrimina%C3%A7%C3%A3o,prova%20contra%20si%20mesmo1./>. Acesso em: 18 abr. 2022</p></div><div data-bbox=)

SOUZA SILVA, B. D. Importance of Laboratory Fingermarks Exams for Police Investigation in Cases of Goiás, Brasil. **Brazilian Journal of Forensic Sciences, Medical Law and Bioethics**, [S. l.], v. 10, n. 2, p. 130–146, 16 fev. 2021. DOI: 10.17063/bjfs10(2)y2021130-146. Disponível em:
<<https://www.ipebj.com.br/bjfs/index.php/bjfs/article/view/794>>. Acesso em: 25 abr. 2022.

TRIBUNAL SUPERIOR ELEITORAL (TSE). **TSE e Polícia Federal vão compartilhar dados biométricos**. 16 nov. 2017. Disponível em:
<<https://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/tse-e-policia-federal-vao-compartilhar-banco-de-dados-biometricos>>. Acesso em: 16 abr. 2022.

TRIBUNAL SUPERIOR ELEITORAL (TSE). **Resolução n.º 23.659, de 26 de outubro de 2021**. Dispõe sobre a gestão do Cadastro Eleitoral e sobre os serviços eleitorais que lhe são correlatos. Disponível em:
<<https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-659-de-26-de-outubro-de-2021>>. Acesso em: 25 mai. 2022.

TRIBUNAL SUPERIOR ELEITORAL (TSE). **90 anos da Justiça Eleitoral: biometria impede fraude na identificação do eleitor no momento da votação**. 23 fev. 2022. Disponível em:
<<https://www.tse.jus.br/imprensa/noticias-tse/2022/Fevereiro/90-anos-da-justica-eleitoral-biometria-impede-fraude-na->